Low autocorrelation sequences and flat polynomials

Habilitation

zur Erlangung des akademischen Grades

doctor rerum naturalium habilitatus

(Dr. rer. nat. habil.)

von Dr.-Ing. Kai-Uwe Schmidt

geboren am 12. März 1978 in Dresden

genehmigt durch die Fakultät für Mathematik

der Otto-von-Guericke-Universität Magdeburg

Gutachter: Prof. Dr. Tom Høholdt

Prof. Dr. Christian Mauduit

Prof. Dr. Alexander Pott

Prof. Dr. Qing Xiang

eingereicht am: 07. 01. 2014

verteidigt am: 02. 07. 2014

To my children,

Miriam, Luis, and Leonard.

Präamble

Die vorliegende Arbeit ist eine kummulative Habilitationsschrift, die auf den Veröffentlichungen [P1], [P2], [P3], [P4], [P5], [P6], [P7], [P8], [P9] basiert. Der erste Teil der Arbeit besteht aus einer detaillierten Zusammenfassung der wichtigsten Ergebnisse. Der zweite Teil der Arbeit enthält Vorabdrucke beziehungsweise Nachdrucke der zugehörigen Veröffentlichungen.

Preamble

This is a cumulative habilitation thesis based on the publications [P1], [P2], [P3], [P4], [P5], [P6], [P7], [P8], [P9]. The first part of this thesis contains a detailed summary of the main results. Preprints or postprints of the publications are included in the second part as appendices.

Acknowledgements

I thank my co-authors, Jonathan Jedwab and Daniel Katz, for a fruitful collaboration leading to results that are part of this thesis. My special thanks go to Jonathan with whom I have worked at Simon Fraser University for four years, a time in which most of the results in this thesis were achieved. Jonathan's advise on various aspects of academics and mathematics remain invaluable to me. I sincerely thank Alexander Pott for supporting me and my academic career in every possible way and for being the internal referee of this thesis. I also wish to express my gratitude to the external referees, Tom Høholdt, Christian Mauduit, and Qing Xiang. Many thanks go to all current and former members of Jonathan's and Alex's research groups for the many interesting discussions and for providing a pleasant working atmosphere. I am also grateful to the German Research Foundation for the many years of funding. Love and deepest thanks for their patience go to my wife, Anke, and to my children, Miriam, Luis, and Leonard.

Magdeburg, August 2014.

Zusammenfassung

Die Ähnlichkeit einer Folge endlicher Länge zu ihren Verschiebungen wird durch ihre aperiodischen Autokorrelationen charakterisiert. Von vorrangigem Interesse sind binäre Folgen, also Folgen von 1 oder -1. Seit etwa 1950 interessiert man sich für Folgen, deren aperiodische Autokorrelationen betragsmäßig klein relativ zur Folgenlänge sind. Die zugrunde liegende Motivation ist, dass solche Folgen eine zuverlässige Detektion von Signalen erlauben und somit von zentraler Bedeutung in der modernen Nachrichten- und Radartechnik sind. Obwohl der Ursprung dieses Gebietes in einer praktischen Anwendung liegt, haben sich daraus höchst interessante Fragestellungen in der Kombinatorik, Analysis und Zahlentheorie ergeben, die teilweise seit Jahrzehnten ungelöst sind.

Aus Sicht der Analysis und Zahlentheorie existiert ein natürlicher Zusammenhang zwischen aperiodischen Autokorrelationen und Extremalproblemen für Polynome: Für ein Polynom $f \in \mathbb{C}[z]$ sind die Koeffizienten des Laurent-Polynoms $f(z)\overline{f(z^{-1})}$ genau die aperiodischen Autokorrelationen der Folge der Koeffizienten von f. Klassische Probleme, die L^p-Normen von Polynomen auf dem Einheitskreis betreffen und größtenteils auf Littlewood und Erdős zurückgehen, sind demnach zu Fragestellungen für endliche Folgen verwandt oder sogar äquivalent.

Die meisten Ergebnisse dieser Arbeit betreffen binäre Folgen. Zunächst wird der Fall untersucht, in dem die Elemente einer binären Folge zufällig und unabhängig aus $\{-1, 1\}$ ausgewählt werden. Wie oftmals in der Kombinatorik, lassen sich mit diesem Ansatz gute (und häufig die besten bekannten) Existenzaussagen treffen. Die wichtigsten Ergebnisse sind Grenzwertsätze für Korrelationseigenschaften binärer Folgen. Zum Beispiel wird die stochastische Konvergenz der (normierten) betragsmäßig größten aperiodischen Autokorrelation bewiesen, was ein Problem aus den sechziger Jahren löst. Die Methoden werden auch verwendet, um Grenzwertsätze für Nichtlinearitätsmaße von Booleschen Funktionen zu beweisen.

Unter den Polynom-Normen auf dem Einheitskreis ist die L^4-Norm von besonderem Interesse, da sie sich einfacher als die meisten anderen Normen bestimmen lässt. Dadurch motiviert, interessierte sich Littlewood für die Fragestellung, wie klein der Quotient aus L^4- und L^2-Norm für Polynome mit Koeffizienten 1 oder -1 sein kann. Dieses Problem ist äquivalent zu der Fragestellung, wie klein das Verhältnis der Summe der quadrierten aperiodischen Autokorrelationen und der Folgenlänge von binären Folgen sein kann. Die besten bekannten Beispiele wurden 1988 gefunden. Von diesen wurde vermutet, dass sie bestmöglich sind. Diese Vermutung wird durch eine explizite Konstruktion widerlegt. Die Methode ist sehr allgemein anwendbar und wird weiterentwickelt, um eine Reihe von Vermutungen zu beweisen und einfachere und vereinheitlichende Beweise für viele bekannte Resultate in diesem Gebiet zu geben.

Abstract

The extent to which a sequence of finite length differs from a shifted version of itself is measured by its aperiodic autocorrelations. Of particular interest are sequences whose entries are 1 or -1, called binary sequences. Since the 1950s, there is sustained interest in sequences with small aperiodic autocorrelations relative to the sequence length. One of the main motivations is that a sequence with small aperiodic autocorrelations is intrinsically suited for the separation of signals from noise, and therefore has natural applications in digital communications. Although the subject has its origin in an engineering problem, interesting questions in combinatorics, analysis, and number theory have emerged, some of which remain open since decades.

For analysts and number theorists, the aperiodic autocorrelations naturally arise in the study of extremal polynomial problems. Specifically, if $f \in \mathbb{C}[z]$ is a polynomial, then the coefficients of the Laurent polynomial $f(z)\overline{f(z^{-1})}$ are precisely the aperiodic autocorrelations of the sequence formed from the coefficients of f. Therefore, classical problems, mostly due to Littlewood and Erdős, about polynomials that are extremal with respect to L^p norms on the unit circle are related or equivalent to problems involving aperiodic autocorrelations of sequences.

The majority of the results of this thesis concerns binary sequences. We first study the situation, in which the entries of a binary sequence are drawn independently and uniformly at random from $\{1, -1\}$. The best known existence results are often obtained with this approach. Our main results include the determination of the limiting distributions of several characteristics of the aperiodic autocorrelations and related measures. Most notably, we obtain the limiting distribution of the (suitably normalised) largest magnitude of the nontrivial aperiodic autocorrelations, which settles a problem first studied in the 1960s. The methods are also applied to prove limit theorems for nonlinearity measures of Boolean functions.

Among the norms of polynomials on the unit circle, the L^4 norm has received particular attention because it is easier to calculate than most other norms. Indeed, Littlewood was interested in finding polynomials with coefficients 1 or -1 having a small ratio of L^4 and L^2 norm. This problem is equivalent to finding binary sequences for which the sum of squared aperiodic autocorrelations is small relative to the sequence length. The best known examples date back to 1988 and were conjectured to be best possible. We disprove this conjecture in by an explicit construction. The method appears to be powerful and is developed further in order to prove a series of conjectures as well as to give simpler and unifying proofs and generalisations of many prior results.

Contents

1 Introduction and background

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a complex-valued vector, which we call a *sequence* of *length* n. The *aperiodic autocorrelation* of A at shift $u \in \mathbb{Z}$ is defined to be

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

Notice that $C_{-u}(A) = \overline{C_u(A)}$, so that it is sufficient to consider u to be nonnegative. Since the 1950s, there is sustained interest in sequences whose aperiodic autocorrelations at all nonzero shifts are small in magnitude relative to their lengths (see Turyn [67] and Jedwab [34] for excellent surveys). One of the main motivations is that a sequence for which all aperiodic autocorrelations at nonzero shifts are small in magnitude relative to the sequence length is intrinsically suited for the separation of signals from noise, and therefore has natural applications in digital communications.

The numbers $C_u(A)$ are also related to several old unsolved problems concerning the behaviour on the unit circle of the polynomial

$$A(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \tag{1}$$

(see Littlewood [46], Borwein [8], and Erdélyi [22], for example, for surveys on selected problems). This relationship arises since

$$\left|A(e^{i\theta})\right|^2 = \sum_{u \in \mathbb{Z}} C_u(A)\, e^{-iu\theta} \quad \text{for } \theta \in \mathbb{R}. \tag{2}$$

Whenever convenient, we shall represent the sequence A as the polynomial (1) and call the sequence A the *coefficient sequence* of this polynomial.

We consider the class of sequences whose entries are -1 or 1, called *binary* sequences, and the class of sequences whose entries have unit magnitude, called *unimodular* sequences. The meta problem that is considered in this thesis can be roughly summarised as follows.

Problem 1.A. *Let A be a binary (unimodular) sequence of length n. How small can the elements in the list $\{|C_u(A)| : 0 < u < n\}$ collectively be and how can we find binary (unimodular) sequences that attain the minimum?*

We are primarily interested in binary sequences, in which case the ideal solution to Problem 1.A is a binary sequence A for which $|C_u(A)|$ is either 0 or 1 for all nonzero u. Such a sequence is called a *Barker sequence*. Barker sequences exist for lengths 2, 3, 4, 5, 7, 11, and 13, but it has been conjectured since at least 1960 [63] that there is no Barker sequence of length greater than 13. This conjecture is known to be true for sequences of

odd lengths, as proven by Turyn and Storer [65]. Fairly deep methods have been devised to attack the case that the length is even, including the character-theoretic approach by Turyn [66] and the field-descent method by B. Schmidt [60]. The currently smallest undecided case is the length

$$3\,979\,201\,339\,721\,749\,133\,016\,171\,583\,224\,100$$

(see Borwein and Mossinghoff [15]).

In response to the presumed nonexistence of long Barker sequences, several authors have studied different measures for the collective smallness of binary or unimodular sequences. For real $r > 0$, define

$$M_r(A) = \left(\sum_{u>0} |C_u(A)|^r \right)^{1/r} \tag{3}$$

and

$$M(A) = \max_{u>0} |C_u(A)|, \tag{4}$$

which equals the limit of $M_r(A)$ as $r \to \infty$. In view of Problem 1.A, we are interested in minimising these functions over the set of binary sequences or over the set of unimodular sequences of a given length. Two measures have received particular attention: the *peak sidelobe level* $M(A)$ of A and the normalised measure

$$F(A) = \frac{C_0(A)^2}{2M_2(A)^2}, \tag{5}$$

which is called the *merit factor* of A. The determination of the largest possible merit factor of long binary and unimodular sequences is of considerable importance in various disciplines (see Jedwab [33] and Høholdt [30] for surveys). In digital communications, sequences with large merit factor correspond to signals whose energy is very uniformly distributed over frequency [6]. In theoretical physics, binary sequences achieving the largest merit factor for their length correspond to the ground states of Bernasconi's Ising spin model [7]. The growth rate of the optimal merit factor of binary and unimodular sequences, as the sequence length increases, is related to classical conjectures due to Littlewood [45], [46] and Erdős [23, Problem 22], [24], [53] on the asymptotic behaviour of norms of polynomials on the unit circle. The latter relationship arises from (2) and is explained next. For $p \geq 1$, the *L^p norm* of a polynomial $f \in \mathbb{C}[z]$ on the unit circle is

$$\|f\|_p = \left(\frac{1}{2\pi} \int_0^{2\pi} \left| f(e^{i\theta}) \right|^p d\theta \right)^{1/p}.$$

Notice that $\|f\|_2 = \sqrt{n}$ if f has degree $n-1$ and all of its coefficients have magnitude 1. Representing the sequence A as the polynomial (1), it is a consequence of (2) that

$$\sum_{u\in\mathbb{Z}} \left|C_u(A)\right|^2 = \|A\|_4^4. \tag{6}$$

Alternatively, we have

$$F(A) = \frac{\|A\|_2^4}{\|A\|_4^4 - \|A\|_2^4}.$$

Indeed, while the term "merit factor" was coined by Golay in 1972 [25], implicitly the merit factor of binary and unimodular sequences has been studied independently by complex analysts for decades since Littlewood's seminal paper [45] from 1966. To make this summary consistent, we shall express results concerning the L^4 norm of polynomials in terms of the merit factor of the corresponding coefficient sequences.

2 The behaviour of random binary sequences

In this section, we study the asymptotic behaviour, as $n \to \infty$, of $M(A)$ and $M_r(A)$ for most binary sequences A of length n. This problem was first studied by Moon and Moser [51] for the peak sidelobe level $M(A)$.

Throughout this section, $\mathfrak{B}_n$ denotes the set of binary sequences of length n and A_n is drawn at random from $\mathfrak{B}_n$, equipped with the uniform probability measure. In other words, each of the n entries in A_n is drawn independently from $\{-1, 1\}$ with $\Pr[-1] = \Pr[1] = 1/2$.

Mercer [48] proved that, for all $\epsilon > 0$,

$$\lim_{n\to\infty} \Pr\left[M(A_n) < (1+\epsilon)\sqrt{2n\log n}\right] = 1.$$

In fact, Mercer proved a weaker result but pointed out in a final remark [48, p. 670] that his proof establishes the above upper bound. In response to numerical evidence provided by Dmitriev and Jedwab [20], Alon, Litsyn, and Shpunt [4] proved that, for all $\epsilon > 0$,

$$\lim_{n\to\infty} \Pr\left[M(A_n) > (1-\epsilon)\sqrt{n\log n}\right] = 1.$$

The authors of [4] also conjectured that the above equation holds with $n\log n$ replaced by $2n\log n$. This conjecture was proved in [P1] and therefore the limiting distribution of $M(A_n)/\sqrt{n\log n}$ is obtained.

To state the result formally, recall that a sequence of random variables $X_1, X_2, \ldots$ *converges in probability* to a constant c if

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

as $n \to \infty$ for all $\epsilon > 0$.

Theorem 2.1 ([P1, Theorem 1]). *Let A_n be drawn at random from $\mathfrak{B}_n$, equipped with the uniform probability measure. Then, as $n \to \infty$,*

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

and

$$\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} \to \sqrt{2}.$$

In [P2], the following complementary result on $M_r(A_n)$ was proved, in which $\Gamma(z) = \int_0^\infty e^{-t} t^{z-1}\, dt$ denotes the gamma function, satisfying $\Gamma(p+1) = p!$ when p is a nonnegative integer.

Theorem 2.2 ([P2, Theorem 2]). *Let A_n be drawn at random from $\mathfrak{B}_n$, equipped with the uniform probability measure, and let r be a positive real number. Then, as $n \to \infty$,*

$$\frac{M_r(A_n)}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r} \quad \textit{in probability} \tag{7}$$

and

$$\frac{\mathrm{E}\left[M_r(A_n)^r\right]}{n^{r/2+1}} \to \frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}. \tag{8}$$

Moreover, for $r \geq 1$, as $n \to \infty$,

$$\frac{\mathrm{E}\left[M_r(A_n)\right]}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r}.$$

Define the arithmetic functions

$$m(n) = \min_{A_n \in \mathfrak{B}_n} M(A_n) \tag{9}$$

and

$$m_r(n) = \min_{A_n \in \mathfrak{B}_n} M_r(A_n).$$

Theorems 2.1 and 2.2 provide upper bounds for the growth rate of these functions, namely

$$\limsup_{n\to\infty} \frac{m(n)}{\sqrt{n \log n}} \leq \sqrt{2}$$

and

$$\limsup_{n\to\infty} \frac{m_r(n)}{n^{1/2+1/r}} \leq \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r}. \tag{10}$$

For $m(n)$ and $m_r(n)$ with $r \neq 2$, nothing stronger is known. For $r = 2$, the best known result (see Section 4), obtained by binary sequences X_n formed by the Legendre symbol, is $M_2(X_n)/n \to c$, where $c < 25/89$ is strictly smaller than $1/\sqrt{2}$, the right hand side of (10).

For $r = 2$, assertions (7) and (8) of Theorem 2.2 follow from [13, Theorem 1] by Borwein and Lockhart, which deals with L^p norms of random polynomials. The relationship arises from (6). Sarwate [58], and independently Newman and Byrnes [53], established the exact, rather than asymptotic, value of $\mathrm{E}[M_2(A_n)^2]$ to be $n(n-1)/2$. Assertion (8) of Theorem 2.2 was proved by Mercer [48, p. 669] when r is an even positive integer. In fact, Mercer [48, p. 669] showed how $\mathrm{E}[M_r(A_n)^r]$ can be computed exactly from a recurrence relation.

To do so, the first observation is that $C_{n-k}(A_n)$ is a transformed binomial random variable with parameters k and $1/2$. Hence, for $k \in \{1, 2, \ldots, n-1\}$ and real $r \geq 0$, the absolute moments $\mathrm{E}[|C_{n-k}(A_n)|^r]$ are given by

$$\frac{1}{2^{k-1}} \sum_{j<k/2} (k-2j)^r \binom{k}{j}. \tag{11}$$

When $r \geq 2$ is an even integer, Mercer [48, Theorem 1.4] gave a nice recurrence relation for the numbers (11). This shows that, when r is an even positive integer, (11) is a polynomial of degree $r/2$ in k, and therefore, $\mathrm{E}(M_r(A_n)^r)$ is a polynomial of degree $r/2+1$ in n. For example,

$$\begin{aligned} \mathrm{E}\left[M_2(A_n)^2\right] &= \tfrac{1}{2}(n^2 - n), \\ \mathrm{E}\left[M_4(A_n)^4\right] &= \tfrac{1}{2}(2n^3 - 5n^2 + 3n). \end{aligned}$$

In fact, it is possible [P2, Proposition 9] to get a recurrence relation for the numbers (11) for all real $r \geq 2$. This result together with an evaluation of (11) for $r = 1$ shows that, when r is an odd positive integer, then

$$\frac{4^n}{\binom{2n}{n}} \mathrm{E}\left[M_r(A_{2n})^r\right] \quad \text{and} \quad \frac{4^n}{\binom{2n}{n}} \mathrm{E}\left[M_r(A_{2n+1})^r\right]$$

are polynomials of degree $(r+3)/2$ in n. For example,

$$\begin{aligned} \mathrm{E}\left[M_1(A_{2n})\right] &= \binom{2n}{n} \frac{8n^2 - 2n}{3 \cdot 4^n}, \\ \mathrm{E}\left[M_1(A_{2n+1})\right] &= \binom{2n}{n} \frac{8n^2 + 4n}{3 \cdot 4^n}, \\ \mathrm{E}\left[M_3(A_{2n})^3\right] &= \binom{2n}{n} \frac{96n^3 - 68n^2 + 2n}{15 \cdot 4^n}, \\ \mathrm{E}\left[M_3(A_{2n+1})^3\right] &= \binom{2n}{n} \frac{96n^3 + 52n^2 + 2n}{15 \cdot 4^n}. \end{aligned}$$

3 Binary sequences with small peak sidelobe level

It has long been of significant interest to find those binary sequences whose peak sidelobe level is as small as possible. Currently, binary sequences of length n with minimum

peak sidelobe level are known for all $n \leq 61$ and for $n = 64$ (see Coxson and Russo [18] for most recent results). Many authors have put considerable computational effort in finding binary sequences with small peak sidelobe level (see Nunn and Coxson [54], for example), showing that the function $m(n)$, defined in (9), satisfies

$$\begin{aligned} m(n) &\leq 2 \quad \text{for each } n \leq 21, \\ m(n) &\leq 3 \quad \text{for each } n \leq 48, \\ m(n) &\leq 4 \quad \text{for each } n \leq 82, \\ m(n) &\leq 5 \quad \text{for each } n \leq 105. \end{aligned}$$

Turyn conjectured [67, p. 198] that the infimum limit of $m(n)$ is infinite. More specifically, based on a heuristic argument, Ein-Dor, Kanter, and Kinzel [21] conjectured that, as $n \to \infty$,

$$\frac{m(n)}{\sqrt{n}} \to d, \quad \text{where} \quad d = 0.435\ldots .$$

As shown by Sarwate [59], the peak sidelobe level of m-sequences of length n (which are cyclic shifts of Galois sequences defined by (14)) grows not faster than $\sqrt{n}\log n$. For a long time, no construction (in polynomial time) was known for binary sequences whose peak sidelobe level is proven to grow more slowly than $\sqrt{n}\log n$. In light of Theorem 2.1, this is rather surprising and an indication of the difficulty of the problem.

In [P3] a construction is given for a binary sequence of length n with peak sidelobe level at most $\sqrt{2n\log(2n)}$ for every $n > 1$. The construction is based on a method in probabilistic combinatorics, known as derandomisation.

Construction 3.1 ([P3, Construction 3]). *Let n be a positive integer and construct a binary sequence $B_n = (b_0, b_1, \ldots, b_{n-1})$ of length n recursively by*

$$b_r = -\operatorname{sign}\left[\sum_{u=1}^{r-1} b_{r-u} \sinh\left(\sqrt{\frac{2\log(2n)}{n}} \sum_{j=0}^{r-u-1} b_j b_{j+u}\right)\right],$$

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

As shown in [P3], the sequence B_n can be constructed with $O(n^2)$ multiplications and additions. The following theorem gives an upper bound on the peak sidelobe level of B_n.

Theorem 3.2 ([P3, Theorem 4]). *The binary sequence B_n of length $n > 1$ obtained under Construction 3.1 satisfies*

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

Theorem 3.2 gives the currently best known upper bound for the peak sidelobe level for an explicit family of binary sequences, although it guarantees only a peak sidelobe level roughly the same as that of a typical binary sequence. Numerical results [P3] however lend evidence to the following conjecture.

Conjecture 3.3 ([P3, Conjecture 5]). *Let B_n be the binary sequence of length n obtained under Construction 3.1. Then there exist positive constants c_1 and c_2 such that, for all $n > 1$,*

$$c_1\sqrt{n\log\log n} \leq M(B_n) \leq c_2\sqrt{n\log\log n}.$$

Some examples for small n reveal that, if c_2 in Conjecture 3.3 exists, then c_2 must be strictly greater than 1. It is however conceivable that

$$\limsup_{n\to\infty} \frac{M(B_n)}{\sqrt{n\log\log n}} \leq 1.$$

The correctness of Conjecture 3.3 implies that the sequences B_n are exceptional in the sense that their peak sidelobe level grows strictly more slowly than that of most binary sequences, as given in Theorem 2.1. Although there is currently no proof of Conjecture 3.3, the author believes that Construction 3.1 meets the challenge of finding binary sequences of arbitrary lengths with small peak sidelobe level, as even the identification of good candidates of binary sequences with exceptionally small peak sidelobe level appears to be a challenging problem.

4 The merit factor of binary sequences

In this section we study the merit factor, as defined in (5), of specific families of binary sequences. We are in particular interested in asymptotic results.

It follows from Theorem 2.2 that the merit factor of a random binary sequence of length n is approximately 1 with probability tending to 1 as $n \to \infty$. Littlewood [45] regarded calculations carried out by Swinnerton-Dyer as evidence that the merit factor can be made arbitrarily large for binary sequences. However, he could prove nothing stronger than that the merit factor of Rudin-Shapiro sequences tends to 3 as their length tends to infinity [46, Chapter III, Problem 19]. Høholdt and Jensen [31], building on studies due to Turyn and Golay [28], proved in 1988 that the merit factor of Legendre sequences rotated by a quarter of their length is asymptotically 6, and conjectured that 6 is asymptotically the largest possible merit factor for binary sequences. Although Golay conjectured [27], based on heuristic reasoning, that the largest asymptotic merit factor for binary sequences is $12.32\ldots$, he later cautioned [28] that "the eventuality must be considered that no systematic synthesis will ever be found which yield higher merit factors [than 6]".

A main result of this section, proved in [P4], is an explicit construction of binary sequences whose asymptotic merit factor is larger than 6. This sets a new record and disproves the conjecture by Høholdt and Jensen [31] that 6 is the largest asymptotic merit factor for binary sequences.

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

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

and the coefficient sequence of

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

is a binary sequence called the *Legendre sequence* of length p. The polynomial $X_p(z) - 1$ is also known as the *Fekete polynomial* of degree $p - 1$. Let

$$A(z) = \sum_{j=0}^{n-1} a_j z^j \tag{12}$$

be an arbitrary polynomial of degree $n - 1$. Let r and t be integers that can depend on n, where $t \geq 0$, and define the polynomial

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

where henceforth we extend the definition of a_j so that $a_{j+n} = a_j$ for all $j \in \mathbb{Z}$. The coefficient sequence of $A^{r,t}$ is derived from that of A by cyclically permuting (rotating) the sequence elements through r positions, and then truncating when $t < n$ or periodically extending (appending) when $t > n$.

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

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

where $\mathbb{N}$ is the set of positive integers.

Theorem 4.1 ([P4, Corollary 3.1])**.** *Let X_p be the Legendre sequence of length p and let R and $T > 0$ be real. Then the following holds, as $p \to \infty$. If $r/p \to R$ and $t/p \to T$, then $F(X_p^{r,t}) \to g(R,T)$.*

The case $T = 1$ of Theorem 4.1 implies that $X_p^{r,p}$ has asymptotic merit factor $g(R,1)$ if $r/p \to R$ as $p \to \infty$. Since

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

the maximum asymptotic merit factor that can be attained in this way is $g(1/4, 1) = 6$. This recovers the result by Høholdt and Jensen [31], which was mentioned above.

The function g satisfies $g(R, T) = g(R+1/2, T)$ on its entire domain. As shown in [P4, Corollary 3.2], the global maximum of $g(R, T)$ exists and equals

$$F_a = 6.342061\ldots, \text{ the largest root of } 29x^3 - 249x^2 + 417x - 27. \tag{13}$$

The global maximum is unique for $R \in [0, 1/2)$, and is attained when $T = 1.057827\ldots$ is the middle root of $4x^3 - 30x + 27$ and $R = 3/4 - T/2$. We therefore obtain the following consequence of Theorem 4.1.

Corollary 4.2 ([P4, Theorem 1.1])**.** *There exist binary sequences $B_1, B_2, \ldots$ of strictly increasing length satisfying $F(B_n) \to F_a$ as $n \to \infty$, where F_a is given in* (13)*.*

Corollary 4.2 gives the currently best known result on the asymptotic merit factor of binary sequences and disproves the 1988 conjecture by Høholdt and Jensen [31] that 6 is the largest asymptotic merit factor for binary sequences.

Borwein, Choi, and Jedwab [12] conjectured, based on extensive numerical data, that Theorem 4.1 holds with the additional constraint $T \in (0, 1]$ and proved that Corollary 4.2 holds subject to this conjecture. Indeed, Theorem 4.1 proves their conjecture (and explains its seemingly complicated nature involving piecewise polynomial formulae) and directly leads to Corollary 4.2.

Prior to the paper [P4], only two methods were known for calculating the asymptotic merit factor of a family of binary sequences [30]. The first is direct calculation, particularly in the case that the sequences are recursively defined [46]. The second, introduced by Høholdt and Jensen [31] in 1988, is more widely applicable [37], [38], [9], [10], [8], [11], [61], [36], [P6]. The new approach of [P4] made it possible for the first time to handle appended rotated Legendre sequences, thereby proving Theorem 4.1.

The method of [P4] was developed further in [P5] and its general version combines Fourier analysis, estimation of character sums, and estimation of the number of lattice points in polyhedra. The method was applied in [P5] to explain several previous numerical results and to prove a series of conjectures [56], [71], [69], [35], as well as to give simple and unifying proofs and generalisations of the main results of [31], [37], [38], [55], [12], [69], [61], [36], [P6], [P4]. In order to state the principal results of [P5], some further notation is needed.

Let $A(z)$ be the polynomial (12). We follow Parker [55, Lemma 3] by applying a "negaperiodic" construction to A to give the polynomial

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

whose coefficient sequence is the element-wise product of the coefficient sequence of $A^{0,4n}$ with the sequence

$$(+,+,-,-,+,+,-,-,\cdots,+,+,-,-)$$

of length $4n$. We also follow Parker [55, Lemma 4] by applying a "periodic" construction to A to give the polynomial

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

whose coefficient sequence is the element-wise product of the coefficient sequence of $A^{0,4n}$ with the sequence

$$(+,+,-,+,+,+,-,+,\cdots,+,+,-,+)$$

of length $4n$.

We have the following asymptotic merit factor result for the negaperiodic and periodic versions of Legendre sequences.

Theorem 4.3 ([P5, Theorem 2.1]). *Let X_p be the Legendre sequence of length p and let R and $T > 0$ be real. Then the following hold, as $p \to \infty$:*

(i) If $r/(2p) \to R$ and $t/(2p) \to T$, then $F(N(X_p)^{r,t}) \to g(R + 1/4, T)$.

(ii) If $r/(4p) \to R$ and $t/(4p) \to T$, then $F(P(X_p)^{r,t}) \to g(R, T)$.

Theorem 4.3 (i) shows how $N(X_p)^{r,t}$ can achieve an asymptotic merit factor F_a, as defined in (13), proving a conjecture due to Parker [56, Conjecture 4], and how $N(X_p)^{0,t}$ can achieve an asymptotic merit factor greater than 6.17, explaining numerical results presented by Xiong and Hall [69, Section VI]. Theorem 4.3 (ii) shows how $P(X_p)^{r,t}$ can achieve an asymptotic merit factor F_a, proving a conjecture due to Yu and Gong [71, Conjecture 3].

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

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

Historically, skew-symmetric binary sequences have been considered good candidates for a large merit factor (see [33, Section 3.1] for background), in part because half of their aperiodic autocorrelations are zero [65], [25]. It is known [65, (3)] that Barker sequences of odd length are necessarily skew-symmetric. It is also known [26, Table III], [50] that skew-symmetric binary sequences have largest possible merit factor among all binary sequences of their length, for all odd lengths between 2 and 60 except 19, 23, 25, 31, 33, 35,

and 37. Golay conjectured [26], [27], based on a heuristic argument, that the largest asymptotic merit factor among all binary sequences is attained by skew-symmetric sequences.

The following corollary for skew-symmetric sequences is an immediate consequence of Theorem 4.3, and the fact that $(j\,|\,p) = (-j\,|\,p)$ when $p \equiv 1 \pmod 4$.

Corollary 4.4 ([P5, Corollary 2.4]). *Let X_p be the Legendre sequence of length p with $p \equiv 1 \pmod 4$. Then the coefficient sequence of each of the polynomials*

$$N(X_p)^{p-s,2s+1} \quad \textit{and} \quad P(X_p)^{p-s,2s+1}$$

is skew-symmetric for each nonnegative integer s, and for real $T > 0$ the following hold, as $p \to \infty$:

(i) If $s/p \to T$, then $F(N(X_p)^{p-s,2s+1}) \to g(\frac{1}{4} - \frac{T}{2}, T)$.

(ii) If $s/(2p) \to T$, then $F(P(X_p)^{p-s,2s+1}) \to g(\frac{1}{4} - \frac{T}{2}, T)$.

Since the global maximum F_a of $g(R,T)$, as given in (13), occurs when $R = 1/4 - T/2$, Corollary 4.4 shows that the largest known asymptotic merit factor for a family of binary sequences can be achieved by families of skew-symmetric binary sequences. This is of particular interest in view of Golay's conjecture, mentioned above.

We next state a more general result, which contains Theorems 4.1 and 4.3 as special cases. For j an integer and n a positive odd integer, the *Jacobi symbol* $(j\,|\,n)$ extends the Legendre symbol via $(j\,|\,1) = 1$ and $(j\,|\,n_1)(j\,|\,n_2) = (j\,|\,n_1 n_2)$ for positive odd integers n_1, n_2. For n a positive odd square-free integer, the coefficient sequence of

$$X_n(z) = \sum_{j=0}^{n-1} \left(j \,\Big|\, \tfrac{n}{\gcd(j,n)}\right) z^j$$

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

We denote by $\omega(n)$ and $\kappa(n)$ the number of distinct prime divisors of n and the smallest prime divisor of n, respectively. Then, subject to a condition on the growth rates of $\omega(n)$ and $\kappa(n)$, the merit factor of Jacobi sequences of length n and their negaperiodic and periodic versions has the same asymptotic form as that for Legendre sequences, as presented in Theorems 4.1 and 4.3.

Theorem 4.5 ([P5, Theorem 2.3]). *Let $n > 1$ take values in an infinite set of positive odd square-free integers such that*

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

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

(i) If $r/n \to R$ *and* $t/n \to T$, *then* $F(X_n^{r,t}) \to g(R,T)$.

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

(iii) If $r/(4n) \to R$ *and* $t/(4n) \to T$, *then* $F(P(X_n)^{r,t}) \to g(R,T)$.

Theorem 4.5 (i) shows how $X_n^{r,t}$ can attain an asymptotic merit factor F_a, as defined in (13), for composite n, explaining numerical evidence reported by Parker [56, p. 82].

The polynomials X_n are closely related to the polynomials

$$W_n(z) = \sum_{j=0}^{n-1} \left(j \,\middle|\, n\right) z^j.$$

If $r/n \to R$ as $n \to \infty$, then the asymptotic merit factor of the coefficient sequence of $W_n^{r,n}$ equals $g(R,1)$, as shown by Borwein and Choi [10]. Let $\phi(n)$ be the Euler function. Then $\phi(n)$ coefficients of W_n equal -1 or $+1$ and the remaining coefficients are zero. Call a polynomial of degree $n-1$ obtained by changing the zero coefficients of W_n to -1 or $+1$ a *binary completion* of W_n. There are $2^{n-\phi(n)}$ binary completions of W_n and one example is X_n. The merit factor of the binary completions of W_n has been studied extensively in [P6]. For example, it is shown that, if $r/n \to R$ and $(\log n)^7/\omega(n) \to 0$ as $n \to \infty$, then the asymptotic merit factor of most binary completions of $W_n^{r,n}$ equals $g(R,1)$ [P6, Theorem 2.4] and never exceeds this value [P6, Theorem 2.3].

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

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

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

$$Y_{n,\theta}(z) = \sum_{j=0}^{n-1} \psi(\theta^j)\, z^j. \tag{14}$$

The coefficient sequence of $Y_{n,\theta}$ is a binary sequence which we call the *Galois sequence* of length n with respect to θ.[1]

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

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

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

[1] The coefficient sequences of $Y_{n,\theta}^{r,n}$ for $r = 0, 1 \ldots, n-1$ are also called the *m-sequences* associated with θ.

Theorem 4.6 ([P5, Theorem 2.2]). *For each $n = 2^d - 1$, choose an integer r and a primitive $\theta \in \mathbb{F}_{2^d}$, and let $Y_{n,\theta}$ be the Galois sequence of length n with respect to θ. Let $T > 0$ be real. Then the following hold, as $n \to \infty$:*

(i) If $t/n \to T$, then $F(Y_{n,\theta}^{r,t}) \to h(T)$.

(ii) If $t/(2n) \to T$, then $F(N(Y_{n,\theta})^{r,t}) \to h(T)$.

(iii) If $t/(4n) \to T$, then $F(P(Y_{n,\theta})^{r,t}) \to h(T)$.

As shown in [P5], the global maximum of $h(T)$ exists and equals

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

The global maximum is unique and is attained for $T = 1.115749\ldots$, which is the middle root of $x^3 - 12x + 12$. It is rather curious that, if (R_a, T_a) is the pair (R, T) that maximises $g(R, T)$ and T_b is the T that maximises $h(T)$, then the algebraic numbers

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

and

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

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

$$T_a - 1 = 0.057827\ldots$$

and

$$\tfrac{1}{2}(T_b - 1) = 0.057874\ldots$$

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

It should be noted that it is possible [P5, Section 7.2], though notationally cumbersome, to prove a meta-theorem that contains Theorems 4.5 and 4.6 as special cases. To the author's knowledge, this theorem contains all currently known results on the asymptotic merit factor of nontrivial families of binary sequences, except for Rudin-Shapiro sequences [46] and related binary sequence families [32], [14], and certain modifications of Jacobi sequences [P6], [70], [68]. For a detailed summary on how various scattered results in the literature follow from Theorems 4.5 and 4.6, the reader is referred to [P5, Section 3]. For an explanation on how the periodic and negaperiodic constructions naturally arise in the context of merit factors, the reader is referred to [P5, Section 7.1].

5 The merit factor of unimodular sequences

In this section we study the merit factor of specific families of unimodular sequences. As in Section 4, we are primarily interested in asymptotic results.

The coefficient sequence of the polynomial[2]

$$U_n(z) = \sum_{k=0}^{n-1} e^{\pi i k^2/n}\, z^k$$

of degree $n-1$ is called the *Chu sequence* of length n in the radar literature [41, Chapter 10]. The behaviour of the polynomials U_n on the unit circle has been studied by Littlewood in several papers [43], [44], [45] and in the monograph [46]. They are also the main ingredient in Kahane's celebrated semi-probabilistic construction of ultra-flat polynomials [39], which disproves a conjecture due to Erdős [24].

Write $F(U_n)$ for the merit factor of the coefficient sequence of U_n. Lower and upper bounds for $F(U_n)$ have been studied independently by several authors [52], [62], [49]. Borwein and Choi [9] conjectured that, as $n \to \infty$,

$$\frac{\sqrt{n}}{F(U_n)} = \frac{2}{\pi} + \frac{\delta_n}{3n} + O(n^{-2}), \tag{15}$$

where $\delta_n = -2$ for $n \equiv 0, 1 \pmod 4$ and $\delta_n = 1$ for $n \equiv 2, 3 \pmod 4$. This conjecture implies in particular

$$\lim_{n\to\infty} \frac{F(U_n)}{\sqrt{n}} = \frac{\pi}{2}. \tag{16}$$

It is interesting to note that, based on the work [43] and [44] and calculations carried out by Swinnerton-Dyer, Littlewood concluded in [45] that

$$\frac{\sqrt{n}}{F(U_n)} = \sqrt{2} - \frac{2}{\pi}(\sqrt{2}-1) + O(n^{-1/2}), \tag{17}$$

which contradicts the conjecture (15). Based on numerical investigations, Littlewood expressed doubt in his own conclusion and noted [45, Appendix] "There is a considerable mystery here. I have checked my calculations at least six times, and they have been checked also in great detail by Dr. Flett." Littlewood raised this issue again in his monograph [46, p. 27] and asked for a resolution of this puzzle.

Littlewood's puzzle gets resolved in [P7] by proving that (17) is incorrect and the conjecture (16) is true.

Theorem 5.1 ([P7, Theorem 1]). *We have*

$$\lim_{n\to\infty} \frac{F(U_n)}{\sqrt{n}} = \frac{\pi}{2}.$$

[2]Some authors consider $U_n(e^{\pm \pi i/n} z)$, which however has the same L^p norm as $U_n(z)$.

It is also shown in [P7] that Theorem 5.1 does not give the largest possible asymptotic merit factor for unimodular sequences. Consider the polynomials

$$V_n(z) = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} e^{2\pi ijk/n} z^{nj+k}$$

of degree $n^2 - 1$, which have been studied by Turyn [64], among others. In the radar literature [41, Chapter 10], the coefficient sequence of V_n is known as the *Frank* sequence of length n^2; write $F(V_n)$ for its merit factor.

Theorem 5.2 ([P7, Theorem 2])**.** *We have*

$$\lim_{n\to\infty} \frac{F(V_n)}{n} = \frac{\pi^2}{4}.$$

Theorems 5.1 and 5.2 imply that the merit factor of Chu and Frank sequences grows like a constant times the square root of their lengths, where the constant is $\pi/2$ for Chu sequences and $\pi^2/4$ for Frank sequences. This explains numerical results presented by Antweiler and Bömer [5]. Theorem 5.2 gives the currently best known result for the asymptotic merit factor of unimodular sequences. In particular, the merit factor of unimodular sequences can grow without bound, whereas the best known asymptotic merit factor for binary sequences, namely (13), is finite.

We remark that the methods used to prove Theorems 5.1 and 5.2 are completely different from those used to prove the results in Section 4. At heart, Theorem 5.1 is proved by showing that

$$\lim_{n\to\infty} \frac{1}{n^{3/2}} \sum_{1\le u\le n/2} \left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right)^2 = \frac{1}{2\pi}, \tag{18}$$

while Theorem 5.2 is proved by showing that

$$\lim_{n\to\infty} \frac{1}{n^2} \sum_{1\le v\le n/2} \sum_{1\le k\le v} \left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)}\right)^2 = \frac{1}{2\pi^2}.$$

It would be interesting to find an asymptotic expansion of the expression within the limit of (18), since this could prove the conjecture (15).

6 Generalised correlation measures

We now turn back to binary sequences. For a binary sequence A, Mauduit and Sárközy [47] introduced three measures of pseudorandomness: the *well-distribution measure* $W(A)$, the *normality measure* $\mathcal{N}(A)$, and the *r-th order correlation measure* $S_r(A)$. Binary sequences for which these measures are small are considered to possess a high 'level of randomness'. These measures have been studied extensively since their introduction in [47].

We are concerned with the correlation measures of binary sequences. Let $A = (a_0, a_1, \dots, a_{n-1})$ be a binary sequence of length n. For $2 \le r \le n$, the *r-th order correlation measure* of A is defined as

$$S_r(A) = \max_{0 \le u_1 < u_2 < \cdots < u_r < n} \max_{1 \le m \le n - u_r} \left| \sum_{j=0}^{m-1} a_{j+u_1} a_{j+u_2} \cdots a_{j+u_r} \right|.$$

From the definition (4) of the peak sidelobe level $M(A)$, we see that $S_2(A) \ge M(A)$ for all binary sequences A.

Following earlier work, Alon, Kohayakawa, Mauduit, Moreira, and Rödl [3] studied the behaviour of $W(A_n)$, $\mathcal{N}(A_n)$, and $S_r(A_n)$ when A_n is drawn at random from $\{-1, 1\}^n$, equipped with the uniform probability measure. They posed the following problem.

Problem 6.A ([3, Problem 33])**.** *Investigate the existence of the limiting distributions of*

$$\left\{ \frac{W(A_n)}{\sqrt{n}} \right\}_{n \ge 1} \quad \text{and} \quad \left\{ \frac{\mathcal{N}(A_n)}{\sqrt{n}} \right\}_{n \ge 1}$$

and

$$\left\{ \frac{S_r(A_n)}{\sqrt{n \log \binom{n}{r}}} \right\}_{n \ge r}. \tag{19}$$

Investigate these distributions.

The first two instances of Problem 6.A have been solved recently: Aistleitner [2], [1] proved that the limiting distributions of $W(A_n)/\sqrt{n}$ and $\mathcal{N}(A_n)/\sqrt{n}$ exist. It is known that, if (19) has a limiting distribution, then it is a Dirac measure [3, Theorem 3].

A solution to the third instance of Problem 6.A is given in [P8] by proving strong convergence of (19). In order to state the result, consider the set $\mathfrak{B}$ of infinite sequences of elements -1 or 1 and endow $\mathfrak{B}$ in the standard way with the probability measure defined by

$$\Pr\left[(a_0, a_1, \dots) \in \mathfrak{B} : a_0 = c_0, a_1 = c_1, \dots, a_{n-1} = c_{n-1}\right] = 2^{-n} \tag{20}$$

for all $(c_0, c_1, \dots, c_{n-1}) \in \{-1, 1\}^n$ and all positive integers n.

Theorem 6.1 ([P8, Theorem 1.1, Proposition 3.1])**.** *Let $(a_0, a_1, \dots)$ be drawn at random from $\mathfrak{B}$, equipped with the probability measure defined by* (20)*, and write $A_n = (a_0, a_1, \dots, a_{n-1})$. Then, as $n \to \infty$,*

$$\frac{S_r(A_n)}{\sqrt{2n \log \binom{n}{r-1}}} \to 1 \quad \textit{almost surely}$$

and

$$\frac{\mathrm{E}\left[S_r(A_n)\right]}{\sqrt{2n \log \binom{n}{r-1}}} \to 1.$$

Alon, Kohayakawa, Mauduit, Moreira, and Rödl [3] also proved a result on the asymptotic order of $S_r(A_n)$ that holds uniformly for a large range of r.

Theorem 6.B ([3, Theorem 2]). *Let A_n be drawn at random from $\{-1,1\}^n$, equipped with the uniform probability measure. Then the probability that*

$$\frac{2}{5}\sqrt{n\log\binom{n}{r}} < S_r(A_n) < \sqrt{\left(2+\frac{\log\log n}{\log n}\right)n\log\left(n\binom{n}{r}\right)}$$

holds for all r satisfying $2 \le r \le n/4$ tends to 1 as $n \to \infty$.

The upper bound in Theorem 6.B is improved in [P8] as follows.

Theorem 6.2 ([P8, Theorem 1.2]). *Let A_n be drawn at random from $\{-1,1\}^n$, equipped with the uniform probability measure, and let $\epsilon > 0$ be real. Then, as $n \to \infty$,*

$$\Pr\left[S_r(A_n) \le (1+\epsilon)\sqrt{2n\log\tbinom{n}{r-1}} \quad \textit{for all } r \textit{ satisfying } 2 \le r \le n\right] \to 1.$$

In view of Theorem 6.1, the bound in Theorem 6.2 is essentially best possible. We also note that Theorem 6.2 gives the currently strongest existence result.

7 Nonlinearity measures of random Boolean functions

Nonlinearity measures of Boolean functions are related to the flatness of certain multivariate polynomials on the hypercube $\{-1,1\}^n$, though there is no direct relation to autocorrelations of sequences. However, the main result of this section, Theorem 7.1, is proved with a method that is similar to that used to prove Theorems 2.1 and 6.1.

Let $\mathbb{F}_2$ be a field with two elements. A *Boolean function* f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and its *truth table* is the list of values $f(x)$ as x ranges over $\mathbb{F}_2^n$ in some fixed order. Let $\mathfrak{F}_n$ be the space of Boolean functions on $\mathbb{F}_2^n$. Every $f \in \mathfrak{F}_n$ can be written uniquely in the form

$$f(x_1,\dots,x_n) = \sum_{k_1,\dots,k_n\in\{0,1\}} a_{k_1,\dots,k_n}\, x_1^{k_1}\cdots x_n^{k_n},$$

where $a_{k_1,\dots,k_n} \in \mathbb{F}_2$. The *degree* of f is defined to be the algebraic degree of this polynomial. The *r-th order nonlinearity* $N_r(f)$ of a Boolean function f is the minimum number of elements that have to be changed in its truth table to arrive at the truth table of a Boolean function of degree at most r.

These nonlinearity measures are of significant relevance in cryptography, since they measure the resistance of a Boolean function against low-degree approximation attacks (see [40], for example), and in coding theory, since the maximum of $N_r(f)$ over $f \in \mathfrak{F}_n$ equals the covering radius of the r-th order Reed-Muller code of length 2^n (see [17], for

example, for background). The first order nonlinearity of Boolean functions is also related to the flatness of certain polynomials. To make this link precise, identify a Boolean function $f \in \mathfrak{F}_n$ with the polynomial $P_f \in \mathbb{Z}[z_1, \dots, z_n]$ given by

$$P_f(z_1, \dots, z_n) = \sum_{c_1,\dots,c_n \in \mathbb{F}_2} (-1)^{f(c_1,\dots,c_n)} z_1^{c_1} \cdots z_n^{c_n}.$$

The evaluations of P_f on the hypercube $\{-1, 1\}^n$ are called the *Walsh coefficients* of f, which are related to the first order nonlinearity of f via

$$N_1(f) = 2^{n-1} - \frac{1}{2} \max_{z_1,\dots,z_n \in \{-1,1\}} \bigl|P_f(z_1, \dots, z_n)\bigr|.$$

Our interest is the distribution of the nonlinearity of Boolean functions. Let Ω be the set of infinite sequences of elements from $\mathbb{F}_2$ and let $\mathfrak{F}$ be the space of functions from Ω to $\mathbb{F}_2$. For $f \in \mathfrak{F}$, we denote the function given by $f(x_1, \dots, x_n, 0, 0, \dots)$ by f_n, which is in $\mathfrak{F}_n$. We endow $\mathfrak{F}$ with a probability measure defined by

$$\Pr\bigl[f \in \mathfrak{F} : f_n = g\bigr] = 2^{-2^n} \quad \text{for all } g \in \mathfrak{F}_n \text{ and all } n \in \mathbb{N}. \tag{21}$$

A basic probabilistic method can be used to show that, if f is drawn from $\mathfrak{F}$, equipped with the probability measure defined by (21), then

$$\limsup_{n\to\infty} \frac{2^{n-1} - N_r(f_n)}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \le 1 \quad \text{almost surely.} \tag{22}$$

This was proved with a weaker convergence mode by Carlet [16, Theorem 1]. The main result of [P9] is that the normalised r-th order nonlinearity converges strongly, which shows that the bound (22) is best possible.

Theorem 7.1 ([P9, Theorem 1])**.** *Let f be drawn at random from $\mathfrak{F}$, equipped with the probability measure defined by* (21)*. Then for all $r \ge 1$, as $n \to \infty$,*

$$\frac{2^{n-1} - N_r(f_n)}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \to 1 \quad \textit{almost surely} \tag{23}$$

and

$$\frac{2^{n-1} - \mathrm{E}[N_r(f_n)]}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \to 1.$$

Using Fourier analytic methods due to Halász [29], Rodier [57] proved (23) for $r = 1$. More precise estimates on the rate of convergence in this case were given by Litsyn and Shpunt [42], using different methods. Dib [19] used a more combinatorial approach to prove (23) with a weaker convergence mode for $r = 2$. The methods used to prove Theorem 7.1 are mostly of elementary combinatorial nature and are similar to those used to prove Theorems 2.1 and 6.1. They also lead to simpler proofs of (23) in the cases that $r = 1$ or 2.

List of publications

[P1] K.-U. Schmidt. The peak sidelobe level of random binary sequences. *Bull. London Math. Soc.*, 46(3):643–652, 2014.

[P2] K.-U. Schmidt. On random binary sequences. In *Sequences and Their Applications*, volume 7280 of *Lecture Notes in Comput. Sci.*, pages 303–314. Springer, 2012.

[P3] K.-U. Schmidt. Binary sequences with small peak sidelobe level. *IEEE Trans. Inform. Theory*, 58(4):2512–2515, 2012.

[P4] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Littlewood polynomials with small L^4 norm. *Adv. Math.*, 241:127–136, 2013.

[P5] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Advances in the merit factor problem for binary sequences. *J. Combin. Theory Ser. A*, 120(4):882–906, 2013.

[P6] J. Jedwab and K.-U. Schmidt. The L_4 norm of Littlewood polynomials derived from the Jacobi symbol. *Pacific J. Math.*, 257(2):395–418, 2012.

[P7] K.-U. Schmidt. On a problem due to Littlewood concerning polynomials with unimodular coefficients. *J. Fourier Anal. Appl.*, 19(3):457–466, 2013.

[P8] K.-U. Schmidt. The correlation measures of finite sequences: limiting distributions and minimum values. arXiv:1404.0172v1 [math.PR].

[P9] K.-U. Schmidt. Nonlinearity measures of random Boolean functions. arXiv:1308.3112v1 [math.CO].

References

[1] C. Aistleitner. On the limit distribution of the normality measure of random binary sequences. arXiv:1301.6454v1 [math.CO] (to appear in Bull. London Math. Soc.).

[2] C. Aistleitner. On the limit distribution of the well-distribution measure of random binary sequences. *J. Theor. Nombres Bordeaux*, 25(2):245–259, 2013.

[3] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl. Measures of pseudorandomness: Typical values. *Proc. London Math. Soc*, 95(3):778–812, 2007.

[4] N. Alon, S. Litsyn, and A. Shpunt. Typical peak sidelobe level of binary sequences. *IEEE Trans. Inform. Theory*, 56(1):545–554, 2010.

[5] M. Antweiler and L. Bömer. Merit factor of Chu and Frank sequences. *IEE Electron. Lett.*, 46(25):2068–2070, 1990.

[6] 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(5):289–304, 1985.

[7] J. Bernasconi. Low autocorrelation binary sequences: statistical mechanics and configuration state analysis. *J. Physique*, 48(4):559–567, 1987.

[8] P. Borwein. *Computational Excursions in Analysis and Number Theory*. CMS Books in Mathematics. Springer-Verlag, New York, NY, 2002.

[9] P. Borwein and K.-K. S. Choi. Merit factors of character polynomials. *J. London Math. Soc.*, 61(2):706–720, 2000.

[10] P. Borwein and K.-K. S. Choi. Merit factors of polynomials formed by Jacobi symbols. *Canad. J. Math.*, 53(1):33–50, 2001.

[11] P. Borwein and K.-K. S. Choi. Explicit merit factor formulae for Fekete and Turyn polynomials. *Trans. Amer. Math. Soc.*, 354(1):219–234, 2002.

[12] P. Borwein, K.-K. S. Choi, and J. Jedwab. Binary sequences with merit factor greater than 6.34. *IEEE Trans. Inform. Theory*, 50(12):3234–3249, 2004.

[13] P. Borwein and R. Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, 129(5):1463–1472, 2001.

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

[15] P. Borwein and M. J. Mossinghoff. Wieferich pairs and Barker sequences, II. *LMS J. Comput. Math.*, 17(1):24–32, 2014.

[16] C. Carlet. The complexity of Boolean functions from cryptographic viewpoint. In *Complexity of Boolean Functions*, number 06111 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2006.

[17] C. Carlet and S. Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 53(1):162–173, 2007.

[18] G. Coxson and J. Russo. Efficient exhaustive search for optimal-peak-sidelobe binary codes. *IEEE Trans. Aerosp. Electron. Sys.*, 41(1):302–308, 2005.

[19] S. Dib. Distribution of Boolean functions according to the second-order nonlinearity. In *Arithmetic of finite fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, pages 86–96. Springer, Berlin, 2010.

[20] D. Dmitriev and J. Jedwab. Bounds on the growth rate of the peak sidelobe level of binary sequences. *Adv. Math. Commun.*, 1(4):461–475, 2007.

[21] L. Ein-Dor, I. Kanter, and W. Kinzel. Low autocorrelated multiphase sequences. *Phys. Rev. (E)*, 65(2):020102.1–020102.4, 2002.

[22] T. Erdélyi. Polynomials with Littlewood-type coefficient constraints. In *Approximation theory, X (St. Louis, MO, 2001)*, Innov. Appl. Math., pages 153–196. Vanderbilt Univ. Press, Nashville, TN, 2002.

[23] P. Erdős. Some unsolved problems. *Michigan Math. J.*, 4:291–300, 1957.

[24] P. Erdős. An inequality for the maximum of trigonometric polynomials. *Ann. Polon. Math.*, 12:151–154, 1962.

[25] M. J. E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, IT-18(3):449–450, 1972.

[26] M. J. E. Golay. Sieves for low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, IT-23(1):43–51, 1977.

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

[28] M. J. E. Golay. The merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, 29(6):934–936, 1983.

[29] G. Halász. On a result of Salem and Zygmund concerning random polynomials. *Studia Sci. Math. Hungar.*, 8:369–377, 1973.

[30] T. Høholdt. The merit factor problem for binary sequences. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, pages 51–59. Springer, Berlin, 2006.

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

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

[33] J. Jedwab. A survey of the merit factor problem for binary sequences. In *Proc. of Sequences and Their Applications*, volume 3486 of *Lecture Notes in Comput. Sci.*, pages 30–55. New York: Springer Verlag, 2005.

[34] J. Jedwab. What can be used instead of a Barker sequence? In *Finite fields and applications*, volume 461 of *Contemp. Math.*, pages 153–178. Amer. Math. Soc., Providence, RI, 2008.

[35] J. Jedwab and K.-U. Schmidt. Appended m-sequences with merit factor greater than 3.34. In *Sequences and Their Applications*, volume 6338 of *Lecture Notes in Comput. Sci.*, pages 204–216. Springer, 2010.

[36] J. Jedwab and K.-U. Schmidt. The merit factor of binary sequence families constructed from m-sequences. In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, pages 265–278. Amer. Math. Soc., Providence, RI, 2010.

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

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

[39] J. P. Kahane. Sur les polynômes à coefficients unimodulaires. *Bull. London Math. Soc.*, 12(5):321–342, 1980.

[40] L. R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. In *Proceedings Eurocrypt'96*, volume 1070 of *Lecture Notes Comput. Sci.*, pages 224–236, 1996.

[41] N. Levanon and E. Mozeson. *Radar signals*. Wiley-Interscience, 1st edition, 2004.

[42] S. Litsyn and A. Shpunt. On the distribution of Boolean function nonlinearity. *SIAM J. Discrete Math.*, 23(1):79–95, 2008/09.

[43] J. E. Littlewood. On the mean values of certain trigonometric polynomials. *J. London Math. Soc.*, 36(1):307–334, 1961.

[44] J. E. Littlewood. On the mean values of certain trigonometric polynomials II. *Illinois J. Math.*, 6(1):1–39, 1962.

[45] 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(1):367–376, 1966.

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

[47] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82(4):265–377, 1997.

[48] I. D. Mercer. Autocorrelations of random binary sequences. *Combin. Probab. Comput.*, 15(5):663–671, 2006.

[49] I. D. Mercer. Merit factor of Chu sequences and best merit factor of polyphase sequences. *IEEE Trans. Inform. Theory*, 59(9):6083–6086, 2013.

[50] S. Mertens. Ground states of the Bernasconi model with open boundary conditions. http://www-e.uni-magdeburg.de/mertens/research/labs/open.dat, 2001.

[51] J. W. Moon and L. Moser. On the correlation function of random binary sequences. *SIAM J. Appl. Math.*, 16(12):340–343, 1968.

[52] D. J. Newman. An L^1 extremal problem for polynomials. *Proc. Amer. Math. Soc.*, 16(6):1287–1290, 1965.

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

[54] C. J. Nunn and G. E. Coxson. Best-known autocorrelation peak sidelobe levels for binary codes of length 71 to 105. *IEEE Trans. Aerosp. Electron. Sys.*, 44(4):392–395, 2008.

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

[56] M. G. Parker. Univariate and multivariate merit factors. In *Proc. of Sequences and Their Applications*, volume 3486 of *Lecture Notes in Comput. Sci.*, pages 72–100. Springer, 2005.

[57] F. Rodier. Asymptotic nonlinearity of Boolean functions. *Des. Codes Cryptogr.*, 40(1):59–70, 2006.

[58] D. V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proc.*, 131, Part F(2):101–106, 1984.

[59] D. V. Sarwate. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. *IEEE Trans. Inform. Theory*, IT-30(4):685–687, 1984.

[60] B. Schmidt. Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, 12(4):929–952, 1999.

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

[62] 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 International Zurich Seminar on Broadband Communications*, pages 279–286. IEEE, 2000.

[63] R. Turyn. Optimum codes study. Technical report, Sylvania Electronic Systems, January 1960. Final report, Contract AF19(604)-5473.

[64] R. Turyn. The correlation function of a sequences of roots of 1. *IEEE Trans. Inform. Theory*, 13(3):524–525, 1967.

[65] R. Turyn and J. Storer. On binary sequences. *Proc. Amer. Math. Soc.*, 12(3):394–399, 1961.

[66] R. J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15(1):319–346, 1965.

[67] R. J. Turyn. Sequences with small correlation. In H. B. Mann, editor, *Error Correcting Codes*. Wiley, New York, 1968.

[68] T. Xiong and J. I. Hall. Modifications on character sequences and construction of large even length binary sequences. arXiv:1407.3178v1 [cs.IT].

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

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

[71] N. Y. Yu and G. Gong. The perfect binary sequence of period 4 for low periodic and aperiodic autocorrelations. In *Sequences, subsequences, and consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, pages 37–49. Springer, Berlin, 2007.

The final copy-edited version is published in Bull. London Math. Soc. 46(3), pp. 643-652, 2014
(http://dx.doi.org/10.1112/blms/bdu021).

THE PEAK SIDELOBE LEVEL OF RANDOM BINARY SEQUENCES

KAI-UWE SCHMIDT

Abstract. Let $A_n = (a_0, a_1, \ldots, a_{n-1})$ be drawn uniformly at random from $\{-1, +1\}^n$ and define

$$M(A_n) = \max_{0<u<n} \left| \sum_{j=0}^{n-u-1} a_j a_{j+u} \right| \quad \text{for } n > 1.$$

It is proved that $M(A_n)/\sqrt{n \log n}$ converges in probability to $\sqrt{2}$. This settles a problem first studied by Moon and Moser in the 1960s and proves in the affirmative a recent conjecture due to Alon, Litsyn, and Shpunt. It is also shown that the expectation of $M(A_n)/\sqrt{n \log n}$ tends to $\sqrt{2}$.

1. Introduction

Consider a binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, namely an element of $\{-1, +1\}^n$. Define the *aperiodic autocorrelation* at shift u of A to be

$$C_u(A) = \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } u \in \{0, 1, \ldots, n-1\}$$

and define the *peak sidelobe level* of A as

$$M(A) = \max_{0<u<n} |C_u(A)| \quad \text{for } n > 1.$$

Binary sequences with small autocorrelation at nonzero shifts have a wide range of applications in digital communications, including synchronisation and radar (see [6], for example).

Let $\mu(n)$ be the minimum of $M(A)$ taken over all 2^n binary sequences A of length n. By a parity argument, it is seen that $\mu(n) \geq 1$ and it is known that $\mu(n) = 1$ for $n \in \{2, 3, 4, 5, 7, 11, 13\}$ (binary sequences attaining the minimum are often called *Barker* sequences). It is a classical problem to decide whether $\mu(n) > 1$ for all $n > 13$. Although deep methods have been developed [14], [13], this problem is still open; the currently smallest undecided case arises for $n > 2 \cdot 10^{30}$ [8]. It is conjectured that $\mu(n)$ grows

Date: 21 February 2011 (revised 21 December 2013).

2010 *Mathematics Subject Classification.* Primary: 05D40; Secondary: 94A55, 60F10.

The author was supported by German Research Foundation under Research Fellowship SCHM 2609/1-1.

as $n \to \infty$, perhaps like $\sqrt{n}$. We refer to Turyn [15] and Jedwab [7] for excellent surveys on this problem.

In this paper, we will be concerned with the asymptotic behaviour, as $n \to \infty$, of $M(A)$ for almost all binary sequences A of length n. This problem was first studied by Moon and Moser [12]. Let A_n be a random binary sequence of length n, by which we mean that A_n is drawn uniformly at random from $\{-1,+1\}^n$. In other words, each of the n sequence elements of A_n takes on each of the values -1 and $+1$ independently with probability $1/2$. Until now, the best known bounds are

$$\lim_{n\to\infty} \Pr\left[1-\epsilon < \frac{M(A_n)}{\sqrt{n\log n}} < \sqrt{2}+\epsilon\right] = 1 \quad \text{for all } \epsilon > 0. \tag{1.1}$$

The upper bound is due to Mercer [11]. In fact, Mercer proved a weaker result but pointed out in a final remark [11, p. 670] that his proof establishes the above upper bound. The lower bound was proved by Alon, Litsyn, and Shpunt [2], in response to numerical evidence provided by Dmitriev and Jedwab [4]. The authors of [2] also conjectured that the lower bound can be improved to $\sqrt{2}-\epsilon$. The aim of this paper is to prove this conjecture and therefore to establish the limit distribution, as $n \to \infty$, of $M(A_n)/\sqrt{n\log n}$. In particular, we prove the following.

Theorem 1.1. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

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

and

$$\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} \to \sqrt{2}.$$

Alon, Litsyn, and Shpunt [2] already observed that, as a consequence of McDiarmid's inequality (Lemma 3.1), $M(A_n)$ is concentrated around its expected value, but could only show that

$$\liminf_{n\to\infty} \frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} \ge 1. \tag{1.2}$$

Their proof considers $C_u(A_n)$ only for $u \ge n/2$ and crucially relies on the fact that $C_u(A_n)$ and $C_v(A_n)$ are independent whenever $n/2 \le u < v < n$. Our method considers $C_u(A_n)$ also for $u < n/2$. In particular, by a careful estimation of the moments of $C_u(A_n)C_v(A_n)$ for $0 < u < v < n$, we will show that the lower bound (1.2) can be improved to $\sqrt{2}$, which together with (1.1) establishes the second part of Theorem 1.1. The first part of Theorem 1.1 then follows from McDiarmid's inequality.

As pointed out in [2], given a binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, the quantity $M(A)$ is related to the more general rth-order correlation measure $S_r(A)$, which was defined by Mauduit and Sárközy [9]

to be

$$S_r(A) := \max_{0\le u_1<u_2<\cdots<u_r<n} \max_{0\le k\le n-u_r} \left| \sum_{j=0}^{k-1} a_{j+u_1} a_{j+u_2} \cdots a_{j+u_r} \right| \quad \text{for } n \ge r.$$

Alon, Kohayakawa, Mauduit, Moreira, and Rödl [1] established that, given a random binary sequence A_n of length n, then for all $r \ge 2$,

$$\lim_{n\to\infty} \Pr\left[\frac{2}{5} < \frac{S_r(A_n)}{\sqrt{n \log \binom{n}{r}}} < \sqrt{3} + \epsilon \right] = 1 \quad \text{for all } \epsilon > 0.$$

Since, for every binary sequence A, we have $M(A) \le S_2(A)$, Theorem 1.1 implies that for $r = 2$ the lower bound can be improved from $2/5$ to $1 - \epsilon$.

2. Preliminary Results

The main results of this section are the following. Given a random binary sequence A_n of length n, Proposition 2.2 gives a lower bound for

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n \log n} \right] \tag{2.1}$$

for small u. This result can also be concluded from [2]. However, the proof presented here is considerably simpler and more direct. Proposition 2.7 gives an upper bound for

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n \log n} \cap |C_v(A_n)| \ge \sqrt{2n \log n} \right] \tag{2.2}$$

for $0 < u < v < n$. These bounds will be the crucial ingredients to prove the main result of this paper.

2.1. To bound (2.1), we shall need the following refinement of the central limit theorem.

Lemma 2.1 (Cramér [3, Thm. 2])**.** *Let $X_0, X_1, \ldots$ be identically distributed mutually independent random variables satisfying $\mathrm{E}[X_0] = 0$ and $\mathrm{E}[X_0^2] = 1$ and suppose that there exists $T > 0$ such that $\mathrm{E}[e^{tX_0}] < \infty$ for all $|t| < T$. Write $Y_k = X_0 + X_1 + \cdots + X_{k-1}$ and let Φ be the distribution function of a normal random variable with zero mean and unit variance. If $\theta_k > 1$ and $\theta_k / k^{1/6} \to 0$ as $k \to \infty$, then*

$$\frac{\Pr\left[|Y_k| \ge \theta_k \sqrt{k} \right]}{2\Phi(-\theta_k)} \to 1.$$

Proposition 2.2. *Let A_n be a random binary sequence of length $n > 2$ and let u be an integer satisfying $1 \le u \le \frac{n}{\log n}$. Then*

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n \log n} \right] \ge \frac{1}{5n\sqrt{\log n}}$$

for all sufficiently large n.

Proof. Write $A_n = (a_0, a_1, \dots, a_{n-1})$. It is well known that the $n-u$ products

$$a_0 a_u,\ a_1 a_{1+u}, \dots, a_{n-u-1} a_{n-1}$$

are mutually independent. A proof of this fact was given by Mercer [11, Prop. 1.1]. Hence $C_u(A_n)$ is a sum of $n-u$ mutually independent random variables, each taking each of the values -1 and $+1$ with probability $1/2$. Notice that $\mathrm{E}[e^{ta_0a_u}] = \cosh(t)$ and, setting

$$\xi_n = \sqrt{\frac{2n\log n}{n-u}},$$

we find that $\xi_n/(n-u)^{1/6} \to 0$ since $u \le \frac{n}{\log n}$. We can therefore apply Lemma 2.1 to conclude, as $n \to \infty$,

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \sim 2\Phi(-\xi_n), \tag{2.3}$$

where Φ is the distribution function of a standard normal random variable. It is well known (see [5, Thm. 1.2.3], for example) that

$$\frac{1}{\sqrt{2\pi}\,z}\Big(1-\frac{1}{z^2}\Big)\,e^{-z^2/2} \le \Phi(-z) \le \frac{1}{\sqrt{2\pi}\,z}\,e^{-z^2/2} \quad \text{for } z>0,$$

so that, since $\frac{n}{n-u} \sim 1$, as $n \to \infty$,

$$2\Phi(-\xi_n) \sim \frac{1}{\sqrt{\pi\log n}}\,e^{-\frac{n}{n-u}\log n}.$$

Using $u \le \frac{n}{\log n}$, we conclude

$$e^{-\frac{n}{n-u}\log n} \ge e^{-\frac{\log n}{\log n-1}\log n} \sim \frac{1}{en}$$

as $n \to \infty$. It then follows from (2.3) that for all $\alpha > e\sqrt{\pi}$ and all sufficiently large n we have

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \ge \frac{1}{\alpha n\sqrt{\log n}}.$$

The lemma follows since $5 > e\sqrt{\pi}$. □

2.2. We now turn to the derivation of an upper bound for (2.2). It will be convenient to define the notion of an even tuple as follows.

Definition 2.3. A tuple $(x_1, x_2, \dots, x_{2m})$ is *even* if there exists a permutation σ of $\{1, 2, \dots, 2m\}$ such that $x_{\sigma(2i-1)} = x_{\sigma(2i)}$ for each $i \in \{1, 2, \dots, m\}$.

For example, $(1, 3, 1, 4, 3, 4)$ is even, while $(2, 1, 1, 2, 1, 3)$ is not even. In the next two lemmas we will prove two results about even tuples, which we then use to estimate moments of $C_u(A_n)C_v(A_n)$.

Recall that, for positive integer k, the double factorial

$$(2k-1)!! = \frac{(2k)!}{k!\,2^k} = (2k-1)(2k-3)\cdots 3\cdot 1$$

is the number of ways to arrange $2k$ objects into k unordered pairs.

Lemma 2.4. *Let m and q be positive integers and let R be the set of even tuples in*

$$\big\{(x_1, x_2, \ldots, x_{2q}) \,:\, x_i \in \mathbb{Z},\, 0 \le x_i < m\big\}.$$

Then

$$|R| \le (2q-1)!!\, m^q.$$

Proof. There are $(2q-1)!!$ ways to arrange $x_1, x_2, \ldots, x_{2q}$ into q unordered pairs and to each of these q pairs we assign a value of $\{0, 1, \ldots, m-1\}$. In this way we construct all elements of R at least once, which proves the lemma. □

Lemma 2.5. *Let u, v, and n be integers satisfying $0 < u, v < n$ and $u \ne v$. Write $I = \{1, 2, \ldots, 2q\}$ and let t be an integer satisfying $0 \le t < q$. Let S be the subset of*

$$\big\{(x_i, x_i+u, y_i, y_i+v)_{i\in I} \,:\, x_i, y_i \in \mathbb{Z},\, 0 \le x_i < n-u,\, 0 \le y_i < n-v\big\}$$

containing all even elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ such that $(x_i)_{i\in J}$ is not even for all $(2q-2t)$-element subsets J of I. Then

$$|S| \le (8q-1)!!\, n^{2q-(t+1)/3}.$$

Proof. We will construct a set of tuples that contains S as a subset. Arrange the $8q$ variables

$$x_1, x_1+u, \ldots, x_{2q}, x_{2q}+u, y_1, y_1+v, \ldots, y_{2q}, y_{2q}+v \tag{2.4}$$

into $4q$ unordered pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_{4q}, b_{4q})$ such that there are at most $q-t-1$ pairs (x_i, x_j). This can be done in at most $(8q-1)!!$ ways. We formally set $a_i = b_i$ for all $i \in \{1, 2, \ldots, 4q\}$. If this assignment does not yield a contradiction, then we call the arrangement of (2.4) into $4q$ pairs *consistent*. For example, if there are pairs of the form (x_i, y_j) and (x_i+u, y_j+v), then the arrangement is not consistent since $u \ne v$ by assumption.

Now, for every consistent arrangement, pairs of the form (x_i, x_j) or (y_i, y_j) determine the value of another pair (namely, (x_i+u, x_j+u) or (y_i+v, y_j+v), respectively). On the other hand, for every consistent arrangement, pairs not of the form

$$(x_i, x_j),\ (y_i, y_j),\ (x_i+u, x_j+u),\ \text{or } (y_i+v, y_j+v)$$

determine the value of at least two other pairs. For example, if there exists the pair (x_i, y_j), then x_i+u and y_j+v must lie in different pairs. Therefore, since there are at most $q-t-1$ pairs of the form (x_i, x_j) and at most q pairs of the form (y_i, y_j), for each consistent arrangement, at most

$$\tfrac{1}{2}(4q-2t-2) + \tfrac{1}{3}(2t+2) = 2q - \tfrac{1}{3}(t+1)$$

of the variables $x_1, \ldots, x_{2q}, y_1, \ldots, y_{2q}$ can be chosen independently. We assign to each of these a value of $\{0, 1, \ldots, n-1\}$. In this way, we construct a set of at most $(8q-1)!!\, n^{2q-(t+1)/3}$ tuples that contains S as a subset, as required. □

We now use Lemmas 2.4 and 2.5 to bound moments of $C_u(A_n)C_v(A_n)$.

Lemma 2.6. *Let p and h be integers satisfying $0 \le h < p$ and let A_n be a random binary sequence of length n. Then, for $0 < u < v < n$,*

$$\mathrm{E}\left[\big(C_u(A_n)C_v(A_n)\big)^{2p}\right] \le n^{2p}\big[(2p-1)!!\big]^2\bigg(1+\frac{(8p)^{8h}}{n^{1/3}}+\frac{(8p)^{4p}}{n^{(h+1)/3}}\bigg).$$

Proof. Write $I = \{1, 2, \ldots, 2p\}$ and let T be the set containing all even tuples of

$$\big\{(x_i, x_i+u, y_i, y_i+v)_{i\in I} : x_i, y_i \in \mathbb{Z},\, 0 \le x_i < n-u,\, 0 \le y_i < n-v\big\}.$$

Writing $A_n = (a_0, a_1, \ldots, a_{n-1})$, we have

$$\begin{aligned}
&\mathrm{E}\left[\big(C_u(A_n)C_v(A_n)\big)^{2p}\right]\\
&= \mathrm{E}\left[\bigg(\sum_{i=0}^{n-u-1} a_i a_{i+u}\bigg)^{2p}\bigg(\sum_{j=0}^{n-v-1} a_j a_{j+v}\bigg)^{2p}\right]\\
&= \sum_{i_1,\ldots,i_{2p}=0}^{n-u-1}\ \sum_{j_1,\ldots,j_{2p}=0}^{n-v-1} \mathrm{E}\left[a_{i_1}a_{i_1+u}\cdots a_{i_{2p}}a_{i_{2p}+u}a_{j_1}a_{j_1+v}\cdots a_{j_{2p}}a_{j_{2p}+v}\right]\\
&= |T| \qquad (2.5)
\end{aligned}$$

since $a_0, a_1, \ldots, a_{n-1}$ are mutually independent, $\mathrm{E}[a_j] = 0$, and $a_j^2 = 1$ for all $j \in \{0, 1, \ldots, n-1\}$. We define the following subsets of T.

(1) T_1 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ are even.
(2) T_2 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that $(x_i)_{i\in I}$ or $(y_i)_{i\in I}$ is not even and $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even for some $(2p-2h)$-element subsets J and K of I.
(3) T_3 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that either $(x_i)_{i\in J}$ is not even for all $(2p-2h)$-element subsets J of I or $(y_i)_{i\in K}$ is not even for all $(2p-2h)$-element subsets K of I.

It is immediate that T_1, T_2, and T_3 partition T, so that

$$|T| = |T_1| + |T_2| + |T_3|. \qquad (2.6)$$

We now bound the cardinalities of T_1, T_2, and T_3.

The set T_1. Using Lemma 2.4, we have the crude estimate

$$|T_1| \le \big[(2p-1)!!\big]^2 n^{2p}. \qquad (2.7)$$

The set T_2. Let $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ be an element of T_2. Then there exist $(2p-2h)$-element subsets J and K of I such that $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even and

$$(x_i)_{i\in I\setminus J} \quad \text{or} \quad (y_i)_{i\in I\setminus K} \qquad (2.8)$$

is not even. Since $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even, $(x_i, x_i+u, y_j, y_j+v)_{i\in J,\, j\in K}$ is even. Since $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ is also even, it follows that

$$(x_i, x_i+u, y_j, y_j+v)_{i\in I\setminus J,\, j\in I\setminus K} \tag{2.9}$$

is even as well. There are $\binom{2p}{2h}$ subsets J and $\binom{2p}{2h}$ subsets K. By Lemma 2.4, for each such J and K, there are at most $(2p-2h-1)!!\, n^{p-h}$ even tuples $(x_i)_{i\in J}$ satisfying $0 \le x_i < n$ for each $i \in J$ and at most $(2p-2h-1)!!\, n^{p-h}$ even tuples $(y_i)_{i\in K}$ satisfying $0 \le y_i < n$ for each $i \in K$. By Lemma 2.5 applied with $t = 0$ and by interchanging u and v and $(x_i)_{i\in I\setminus J}$ and $(y_i)_{i\in I\setminus K}$ if necessary, the number of even tuples in $\{0, 1, \dots, n-1\}^{8h}$ of the form (2.9) such that one of the tuples in (2.8) is not even is at most $(8h-1)!!\, n^{2h-1/3}$. Therefore,

$$\begin{aligned} |T_2| &\le 2n^{2h-1/3}\,(8h-1)!!\left[\binom{2p}{2h}(2p-2h-1)!!\, n^{p-h}\right]^2 \\ &\le n^{2p-1/3}\big[(2p-1)!!\big]^2\,(8p)^{8h}, \end{aligned} \tag{2.10}$$

using very crude bounds.

The set T_3. By Lemma 2.5 applied with $t = h$ and by interchanging u and v and $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ if necessary,

$$\begin{aligned} |T_3| &\le 2n^{2p-(h+1)/3}\,(8p-1)!! \\ &\le n^{2p-(h+1)/3}\,(8p)^{4p}. \end{aligned} \tag{2.11}$$

Now the lemma follows by combining (2.5), (2.6), (2.7), (2.10), and (2.11). □

Lemma 2.6 is now used to prove the desired upper bound for (2.2).

Proposition 2.7. *Let A_n be a random binary sequence of length n and write $\lambda_n = \sqrt{2n\log n}$. Then, for $0 < u < v < n$ and all sufficiently large n,*

$$\Pr\big[|C_u(A_n)| \ge \lambda_n \cap |C_v(A_n)| \ge \lambda_n\big] \le \frac{23}{n^2}.$$

Proof. Let (X_1, X_2) be a random vector taking values in $\mathbb{R}\times\mathbb{R}$ and let p be a positive integer. Then by Markov's inequality, for $\theta_1, \theta_2 > 0$,

$$\Pr\big[|X_1| \ge \theta_1 \cap |X_2| \ge \theta_2\big] \le \frac{\mathrm{E}\big[(X_1X_2)^{2p}\big]}{(\theta_1\theta_2)^{2p}}.$$

Let h be an arbitrary integer satisfying $0 \le h < p$. Application of Lemma 2.6 gives

$$\begin{aligned} &\Pr\big[|C_u(A_n)| \ge \lambda_n \cap |C_v(A_n)| \ge \lambda_n\big) \\ &\qquad \le \frac{\big[(2p-1)!!\big]^2}{(2\log n)^{2p}}\big[1 + K_1(n,p,h) + K_2(n,p,h)\big], \end{aligned} \tag{2.12}$$

where

$$K_1(n,p,h) = n^{-1/3}\,(8p)^{8h} \quad \text{and} \quad K_2(n,p,h) = n^{-(h+1)/3}\,(8p)^{4p}.$$

We apply (2.12) with $p = \lfloor \log n \rfloor$ and $h = \lfloor 17 \log\log n \rfloor$, so that for all sufficiently large n we have $h < p$, as assumed. By Stirling's approximation

$$\sqrt{2\pi k}\; k^k e^{-k} \le k! \le \sqrt{3\pi k}\; k^k e^{-k},$$

we have

$$\frac{\big[(2p-1)!!\big]^2}{(2\log n)^{2p}} \le \frac{3p^{2p}e^{-2p}}{(\log n)^{2p}} \le \frac{3e^2}{n^2}.$$

We also have

$$\begin{aligned} K_1(n,p,h) &\le K_1(n, \log n, 17\log\log n) \\ &= n^{-\frac{1}{3}}\, n^{\frac{136(\log\log n)(\log 8 + \log\log n)}{\log n}} \\ &= O(n^{-1/4}) \quad \text{as } n \to \infty \end{aligned}$$

and

$$\begin{aligned} K_2(n,p,h) &\le K_2(n, \log n, 16\log\log n) \\ &= n^{-\frac{1}{3} + 4\log 8 - \frac{4}{3}\log\log n} \\ &= O(n^{-\log\log n}) \quad \text{as } n \to \infty. \end{aligned}$$

Substitute into (2.12) to obtain the claimed result, using $3e^2 < 23$. □

3. Proof of Main Theorem

We require the following result, which is a consequence of Azuma's inequality for martingales.

Lemma 3.1 (McDiarmid [10])**.** *Let $X_0, X_1, \dots, X_{n-1}$ be mutually independent random variables taking values in a set S. Let $f : S^n \to \mathbb{R}$ be a measurable function and suppose that f satisfies*

$$\big|f(x) - f(y)\big| \le c$$

whenever x and y differ only in one coordinate. Define the random variable $Y = f(X_0, X_1, \dots, X_{n-1})$. Then, for $\theta \ge 0$,

$$\Pr\big[\big|Y - \mathrm{E}[Y]\big| \ge \theta\big] \le 2e^{-\frac{2\theta^2}{c^2 n}}.$$

Given a random binary sequence $A_n = (a_0, a_1, \dots, a_{n-1})$ of length n, we will apply Lemma 3.1 with $X_j = a_j$ for $j \in \{0, 1, \dots, n-1\}$ and

$$f(x_0, x_1, \dots, x_{n-1}) = \max_{0<u<n} \left| \sum_{j=0}^{n-u-1} x_j x_{j+u} \right|,$$

so that $M(A_n) = f(a_0, a_1, \dots, a_{n-1})$. We can take $c = 4$ in Lemma 3.1 and obtain the following corollary.

Corollary 3.2. *Let A_n be a random binary sequence of length n. Then, for $\theta \geq 0$,*

$$\Pr\left[\left|M(A_n) - \mathrm{E}[M(A_n)]\right| \geq \theta\right] \leq 2e^{-\frac{\theta^2}{8n}}.$$

We now prove the second part of Theorem 1.1.

Theorem 3.3. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

$$\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} \to \sqrt{2}.$$

Proof. By the triangle inequality and the union bound we have, for all $\epsilon > 0$,

$$\begin{aligned}&\Pr\left[\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} - \sqrt{2} > \epsilon\right] \\ &\quad\leq \Pr\left[\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} - \frac{M(A_n)}{\sqrt{n\log n}} > \tfrac{1}{2}\epsilon\right] + \Pr\left[\frac{M(A_n)}{\sqrt{n\log n}} - \sqrt{2} > \tfrac{1}{2}\epsilon\right].\end{aligned}$$

By Corollary 3.2 and the upper bound of (1.1), the two terms on the right-hand side tend to zero as $n \to \infty$, hence

$$\limsup_{n\to\infty} \frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} \leq \sqrt{2}. \tag{3.1}$$

Let $\delta > 0$ and define the set

$$N(\delta) = \left\{n > 1 : \frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n\log n}} < \sqrt{2} - \delta\right\}. \tag{3.2}$$

We claim that the size of $N(\delta)$ is finite for all choices of δ, which together with (3.1) will prove the theorem. The proof of the claim is based on an idea developed in [2]. Let $n > 2$ and write

$$W = \left\{u \in \mathbb{Z} : 1 \leq u \leq \frac{n}{\log n}\right\}$$

and $\lambda_n = \sqrt{2n\log n}$. Then

$$\begin{aligned}&\Pr\left[M(A_n) \geq \lambda_n\right] \geq \Pr\left[\max_{u\in W} |C_u(A_n)| \geq \lambda_n\right] \\ &\geq \sum_{u\in W} \Pr\left[|C_u(A_n)| \geq \lambda_n\right] - \sum_{\substack{u,v\in W\\ u<v}} \Pr\left[|C_u(A_n)| \geq \lambda_n \cap |C_v(A_n)| \geq \lambda_n\right]\end{aligned}$$

by the Bonferroni inequality. By Propositions 2.2 and 2.7,

$$\begin{aligned}\Pr\left[M(A_n) \geq \lambda_n\right] &\geq |W| \cdot \frac{1}{5n(\log n)^{\frac{1}{2}}} - \frac{|W|^2}{2} \cdot \frac{23}{n^2} \\ &\geq \frac{1}{8(\log n)^{\frac{3}{2}}} - \frac{12}{(\log n)^2} \\ &\geq \frac{1}{10(\log n)^{\frac{3}{2}}} \qquad (3.3)\end{aligned}$$

for all sufficiently large n, using $\frac{2}{3}\frac{n}{\log n} \le |W| \le \frac{n}{\log n}$ for $n > 2$. Now, by the definition (3.2) of $N(\delta)$, for all $n \in N(\delta)$ we have $\lambda_n > \mathrm{E}[M(A_n)]$, so that we can apply Corollary 3.2 with $\theta = \lambda_n - \mathrm{E}[M(A_n)]$ to give, for all $n \in N(\delta)$,

$$\Pr\big[M(A_n) \ge \lambda_n\big] \le 2e^{-\frac{1}{8n}(\lambda_n - \mathrm{E}[M(A_n)])^2}.$$

Comparison with (3.3) yields, for all sufficiently large $n \in N(\delta)$,

$$\frac{1}{10(\log n)^{\frac{3}{2}}} \le 2e^{-\frac{1}{8n}(\lambda_n - \mathrm{E}[M(A_n)])^2},$$

which implies

$$\frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} \ge \sqrt{2} - \sqrt{\frac{12\log\log n + 8\log 20}{\log n}}.$$

From the definition (3.2) of $N(\delta)$ it then follows that $N(\delta)$ has finite size for all $\delta > 0$, as required. □

Using Corollary 3.2, it is now straightforward to prove the first part of Theorem 1.1.

Corollary 3.4. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

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

Proof. By the triangle inequality and the union bound we have, for all $\epsilon > 0$,

$$\begin{aligned}&\Pr\left[\left|\frac{M(A_n)}{\sqrt{n\log n}} - \sqrt{2}\right| > \epsilon\right]\\ &\le \Pr\left[\left|\frac{M(A_n)}{\sqrt{n\log n}} - \frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}}\right| > \tfrac{1}{2}\epsilon\right] + \Pr\left[\left|\frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} - \sqrt{2}\right| > \tfrac{1}{2}\epsilon\right].\end{aligned}$$

By Corollary 3.2 and Theorem 3.3, the two terms on the right-hand side tend to zero as $n \to \infty$, which proves the corollary. □

Acknowledgement

I would like to thank Jonathan Jedwab for many valuable discussions and Jonathan Jedwab and Daniel J. Katz for their careful comments on this paper.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness: Typical values*, Proc. Lond. Math. Soc **95** (2007), no. 3, 778–812.
[2] N. Alon, S. Litsyn, and A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inform. Theory **56** (2010), no. 1, 545–554.
[3] H. Cramér, *Sur un nouveau théorème-limite de la théorie des probabilités*, Actualités Sci. Indust. **736** (1938), 5–23.

[4] D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Adv. Math. Commun. **1** (2007), 461–475.
[5] R. Durrett, *Probability: Theory and examples*, 4th ed., Cambridge University Press, 2010.
[6] S. W. Golomb and G. Gong, *Signal design for good correlation: For wireless communication, cryptography, and radar*, Cambridge University Press, Cambridge, 2005.
[7] J. Jedwab, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.
[8] K. H. Leung and B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64** (2012), no. 1-2, 143–151.
[9] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), no. 4, 265–377.
[10] C. McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics (J. Siemons, ed.), London Math. Soc. Lectures Notes Ser. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188.
[11] I. D. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), no. 5, 663–671.
[12] J. W. Moon and L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), no. 12, 340–343.
[13] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), no. 4, 929–952.
[14] R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), no. 1, 319–346.
[15] ———, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968.

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

Current address: Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany.

E-mail address: kaiuwe.schmidt@ovgu.de

The final copy-edited version is published in Lect. Notes Comput. Science 7280, pp. 303-314, 2012
(http://dx.doi.org/10.1007/978-3-642-30615-0_28).

ON RANDOM BINARY SEQUENCES

KAI-UWE SCHMIDT

Abstract. A binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n is an element of $\{-1, 1\}^n$ and its autocorrelation at shift u is $C_u(A) = \sum_j a_j a_{j+u}$. We use the ℓ_r norm of $(C_1(A), C_2(A), \ldots, C_{n-1}(A))$ to measure the collective smallness of the autocorrelations and, when A is drawn uniformly from $\{-1, 1\}^n$, determine the asymptotic behaviour, as $n \to \infty$, of the expectation of these norms and prove asymptotic concentration around the expected value. For integral r, we also give exact expressions for the expectation of the rth power of these ℓ_r norms. This complements results of Borwein and Lockhart for $r = 2$ and the present author for $r = \infty$ and extends partial results of Mercer for even integral r.

1. Introduction

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be an element of $\{-1, 1\}^n$, which we call a *binary sequence* of length n. The *aperiodic autocorrelation* of A at shift u is defined to be

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

There is sustained interest in binary sequences whose aperiodic autocorrelations at all nonzero shifts are small in magnitude relative to their lengths (see Turyn [17] and Jedwab [7] for excellent surveys). The numbers $C_u(A)$ are also related to several old unsolved problems concerning the behaviour on the unit circle of the polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$ (see Littlewood [9], [10, Problem 19], Erdős [5, Problem 22], [6], and Borwein [2] for surveys). This relationship arises since

$$\left|A(e^{i\theta})\right|^2 = n + 2\sum_{u=1}^{n-1} C_u(A)\cos(u\theta) \quad \text{for } \theta \in \mathbb{R}. \tag{1}$$

Let $x = (x_1, x_2, \ldots, x_k)$ be an element of $\mathbb{R}^k$. For real $r > 0$, we write

$$\|x\|_r = \left(|x_1|^r + |x_2|^r + \cdots + |x_k|^r\right)^{1/r}.$$

Date: 25 March 2012.

K.-U. Schmidt was with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is now with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: kaiuwe.schmidt@ovgu.de.

The author is supported by German Research Foundation.

This defines the ℓ_r norm in $\mathbb{R}^k$ for $r \geq 1$. We also define the ℓ_∞ *norm*

$$\|x\|_\infty = \max\big\{|x_1|, |x_2|, \dots, |x_k|\big\},$$

which equals the limit of $\|x\|_r$ as $r \to \infty$. For the binary sequence A write

$$C(A) = \big(C_1(A), C_2(A), \dots, C_{n-1}(A)\big).$$

Then $\|C(A)\|_r$ measures the collective smallness of the aperiodic autocorrelations of A. In the sequence literature, $\|C(A)\|_\infty$ is called the *peak sidelobe level* of A and $\frac{1}{2}\,n^2/\|C(A)\|_2^2$ is called the *merit factor* of A.

Now let A_n be drawn uniformly from $\{-1,1\}^n$. In other words, each of the n sequence elements of A_n takes each of the values -1 and 1 independently with probability 1/2. We are interested in the asymptotic behaviour of the random variable $\|C(A_n)\|_r$. Recall that a sequence of random variables X_n *converges in probability* to a constant c if $\Pr(|X_n - c| \geq \epsilon) \to 0$ as $n \to \infty$ for all $\epsilon > 0$.

For the ℓ_∞ norm, the following result, proved by the author in [16], gives a complete solution to a problem due to Moon and Moser [12].

Theorem 1. [16, Theorem 1] *Let A_n be drawn uniformly from $\{-1,1\}^n$. Then, as $n \to \infty$,*

$$\frac{\|C(A_n)\|_\infty}{\sqrt{n\log n}} \to \sqrt{2} \quad \textit{in probability}$$

and

$$\frac{\mathrm{E}\left(\|C(A_n)\|_\infty\right)}{\sqrt{n\log n}} \to \sqrt{2}.$$

In this paper, we prove the following complementary result on $\|C(A_n)\|_r$ for finite r, in which $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\,dt$ denotes the gamma function, satisfying $\Gamma(p+1) = p!$ when p is a nonnegative integer.

Theorem 2. *Let A_n be drawn uniformly from $\{-1,1\}^n$ and let r be a real number satisfying $0 < r < \infty$. Then, as $n \to \infty$,*

$$\frac{\|C(A_n)\|_r}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r} \quad \textit{in probability.} \tag{2}$$

and

$$\frac{\mathrm{E}(\|C(A_n)\|_r^r)}{n^{r/2+1}} \to \frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)} \tag{3}$$

Moreover, for $r \geq 1$, as $n \to \infty$,

$$\frac{\mathrm{E}(\|C(A_n)\|_r)}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r}. \tag{4}$$

It is of significant interest to find the asymptotic behaviour of the minimum values of $\|C(A_n)\|_r$. Theorems 1 and 2 provide upper bounds for these minima. For $r = \infty$, nothing stronger is known and for $r = 2$, the best

known result [8], obtained by binary sequences B_n formed by the Legendre symbol, is $\|C(B_n)\|_2/n \to c$, where $c < 25/89$ is strictly smaller than $1/\sqrt{2}$.

For $r = 2$, assertions (2) and (3) of Theorem 2 follow from [3, Theorem 1] by Borwein and Lockhart, which deals with norms of random polynomials. The relationship arises from the fact that, when the binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n is represented as a polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$, then from (1),

$$n^2 + 2\,\|C(A)\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi} \left|A(e^{i\theta})\right|^4 d\theta.$$

Sarwate [15], and independently Newman and Byrnes [13], established the exact, rather than asymptotic, value of $\mathrm{E}(\|C(A_n)\|_2^2)$ to be $n(n-1)/2$. Assertion (3) of Theorem 2 was proved by Mercer [11, p. 669] when r is an even positive integer. In fact, it was shown in [11, Theorem 1.4] that, in this case, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial in n, which can be easily computed using a recurrence relation. The key to this is the following elementary, but very useful, result, which was formally proved by Mercer [11, Proposition 1.1].

Proposition 3. *Let $X_0, X_1, \ldots, X_{n-1}$ be mutually independent random variables, each taking each of the values -1 and 1 with probability $1/2$. Then, for fixed $u \in \{1, 2, \ldots, n-1\}$, the $n-u$ products*

$$X_0X_u,\ X_1, X_{1+u}, \ldots, X_{n-u-1}X_{n-1}$$

are mutually independent.

It is an immediate consequence of Proposition 3 that $C_{n-k}(A_n)$ is a transformed binomial random variable with parameters k and $1/2$. Hence, for $k \in \{1, 2, \ldots, n-1\}$ and real $r \geq 0$, the absolute moments $\mathrm{E}(|C_{n-k}(A_n)|^r)$ are given by

$$\frac{1}{2^{k-1}} \sum_{j<k/2} (k-2j)^r \binom{k}{j}. \tag{5}$$

When $r \geq 2$ is an even integer, Mercer [11, Theorem 1.4], building on a technique due to Romanovsky [14], gave a nice recurrence relation for the numbers (5). This shows that, when r is an even positive integer, (5) is a polynomial of degree $r/2$ in k, and therefore, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial of degree $r/2+1$ in n. Proposition 9 of this paper contains a recurrence relation for the numbers (5) for all real $r \geq 2$. This result together with an evaluation of (5) for $r = 1$ then shows that, when r is an odd positive integer, then

$$\frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n})\|_r^r) \quad \text{and} \quad \frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n+1})\|_r^r)$$

are polynomials of degree $(r+3)/2$ in n. This method enables us to derive exact, rather than asymptotic, values of $\mathrm{E}(\|C(A_n)\|_r^r)$ for odd integral $r \geq 1$.

2. Moments of autocorrelations

Let A_n be drawn uniformly from $\{-1,1\}^n$. In this section we establish the asymptotic behaviour of the moments of the random vector $\big(C_u(A_n), C_v(A_n)\big)$, which will be the key to prove Theorem 2. We follow the method developed in [16]. Fix n and write $A_n = (a_0, a_1, \dots, a_{n-1})$. Then, for nonnegative integers p and q, not both of them zero, we have

$$\begin{aligned}(6)\quad &\mathrm{E}\left(C_u(A_n)^p C_v(A_n)^q\right)\\ &\quad= \sum_{i_1,\dots,i_p=0}^{n-u-1} \sum_{j_1,\dots,j_q=0}^{n-v-1} \mathrm{E}\left[a_{i_1}a_{i_1+u}\cdots a_{i_p}a_{i_p+u}a_{j_1}a_{j_1+v}\cdots a_{j_q}a_{j_q+v}\right].\end{aligned}$$

Since the a_j's are mutually independent, $\mathrm{E}(a_j) = 0$, and $a_j^2 = 1$ for all $j \in \{0,1,\dots,n-1\}$, the expectation in the sum equals either zero or one. In particular, the expectation is nonzero exactly when the indices of the sequence elements occurring in the expectation match in pairs, so that it remains to count the number of cases when this happens. To do so, we define the notion of an even tuple as follows.

Definition 4. A tuple $(x_1, x_2, \dots, x_k)$ is *even* if k is even and there exists a permutation σ of $\{1,2,\dots,k\}$ such that $x_{\sigma(2i-1)} = x_{\sigma(2i)}$ for each $i \in \{1,2,\dots,k/2\}$.

For example, $(1,3,1,4,3,4)$ is even, while $(2,1,1,2,1,3)$ is not even. In the following two lemmas we prove two results about even tuples. Recall that, for positive integer k, the double factorial

$$(2k-1)!! = \frac{(2k)!}{k!\,2^k} = (2k-1)(2k-3)\cdots 3\cdot 1$$

is the number of ways to arrange $2k$ objects into k unordered pairs.

Lemma 5. *Let m and k be positive integers and let R be the set of even tuples in*

$$\big\{(x_1, x_2, \dots, x_{2k}) : x_i \in \mathbb{Z},\, 0 \le x_i < m\big\}.$$

Then

$$(2k-1)!!\, m(m-1)\cdots(m-k+1) \le |R| \le (2k-1)!!\, m^k.$$

Proof. There are $(2k-1)!!$ ways to arrange $x_1, x_2, \dots, x_{2k}$ into k unordered pairs. There are $m(m-1)\cdots(m-k+1)$ choices for k distinct values in $\{0,1,\dots,m-1\}$, which we assign to these pairs. In this way, we construct $(2k-1)!!\, m(m-1)\cdots(m-k+1)$ distinct even tuples in R, giving the lower bound. On the other hand, there are m^k choices for k values in $\{0,1,\dots,m-1\}$. In this way, we construct $(2k-1)!!\, m^k$ (not necessarily distinct) even tuples, which cover all elements of R. This gives the upper bound. □

Lemma 6. *Let u, v, and n be integers satisfying $0 < u < v < n$. Let S be the set of all even tuples in $\{0, 1, \ldots, n-1\}^{2p+2q}$ of the form*

$$(x_1, x_1 + u, \ldots, x_p, x_p + u, y_1, y_1 + v, \ldots, y_q, y_q + v),$$

such that $(x_1, x_2, \ldots, x_p)$ and $(y_1, y_2, \ldots, y_q)$ are not both even. Then

$$|S| \leq (2p + 2q - 1)!! \, (n-u)^{p/2} (n-v)^{(q-1)/2}.$$

Proof. Arrange the $2p + 2q$ variables

$$x_1, x_1 + u, \ldots, x_p, x_p + u, y_1, y_1 + v, \ldots, y_q, y_q + v \tag{7}$$

into $p + q$ unordered pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_{p+q}, b_{p+q})$ such that there are either fewer than $p/2$ pairs of the form (x_i, x_j) or fewer than $q/2$ pairs of the form (y_i, y_j). This can be done in at most $(2p + 2q - 1)!!$ ways. We formally set $a_i = b_i$ for all $i \in \{1, 2, \ldots, p + q\}$. If this assignment does not yield a contradiction, then we call the arrangement of (7) into $p + q$ pairs *consistent*. For example, if there are pairs of the form (x_i, y_j) and $(x_i + u, y_j + v)$, then the arrangement is not consistent since $u \neq v$ by assumption.

Now, for every consistent arrangement, pairs of the form (x_i, x_j) or (y_i, y_j) determine the value of another pair (namely, (x_i+u, x_j+u) or (y_i+v, y_j+v), respectively). On the other hand, for every consistent arrangement, pairs not of the form

$$(x_i, x_j), \ (y_i, y_j), \ (x_i + u, x_j + u), \text{ or } (y_i + v, y_j + v)$$

determine the value of at least two other pairs. For example, if there exists the pair (x_i, y_j), then $x_i + u$ and $y_j + v$ must lie in different pairs. Therefore, since there are either fewer than $p/2$ pairs of the form (x_i, x_j) or fewer than $q/2$ pairs of the form (y_i, y_j), for each consistent arrangement, at most $(p + q - 1)/2$ of the variables $x_1, \ldots, x_p, y_1, \ldots, y_q$ can be chosen independently. Hence, since $u < v$, we can construct a set of at most $(2p + 2q - 1)!! \, (n - u)^{p/2} \, (n - v)^{(q-1)/2}$ tuples that contains S as a subset, as required. □

We now use Lemmas 5 and 6 to estimate the moments (6). We shall normalise the aperiodic autocorrelations of a binary sequence A of length n by defining

$$Y_u(A) = \frac{C_u(A)}{\sqrt{n-u}} \quad \text{for } u \in \{0, 1, \ldots, n-1\}. \tag{8}$$

Let Z be a standard normal random variable (which has zero mean and unit variance). By the definition of the Gamma function, we find that for real $r > -1$,

$$\mathrm{E}(|Z|^r) = \sqrt{\frac{2}{\pi}} \int_0^\infty x^r e^{-x^2/2} \, dx = \frac{2^{r/2}}{\sqrt{\pi}} \Gamma\Big(\frac{r+1}{2}\Big) = \frac{\Gamma(r+1)}{2^{r/2} \, \Gamma(r/2+1)}, \tag{9}$$

so that, since $\Gamma(p+1)=p!$ for nonnegative integral p and Z is symmetric, the moments of Z are

$$\mathrm{E}(Z^p)=\begin{cases}(p-1)!! & \text{for even } p\\ 0 & \text{for odd } p.\end{cases} \tag{10}$$

Proposition 7. *Let A_n be drawn uniformly from $\{-1,1\}^n$. Let $g(n)$ be such that $1/g(n)\to 0$ as $n\to\infty$, and let Z be a standard normal random variable. Then, for nonnegative integers p and q,*

$$\lim_{n\to\infty}\max_{1\le u<v\le n-g(n)}\Big|\mathrm{E}\left(Y_u(A_n)^pY_v(A_n)^q\right)-\mathrm{E}(Z^p)\,\mathrm{E}(Z^q)\Big|=0.$$

Proof. We may assume that p and q are not both zero. Let n be large enough, so that we can choose integers u and v such that $1\le u<v\le n-g(n)$. Let T be the set of even tuples in $\{0,1,\dots,n-1\}^{2p+2q}$ of the form

$$(x_1,x_1+u,\dots,x_p,x_p+u,y_1,y_1+v,\dots,y_q,y_q+v).$$

Then, from (6) and (8),

$$\mathrm{E}\left(Y_u(A_n)^pY_v(A_n)^q\right)=\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}}.$$

First, assume that at least one of p and q is odd. Then, by Lemma 6,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}}\le\frac{(2p+2q-1)!!}{g(n)^{1/2}}$$

using $n-v\ge g(n)$. Since either $\mathrm{E}(Z^p)=0$ or $\mathrm{E}(Z^q)=0$ and the right hand side tends to zero as $n\to\infty$, the lemma is true when at least one of p or q is odd.

Now assume that p and q are both even. Then by Lemmas 5 and 6,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}}\le(p-1)!!\,(q-1)!!+\frac{(2p+2q-1)!!}{g(n)^{1/2}},$$

and by Lemma 5,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}}\ge(p-1)!!\,(q-1)!!\prod_{j=1}^{p/2-1}\left(1-\frac{j}{g(n)}\right)\prod_{\ell=1}^{q/2-1}\left(1-\frac{\ell}{g(n)}\right).$$

Hence, since $1/g(n)\to 0$, we conclude from (10) that the lemma is true when p and q are both even. □

We now use Proposition 7 to prove the following result on absolute moments.

Theorem 8. *Let A_n be drawn uniformly from $\{-1,1\}^n$. Let $g(n)$ be such that $1/g(n)\to 0$ as $n\to\infty$, and let Z be a standard normal random variable. Then, for real r and s satisfying $0\le r,s<\infty$,*

$$\lim_{n\to\infty}\max_{1\le u<v\le n-g(n)}\Big|\mathrm{E}(|Y_u(A_n)|^r|Y_v(A_n)|^s)-\mathrm{E}(|Z|^r)\,\mathrm{E}(|Z|^s)\Big|=0.$$

Before we prove the theorem, we recall some standard concepts from analysis (see [4] or [1] for a detailed treatment). A sequence of random elements $(X_{n,1}, \ldots, X_{n,m})$ in $\mathbb{R}^m$ with distribution function F_n *converges in distribution* to a random element $(X_1, \ldots, X_m)$ in $\mathbb{R}^m$ with distribution function F if F_n converges pointwise to F at all points where F is continuous. The Continuous Mapping Theorem states that if $f : \mathbb{R}^m \to \mathbb{R}^k$ is continuous and $(X_{n,1}, \ldots, X_{n,m})$ converges in distribution to $(X_1, \ldots, X_m)$, then $f(X_{n,1}, \ldots, X_{n,m})$ converges in distribution to $f(X_1, \ldots, X_m)$ [1, Theorem 29.2].

A sufficient condition for convergence in distribution of $(X_{n,1}, \ldots, X_{n,m})$ to $(X_1, \ldots, X_m)$ is that the distribution of $(X_1, \ldots, X_m)$ is uniquely determined by the moments $\mathrm{E}(X_1^{p_1} \cdots X_m^{p_m})$ and that

$$\mathrm{E}(X_{n,1}^{p_1} \cdots X_{n,m}^{p_m}) \to \mathrm{E}(X_1^{p_1} \cdots X_m^{p_m})$$

for all nonnegative integers $p_1, \ldots, p_m$ [1, Exercise 30.6]. We note that the distribution of an m-dimensional standard normal random variable (which has zero mean vector and identity covariance matrix) is uniquely determined by its moments [1, Exercise 30.5].

We shall make use of the following version of the Dominated Convergence Theorem. Let U_n and V_n be random variables satisfying $0 \le U_n \le V_n$ so that U_n converges in distribution to U and V_n converges in distribution to V. Then, if $\mathrm{E}(V_n) \to \mathrm{E}(V) < \infty$, then $\mathrm{E}(U_n) \to \mathrm{E}(U)$ (this is an extension of [4, Section 4.5, Exercise 2], in which $V_n = V$ for all n).

Proof of Theorem 8. Write $(Y_u(A_n), Y_v(A_n))$ in a triangular array such that the nth row contains $(Y_u(A_n), Y_v(A_n))$ for u, v satisfying $1 \le u < v \le n - g(n)$ in some arbitrary order. Construct a sequence of random elements $(X_{k,1}, X_{k,2})$ by reading out the rows of this array. Let Z_1 and Z_2 be independent standard normal random variables. Then Proposition 7 is equivalent to

(11)
$$\mathrm{E}(X_{k,1}^p X_{k,2}^q) \to \mathrm{E}(Z_1^p Z_2^q) \text{ as } k \to \infty, \text{ for all nonnegative integers } p \text{ and } q.$$

Now choose integers a and b such that $r \le 2a$ and $s \le 2b$. We apply the Dominated Convergence Theorem with

$$U_k = |X_{k,1}|^r \, |X_{k,2}|^s$$

and

$$V_k = (1 + |X_{k,1}|^{2a})(1 + |X_{k,2}|^{2b}),$$

so that $0 \le U_k \le V_k$ for all k. By (11) and the discussion preceding this proof, $(X_{k,1}, X_{k,2})$ converges in distribution to (Z_1, Z_2). By the Continuous Mapping Theorem, U_k converges in distribution to $U = |Z_1|^r \, |Z_2|^s$ and V_k converges in distribution to $V = (1 + |Z_1|^{2a})(1 + |Z_2|^{2b})$. By (11), $\mathrm{E}(V_k) \to \mathrm{E}(V)$, and therefore by the Dominated Convergence Theorem, $\mathrm{E}(|X_{k,1}|^r \, |X_{k,2}|^s) \to \mathrm{E}(|Z_1|^r |Z_2|^s)$, which is equivalent to the statement in the theorem. □

3. Proof of Theorem 2

We first prove assertion (3). Let $n > 2$ and $g(n)$ be the largest integer not greater than $\log n$. We use the normalisation (8) of $C_u(A_n)$ to write $\mathrm{E}(\|C(A_n)\|_r^r) = G_1(n) + G_2(n)$, where

$$G_1(n) = \sum_{u=1}^{g(n)-1} u^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)|^r),$$

$$G_2(n) = \sum_{u=g(n)}^{n-1} u^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)|^r).$$

The trivial bound $|Y_{n-u}(A_n)| \le u^{1/2}$ gives $|G_1(n)| < g(n)^{r+1}$, and therefore since $g(n) \le \log n$, the term $G_1(n)/n^{r/2+1}$ tends to zero as $n \to \infty$. Letting Z be a standard normal random variable, we have by Theorem 8 with $r = 0$ or $s = 0$,

$$\lim_{n\to\infty} \frac{G_2(n)}{n^{r/2+1}} = \mathrm{E}(|Z|^r) \lim_{n\to\infty} \frac{1}{n^{r/2+1}} \sum_{u=g(n)}^{n-1} u^{r/2} = \frac{\mathrm{E}(|Z|^r)}{r/2+1}.$$

The last step can be established by Riemann integration. Then, assertion (3) of the theorem follows from (9) and $z\,\Gamma(z) = \Gamma(z+1)$.

To prove assertion (2) of the theorem, we show with the same technique that

$$\frac{\mathrm{E}(\|C(A_n)\|_r^{2r})}{n^{r+2}} \to \left(\frac{\mathrm{E}(|Z|^r)}{r/2+1}\right)^2. \tag{12}$$

We have

$$\begin{aligned}\mathrm{E}(\|C(A_n)\|_r^{2r}) &= \sum_{u=1}^{n-1}\sum_{v=1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r)\\ &= \sum_{u=1}^{n-1} u^r\,\mathrm{E}(|Y_{n-u}(A_n)|^{2r}) + 2\sum_{u=1}^{n-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\,\mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r).\end{aligned}$$

Proceeding as in the proof of assertion (3), we conclude that the first sum divided by n^{r+2} is $O(n^{-1})$, and therefore tends to zero as $n \to \infty$. We partition the second sum into $H_1(n)$ and $H_2(n)$, where

$$H_1(n) = 2\sum_{u=1}^{g(n)-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r),$$

$$H_2(n) = 2\sum_{u=g(n)}^{n-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r).$$

Since $|Y_{n-u}(A_n)Y_{n-v}(A_n)| \le (uv)^{1/2}$ and $g(n) \le \log n$, we have

$$\frac{|H_1(n)|}{n^{r+2}} < \frac{2}{n}(\log n)^{r+1}.$$

From Theorem 8 with $r = s$ we find that

$$\begin{aligned}
\lim_{n\to\infty} \frac{H_2(n)}{n^{r+2}} &= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty} \frac{2}{n^{r+2}} \sum_{u=g(n)}^{n-1} \sum_{v=u+1}^{n-1} (uv)^{r/2} \\
&= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty} \frac{1}{n^{r+2}} \left(\sum_{u=g(n)}^{n-1} \sum_{v=g(n)}^{n-1} (uv)^{r/2} - \sum_{u=g(n)}^{n-1} u^r \right) \\
&= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty} \left(\frac{1}{n^{r/2+1}} \sum_{u=g(n)}^{n-1} u^{r/2} \right)^2 \\
&= \left(\frac{\mathrm{E}(|Z|^r)}{r/2+1} \right)^2,
\end{aligned}$$

which again can be established by Riemann integration. This proves our claim (12). Therefore, the variance of $\|C(A_n)\|_r^r)/n^{r/2+1}$ tends to zero and assertion (2) follows from Chebyshev's inequality and the Continuous Mapping Theorem.

Now notice that convergence in probability to a constant c implies convergence in distribution to c. Assertion (4) of the theorem then follows from the inequality

$$\frac{\|C(A_n)\|_r}{n^{1/2+1/r}} \le 1 + \frac{\|C(A_n)\|_r^r}{n^{r/2+1}} \quad \text{for } r \ge 1$$

and the Dominated Convergence Theorem. □

4. Exact formulas for expected values

As before, we draw A_n uniformly from $\{-1, 1\}^n$. In this section, we prove a recurrence relation for the moments of $C_u(A_n)$ from which the values $\mathrm{E}(\|C(A_n)\|_r^r)$ can be computed exactly when r is a positive integer.

Let $X_1, X_2, \ldots$ be mutually independent identically distributed random variables with $\Pr(X_1 = -1) = \Pr(X_1 = 1) = 1/2$ and define the random variable

$$S_k = \sum_{j=1}^{k} X_j.$$

Then, by Proposition 3, $C_{n-k}(A_n)$ and S_k have the same distribution for $k \in \{1, 2, \ldots, n-1\}$, and hence for real $r \ge 0$,

$$\mathrm{E}(\|C(A_n)\|_r^r) = \sum_{k=1}^{n-1} \mathrm{E}(|S_k|^r). \tag{13}$$

We are therefore interested in the values $\mathrm{E}(|S_k|^r)$, for which we have the following recurrence relation.

Proposition 9. *For integral $k \geq 0$ and real $r \geq 2$, we have*

$$\mathrm{E}(|S_k|^r) = k^2\ \mathrm{E}(|S_k|^{r-2}) - k(k-1)\ \mathrm{E}(|S_{k-2}|^{r-2}).$$

Proof. Recall that

$$\mathrm{E}(|S_k|^r) = \frac{1}{2^{k-1}} \sum_{j<k/2} (k-2j)^r \binom{k}{j}. \tag{14}$$

We have

$$\begin{aligned}(k-2j)^2\binom{k}{j} &= k^2\binom{k}{j} - 4j(k-j)\binom{k}{j}\\ &= k^2\binom{k}{j} - 4k(k-1)\binom{k-2}{j-1}.\end{aligned}$$

Substitution into (14) shows that $\mathrm{E}(|S_k|^r)$ equals

$$\frac{k^2}{2^{k-1}} \sum_{j<k/2} (k-2j)^{r-2}\binom{k}{j} - \frac{k(k-1)}{2^{k-3}} \sum_{j<k/2-1} (k-2-2j)^{r-2}\binom{k-2}{j},$$

from which the required recurrence follows by using (14) again. □

Mercer [11, Theorem 1.4] gave a proof of Proposition 9 when r is an even positive integer by inspecting the moment generating function of S_k. In this case, the initial condition for the recurrence is $\mathrm{E}(|S_k|^0) = 1$, and we get for example,

$$\begin{aligned}\mathrm{E}(|S_k|^2) &= k,\\ \mathrm{E}(|S_k|^4) &= 3k^2 - 2k,\end{aligned}$$

and therefore by (13),

$$\begin{aligned}\mathrm{E}(\|C(A_n)\|_2^2) &= \tfrac{1}{2}(n^2-n),\\ \mathrm{E}(\|C(A_n)\|_4^4) &= \tfrac{1}{2}(2n^3-5n^2+3n).\end{aligned}$$

In general, when r is an even positive integer, $\mathrm{E}(|S_k|^r)$ is a polynomial of degree $r/2$ in k, and therefore, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial of degree $r/2+1$ in n.

To apply Proposition 9 when r is an odd positive integer, we require the following result, which is number A.4 of the 1974 Putnam competition. The proof, which is an evaluation of (14) for $r = 1$, is left to the reader.

Lemma 10. *For positive integral k,*

$$\mathrm{E}(|S_k|) = \frac{1}{2^{k-1}}\binom{k}{\lceil k/2\rceil}\left\lceil\frac{k}{2}\right\rceil.$$

By straightforward manipulations, we can rewrite the recurrence relation of Proposition 9 as

$$\mathrm{E}(|S_k|^r) = \frac{1}{2^{k-1}}\binom{k}{\lceil k/2\rceil}\left\lceil\frac{k}{2}\right\rceil F_r(k),$$

where $F_r(k)$ satisfies, for integral $k \geq 0$ and real $r \geq 2$,

$$F_r(k) = k^2 F_{r-2}(k) - 4\lfloor k/2\rfloor(\lceil k/2\rceil - 1)F_{r-2}(k-2).$$

Now let r be an odd positive integer. Then, since $F_1(k) = 1$ by Lemma 10, $F_r(2k)$ and $F_r(2k+1)$ are polynomials of degree $(r-1)/2$ in k. For example,

$$\begin{aligned} F_3(2k) &= 4k, & F_3(2k+1) &= 4k+1, \\ F_5(2k) &= 32k^2 - 16k, & F_5(2k+1) &= 32k^2 + 8k + 1. \end{aligned}$$

Notice that we can rewrite $\mathrm{E}(|S_{2k+1}|^r)$ in terms of $\binom{2k}{k}$ using

$$\binom{2k+1}{k+1} = \frac{2k+1}{k+1}\binom{2k}{k}.$$

Then, separating the sum in (13) into sums over even and odd k, we get

$$\mathrm{E}(\|C(A_n)\|_r^r) = \sum_{k<n/2}\frac{2k\,F_r(2k)}{4^k}\binom{2k}{k} + \sum_{k<(n-1)/2}\frac{(2k+1)F_r(2k+1)}{4^k}\binom{2k}{k}.$$

It remains to evaluate

$$\lambda_t(n) = \sum_{k=0}^{n-1}\frac{k^t}{4^k}\binom{2k}{k}$$

for integral $t \geq 0$. By telescoping, we find that

$$\lambda_0(n) = \sum_{k=0}^{n-1}\left[\frac{2(k+1)}{4^{k+1}}\binom{2k+2}{k+1} - \frac{2k}{4^k}\binom{2k}{k}\right] = \binom{2n}{n}\frac{2n}{4^n}.$$

When $t > 0$, the sums $\lambda_t(n)$ can then be evaluated via reduction, viz

$$\lambda_t(n) = \sum_{m=1}^{n-1}\sum_{k=0}^{n-1}\frac{k^{t-1}}{4^k}\binom{2k}{k} - \sum_{m=1}^{n-1}\sum_{k=0}^{m-1}\frac{k^{t-1}}{4^k}\binom{2k}{k}.$$

For example,

$$\begin{aligned} \lambda_1(n) &= \binom{2n}{n}\frac{2n(n-1)}{3\cdot 4^n}, \\ \lambda_2(n) &= \binom{2n}{n}\frac{2n(n-1)(3n-1)}{15\cdot 4^n} \end{aligned}$$

(the expression for $\lambda_1(n)$ is a solution to Problem E 995 in the December 1951 issue of the American Mathematical Monthly). We then get, for

example,

$$\mathrm{E}(\|C(A_{2n})\|_1) = \binom{2n}{n}\frac{8n^2-2n}{3\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n+1})\|_1) = \binom{2n}{n}\frac{8n^2+4n}{3\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n})\|_3^3) = \binom{2n}{n}\frac{96n^3-68n^2+2n}{15\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n+1})\|_3^3) = \binom{2n}{n}\frac{96n^3+52n^2+2n}{15\cdot 4^n}.$$

In general, when r is an odd positive integer,

$$\frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n})\|_r^r) \quad\text{and}\quad \frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n+1})\|_r^r)$$

are polynomials of degree $(r+3)/2$ in n.

Acknowledgement

I wish to thank Richard Lockhart for very helpful discussions on the subject of this paper.

References

1. P. Billingsley, *Probability and measure*, 3rd ed., John Wiley & Sons, Inc., 1995.
2. P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics, Springer-Verlag, New York, NY, 2002.
3. P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, Proc. Amer. Math. Soc. **129** (2001), no. 5, 1463–1472.
4. K. L. Chung, *A course in probability theory*, Harcourt, Brace & World, Inc., 1968.
5. P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.
6. ———, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.
7. J. Jedwab, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.
8. J. Jedwab, D. J. Katz, and K.-U. Schmidt, *Littlewood polynomials with small L^4 norm*, preprint (2011).
9. J. E. Littlewood, *On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$*, J. London Math. Soc. **41** (1966), 367–376.
10. ———, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
11. I. D. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), no. 5, 663–671.
12. J. W. Moon and L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), no. 12, 340–343.
13. D. J. Newman and J. S. Byrnes, *The L^4 norm of a polynomial with coeffiecients ± 1*, Amer. Math. Monthly **97** (1990), no. 1, 42–45.
14. V. Romanovsky, *Note on the moments of a binomial $(p+q)^n$ about its mean*, Biometrika **15** (1923), no. 3/4, 410–412.
15. D. V. Sarwate, *Mean-square correlation of shift-register sequences*, IEE Proc. **131, Part F** (1984), no. 2, 101–106.

16. K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, arXiv:1105.5178 [math.CO] (2011).
17. R. J. Turyn, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968.

The final copy-edited version is published in IEEE Trans. Inform. Theory 58(4), pp. 2512-2515, 2012.
(http://dx.doi.org/10.1109/TIT.2011.2178391)

BINARY SEQUENCES WITH SMALL PEAK SIDELOBE LEVEL

KAI-UWE SCHMIDT

Abstract. A binary sequence of length n is an n-tuple with elements in $\{-1, 1\}$ and its peak sidelobe level is the largest absolute value of its aperiodic autocorrelations at nonzero shifts. A classical problem is to find binary sequences whose peak sidelobe level is small compared to the length of the sequence. Using known techniques from probabilistic combinatorics, this paper gives a construction for a binary sequence of length n with peak sidelobe level at most $\sqrt{2n\log(2n)}$ for every $n > 1$. This improves the best known bound for the peak sidelobe level of a family of explicitly constructed binary sequences, which arises for the family of m-sequences. By numerical analysis it is argued that the peak sidelobe level of the constructed sequences grows in fact like order $\sqrt{n\log\log n}$, and therefore grows strictly more slowly than the peak sidelobe level of a typical binary sequence.

1. Introduction

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a binary sequence of length $n > 1$, namely an element of $\{-1, 1\}^n$. The *aperiodic autocorrelation* at shift u of A is given by

$$C_u(A) = \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } u \in \{0, 1, \ldots, n-1\}.$$

A classical problem in digital sequence design is to find binary sequences whose aperiodic autocorrelations (at nonzero shifts) are small in magnitude (see [3], [21], [4], [5], [18], [11], [6], [15], for example, and [10] for a survey). Accordingly, we define the *peak sidelobe level* of A to be

$$M(A) = \max_{0<u<n} |C_u(A)|.$$

By a parity argument, $M(A) \geq 1$ for all binary sequences A of length greater than 1. A *Barker sequence* is a binary sequence B that satisfies $M(B) = 1$. Such sequences exist for lengths $2, 3, 4, 5, 7, 11$, and 13. It has been conjectured since at least 1960 [19] that there is no Barker sequence of length greater than 13. This conjecture has been proved for odd lengths by

Date: 27 July 2011 (revised 01 November 2011).

Key words and phrases. Aperiodic autocorrelation, binary sequence, derandomisation, peak sidelobe level.

The author was supported by German Research Foundation under Research Fellowship SCHM 2609/1-1.

Turyn and Storer [20] and for all even lengths up to $2 \cdot 10^{30}$ (see Leung and B. Schmidt [12] for most recent results).

Let $\mu(n)$ be the minimum of $M(A)$ taken over all binary sequences A of length n. Then $\mu(n) = 1$ if and only if there is a Barker sequence of length n. The value $\mu(n)$ can be computed with an apparent time complexity of $O(1.4^n)$ [4]. Currently, $\mu(n)$ is known for all $n \le 61$ and for $n = 64$ (see Coxson and Russo [5] for most recent results). Many authors have put considerable computational effort in finding binary sequences with small peak sidelobe level (see Nunn and Coxson [15], for example), showing that

$$\begin{aligned}\mu(n) &\le 2 \quad \text{for each } n \le 21,\\ \mu(n) &\le 3 \quad \text{for each } n \le 48,\\ \mu(n) &\le 4 \quad \text{for each } n \le 82,\\ \mu(n) &\le 5 \quad \text{for each } n \le 105.\end{aligned}$$

Turyn conjectured [21, p. 198] that the infimum limit of $\mu(n)$ is infinite. It has also been conjectured by several authors (see Jedwab [9] for historical background) that there exists a positive constant c such that, for all $n > 1$ and all binary sequences A of length n,

$$\sum_{u=1}^{n-1}[C_u(A)]^2 \ge cn^2.$$

This is known as the Merit Factor Conjecture and implies that $\mu(n)/\sqrt{n}$ is bounded away from 0 as $n \to \infty$. More specifically, based on a heuristic argument, Ein-Dor, Kanter, and Kinzel [7] conjectured that, as $n \to \infty$,

$$\frac{\mu(n)}{\sqrt{n}} \to d, \quad \text{where} \quad d = 0.435\ldots .$$

Mercer [13] proved that the peak sidelobe level of a random binary sequence of length n is typically not significantly larger than $\sqrt{2n\log n}$, thereby improving a result by Moon and Moser [14]. The author proved that the peak sidelobe level of a random binary sequence of length n is also typically not significantly smaller than $\sqrt{2n\log n}$, which improves a result by Alon, Litsyn, and Shpunt [1].

Theorem 1 (Schmidt [17])**.** *Let A_n be drawn uniformly from $\{-1,1\}^n$. Then, as $n \to \infty$,*

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

In view of Theorem 1, it is rather surprising that the currently strongest proven result for the peak sidelobe level of a *specific* family of binary sequences grows like order $\sqrt{n}\log n$ as $n \to \infty$. This result occurs for the family of m-sequences, which are binary sequences that exist for all lengths of the form $2^m - 1$ (see Golomb and Gong [8], for example, for background on m-sequences).

Theorem 2 (Sarwate [16]). *Let Y be an m-sequence of length $n = 2^m - 1$. Then*

$$M(Y) \leq 1 + \frac{2}{\pi}\sqrt{n+1}\,\log\Big(\frac{4n}{\pi}\Big).$$

Using known techniques from probabilistic combinatorics, we give a construction for a binary sequence of length n with peak sidelobe level at most $\sqrt{2n\log(2n)}$ for every $n > 1$. The construction is based on a derandomisation approach (see Alon and Spencer [2], for example) and can be implemented with $O(n^2)$ additions and $O(n^2)$ multiplications. By numerical analysis we argue that the peak sidelobe level of the constructed sequences grows like order $\sqrt{n\log\log n}$ as $n \to \infty$, and therefore grows strictly more slowly than the peak sidelobe level of a typical binary sequence.

2. Main Result

We begin with stating the promised construction.

Construction 3. *Let n be a positive integer and write $\theta = \sqrt{(2/n)\log(2n)}$. Construct a binary sequence $B_n = (b_0, b_1, \ldots, b_{n-1})$ of length n recursively by*

$$b_r = -\operatorname{sign}\left[\sum_{u=1}^{r-1} b_{r-u}\sinh\left(\theta\sum_{j=0}^{r-u-1} b_j b_{j+u}\right)\right],$$

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

Notice that we always have $b_0 = b_1 = 1$. The first few nontrivial binary sequences obtained under Construction 3 are

$$\begin{aligned}
B_3 &= (1,1,-1),\\
B_4 &= (1,1,-1,1),\\
B_5 &= (1,1,-1,1,1),\\
B_6 &= (1,1,-1,1,1,1),\\
B_7 &= (1,1,-1,1,1,1,-1).
\end{aligned}$$

The pattern may suggest that B_n is an initial segment of B_{n+1}, which is however not the case in general.

The following theorem gives an upper bound on the peak sidelobe level of B_n.

Theorem 4. *The binary sequence B_n of length $n > 1$ obtained under Construction 3 satisfies*

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

Proof. Fix an integer $n > 1$ and define, for $r \in \{0,1,\dots,n\}$ and $u \in \{1,2,\dots,n-1\}$, the function $f_{u,r} : \{-1,1\}^r \to \mathbb{R}$ by

$$f_{u,r}(x_0,x_1,\dots,x_{r-1}) = \begin{cases} 2e^{-\theta^2 n}(\cosh\theta)^{n-r}\cosh\Big(\theta\sum_{j=0}^{r-u-1}x_jx_{j+u}\Big) & \text{for } 0<u\le r-1\\ 2e^{-\theta^2 n}(\cosh\theta)^{n-u} & \text{for } r-1\le u<n.\end{cases}$$

Notice that $f_{r-1,r}$ is well defined. Let $I[E]$ be the indicator of an event E (which equals 1 if E occurs and equals 0 otherwise), and let $A=(a_0,a_1,\dots,a_{n-1})$ be an arbitrary binary sequence of length n. Straightforward manipulation gives, for each $u \in \{1,2,\dots,n-1\}$,

$$\begin{aligned} I\big[|C_u(A)| > \sqrt{2n\log(2n)}\big] &= I\big[C_u(A) > \theta n\big] + I\big[-C_u(A) > \theta n\big]\\ &= I\big[e^{\theta C_u(A)} > e^{\theta^2 n}\big] + I\big[e^{-\theta C_u(A)} > e^{\theta^2 n}\big]\\ &< e^{-\theta^2 n}\Big(e^{\theta C_u(A)} + e^{-\theta C_u(A)}\Big)\\ &= f_{u,n}(a_0,a_1,\dots,a_{n-1}). \end{aligned} \tag{1}$$

Write $B_n=(b_0,b_1,\dots,b_{n-1})$. We claim that

$$\sum_{u=1}^{n-1} f_{u,n}(b_0,b_1,\dots,b_{n-1}) < 1, \tag{2}$$

so that by (1),

$$\sum_{u=1}^{n-1} I\big[|C_u(B_n)| > \sqrt{2n\log(2n)}\big] < 1.$$

Hence, all of the indicators are zero and therefore

$$|C_u(B_n)| \le \sqrt{2n\log(2n)} \quad \text{for each } u \in \{1,2,\dots,n-1\},$$

proving the theorem.

It remains to prove the claim (2). We first show that, for $u \in \{1,2,\dots,n-1\}$ and $r \in \{0,1,\dots,n-1\}$, we have

$$f_{u,r}(x_0,x_1,\dots,x_{r-1}) = \tfrac{1}{2}\,f_{u,r+1}(x_0,\dots,x_{r-1},1) + \tfrac{1}{2}\,f_{u,r+1}(x_0,\dots,x_{r-1},-1). \tag{3}$$

This holds trivially for $u \ge r$. For $u < r$, we use

$$\cosh(y+z)+\cosh(y-z) = 2\cosh(z)\cosh(y)$$

to conclude

$$\begin{aligned} &\tfrac{1}{2}\,f_{u,r+1}(x_0,\dots,x_{r-1},1) + \tfrac{1}{2}\,f_{u,r+1}(x_0,\dots,x_{r-1},-1)\\ &= 2e^{-\theta^2 n}(\cosh\theta)^{n-r-1}\cosh(\theta\,x_{r-u})\cosh\Big(\theta\sum_{j=0}^{r-u-1}x_jx_{j+u}\Big)\\ &= f_{u,r}(x_0,x_1,\dots,x_{r-1}) \end{aligned}$$

since $x_{r-u} \in \{-1, 1\}$ and cosh is an even function.

Now, since sinh is an odd function, we can rewrite b_r as

$$b_r = -\operatorname{sign}\left[\sum_{u=1}^{r-1} 2\sinh(\theta b_{r-u})\sinh\left(\theta \sum_{j=0}^{r-u-1} b_j b_{j+u}\right)\right].$$

Use

$$2\sinh(z)\sinh(y) = \cosh(y+z) - \cosh(y-z)$$

to conclude that b_r is an $x \in \{-1, 1\}$ that minimises

$$\sum_{u=1}^{r-1} \cosh\left(\theta \sum_{j=0}^{r-u-1} b_j b_{j+u} + \theta b_{r-u} x\right).$$

We therefore find from (3) that

$$\sum_{u=1}^{n-1} f_{u,r+1}(b_0, b_1, \ldots, b_r) \le \sum_{u=1}^{n-1} f_{u,r}(b_0, b_1, \ldots, b_{r-1}) \tag{4}$$

for each $r \in \{0, 1, \ldots, n-1\}$. Using $\cosh x \le e^{x^2/2}$, we have

$$\begin{aligned}\sum_{u=1}^{n-1} f_{u,0} &\le \sum_{u=1}^{n-1} 2e^{-\theta^2(n+u)/2} \\ &\le 2(n-1)e^{-\theta^2 n/2} \\ &= 1 - \frac{1}{n}\end{aligned}$$

since $\theta^2 n = 2\log(2n)$. The claim (2) then follows by combination with (4) and induction on r. □

3. Efficient Implementation

Fix an integer $n > 1$ and assume the notation used in Construction 3. Define, for $r \in \{1, 2, \ldots, n\}$ and $u \in \{1, 2, \ldots, r\}$, the functions $c_{u,r}, s_{u,r} : \{-1, 1\}^r \to \mathbb{R}$ by

$$c_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \cosh\left(\theta \sum_{j=0}^{r-u-1} x_j x_{j+u}\right)$$

$$s_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \sinh\left(\theta \sum_{j=0}^{r-u-1} x_j x_{j+u}\right).$$

Assume that $b_0, \ldots, b_{r-1}$ have been already determined. Since $b_0 = b_1 = 1$, we may also assume that $r > 1$. We wish to calculate $s_{u,r}(b_0, \ldots, b_{r-1})$ for $u \in \{1, 2, \ldots, r-1\}$. This can be done recursively as follows. We clearly have

$$\begin{aligned}c_{r-1,r-1}(x_0, x_1, \ldots, x_{r-2}) &= 1 \\ s_{r-1,r-1}(x_0, x_1, \ldots, x_{r-2}) &= 0\end{aligned}$$

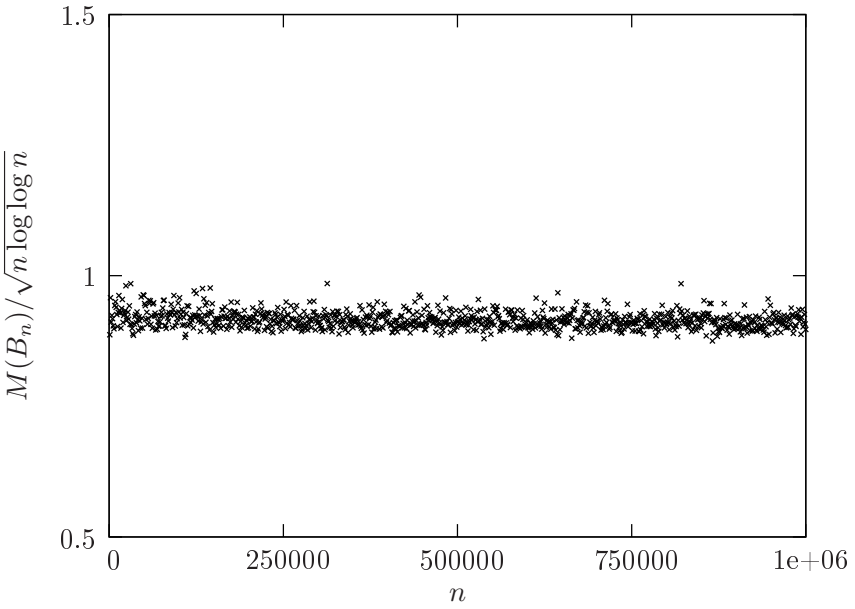

FIGURE 1. The peak sidelobe level of B_n compared to $\sqrt{n \log\log n}$.

for all $x_0, \ldots, x_{r-2} \in \{-1, 1\}$. Suppose $c_{u,r-1}(b_0, \ldots, b_{r-2})$ and $s_{u,r-1}(b_0, \ldots, b_{r-2})$ have been already computed for $u \in \{1, 2, \ldots, r-1\}$. Then, using

$$\cosh(y+z) = \cosh(z)\cosh(y) + \sinh(z)\sinh(y)$$
$$\sinh(y+z) = \cosh(z)\sinh(y) + \sinh(z)\cosh(y)$$

and the fact that cosh is an even function and sinh is an odd function, we have for $u \in \{1, 2, \ldots, r-1\}$,

$$c_{u,r}(b_0, \ldots, b_{r-1}) = \alpha\, c_{u,r-1}(b_0, \ldots, b_{r-2}) + \beta\, b_{r-u-1} b_{r-1}\, s_{u,r-1}(b_0, \ldots, b_{r-2})$$
$$s_{u,r}(b_0, \ldots, b_{r-1}) = \alpha\, s_{u,r-1}(b_0, \ldots, b_{r-2}) + \beta\, b_{r-u-1} b_{r-1}\, c_{u,r-1}(b_0, \ldots, b_{r-2}),$$

where $\alpha = \cosh\theta$ and $\beta = \sinh\theta$. Hence, except for determining α and β, no values of cosh or sinh have to be computed, and Construction 3 can be implemented with $O(n^2)$ additions and $O(n^2)$ multiplications.

4. A Conjecture

For the binary sequence B_n of length n obtained under Construction 3, we have computed $M(B_n)$ for $n \in \{1000, 2000, \ldots, 10^6\}$. The data suggest that $M(B_n)$ is much smaller than the upper bound given in Theorem 4. Figure 1 compares $M(B_n)$ with the function $\sqrt{n \log\log n}$ and lends evidence to the following conjecture.

Conjecture 5. *Let B_n be the binary sequence of length n obtained under Construction 3. Then there exist positive constants c_1 and c_2 such that, for all $n > 1$,*

$$c_1 \sqrt{n \log\log n} \le M(B_n) \le c_2 \sqrt{n \log\log n}.$$

Some examples for small n reveal that, if c_2 in Conjecture 5 exists, then c_2 must be strictly greater than 1. It is however conceivable that

$$\limsup_{n\to\infty} \frac{M(B_n)}{\sqrt{n \log\log n}} \leq 1.$$

The correctness of Conjecture 5 implies that the sequences B_n are exceptional in the sense that their peak sidelobe level grows strictly more slowly than that of most binary sequences, as given in Theorem 1. Although we cannot prove Conjecture 5, in the light of Figure 1, we believe that Construction 3 meets the challenge of finding binary sequences of arbitrary lengths with small peak sidelobe level.

References

1. N. Alon, S. Litsyn, and A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inf. Theory **56** (2010), no. 1, 545–554.
2. N. Alon and J. H. Spencer, *The probabilistic method*, 3rd ed., Wiley, 2008.
3. A. M. Boehmer, *Binary pulse compression codes*, IEEE Trans. Inf. Theory **IT-13** (1967), no. 2, 156–167.
4. M. N. Cohen, M. R. Fox, and J. M. Baden, *Minimum peak sidelobe pulse compression codes*, Record of the IEEE 1990 International Radar Conference, Arlington, VA, USA, IEEE, May 1990, pp. 633–638.
5. G. Coxson and J. Russo, *Efficient exhaustive search for optimal-peak-sidelobe binary codes*, IEEE Trans. Aerosp. Electron. Sys. **41** (2005), no. 1, 302–308.
6. D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Adv. Math. Commun. **1** (2007), no. 4, 461–475.
7. L. Ein-Dor, I. Kanter, and W. Kinzel, *Low autocorrelated multiphase sequences*, Phys. Rev. (E) **65** (2002), no. 2, 020102.1–020102.4.
8. S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge University Press, New York, NY, 2005.
9. J. Jedwab, *A survey of the merit factor problem for binary sequences*, Proc. of Sequences and Their Applications (SETA), Lecture Notes in Computer Science, vol. 3486, New York: Springer Verlag, 2005, pp. 30–55.
10. ———, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.
11. J. Jedwab and K. Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE Trans. Inf. Theory **52** (2006), no. 5, 2247–2254.
12. K. H. Leung and B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr., accepted (2011), doi:10.1007/s10623-010-9472-y.
13. I. D. Mercer, *Autocorrelations of random binary sequences*, Comb. Probab. Comput. **15** (2006), no. 5, 663–671.
14. J. W. Moon and L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), no. 12, 340–343.
15. C. J. Nunn and G. E. Coxson, *Best-known autocorrelation peak sidelobe levels for binary codes of length* 71 *to* 105, IEEE Trans. Aerosp. Electron. Sys. **44** (2008), no. 1, 392–395.
16. D. V. Sarwate, *An upper bound on the aperiodic autocorrelation function for a maximal-length sequence*, IEEE Trans. Inf. Theory **IT-30** (1984), no. 4, 685–687.
17. K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, submitted for publication (2011).

18. H. D. Schotten and H. D. Lüke, *On the search for low correlated binary sequences*, AEU – Int. J. Electron. Commun. **59** (2005), no. 2, 67–78.
19. R. Turyn, *Optimum codes study*, Tech. report, Sylvania Electronic Systems, January 1960, Final report, Contract AF19(604)-5473.
20. R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), no. 3, 394–399.
21. R. J. Turyn, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968.

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

E-mail address: kuschmidt@sfu.ca

The final copy-edited version is published in Adv. Math. 241, pp. 127-136, 2013.
(http://dx.doi.org/10.1016/j.aim.2013.03.015)

LITTLEWOOD POLYNOMIALS WITH SMALL L^4 NORM

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

Abstract

Littlewood asked how small the ratio $||f||_4/||f||_2$ (where $||\cdot||_\alpha$ denotes the L^α norm on the unit circle) can be for polynomials f having all coefficients in $\{1,-1\}$, as the degree tends to infinity. Since 1988, the least known asymptotic value of this ratio has been $\sqrt[4]{7/6}$, which was conjectured to be minimum. We disprove this conjecture by showing that there is a sequence of such polynomials, derived from the Fekete polynomials, for which the limit of this ratio is less than $\sqrt[4]{22/19}$.

1. Introduction

The L^α norm on the unit circle of polynomials having all coefficients in $\{1,-1\}$ (*Littlewood polynomials*) has attracted sustained interest over the last sixty years [36], [13], [33], [30], [26], [27], [34], [31], [2], [10]. For $1 \le \alpha < \infty$, the L^α norm of a polynomial $f \in \mathbb{C}[z]$ on the unit circle is

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

while $||f||_\infty$ is the supremum of $|f(z)|$ on the unit circle. The norms L^1, L^2, L^4, and L^∞ are of particular interest in analysis.

Littlewood was interested in how closely the ratio $||f||_\infty/||f||_2$ can approach 1 as $\deg(f) \to \infty$ for f in the set of polynomials now named after him [26]. Note that if f is a Littlewood polynomial, then $||f||_2^2$ is $\deg(f)+1$. In view of the monotonicity of L^α norms, Littlewood and subsequent researchers used $||f||_4/||f||_2$ as a lower bound for $||f||_\infty/||f||_2$. The L^4 norm is particularly suited to this purpose because it is easier to calculate than most other L^α norms. The L^4 norm is also of interest in the theory of communications, because $||f||_4^4$ equals the sum of squares of the aperiodic autocorrelations of the sequence formed from the coefficients of f [20, eqn. (4.1)],

Date: 17 June 2011 (revised 25 April 2013).

J. Jedwab and D.J. Katz are with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. K.-U. Schmidt was with Department of Mathematics, Simon Fraser University and is now with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: jed@sfu.ca, daniel_katz_2@sfu.ca, kaiuwe.schmidt@ovgu.de.

J. Jedwab is supported by NSERC.

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

[4, p. 122]; in this context one considers the *merit factor* $||f||_2^4/(||f||_4^4 - ||f||_2^4)$. We shall express merit factor results in terms of $||f||_4/||f||_2$.

If $||f||_4/||f||_2$ is bounded away from 1, then so is $||f||_\infty/||f||_2$, which would prove a modification of a conjecture due to Erdős [14], [13, Problem 22] asserting that there is some $c > 0$ such that $||f||_\infty/||f||_2 \geq 1 + c$ for all non-constant polynomials f whose coefficients have absolute value 1. It is known from Kahane's work that there is no such c [24], but the modified conjecture where f is restricted to be a Littlewood polynomial remains resistant [31].

Littlewood regarded calculations carried out by Swinnerton-Dyer as evidence that the ratio $||f||_4/||f||_2$ can be made arbitrarily close to 1 for Littlewood polynomials [26]. However, he could prove nothing stronger than that this ratio is asymptotically $\sqrt[4]{4/3}$ for the Rudin-Shapiro polynomials [27, Chapter III, Problem 19]. Høholdt and Jensen, building on studies due to Turyn and Golay [18], proved in 1988 that this ratio is asymptotically $\sqrt[4]{7/6}$ for a sequence of Littlewood polynomials derived from the Fekete polynomials [20]. Høholdt and Jensen conjectured that no further reduction in the asymptotic value of $||f||_4/||f||_2$ is possible for Littlewood polynomials. Although Golay conjectured, based on heuristic reasoning, that the minimum asymptotic ratio $||f||_4/||f||_2$ for Littlewood polynomials is approximately $\sqrt[4]{333/308}$ [17], he later cautioned that "the eventuality must be considered that no systematic synthesis will ever be found which will yield [a smaller asymptotic ratio than $\sqrt[4]{7/6}$]" [18].

Indeed, for more than twenty years $\sqrt[4]{7/6}$ has remained the smallest known asymptotic value of $||f||_4/||f||_2$ for a sequence of Littlewood polynomials f. We shall prove that this is not the minimum asymptotic value.

Theorem 1.1. *There is a sequence $h_1, h_2, \ldots$ of Littlewood polynomials with $\deg(h_n) \to \infty$ and $||h_n||_4/||h_n||_2 \to \sqrt[4]{c}$ as $n \to \infty$, where $c < 22/19$ is the smallest root of $27x^3 - 498x^2 + 1164x - 722$.*

To date, two principal methods have been used to calculate the L^4 norm of a sequence of polynomials [19]. The first is direct calculation, in the case that the polynomials are recursively defined [27]. The second, introduced by Høholdt and Jensen [20] and subsequently employed widely for its generality [22], [23], [5], [6], [4], [7], [35], [21], obtains $||f||_4$ from a Fourier interpolation of f. In this paper, we use a simpler method that also obtains the L^4 norm of truncations and periodic extensions of f. We apply this method to Littlewood polynomials derived from the Fekete polynomials, themselves the fascinating subject of many studies [15], [32], [28], [1], [11], [9], [7]. The possibility that these derived polynomials could have an asymptotic ratio $||f||_4/||f||_2$ smaller than $\sqrt[4]{7/6}$ was first recognized by Kirilusha and Narayanaswamy [25] in 1999. Borwein, Choi, and Jedwab subsequently used extensive numerical data to conjecture conditions under which the value $\sqrt[4]{c}$ in Theorem 1.1 could be attained asymptotically (giving a corresponding asymptotic merit factor $1/(c-1) > 6.34$) [8], but until now no explanation

has been given as to whether their conjecture might be correct, nor if so why.

2. The Asymptotic L^4 Norm of Generalized Fekete Polynomials

Henceforth, let p be an odd prime and let r and t be integers with $t \geq 0$. The *Fekete polynomial* of degree $p-1$ is $\sum_{j=0}^{p-1} (j\,|\,p) z^j$, where $(\cdot\,|\,p)$ is the Legendre symbol. We define the *generalized Fekete polynomial*

$$f_p^{(r,t)}(z) = \sum_{j=0}^{t-1} (j+r\,|\,p) z^j.$$

The polynomial $f_p^{(r,t)}$ is formed from the Fekete polynomial of degree $p-1$ by cyclically permuting the coefficients through r positions, and then truncating when $t < p$ or periodically extending when $t > p$. We wish to determine the asymptotic behavior of the L^4 norm of the generalized Fekete polynomials for all r, t.

Since the Legendre symbol is a multiplicative character, we can use

$$||f||_4^4 = \frac{1}{2\pi} \int_0^{2\pi} \left[f(e^{i\theta}) \overline{f(e^{i\theta})} \right]^2 d\theta$$

to obtain

$$||f_p^{(r,t)}||_4^4 = \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} ((j_1+r)(j_2+r)(j_3+r)(j_4+r)\,|\,p). \tag{1}$$

Until now, the asymptotic evaluation of (1) has been considered intractable because, when t is not a multiple of p, the expression (1) is an incomplete character sum whose indices are subject to an additional constraint. We shall overcome this apparent difficulty by using the Fourier expansion of the multiplicative character $(j\,|\,p)$ in terms of additive characters of $\mathbb{F}_p$, with Gauss sums playing the part of Fourier coefficients. This expansion introduces complete character sums over $\mathbb{F}_p$ which, once computed, allow an easy asymptotic evaluation of (1). This method is considerably simpler and more general than the Fourier interpolation method of [20].

Theorem 2.1. *Let $r/p \to R < \infty$ and $t/p \to T < \infty$ as $p \to \infty$. Then*

$$\frac{||f_p^{(r,t)}||_4^4}{p^2} \to -\frac{4T^3}{3} + 2\sum_{n \in \mathbb{Z}} \max(0, T - |n|)^2 + \sum_{n \in \mathbb{Z}} \max(0, T - |T + 2R - n|)^2$$

as $p \to \infty$.

Proof. Let $\epsilon_j = e^{2\pi i j/p}$ for $j \in \mathbb{Z}$. Gauss [16], [3] showed that

$$\sum_{k \in \mathbb{F}_p} \epsilon_j^k (k\,|\,p) = i^{(p-1)^2/4} \sqrt{p}\,(j\,|\,p).$$

Substitution in (1) gives

$$||f_p^{(r,t)}||_4^4 = \frac{1}{p^2} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{k_1,k_2,k_3,k_4\in\mathbb{F}_p} \epsilon_{j_1+r}^{k_1}\epsilon_{j_2+r}^{k_2}\epsilon_{j_3+r}^{k_3}\epsilon_{j_4+r}^{k_4}(k_1k_2k_3k_4\,|\,p).$$

Re-index with $k_1 = x$, $k_2 = x-a$, $k_3 = b-x$, $k_4 = c-x$ to obtain

$$||f_p^{(r,t)}||_4^4 = \frac{1}{p^2} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{a,b,c\in\mathbb{F}_p} \epsilon_a^{-(j_2+r)}\epsilon_b^{j_3+r}\epsilon_c^{j_4+r} L(a,b,c), \qquad (2)$$

where

$$L(a,b,c) = \sum_{x\in\mathbb{F}_p} (x(x-a)(x-b)(x-c)\,|\,p).$$

A Weil-type bound on character sums [37], [29, Lemma 9.25], shows that $|L(a,b,c)| \le 3\sqrt{p}$ when $x(x-a)(x-b)(x-c)$ is not a square in $\mathbb{F}_p[x]$. This polynomial is a square in $\mathbb{F}_p[x]$ if and only if it either has two distinct double roots, in which case $L(a,b,c) = p-2$, or else has a quadruple root, in which case $L(a,b,c) = p-1$. We shall see that contributions from $L(a,b,c)$ much smaller than p will not influence the asymptotic value of the L^4 norm. Accordingly, we write $L(a,b,c) = M(a,b,c) + N(a,b,c)$, with a main term

$$M(a,b,c) = \begin{cases} p & \text{if } x(x-a)(x-b)(x-c) \text{ is a square in } \mathbb{F}_p[x], \\ 0 & \text{if } x(x-a)(x-b)(x-c) \text{ is not a square in } \mathbb{F}_p[x], \end{cases}$$

and an error term $N(a,b,c)$ satisfying

$$|N(a,b,c)| \le 3\sqrt{p}. \qquad (3)$$

There are three ways of pairing the roots of $x(x-a)(x-b)(x-c)$: (i) $a=c$ and $b=0$, (ii) $b=a$ and $c=0$, or (iii) $c=b$ and $a=0$. So $M(a,b,c)=p$ if at least one of these conditions is met, and vanishes otherwise. The only triple (a,b,c) that satisfies more than one of these conditions is $(0,0,0)$. We now reorganize (2) by writing $L(a,b,c)$ as $M(a,b,c)+N(a,b,c)$, and then break the sum involving $M(a,b,c)$ into four parts: three sums corresponding to the three pairings, and a fourth sum to correct for the triple counting of $(a,b,c)=(0,0,0)$. We keep the sum over $N(a,b,c)$ entire, and thus have

$$||f_p^{(r,t)}||_4^4 = A + B + C + D + E, \qquad (4)$$

where

$$\begin{aligned}
A &= \frac{1}{p} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{a\in\mathbb{F}_p} \epsilon_a^{j_4-j_2}, \\
B &= \frac{1}{p} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{b\in\mathbb{F}_p} \epsilon_b^{j_3-j_2}, \\
C &= \frac{1}{p} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{c\in\mathbb{F}_p} \epsilon_c^{j_3+j_4+2r}, \\
D &= -\frac{2}{p} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} 1, \\
E &= \frac{1}{p^2} \sum_{a,b,c\in\mathbb{F}_p} N(a,b,c)\epsilon^r_{-a+b+c} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \epsilon_a^{-j_2}\epsilon_b^{j_3}\epsilon_c^{j_4}.
\end{aligned}$$

Note that $A = B$, and that A counts the quadruples (j_1, j_2, j_3, j_4) of integers in $[0, t)$ with $j_1 + j_2 = j_3 + j_4$ and $j_4 \equiv j_2 \pmod p$, or equivalently, with $j_4 - j_2 = np$ and $j_3 - j_1 = -np$ for some $n \in \mathbb{Z}$. For each $n \in \mathbb{Z}$ there are $\max(0, t - |n|p)$ ways to obtain $j_4 - j_2 = np$ and the same number of ways to obtain $j_3 - j_1 = -np$. Therefore $A = B = \sum_{n\in\mathbb{Z}} \max(0, t - |n|p)^2$. This is a locally finite sum of continuous functions, and since $t/p \to T$ as $p \to \infty$ we have

$$\frac{A}{p^2} + \frac{B}{p^2} \to 2\sum_{n\in\mathbb{Z}} \max(0, T - |n|)^2.$$

The summation in D counts the quadruples (j_1, j_2, j_3, j_4) of integers in $[0, t)$ with $j_1 + j_2 = j_3 + j_4$. For each $n \in \mathbb{Z}$ there are $\max(0, t - |t - 1 - n|)$ ways to represent n as $j_1 + j_2$ with $j_1, j_2 \in [0, t)$, and so

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

Thus $D = -\frac{2t(2t^2+1)}{3p}$, and since $t/p \to T$ as $p \to \infty$ we get $D/p^2 \to -4T^3/3$.

Similarly, C counts the quadruples (j_1, j_2, j_3, j_4) of integers in $[0, t)$ with $j_1 + j_2 = j_3 + j_4 = -2r + np$ for some $n \in \mathbb{Z}$. Replacing n by $-2r + np$ in the above argument for D, we find that

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

This is a locally finite sum of continuous functions $\psi_n(x, y) = \max(0, x - |y - n|)^2$ evaluated at $x = t/p$ and $y = (t - 1 + 2r)/p$. Since $r/p \to R$ and

$t/p \to T$ as $p \to \infty$, it follows that

$$\frac{C}{p^2} \to \sum_{n \in \mathbb{Z}} \max(0, T - |T + 2R - n|)^2.$$

By (4), it remains to show that $|E|/p^2 \to 0$ as $p \to \infty$. Use (3) to bound $|N(a,b,c)|$, and then use Lemma 2.2 below to bound the resulting outer sum over a, b, c to give $|E|/p^2 \le 192 p^{-7/2} \max(p,t)^3 (1 + \log p)^3$. Since $t/p \to T < \infty$ as $p \to \infty$, we then obtain $E/p^2 \to 0$ as required. □

We now prove the technical result invoked in the proof of Theorem 2.1.

Lemma 2.2. *Let n be a positive integer and $\epsilon_j = e^{2\pi i j/n}$ for $j \in \mathbb{Z}$. Then*

$$\sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4} \right| \le 64 \max(n,t)^3 (1 + \log n)^3.$$

Proof. Let G be the entire sum. Re-index with $k = -a$, $\ell = c - b$, $m = b$, to obtain

$$G = \sum_{k,\ell,m \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \epsilon_k^{j_2} \epsilon_\ell^{j_4} \epsilon_m^{j_3 + j_4} \right|.$$

Re-index the inner sum with $h = j_3 + j_4$, separating into ranges $h \le t - 1$ and $h \ge t$, so that $G \le H + J$, where

$$H = \sum_{k,\ell,m \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{h=0}^{t-1} \epsilon_m^h \sum_{j_2, j_4 = 0}^{h} \epsilon_k^{j_2} \epsilon_\ell^{j_4} \right|,$$

$$J = \sum_{k,\ell,m \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{h=t}^{2t-2} \epsilon_m^h \sum_{j_2, j_4 = h-(t-1)}^{t-1} \epsilon_k^{j_2} \epsilon_\ell^{j_4} \right|.$$

We shall show that $H \le 32 \max(n,t)^3 (1 + \log n)^3$, from which we can deduce the same bound on J after re-indexing with $h' = 2(t-1) - h$, $j_2' = j_2 + h' - (t-1)$, $j_4' = j_4 + h' - (t-1)$, and $m' = -(k + \ell + m)$.

Partition the sum H into a sum with $k, \ell \ne 0$, two sums where one of k, ℓ is zero and the other is nonzero, and a sum where $k = \ell = 0$; then sum over

the indices j_2 and j_4 to obtain $H = H_1 + 2H_2 + H_3$, where

$$\begin{aligned} H_1 &= \sum_{\substack{k,\ell,m\in\mathbb{Z}/n\mathbb{Z}\\ k,\ell\neq 0}} \left| \sum_{h=0}^{t-1} \frac{\epsilon_m^h - \epsilon_k\epsilon_{m+k}^h - \epsilon_\ell\epsilon_{m+\ell}^h + \epsilon_{k+\ell}\epsilon_{m+k+\ell}^h}{(1-\epsilon_k)(1-\epsilon_\ell)} \right|, \\ H_2 &= \sum_{\substack{k,m\in\mathbb{Z}/n\mathbb{Z}\\ k\neq 0}} \left| \sum_{h=0}^{t-1} \frac{(h+1)\left(\epsilon_m^h - \epsilon_k\epsilon_{m+k}^h\right)}{1-\epsilon_k} \right|, \\ H_3 &= \sum_{m\in\mathbb{Z}/n\mathbb{Z}} \left| \sum_{h=0}^{t-1} (h+1)^2\epsilon_m^h \right|, \end{aligned} \tag{5}$$

To bound these sums, we prove by induction on $d \geq 0$ that for $s \geq 0$,

$$\sum_{\substack{j\in\mathbb{Z}/n\mathbb{Z}\\ j\neq 0}} \left| \sum_{h=0}^{s-1} (h+1)^d\epsilon_j^h \right| \leq 2^{d+1}s^d n\log n. \tag{6}$$

The base case follows from $\left|\sum_{h=0}^{s-1}\epsilon_j^h\right| \leq 2/|1-\epsilon_j|$ and the bound [12, p. 136]

$$\sum_{j=1}^{n-1} \frac{1}{|1-\epsilon_j|} \leq n\log n. \tag{7}$$

For the inductive step, apply the triangle inequality to the identity

$$\sum_{h=0}^{s-1}(h+1)^d\epsilon_j^h = \sum_{g=0}^{s-1}\sum_{h=0}^{s-1}(h+1)^{d-1}\epsilon_j^h - \sum_{g=0}^{s-1}\sum_{h=0}^{g-1}(h+1)^{d-1}\epsilon_j^h,$$

to obtain a bound for the left hand side as the sum of the magnitudes of $2s$ summations over h involving $(h+1)^{d-1}\epsilon_j^h$, then sum over $j \neq 0$ and use the inductive hypothesis.

Now from (6) we find

$$\sum_{j\in\mathbb{Z}/n\mathbb{Z}} \left| \sum_{h=0}^{t-1} (h+1)^d\epsilon_j^h \right| \leq t^{d+1} + 2^{d+1}t^d n\log n, \tag{8}$$

since $\sum_{h=0}^{t-1}(h+1)^d \leq t^{d+1}$. Apply the triangle inequality, (7), and (8) to the expressions (5) to obtain $H_1 \leq 4(t+2n\log n)(n\log n)^2$, $H_2 \leq 2(t^2 + 4tn\log n)n\log n$, and $H_3 \leq t^3 + 8t^2 n\log n$. Therefore $H = H_1 + 2H_2 + H_3 \leq 32\max(n,t)^3(1+\log n)^3$, as required. □

3. Littlewood Polynomials with Small L^4 Norm

The generalized Fekete polynomial $f_p^{(r,t)}$ is not necessarily a Littlewood polynomial, because its coefficient of z^j is 0 for $0 \leq j < t$ and $j + r \equiv 0$

(mod p). Replace each such zero coefficient of $f_p^{(r,t)}$ with 1 to define a family of Littlewood polynomials

$$g_p^{(r,t)}(z) = f_p^{(r,t)}(z) \ + \sum_{\substack{0 \le j < t \\ j+r \equiv 0 \,(\mathrm{mod}\ p)}} z^j. \tag{9}$$

We now show that the asymptotic L^4 norm of $g_p^{(r,t)}$ as $p \to \infty$ behaves in the same way as that of $f_p^{(r,t)}$.

Corollary 3.1. *Let $r/p \to R < \infty$ and $t/p \to T < \infty$ as $p \to \infty$. Then*

$$\frac{||g_p^{(r,t)}||_4^4}{p^2} \to -\frac{4T^3}{3} + 2\sum_{n \in \mathbb{Z}} \max(0, T - |n|)^2 + \sum_{n \in \mathbb{Z}} \max(0, T - |T + 2R - n|)^2.$$

as $p \to \infty$.

Proof. Write $f = f_p^{(r,t)}$ and $g = g_p^{(r,t)}$ and $v = \lceil t/p \rceil$. Since the L^4 norm of each z^j in (9) is 1, the triangle inequality for the L^4 norm gives

$$\frac{1}{p^2}\Big|\,||g||_4^4 - ||f||_4^4\Big| \le \frac{1}{p^2}\left(4v||f||_4^3 + 6v^2||f||_4^2 + 4v^3||f||_4 + v^4\right).$$

The limit as $p \to \infty$ of the right hand side is 0, because $||f||_4/\sqrt{p}$ has a finite limit by Theorem 2.1 and because $v/\sqrt{p} \to 0$ follows from $t/p \to T < \infty$. □

The specialization of Corollary 3.1 to $T = 1$ and $|R| \le 1/2$ recovers the result due to Høholdt and Jensen [20] that the asymptotic ratio $||g_p^{(r,p)}||_4/||g_p^{(r,p)}||_2$ is $\sqrt[4]{7/6 + 8(|R| - 1/4)^2}$ (which achieves its minimum value of $\sqrt[4]{7/6}$ at $R = \pm 1/4$). The specialization of Corollary 3.1 to $T \in (0, 1]$ proves the conjecture of Borwein, Choi, and Jedwab [8, Conjecture 7.5] mentioned at the end of the Introduction. The authors of [8] gave a proof that, subject to the truth of their conjecture, Theorem 1.1 holds. In fact, Theorem 1.1 follows from Corollary 3.1 directly. We now show this, and demonstrate that the asymptotic ratio $||g_p^{(r,t)}||_4/||g_p^{(r,t)}||_2$ for $T > 0$ and arbitrary R cannot be made less than the value $\sqrt[4]{c}$ given in Theorem 1.1.

Corollary 3.2. *If $r/p \to R < \infty$ and $t/p \to T \in (0, \infty)$ as $p \to \infty$ then*

$$\lim_{p \to \infty} \frac{||g_p^{(r,t)}||_4}{||g_p^{(r,t)}||_2} \ge \sqrt[4]{c},$$

where $c < 22/19$ is the smallest root of $27x^3 - 498x^2 + 1164x - 722$, with equality if and only if T is the middle root T_0 of $4x^3 - 30x + 27$ and $R = \frac{1}{4}(3 - 2T_0) + \frac{n}{2}$ for some integer n. If $t/p \to \infty$ as $p \to \infty$, then $||g_p^{(r,t)}||_4/||g_p^{(r,t)}||_2 \to \infty$ as $p \to \infty$.

Proof. Recall that $||f||_2^2 = t$ for a Littlewood polynomial f of degree $t-1$. In the case $t/p \to \infty$, the required result is an easy consequence of Lemma 3.3 below. This leaves the case where $r/p \to R < \infty$ and $t/p \to T \in (0, \infty)$ as $p \to \infty$. We have already noted that when $R = 1/4$ and $T = 1$, the

asymptotic ratio $||g_p^{(r,t)}||_4^4/||g_p^{(r,t)}||_2^4$ is 7/6. If $t/p > 3/2$, we know from Lemma 3.3 that $||g_p^{(r,t)}||_4^4/||g_p^{(r,t)}||_2^4 \geq 1 + 2(1-p/t)^2 > 11/9 > 7/6$, and so we may assume $T \leq 3/2$.

By Corollary 3.1, $\lim_{p\to\infty} ||g_p^{(r,t)}||_4^4/||g_p^{(r,t)}||_2^4$ is

$$\frac{1}{T^2}\left[-\frac{4T^3}{3} + 2\sum_{n\in\mathbb{Z}} \max(0, T-|n|)^2 + \sum_{n\in\mathbb{Z}} \max(0, T-|T+2R-n|)^2\right].$$

Call this function $u(R,T)$ and note that it is always at least $-\frac{4T}{3}+2$, so that $u(R,T) > 4/3$ if $T < 1/2$. By combination with the previous bound on T, we may assume $T \in [1/2,\, 3/2]$. Furthermore, $u(R,T)$ does not change when R is replaced by $R+1/2$, so it is sufficient to consider points (R,T) in the set $D = [0,\, 1/2] \times [1/2,\, 3/2]$. We cover D with six compact sets:

$$\begin{aligned}
D_1 &= \{(R,T) \in D : T + 2R \leq 1\},\\
D_2 &= \{(R,T) \in D : 1 \leq T + 2R,\ T + R \leq 1\},\\
D_3 &= \{(R,T) \in D : 1 \leq T + R,\ T \leq 1\},\\
D_4 &= \{(R,T) \in D : 1 \leq T,\ T + R \leq 3/2\},\\
D_5 &= \{(R,T) \in D : 3/2 \leq T + R,\ T + 2R \leq 2\},\\
D_6 &= \{(R,T) \in D : 2 \leq T + 2R\}.
\end{aligned}$$

These sets are chosen so that the restriction of $u(R,T)$ to D_k is a continuous rational function $u_k(R,T)$, and so $u(R,T)$ attains a minimum value on each D_k. For example,

$$u_4(R,T) = -\frac{4T}{3} + 2 + 4\frac{(T-1)^2}{T^2} + \frac{(1-2R)^2}{T^2} + \frac{(2T+2R-2)^2}{T^2}.$$

For each T, the function $u_4(R,T)$ is minimized when $R = (3-2T)/4$, and $u_4(\frac{1}{4}(3-2T), T) = \frac{1}{6T^2}(-8T^3 + 48T^2 - 60T + 27)$ is minimized on D_4 when T is the middle root T_0 of $4x^3 - 30x + 27$. Let $R_0 = (3-2T_0)/4$. The point (R_0, T_0) lies in the interior of D_4. One can show that $u_4(R_0,T_0)$ is the smallest root c of $27x^3 - 498x^2 + 1164x - 722$, and that $c < 22/19$.

Following the same method, the minimum value of $u_3(R,T)$ on D_3 is 7/6, attained at $(1/4, 1)$. Partial differentiation with respect to R shows that the minimum of $u_2(R,T)$ on D_2 lies on the boundary with D_3, and that the minimum of $u_5(R,T)$ on D_5 lies on the boundary with D_4. The involution $(R,T) \mapsto (1-R-T, T)$ maps D_1 onto D_2 while preserving the value of $u(R,T)$; likewise with $(R,T) \mapsto (2-R-T, T)$ for D_6 and D_5. Therefore the unique global minimum of $u(R,T)$ on D is c, attained at (R_0, T_0). □

We close by proving the bound on $||f||_4^4$ used in the proof of Corollary 3.2.

Lemma 3.3. *Let m be a positive integer, and let $f(z) = \sum_{j=0}^{t-1} f_j z^j$ be a Littlewood polynomial for which $f_j = f_k$ whenever $j \equiv k \pmod m$. Then*

$$||f||_4^4 \geq \sum_{n\in\mathbb{Z}} \max(0, t-|n|m)^2.$$

Proof. Note that $\overline{f(z)} = f(z^{-1})$ for z on the unit circle. By treating $f(z)$ and $f(z^{-1})$ as formal elements of $\mathbb{C}[z, z^{-1}]$, it is straightforward to show that $||f||_4^4$ is the sum of the squares of the coefficients of $f(z)f(z^{-1})$. For each $n \in \mathbb{Z}$, the coefficient of z^{nm} in $f(z)f(z^{-1})$ is

$$\sum_{\substack{0 \le j,k < t \\ j-k=nm}} f_j f_k.$$

By the periodicity of the coefficients of f, this equals the number of pairs of integers (j, k) in $[0, t)$ with $j - k = nm$, which is $\max(0, t - |n|m)$. Sum the square of this over $n \in \mathbb{Z}$ to obtain the desired bound. □

References

[1] R. C. Baker and H. L. Montgomery. Oscillations of quadratic L-functions. *Progr. Math.*, 85:23–40, 1990.

[2] J. Beck. Flat polynomials on the unit circle—note on a problem of Littlewood. *Bull. London Math. Soc.*, 23(3):269–277, 1991.

[3] B. C. Berndt and R. J. Evans. The determination of Gauss sums. *Bull. Amer. Math. Soc. (N.S.)*, 5(2):107–129, 1981.

[4] P. Borwein. *Computational Excursions in Analysis and Number Theory*. Springer-Verlag, New York, 2002.

[5] P. Borwein and K.-K. S. Choi. Merit factors of character polynomials. *J. London Math. Soc. (2)*, 61(3):706–720, 2000.

[6] P. Borwein and K.-K. S. Choi. Merit factors of polynomials formed by Jacobi symbols. *Canad. J. Math.*, 53(1):33–50, 2001.

[7] P. Borwein and K.-K. S. Choi. Explicit merit factor formulae for Fekete and Turyn polynomials. *Trans. Amer. Math. Soc.*, 354(1):219–234, 2002.

[8] P. Borwein, K.-K. S. Choi, and J. Jedwab. Binary sequences with merit factor greater than 6.34. *IEEE Trans. Inform. Theory*, 50(12):3234–3249, 2004.

[9] P. Borwein, K.-K. S. Choi, and S. Yazdani. An extremal property of Fekete polynomials. *Proc. Amer. Math. Soc.*, 129(1):19–27, 2001.

[10] P. Borwein and R. Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, 129(5):1463–1472, 2001.

[11] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan. Zeros of Fekete polynomials. *Ann. Inst. Fourier (Grenoble)*, 50(3):865–889, 2000.

[12] H. Davenport, revised by H. L. Montgomery. *Multiplicative Number Theory*. Springer-Verlag, New York, third edition, 2000.

[13] P. Erdős. Some unsolved problems. *Michigan Math. J.*, 4:291–300, 1957.

[14] P. Erdős. An inequality for the maximum of trigonometric polynomials. *Ann. Polon. Math.*, 12:151–154, 1962.

[15] M. Fekete and G. Pólya. Über ein Problem von Laguerre. *Rend. Circ. Mat. Palermo*, 34(1):89–120, 1912.

[16] C. F. Gauss. Summatio quarumdam serierum singularium. *Comment. Soc. Reg. Sci. Gottingensis*, 1, 1811.

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

[18] M. J. E. Golay. The merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, 29(6):934–936, 1983.

[19] T. Høholdt. The merit factor problem for binary sequences. *Lecture Notes in Comput. Sci.*, 3857:51–59, 2006.

[20] T. Høholdt and H. E. Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, 34(1):161–164, 1988.
[21] J. Jedwab and K.-U. Schmidt. The merit factor of binary sequence families constructed from m-sequences. *Contemp. Math.*, 518:265–278, 2010.
[22] H. E. Jensen and T. Høholdt. Binary sequences with good correlation properties. *Lecture Notes in Comput. Sci.*, 356:306–320, 1989.
[23] J. M. Jensen, H. E. Jensen, and T. Høholdt. The merit factor of binary sequences related to difference sets. *IEEE Trans. Inform. Theory*, 37(3, part 1):617–626, 1991.
[24] J.-P. Kahane. Sur les polynômes à coefficients unimodulaires. *Bull. London Math. Soc.*, 12(5):321–342, 1980.
[25] A. Kirilusha and G. Narayanaswamy. Construction of new asymptotic classes of binary sequences based on existing asymptotic classes. Summer Science Program Tech. Rep., Dept. Math. Comput. Sci., Univ. Richmond, VA, 1999.
[26] J. E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$. *J. London Math. Soc.*, 41:367–376, 1966.
[27] J. E. Littlewood. *Some Problems in Real and Complex Analysis*. D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
[28] H. L. Montgomery. An exponential polynomial formed with the Legendre symbol. *Acta Arith.*, 37:375–380, 1980.
[29] H. L. Montgomery and R. C. Vaughan. *Multiplicative Number Theory: I. Classical Theory*. Cambridge University Press, Cambridge, 2007.
[30] D. J. Newman. Norms of polynomials. *Amer. Math. Monthly*, 67:778–779, 1960.
[31] D. J. Newman and J. S. Byrnes. The L^4 norm of a polynomial with coefficients ± 1. *Amer. Math. Monthly*, 97(1):42–45, 1990.
[32] G. Pólya. Verschiedene Bemerkungen zur Zahlentheorie. *Jahresber. Dtsch. Math.-Ver.*, 28:31–40, 1919.
[33] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.
[34] D. V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proc., Part F*, 131(2):101–106, 1984.
[35] K.-U. Schmidt, J. Jedwab, and M. G. Parker. Two binary sequence families with large merit factor. *Adv. Math. Commun.*, 3(2):135–156, 2009.
[36] H. S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, Massachusetts Institute of Technology, Cambridge, 1951.
[37] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.

The final copy-edited version is published in J. Combin. Theory Ser. A 120(4), pp. 882-906, 2013.
(http://dx.doi.org/10.1016/j.jcta.2013.01.010)

ADVANCES IN THE MERIT FACTOR PROBLEM FOR BINARY SEQUENCES

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

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

1. Introduction

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

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

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

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

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

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

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

J. Jedwab is supported by NSERC.

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Results

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

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

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

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

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

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

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

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

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

and the coefficient sequence of

$$X_p(z) = 1 + \sum_{j=1}^{p-1} \left(j \,\middle|\, p\right) z^j \tag{2.1}$$

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

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

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

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

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

(i) If $r/p \to R$ and $t/p \to T$, then $F(X_p^{r,t}) \to g(R,T)$.

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

(iii) If $r/(4p) \to R$ and $t/(4p) \to T$, then $F(P(X_p)^{r,t}) \to g(R,T)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) If $t/n \to T$, then $F(Y_{n,\theta}^{r,t}) \to h(T)$.

(ii) If $t/(2n) \to T$, then $F(N(Y_{n,\theta})^{r,t}) \to h(T)$.

(iii) If $t/(4n) \to T$, then $F(P(Y_{n,\theta})^{r,t}) \to h(T)$.

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

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

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

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

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

and

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

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

$$T_a - 1 = 0.057827\ldots$$

and

$$\tfrac{1}{2}(T_b - 1) = 0.057874\ldots$$

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

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

$$X_n(z) = \sum_{j=0}^{n-1} \left(j \,\Big|\, \tfrac{n}{\gcd(j,n)}\right) z^j$$

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

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

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

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

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

(i) If $r/n \to R$ and $t/n \to T$, then $F(X_n^{r,t}) \to g(R,T)$.

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

(iii) If $r/(4n) \to R$ and $t/(4n) \to T$, then $F(P(X_n)^{r,t}) \to g(R,T)$.

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

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

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

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

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

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

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

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

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

3. Relationship to Previous Results

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

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

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

$$\frac{1}{g(R,1)} = \tfrac{1}{6} + 8\big(R - \tfrac{1}{4}\big)^2 \quad \text{for } 0 \le R \le \tfrac{1}{2},$$

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

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

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

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

4. Asymptotic Merit Factor Calculation

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

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

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

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

and

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

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

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

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

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

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

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

(i) If $r/n \to R$ and $t/n \to T$, then $F(V_n^{r,t}) \to g(R,T)$.

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

(iii) If each n is odd, $r/(4n) \to R$, and $t/(4n) \to T$, then $F(P(V_n)^{r,t}) \to g(R,T)$.

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

parts, U_n can written in polynomial form as

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

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

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

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

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

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

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

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

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

where

$$A = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \epsilon_a^{j_4 - j_2},$$

$$B = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{b \in \mathbb{Z}/n\mathbb{Z}} \epsilon_b^{j_3 - j_2},$$

$$C = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{c \in \mathbb{Z}/n\mathbb{Z}} \epsilon_c^{j_3 + j_4 + 2r},$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Likewise,

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

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

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

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

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

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

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

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

and

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

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

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

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

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

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

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

(i) If $t/n \to T$, then $F(V_n^{r,t}) \to h(T)$.

(ii) If each n is odd and $t/(2n) \to T$, then $F(N(V_n)^{r,t}) \to h(T)$.

(iii) If each n is odd and $t/(4n) \to T$, then $F(P(V_n)^{r,t}) \to h(T)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$G_1 = \sum_{\substack{a,b,c \in \mathbb{Z}/n\mathbb{Z} \\ b,c \neq 0}} \left| \sum_{v \in V} \frac{\epsilon_a^v (\epsilon_b^{jv-w} - \epsilon_b^{x+1+kv})(\epsilon_c^{\ell v - y} - \epsilon_c^{z+1+mv})}{(1 - \epsilon_b)(1 - \epsilon_c)} \right|,$$

$$G_2 = \sum_{\substack{a,b \in \mathbb{Z}/n\mathbb{Z} \\ b \neq 0}} \left| \sum_{v \in V} \big((y + z + 1) + (m - \ell)v\big) \frac{\epsilon_a^v (\epsilon_b^{jv-w} - \epsilon_b^{x+1+kv})}{1 - \epsilon_b} \right|,$$

$$G_3 = \sum_{\substack{a,c \in \mathbb{Z}/n\mathbb{Z} \\ c \neq 0}} \left| \sum_{v \in V} \big((w + x + 1) + (k - j)v\big) \frac{\epsilon_a^v (\epsilon_c^{\ell v - y} - \epsilon_c^{z+1+mv})}{1 - \epsilon_c} \right|,$$

$$G_4 = \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{v \in V} \big((w + x + 1) + (k - j)v\big)\big((y + z + 1) - (m - \ell)v\big)\epsilon_a^v \right|.$$

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

$$G_1 \le \sum_{\substack{b,c,d \in \mathbb{Z}/n\mathbb{Z} \\ b,c \neq 0}} \frac{4}{|1 - \epsilon_b| \cdot |1 - \epsilon_c|} \left| \sum_{v \in V} \epsilon_d^v \right|,$$

$$G_2, G_3 \le \sum_{\substack{b,d \in \mathbb{Z}/n\mathbb{Z} \\ b \neq 0}} \frac{1}{|1 - \epsilon_b|} \left(4u \left| \sum_{v \in V} \epsilon_d^v \right| + 2 \left| \sum_{v \in V} v \epsilon_d^v \right| \right),$$

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

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

$$\sum_{\substack{a\in\mathbb{Z}/n\mathbb{Z}\\ a\ne 0}} \left| \sum_{v\in V} v^h \epsilon_a^v \right| \le 2u^h n \log n, \tag{4.11}$$

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

$$\sum_{a=1}^{n-1} \frac{1}{|1-\epsilon_a|} \le n \log n. \tag{4.12}$$

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

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

Apply the triangle inequality and the inductive hypothesis to obtain

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

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

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

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

$$\begin{aligned} G_1 &\le 4(n\log n)^2(u + 2n\log n) \\ G_2, G_3 &\le 4u(n\log n)(u+2n\log n) + 2n\log n(u^2 + 2un\log n) \\ G_4 &\le 2u^2(u+2n\log n) + 3u(u^2+2un\log n) + (u^3 + 2u^2 n\log n). \end{aligned}$$

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

5. Legendre and Galois sequences

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Jacobi sequences

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

plus an error term whose magnitude is bounded by

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

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

$$\frac{18(2^{\omega(n)} - 1)}{t^2 n\, \kappa(n)^{1/2}} \sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \zeta_n^{-aj_2}\, \zeta_n^{bj_3}\, \zeta_n^{cj_4} \right|. \tag{6.5}$$

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

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

where, for integral m and j,

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

Hence, (6.4) equals

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

By expanding the product, this expression can be written as

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

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

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

where

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

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

$$C = \frac{1}{t^2} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_n(j_3 + j_4 + 2r),$$

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

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

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

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

plus an error term whose magnitude is at most

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

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

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

Therefore each summand of the outer sum of D equals

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

plus an error term whose magnitude is at most

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

Hence D equals

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

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

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

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

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

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

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

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

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

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

where

$$A = \frac{1}{t^2} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \, \delta_n(j_4 - j_2),$$

$$B = \frac{1}{t^2} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \, \delta_n(j_3 - j_2),$$

$$C = \frac{1}{t^2} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \, \delta_n(j_3 + j_4 + 2r),$$

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

$$\times \delta_{P_1^{\times}}(j_4 - j_2) \delta_{P_2^{\times}}(j_3 - j_2) \delta_{P_3^{\times}}(j_3 + j_4 + 2r),$$

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

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

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

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

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

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

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

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

and let K be a translation of Λ. Then

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

if a, b, and c are odd, and

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

if a, b, and c are even.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Closing Comments

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

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

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

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

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

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

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

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

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

above together with the additional condition

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

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

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

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

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

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

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

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

$$\Big(\bigotimes_{p \in P} X_p \Big) \otimes \Big(\bigotimes_{n \in M} Y_{n,\theta} \Big) \tag{7.4}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

References

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

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

[3] B. C. Berndt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), 107–129.

[4] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 10, Springer-Verlag, New York, 2002.

[5] P. Borwein and K.-K. S. Choi, *Merit factors of character polynomials*, J. London Math. Soc. **61** (2000), 706–720.

[6] ———, *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math. **53** (2001), 33–50.

[7] ———, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), 219–234.

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

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

[10] H. Davenport, revised by H. L. Montgomery, *Multiplicative number theory*, third ed., Springer-Verlag, New York, 2000.

[11] P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.

[12] ———, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.

[13] C. F. Gauss, *Summatio quarumdam serierum singularium*, Comment. Soc. Reg. Sci. Gottingensis **1** (1811).

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

[15] ———, *Sieves for low autocorrelation binary sequences*, IEEE Trans. Inf. Theory **IT-23** (1977), 43–51.

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

[17] ———, *The merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **29** (1983), 934–936.

[18] K. G. Hare and S. Yazdani, *Fekete-like polynomials*, J. Number Theory **130** (2010), 2198–2213.

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

[19] T. Høholdt, *The merit factor problem for binary sequences*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 3857, Springer, Berlin, 2006, pp. 51–59.

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

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

[22] F. Huo, *Sequences design for OFDM and CDMA systems*, Master's thesis, University of Waterloo, 2011.

[23] J. Jedwab, *Generalized perfect arrays and Menon difference sets*, Des. Codes Cryptogr. **2** (1992), 19–68.

[24] J. Jedwab, *A survey of the merit factor problem for binary sequences*, Proc. of Sequences and Their Applications, Lecture Notes in Comput. Sci., vol. 3486, New York: Springer Verlag, 2005, pp. 30–55.

[25] J. Jedwab, *What can be used instead of a Barker sequence?*, Finite fields and applications, Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 2008, pp. 153–178.

[26] J. Jedwab, D. J. Katz, and K.-U. Schmidt, *Littlewood polynomials with small L^4 norm*, arXiv:1205.0260v1 [math.NT] (2011).

[27] J. Jedwab and K.-U. Schmidt, *Appended m-sequences with merit factor greater than* 3.34, Sequences and Their Applications (C. Carlet and A. Pott, eds.), Lecture Notes in Comput. Sci., vol. 6338, Springer, 2010, pp. 204–216.

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

[29] ———, *The L_4 norm of Littlewood polynomials derived from the Jacobi symbol*, Pac. J. Math. **257** (2012), 395–418.

[30] H. E. Jensen and T. Høholdt, *Binary sequences with good correlation properties*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 356, Springer, Berlin, 1989, pp. 306–320.

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

[32] E. C. Johnsen, *The inverse multiplier for abelian group difference sets*, Canad. J. Math. **16** (1964), 787–796.

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

[34] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), 171–188.

[35] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[36] J. E. Littlewood, *On polynomials* $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$, J. London Math. Soc. **41** (1966), 367–376.

[37] ———, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.

[38] H.D. Lüke, H.D. Schotten, and H. Hadinejad-Mahram, *Binary and quadriphase sequences with optimal autocorrelation properties: a survey*, IEEE Trans. Inform. Theory **49** (2003), 3271–3282.

[39] S. Mertens, *Ground states of the Bernasconi model with open boundary conditions*, http://www-e.uni-magdeburg.de/mertens/research/labs/open.dat, 2001.

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

[41] M. G. Parker, *Even length binary sequence families with low negaperiodic autocorrelation*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 200–209.

[42] M. G. Parker, *Univariate and multivariate merit factors*, Proc. of Sequences and Their Applications, Lecture Notes in Computer Science, vol. 3486, New York: Springer Verlag, 2005, pp. 72–100.

[43] A. Pott, *Two applications of relative difference sets: difference triangles and negaperiodic autocorrelation functions*, Discrete Math. **308** (2008), no. 13, 2854–2861.

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

[45] R. A. Scholtz and L. R. Welch, *GMW sequences*, IEEE Trans. Inf. Theory **30** (1984), 548–553.

[46] M. R. Schroeder, *Number theory in science and communication*, fifth ed., Springer-Verlag, Berlin, 2009.

[47] V. M. Sidel'nikov, *Some k-valued pseudo-random sequences and nearly equidistant codes*, Probl. Inf. Transm. **5** (1969), 12–16.

[48] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **34** (1948), 204–207. MR 0027006 (10,234e)

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

[50] T. Xiong and J. I. Hall, *Modifications on character sequences and construction of large even length binary sequences*, preprint (2010).

[51] ———, *Modifications of modified Jacobi sequences*, IEEE Trans. Inf. Theory **57** (2011), 493–504.

[52] N. Y. Yu and G. Gong, *The perfect binary sequence of period* 4 *for low periodic and aperiodic autocorrelations*, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 37–49.

The final copy-edited version is published in Pacific J. Math. 257(2), pp. 395-418, 2012.
(http://dx.doi.org/10.2140/pjm.2012.257.395)

THE L_4 NORM OF LITTLEWOOD POLYNOMIALS DERIVED FROM THE JACOBI SYMBOL

JONATHAN JEDWAB AND KAI-UWE SCHMIDT

Abstract. Littlewood raised the question of how slowly the L_4 norm $\|f\|_4$ of a Littlewood polynomial f (having all coefficients in $\{-1,+1\}$) of degree $n-1$ can grow with n. We consider such polynomials for odd square-free n, where $\phi(n)$ coefficients are determined by the Jacobi symbol, but the remaining coefficients can be freely chosen. When n is prime, these polynomials have the smallest published asymptotic value of the normalised L_4 norm $\|f\|_4/\|f\|_2$ among all Littlewood polynomials, namely $(7/6)^{1/4}$. When n is not prime, our results show that the normalised L_4 norm varies considerably according to the free choices of the coefficients and can even grow without bound. However, by suitably choosing these coefficients, the limit of the normalised L_4 norm can be made as small as the best published value $(7/6)^{1/4}$.

1. Introduction

For real $\alpha \geq 1$, the L_α norm of a polynomial $A \in \mathbb{C}[z]$ on the unit circle is given by

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

The polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$ is called a *Littlewood polynomial* if $a_j \in \{-1,+1\}$ for each j. In 1966, Littlewood [21, § 6] raised the question of how slowly the L_4 norm of a Littlewood polynomial of degree $n-1$ can grow with n. An equivalent question was posed by Turyn [29, p. 199] in a different context. Littlewood's question is closely related to other classical problems involving norms of Littlewood polynomials [24], [14], [22], [25], [3], [7].

For a polynomial $A \in \mathbb{C}[z]$, a small L_4 norm corresponds to a large *merit factor*, defined as

$$F(A) := \frac{\|A\|_2^4}{\|A\|_4^4 - \|A\|_2^4}$$

Date: 7 September 2010 (revised 4 August 2011 and 29 June 2012).

2010 *Mathematics Subject Classification.* Primary: 11B08, 11B83; Secondary: 94A55.

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. Email: jed@sfu.ca.

K.-U. Schmidt was with Department of Mathematics, Simon Fraser University and is now with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: kaiuwe.schmidt@ovgu.de.

J. Jedwab is supported by NSERC of Canada.

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

provided that the denominator is nonzero. This normalised measure appears natural since it often attains an integer value when the polynomial degree tends to infinity. Littlewood's question concerns the growth rate of $F(A)$ since $\|A\|_2^4 = n^2$ for every Littlewood polynomial of degree $n-1$. The determination of the largest possible merit factor of Littlewood polynomials of large degree is also of importance in the theory of communications, where Littlewood polynomials with large merit factor correspond to signals whose energy is very evenly distributed over frequency [4], and in theoretical physics, where Littlewood polynomials with largest merit factor correspond to the ground states of Bernasconi's Ising spin model [5].

If A is drawn uniformly from the set of Littlewood polynomials of degree $n-1$, then $F(A) \to 1$ in probability as $n \to \infty$ [12]. Littlewood [22] constructed a sequence of Littlewood polynomials with asymptotic merit factor 3. Since then Littlewood's question has been attacked by mathematicians, engineers, and physicists (see [19] for a survey of results and historical developments).

Given a polynomial $A \in \mathbb{C}[z]$ of degree $n-1$ and real r, define the *rotation* A_r of A by

$$A_r(z) := z^{-\lfloor nr \rfloor} A(z) \bmod (z^n - 1). \tag{1.1}$$

For odd n, let $(\cdot \,|\, n)$ be the Jacobi symbol (see [2], for example), and call

$$J(z) := \sum_{j=1}^{n-1} (j \,|\, n)\, z^j$$

the *character polynomial* of degree $n-1$. For prime n, this polynomial is known as the *Fekete polynomial*, which has been studied extensively and whose asymptotic merit factor has been determined for all rotations (see [23], [18], [13], [11], [9], for example). Indeed, defining

$$f(r) := \begin{cases} \dfrac{1}{\frac{1}{6} + 8\left(|r| - \frac{1}{4}\right)^2} & \text{for } -\frac{1}{2} < r \le \frac{1}{2} \\ f(r+1) & \text{otherwise,} \end{cases} \tag{1.2}$$

the following result is known.

Theorem 1.1 (Høholdt and Jensen [18])**.** *Let p take values in an infinite set of odd primes, and let r be real. Let $X = J + 1$, where J is the character polynomial of degree $p-1$. Then*

$$\lim_{p \to \infty} F(X_r) = f(r).$$

Borwein and Choi [9] also calculated the exact, rather than the asymptotic, values of $F(X)$ and $F(X_{1/4})$ by refining the proof of Theorem 1.1. The largest asymptotic merit factor occurring in Theorem 1.1 is 6. The polynomial X of degree $p-1$ in Theorem 1.1 has been used to construct Littlewood polynomials of degree $2p-1$ [30] and $4p-1$ [27] that also have asymptotic merit factor 6, and the value 6 remains the largest published asymptotic merit factor for all sequences of Littlewood polynomials. Høholdt and Jensen [18] conjectured that no larger value is possible, although there are various contradicting opinions [22, p. 29], [15],

[10]. In contrast, there are sequences of polynomials, not all of whose coefficients lie in $\{-1,+1\}$, for which the merit factor grows without bound as the degree increases [21, § 6].

In this paper we study the case when n is square-free but not prime. The character polynomial J of degree $n-1$ has $\phi(n)$ nonzero coefficients since $(j\,|\,n)=0$ exactly when $\gcd(j,n)>1$. Define

$$\mathcal{V}_n := \left\{ \sum_{j=0}^{n-1} v_j z^j : v_j \in \{0,-1,+1\} \text{ and } v_j = 0 \Leftrightarrow \gcd(j,n)=1 \right\}.$$

The polynomial $J+V$ is then a Littlewood polynomial for each $V \in \mathcal{V}_n$, and we call $J+V$ a *Littlewood completion* of J. We wish to determine the choice of $V \in \mathcal{V}_n$ for each n and the choice of r that maximise the asymptotic merit factor of $J_r + V_r$. In the case when n is prime, there are only two possible Littlewood completions of J, namely $J+1$ and $J-1$. Theorem 1.1 deals with $J+1$, and it is readily seen that the same result holds for $J-1$. However, for general n there are $2^{n-\phi(n)}$ possible Littlewood completions of J. The choice of the Littlewood completion and rotation that maximise the asymptotic merit factor is then by no means obvious and the analysis is considerably more difficult.

2. Results

Throughout this paper, we will use the following notation. For integer $n>1$, we define p_n to be the smallest prime factor of n and, as usual, $\omega(n)$ denotes the number of distinct prime factors of n.

As a starting point we establish the asymptotic merit factor of the character polynomial J itself at all rotations.

Theorem 2.1. *Let n take values only in an infinite set of odd square-free integers greater than 1, where*

$$\frac{(\log n)^3}{p_n} \to 0 \quad \text{as } n \to \infty, \tag{2.1}$$

and let r be real. Let J be the character polynomial of degree $n-1$. Then

$$\lim_{n\to\infty} F(J_r) = f(r).$$

We next examine the special Littlewood completion $J+V$ of J in which each nonzero coefficient of V is chosen to be $+1$.

Theorem 2.2. *Let n take values only in an infinite set of odd square-free integers greater than 1 and let r be real. Let J be the character polynomial of degree $n-1$ and define*

$$V(z) = \sum_{\substack{j=0 \\ \gcd(j,n)>1}}^{n-1} z^j.$$

Then

$$\liminf_{n\to\infty} \frac{1}{F(J_r+V_r)} \geq \liminf_{n\to\infty} \frac{1}{F(J_r)} + \liminf_{n\to\infty} \frac{n}{2p_n^3}. \tag{2.2}$$

Hence, if $p_n/n^{1/3}$ is bounded (which occurs for example if $\omega(n) \geq 3$ for all sufficiently large n), then

$$\limsup_{n\to\infty} F(J_r + V_r) < \limsup_{n\to\infty} F(J_r),$$

and if $p_n/n^{1/3} \to 0$ (which occurs for example if $\omega(n) \geq 4$ for all sufficiently large n), then

$$\lim_{n\to\infty} F(J_r + V_r) = 0.$$

Subject to the condition (2.1), we may replace $\liminf_{n\to\infty} 1/F(J_r)$ in Theorem 2.2 by $1/f(r)$. Theorem 2.2 therefore shows that the asymptotic merit factor of J_r+V_r can be strictly less than $f(r)$ for all r. This prompts the question of whether there is a choice of V for which the asymptotic merit factor of $J_r + V_r$ is *greater* than $f(r)$ for some r. However, we show that, subject to a mild condition on the growth rate of p_n relative to n, there is no such V.

Theorem 2.3. *Let n take values only in an infinite set of odd square-free integers greater than 1, where*

$$\frac{(\log n)^7}{p_n} \to 0 \quad \text{as } n \to \infty, \tag{2.3}$$

and let r be real. Let J be the character polynomial of degree $n-1$. Then

$$\limsup_{n\to\infty} \max_{V\in\mathcal{V}_n} F(J_r + V_r) \leq f(r).$$

We then ask whether the deterioration in asymptotic merit factor obtained in Theorem 2.2 for a specific choice of V is typical of Littlewood completions of J. We show it is not: subject to the same condition (2.3) as in Theorem 2.3, for almost all choices of V we have $F(J_r + V_r) \sim f(r)$.

Theorem 2.4. *Let n take values only in an infinite set of odd square-free integers greater than 1, where*

$$\frac{(\log n)^7}{p_n} \to 0 \quad \text{as } n \to \infty, \tag{2.4}$$

and let r be real. Let J be the character polynomial of degree $n-1$ and let V be drawn uniformly from $\mathcal{V}_n$. Then, as $n \to \infty$,

$$F(J_r + V_r) \to f(r) \quad \text{in probability.}$$

In view of Theorem 2.4, we wish to exhibit polynomials $V \in \mathcal{V}_n$ satisfying $\lim_{n\to\infty} F(J_r + V_r) = f(r)$ under suitable conditions on the growth rate of p_n relative to n. We present two such choices of polynomials V. The first choice is given in the following theorem.

Theorem 2.5. *Let n take values only in an infinite set of odd square-free integers greater than 1, where*

$$\frac{(\log n)^7}{p_n} \to 0 \quad \text{as } n \to \infty, \tag{2.5}$$

and let r be real. Let J be the character polynomial of degree $n-1$ and define

$$V(z) = \sum_{\substack{j=0 \\ \gcd(j,n)>1}}^{n-1} \left(j \mid \tfrac{n}{\gcd(j,n)}\right) z^j. \tag{2.6}$$

Then

$$\lim_{n\to\infty} F(J_r + V_r) = f(r).$$

The special case of Theorem 2.5 when $\omega(n) = 1$ for all n gives Theorem 1.1.

The second choice of polynomials $V \in \mathcal{V}_n$ satisfying $\lim_{n\to\infty} F(J_r + V_r) = f(r)$ uses a more restrictive condition than (2.5) in Theorem 2.5, but applies to *all* Littlewood completions.

Theorem 2.6. *Let n take values only in an infinite set of odd square-free integers greater than 1, where*

$$\frac{n^{1/3}}{p_n} \to 0 \quad \text{as } n \to \infty, \tag{2.7}$$

and let r be real. Let J be the character polynomial of degree $n-1$. Then

$$\lim_{n\to\infty} \max_{V\in\mathcal{V}_n} F(J_r + V_r) = \lim_{n\to\infty} \min_{V\in\mathcal{V}_n} F(J_r + V_r) = f(r).$$

The condition (2.7) is essentially the least restrictive condition under which Theorem 2.6 holds: for if $\liminf_{n\to\infty} n^{1/3}/p_n > 0$, then by Theorem 2.2 the conclusion of Theorem 2.6 fails for at least one Littlewood completion $J + V$; but otherwise $\liminf_{n\to\infty} n^{1/3}/p_n = 0$, and then the infinite set in which n takes values contains a subset satisfying the condition (2.7).

We shall prove Theorems 2.1 to 2.6 in Sections 4 to 9, respectively. Our results provide a comprehensive analysis of the $2^{n-\phi(n)}$ Littlewood completions of the character polynomial J of degree $n-1$, and significantly enlarge the set of explicitly defined sequences of Littlewood polynomials whose asymptotic merit factor equals the current best known value 6.

We close this section with a brief review of related work. Jensen, Jensen and Høholdt [20] gave the asymptotic merit factor of two Littlewood completions $J+V$ of J in the case that $\omega(n) = 2$ for all n. For one of these completions, the polynomial V coincides with (2.6); for the other, writing $n = pq$ for primes p, q satisfying $p > q$, the polynomial V is given by

$$V(z) = \sum_{j=0}^{p-1} z^{jq} - \sum_{j=1}^{q-1} z^{jp}.$$

The results of [20] for both of these Littlewood completions are special cases of Theorem 2.6. The authors of [20] also stated that the conclusion of Theorem 2.5 holds when $\omega(n)$ is fixed, but did not give a proof or specify conditions on the growth rate of p_n.

Motivated by the results of [20], Borwein and Choi [8] proved a result that gives the same conclusion as Theorem 2.1 under the more restrictive condition $n^\epsilon/p_n \to 0$ for some fixed $\epsilon > 0$. The authors of [8] remarked that

> "the merit factors [of the polynomials $J_{1/4}$ as $n \to \infty$] approach 6 which is conjectured by some to be best possible [16],"

and that their result

> "should be compared with the results of T. Høholdt, H. Jensen and J. Jensen in [20]. They showed that the same asymptotic formula but a weaker error term $O\Big(\frac{(p+q)^5 \log^4 N}{N^3}\Big)$ for the special case $N = pq$. So we generalize their result to $N = p_1 p_2 \dots p_r$ and also improve the error term."

However, the authors of [8] did not take into account the crucial distinction between the polynomial J of degree $n-1$ and its $2^{n-\phi(n)}$ Littlewood completions. Indeed, Theorem 2.2 shows that there is a sequence of Littlewood completions of J whose asymptotic merit factor at every rotation r drops to zero. Therefore the result of [8] cannot be considered a generalisation of the results of [20], and the comparison given in [8] with the conjecture of [16] (which applies only to Littlewood polynomials) is misplaced.

T. Xiong and J. I. Hall have kindly supplied us with two preprints of their recent independent work. In the first preprint, now published as [32], they obtain the same asymptotic form as in Theorem 2.6, subject to the more restrictive condition that $(n \log n)^{2/5}/p_n \to 0$. In the second preprint [31], they show that a previously unspecified Littlewood completion satisfies $\lim_{n\to\infty} F(J_r + V_r) = f(r)$ when $\omega(n)$ is fixed.

3. Preliminary Results

In this section we introduce some notation and give some auxiliary results. Throughout the paper, ζ_m denotes the primitive mth root of unity

$$\zeta_m := e^{2\pi i/m}.$$

We next derive some elementary bounds on the functions $\omega(n)$ and $\phi(n)$. The number of distinct prime factors $\omega(n)$ of n can be trivially bounded by

$$\omega(n) \le \log n \quad \text{for } n > 2 \text{ and } n \ne 6. \tag{3.1}$$

Since $\phi(n)/n = \prod_{p|n}(1 - 1/p)$, where the product is over the prime factors of n, the totient function $\phi(n)$ then satisfies

$$\begin{aligned} \frac{\phi(n)}{n} &\ge \left(1 - \frac{1}{p_n}\right)^{\omega(n)} \\ &\ge 1 - \frac{\omega(n)}{p_n} \\ &\ge 1 - \frac{\log n}{p_n} \quad \text{for } n > 2 \text{ and } n \ne 6, \end{aligned}$$

so we can estimate its growth rate as

$$\phi(n) = n\left(1 + O(p_n^{-1} \log n)\right) \quad \text{as } n \to \infty. \tag{3.2}$$

For convenience, we define the *cototient function* to be

$$\psi(n) := n - \phi(n).$$

It follows that

$$\frac{\psi(n)}{n} \le \frac{\omega(n)}{p_n} \tag{3.3}$$

$$\le \frac{\log n}{p_n} \quad \text{for } n > 2 \text{ and } n \ne 6 \tag{3.4}$$

and therefore

$$\psi(n) = O(p_n^{-1} n \log n) \quad \text{as } n \to \infty. \tag{3.5}$$

We shall need the following evaluation of Ramanujan's sum (see [17, Thm. 272], for example).

Lemma 3.1. *For integer u and positive square-free integer n, we have*

$$\sum_{\substack{j=0 \\ \gcd(j,n)=1}}^{n-1} \zeta_n^{ju} = \mu\left(\frac{n}{\gcd(u,n)}\right) \phi\big(\gcd(u,n)\big),$$

where μ is the Möbius function.

We also require the following evaluation of a Gauss sum involving the Jacobi symbol.

Lemma 3.2. *Let m be a positive odd square-free integer. Then for integer j,*

$$\sum_{\ell=0}^{m-1} (\ell \,|\, m)\, \zeta_m^{j\ell} = i^{(m-1)^2/4}\, (j \,|\, m)\, m^{1/2}.$$

The case $\gcd(j,m) = 1$ of Lemma 3.2 is given by Thm. 1.5.2 and Ch. 1, Problem 24 of [6], for example. The case $\gcd(j,m) > 1$ then follows by application of Parseval's identity.

Now let n be an odd square-free integer and let J be the character polynomial of degree $n-1$. Lemma 3.2 with $m = n$ implies that, for integer j,

$$J(\zeta_n^j) = i^{(n-1)^2/4}\, (j \,|\, n)\, n^{1/2}. \tag{3.6}$$

Given a polynomial A of degree $n-1$, then by the definition (1.1) of the rotation A_r, we have for integer j

$$A_r(\zeta_n^j) = \zeta_n^{-j\lfloor nr \rfloor} A(\zeta_n^j) \tag{3.7}$$

and therefore,

$$J_r(\zeta_n^j) = i^{(n-1)^2/4}\, \zeta_n^{-j\lfloor nr \rfloor}\, (j \,|\, n)\, n^{1/2}. \tag{3.8}$$

We shall need the following bound for the magnitude of a polynomial of degree $n-1$ over $\mathbb{C}$ on the unit circle in terms of its values at the nth roots of unity.

Lemma 3.3. *Let $A \in \mathbb{C}[z]$ have degree at most $n-1$ for $n > 2$. Then*

$$\max_{|z|=1} |A(z)| \le (2 \log n) \max_{0 \le k < n} |A(\zeta_n^k)|.$$

Proof. By bounding the coefficients that occur in the Lagrange interpolation of A from its evaluations at the nth roots of unity, it can be shown that

$$\max_{|z|=1} |A(z)| \le c(n) \max_{0\le k<n} |A(\zeta_n^k)|,$$

where $c(n) = 1 + (1/n)\sum_{j=1}^{n-1} 1/\sin(\frac{\pi j}{2n})$ (see [26, Appendix], for example). Since $c(n) < 1 + \sum_{j=1}^{n-1} 1/j$ and $\sum_{j=2}^{n-1} 1/j < \log n$, the lemma holds for $n > 7$. By direct verification we also have $c(n) \le 2\log n$ for $3 \le n \le 7$. □

Using (3.8), Lemma 3.3 gives

$$\max_{|z|=1} |J_r(z)| \le 2n^{1/2}\log n. \tag{3.9}$$

We next prove our main tool for comparing the asymptotic merit factor of J with that of a Littlewood completion $J+V$.

Proposition 3.4. *Let $n > 1$ be an odd square-free integer, and let r be real. Then all Littlewood completions $J+V$ of the character polynomial J of degree $n-1$ satisfy*

$$\left|\frac{1}{F(J_r+V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} - \frac{\|V_r\|_4^4}{n^2}\right| < 8\,p_n^{-1/2} n^{-1} (\log n)^{3/2} \|V_r\|_4^2 + 58 p_n^{-1/2} (\log n)^{7/2}.$$

In the application of Proposition 3.4 it is sometimes useful to further bound $\|V_r\|_4^4$ as

$$\|V_r\|_4^4 \le [\psi(n)]^3, \tag{3.10}$$

which follows from $\|V_r\|_2^2 = \psi(n)$ and the simple inequality

$$\|A\|_4^4 \le \|A\|_2^2 \max_{|z|=1} |A(z)|^2 \quad \text{for all } A \in \mathbb{C}[z]. \tag{3.11}$$

Proof of Proposition 3.4. Let $V \in \mathcal{V}_n$ and let

$$\beta(n) := \left|\frac{1}{F(J_r+V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} - \frac{\|V_r\|_4^4}{n^2}\right|.$$

Since $\|J_r\|_2^2 = \phi(n)$ and $\|J_r + V_r\|_2^2 = n$, we have by the definition of the merit factor

$$\beta(n) = \left|\frac{1}{n^2}\left(\|J_r+V_r\|_4^4 - \|J_r\|_4^4 - \|V_r\|_4^4\right) + \left(\frac{\phi(n)}{n}\right)^2 - 1\right|. \tag{3.12}$$

Since

$$\left|\left(\frac{\phi(n)}{n}\right)^2 - 1\right| = \frac{1}{n^2}\Big|\big(\phi(n)+n\big)\big(\phi(n)-n\big)\Big| < \frac{2\psi(n)}{n}$$

by the trivial inequality $\phi(n) + n < 2n$, it follows from (3.12) that

$$\beta(n) < \left|\frac{1}{n^2}\left(\|J_r+V_r\|_4^4 - \|J_r\|_4^4 - \|V_r\|_4^4\right)\right| + \frac{2\psi(n)}{n}. \tag{3.13}$$

Now for $a, b \in \mathbb{C}$, by expanding $|a+b|^4$, we get the inequality

$$\Big| |a+b|^4 - |a|^4 - |b|^4 \Big| \le 4\,|a|^3 \cdot |b| + 6\,|a|^2 \cdot |b|^2 + 4\,|a| \cdot |b|^3.$$

Use (3.9) and the definition of the L_α norm to conclude from (3.13) that

$$\beta(n) < \frac{32(\log n)^3}{n^{1/2}}\,\|V_r\|_1 + \frac{24(\log n)^2}{n}\,\|V_r\|_2^2 + \frac{8\log n}{n^{3/2}}\,\|V_r\|_3^3 + \frac{2\psi(n)}{n}. \tag{3.14}$$

We have $\|V_r\|_2^2 = \psi(n)$. By the Cauchy-Schwarz inequality,

$$\|V_r\|_{m+1}^{m+1} \le \|V_r\|_2 \left(\frac{1}{2\pi}\int_0^{2\pi} \big|V_r(e^{i\theta})\big|^{2m}\,d\theta\right)^{1/2}.$$

Hence $\|V_r\|_1 \le [\psi(n)]^{1/2}$ and $\|V_r\|_3^3 \le [\psi(n)]^{1/2}\,\|V_r\|_4^2$, by taking $m = 0$ and $m = 2$, respectively. Therefore, using (3.4) to bound $\psi(n)$, we find from (3.14) that

$$\begin{aligned}\beta(n) &< 32p_n^{-1/2}(\log n)^{7/2} + 24p_n^{-1}(\log n)^3 + 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 + 2p_n^{-1}\log n \\ &< 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 + (32+24+2)p_n^{-1/2}(\log n)^{7/2}\end{aligned}$$

since $n > 2$. □

4. Proof of Theorem 2.1

In this section we determine the asymptotic merit factor of the character polynomial J of degree $n-1$ at all rotations, proving Theorem 2.1.

We need the following evaluation of a character sum.

Lemma 4.1. *Let n be a positive odd square-free integer. Then, for integer u,*

$$\sum_{j=0}^{n-1} (j\,|\,n)(j+u\,|\,n) = \mu\left(\frac{n}{\gcd(u,n)}\right)\,\phi\big(\gcd(u,n)\big).$$

Proof. Given a polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$ with real-valued coefficients, it is readily verified that

$$\sum_{j=0}^{n-1} a_j a_{(j+u) \bmod n} = \frac{1}{n}\sum_{j=0}^{n-1} |A(\zeta_n^j)|^2\,\zeta_n^{ju}.$$

Applying this relation to the character polynomial J of degree $n-1$ and using (3.6), then gives

$$\sum_{j=0}^{n-1} (j\,|\,n)(j+u\,|\,n) = \sum_{\substack{j=0 \\ \gcd(j,n)=1}}^{n-1} \zeta_n^{ju},$$

which is Ramanujan's sum. The result now follows from Lemma 3.1. □

Høholdt and Jensen [18] introduced a method for calculating the merit factor of a polynomial of even degree. The following result summarises their method (and occurs as a special case of the slightly more general result of [27, Lem. 10]).

Lemma 4.2. *Let $A \in \mathbb{R}[z]$ be a polynomial of even degree $n-1$. Define*

$$\Lambda_A(j,k,\ell) := \sum_{a=0}^{n-1} A(\zeta_n^a)\overline{A(\zeta_n^{a+j})}A(\zeta_n^{a+k})\overline{A(\zeta_n^{a+\ell})} \quad \text{for integer } j,\ k,\ \ell. \tag{4.1}$$

Then

$$\frac{\|A\|_4^4}{n^2} = \frac{2n^2+1}{3n^5}\,\Lambda_A(0,0,0) + B + C + D, \tag{4.2}$$

where

$$B = \frac{2}{n^5}\sum_{k=1}^{n-1} \frac{\Lambda_A(0,0,k) + \zeta_n^k\,\overline{\Lambda_A(0,0,k)}}{(1-\zeta_n^k)^2}\cdot(1+\zeta_n^k),$$

$$C = -\frac{2}{n^5}\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}} \frac{4\,\zeta_n^k\,\Lambda_A(0,k,\ell) + \Lambda_A(k,0,\ell) + \zeta_n^k\zeta_n^\ell\,\overline{\Lambda_A(k,0,\ell)}}{(1-\zeta_n^k)(1-\zeta_n^\ell)},$$

$$D = \frac{4}{n^5}\sum_{k=1}^{n-1} \frac{2\Lambda_A(0,k,k) + \zeta_n^{-k}\,\Lambda_A(k,0,k)}{|1-\zeta_n^k|^2}.$$

We are now ready to calculate the asymptotic merit factor of the character polynomial at all rotations.

Proof of Theorem 2.1. Without loss of generality, we may assume that $-\frac{1}{2} < r \le \frac{1}{2}$. Since $\|J_r\|_2^2 = \phi(n)$, we have by the definition of the merit factor

$$\frac{1}{F(J_r)} = \left(\frac{n}{\phi(n)}\right)^2 \left(\frac{\|J_r\|_4^4}{n^2}\right) - 1.$$

We claim that

$$\frac{\|J_r\|_4^4}{n^2} = 1 + \frac{1}{f(r)} + O\big(p_n^{-1}(\log n)^3\big), \tag{4.3}$$

which then implies the desired result using the condition (2.1) and the growth rate (3.2) of $\phi(n)$.

It remains to prove the claim (4.3). Write $R := \lfloor nr \rfloor$. We apply Lemma 4.2 to the polynomial J_r to give an expression for $\|J_r\|_4^4/n^2$. We find the asymptotic form of this expression, evaluating the term involving $\Lambda_{J_r}(0,0,0)$ and the sum D, and bounding the sums B and C.

Using (3.8) and (4.1), we have

$$\Lambda_{J_r}(j,k,\ell) = \zeta_n^{R(j-k+\ell)}\cdot n^2 \sum_{a=0}^{n-1} (a\,|\,n)(a+j\,|\,n)(a+k\,|\,n)(a+\ell\,|\,n). \tag{4.4}$$

The term involving $\Lambda_{J_r}(0,0,0)$***:*** By (4.4) we have

$$\begin{aligned}\frac{2n^2+1}{3n^5}\,\Lambda_{J_r}(0,0,0) &= \frac{2n^2+1}{3n^5}\,n^2\,\phi(n)\\ &= \frac{2}{3} + O\big(p_n^{-1}\log n\big)\end{aligned} \tag{4.5}$$

from the growth rate (3.2) of $\phi(n)$.

The sum D.: By (4.4), for each k we have

$$\phi(n) - \psi(n) \le \frac{1}{n^2}\,\Lambda_{J_r}(0,k,k) \le \phi(n).$$

From the growth rate (3.2) of $\phi(n)$ and the growth rate (3.5) of $\psi(n)$ we then obtain

$$\Lambda_{J_r}(0,k,k) = n^3\big[1 + O(p_n^{-1}\log n)\big]$$

and similarly

$$\Lambda_{J_r}(k,0,k) = \zeta_n^{2Rk}\cdot n^3\big[1 + O(p_n^{-1}\log n)\big].$$

The sum D then becomes

$$D = \frac{4}{n^2}\Big[1 + O(p_n^{-1}\log n)\Big]\sum_{k=1}^{n-1}\frac{2+\zeta_n^{(2R-1)k}}{|1-\zeta_n^k|^2}. \tag{4.6}$$

We will evaluate the summation in (4.6) by using the identity

$$\sum_{k=1}^{n-1}\frac{\zeta_n^{jk}}{|1-\zeta_n^k|^2} = \frac{n^2}{2}\left(\frac{|j|}{n}-\frac{1}{2}\right)^2 - \frac{n^2+2}{24} \quad \text{for integer } j \text{ satisfying } |j|\le n \tag{4.7}$$

(see, [20, p. 621], for example). The assumption $-\frac12 < r \le \frac12$ implies that $-n < 2R-1 < n$ for all sufficiently large n. We can therefore use (4.7) to evaluate the summation in (4.6) for all sufficiently large n, so that we have

$$D = \frac{4}{n^2}\big[1 + O(p_n^{-1}\log n)\big]\left[\frac{n^2}{2}\left(\frac{|2R-1|}{n}-\frac12\right)^2 + \frac{n^2-2}{8}\right].$$

By definition of R, we have $R = nr + O(1)$. We then find that

$$D = \tfrac12 + 8\left(|r| - \tfrac14\right)^2 + O(p_n^{-1}\log n). \tag{4.8}$$

The sum B.: We bound the sum B via

$$\begin{aligned} |B| &\le \frac{2}{n^5}\sum_{k=1}^{n-1}\frac{4\,\big|\Lambda_{J_r}(0,0,k)\big|}{|1-\zeta_n^k|^2} \\ &= \frac{8}{n^5}\sum_{k=1}^{n-1}\frac{n^2}{|1-\zeta_n^k|^2}\left|\sum_{a=0}^{n-1}(a\,|\,n)(a+k\,|\,n)\right| \end{aligned} \tag{4.9}$$

by (4.4). But from Lemma 4.1 we know that

$$\left|\sum_{a=0}^{n-1}(a\,|\,n)(a+k\,|\,n)\right| \le \phi(p_n^{-1}n) < \frac{n}{p_n} \quad \text{for } k \not\equiv 0 \pmod n. \tag{4.10}$$

Substitution in (4.9) gives

$$|B| < \frac{8}{n^2\,p_n} \sum_{k=1}^{n-1} \frac{1}{|1-\zeta_n^k|^2},$$
$$= \frac{2(n^2-1)}{3n^2\,p_n}$$

from (4.7). Hence,

$$B = O(p_n^{-1}). \tag{4.11}$$

The sum C**.:** Since $|\Lambda_{J_r}(0,k,\ell)| = |\Lambda_{J_r}(k,0,\ell)|$ by (4.4), we can bound the sum C via

$$|C| \le \frac{2}{n^5} \sum_{\substack{1\le k,\ell<n\\ k\ne\ell}} \frac{6\,\big|\Lambda_{J_r}(0,k,\ell)\big|}{|1-\zeta_n^k|\cdot|1-\zeta_n^\ell|}. \tag{4.12}$$

Now from (4.4) we have

$$\frac{1}{n^2}\big|\Lambda_{J_r}(0,k,\ell)\big| = \left|\sum_{a=0}^{n-1}(a+k\,|\,n)(a+\ell\,|\,n) \;-\; \sum_{\substack{a=0\\ \gcd(a,n)>1}}^{n-1}(a+k\,|\,n)(a+\ell\,|\,n)\right|$$
$$\le \left|\sum_{a=0}^{n-1}(a\,|\,n)(a+\ell-k\,|\,n)\right| + \psi(n)$$
$$< \frac{n}{p_n} + \psi(n) \quad \text{for } k \not\equiv \ell \pmod n$$

by (4.10). Substitution in (4.12) then gives

$$|C| < \frac{12}{n^3}\left(\frac{n}{p_n}+\psi(n)\right) \sum_{\substack{1\le k,\ell<n\\ k\ne\ell}} \frac{1}{|1-\zeta_n^k|\cdot|1-\zeta_n^\ell|}$$
$$< \frac{12}{n^3}\left(\frac{n}{p_n}+\psi(n)\right)\left(\sum_{k=1}^{n-1}\frac{1}{|1-\zeta_n^k|}\right)^2$$
$$\le \frac{12(\log n)^2}{n}\left(\frac{n}{p_n}+\psi(n)\right)$$

since $\sum_{k=1}^{n-1} 1/|1-\zeta_n^k| \le n\log n$ (see [18, p. 163], for example). Then from the growth rate (3.5) of $\psi(n)$ we obtain

$$C = O(p_n^{-1}(\log n)^3). \tag{4.13}$$

The claim (4.3) now follows by substituting the asymptotic forms (4.5), (4.8), (4.11), and (4.13) in (4.2), and then using the definition (1.2) of f. □

5. Proof of Theorem 2.2

By Proposition 3.4, we have

$$\frac{1}{F(J_r+V_r)} > \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} + \delta(n),$$

where

$$\begin{aligned}\delta(n) &= \frac{1}{n^2}\|V_r\|_4^4 - 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 - 58p_n^{-1/2}(\log n)^{7/2}\\ &= \frac{1}{n^2}\|V_r\|_4^4 + O\big(p_n^{-2}n^{1/2}(\log n)^3\big) + O\big(p_n^{-1/2}(\log n)^{7/2}\big), \qquad (5.1)\end{aligned}$$

using the upper bound (3.10) for $\|V_r\|_4^4$ and the upper bound (3.4) for $\psi(n)$. Therefore

$$\liminf_{n\to\infty} \frac{1}{F(J_r+V_r)} \ge \liminf_{n\to\infty}\left[\left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)}\right] + \liminf_{n\to\infty}\delta(n). \qquad (5.2)$$

We next derive a lower bound for the term $\|V_r\|_4^4/n^2$ in (5.1), giving an asymptotic lower bound for $\delta(n)$. For a polynomial $A \in \mathbb{C}[z]$ of degree at most $n-1$, we have the identity

$$\|A\|_4^4 = \frac{1}{2n}\left(\sum_{j=0}^{n-1}|A(\zeta_n^j)|^4 + \sum_{j=0}^{n-1}|A(-\zeta_n^j)|^4\right)$$

(see [18], for example), which gives the inequality

$$\frac{1}{n^2}\|V_r\|_4^4 \ge \frac{1}{2n^3}\sum_{j=0}^{n-1}|V_r(\zeta_n^j)|^4.$$

Restrict the summation to the set $U = \{\frac{n}{p_n}, 2\frac{n}{p_n}, \dots, (p_n-1)\frac{n}{p_n}\}$ and use (3.7) to obtain

$$\frac{1}{n^2}\|V_r\|_4^4 \ge \frac{1}{2n^3}\sum_{u\in U}|V(\zeta_n^u)|^4. \qquad (5.3)$$

Now let $u \in U$. From the definition of V we have

$$\begin{aligned}V(\zeta_n^u) &= \sum_{\substack{j=0\\ \gcd(j,n)>1}}^{n-1} \zeta_n^{ju}\\ &= \sum_{j=0}^{n-1}\zeta_n^{ju} - \sum_{\substack{j=0\\ \gcd(j,n)=1}}^{n-1}\zeta_n^{ju}.\end{aligned}$$

The first sum evaluates to 0 because $\zeta_n^u \ne 1$. The second sum is Ramanujan's sum, and using $\gcd(u,n) = p_n^{-1}n$ in Lemma 3.1, we get

$$V(\zeta_n^u) = \phi\big(p_n^{-1}n\big) = \frac{\phi(n)}{p_n-1}.$$

Substitution in (5.3) then gives the desired lower bound

$$\begin{aligned}\frac{1}{n^2}\,\|V_r\|_4^4 &\geq \frac{1}{2n^3}(p_n-1)\left(\frac{\phi(n)}{p_n-1}\right)^4\\ &> \frac{n}{2p_n^3}\left(\frac{\phi(n)}{n}\right)^4.\end{aligned}$$

By substituting this lower bound in (5.1) we find that

$$\delta(n) > \frac{n}{2p_n^3}\left(\frac{\phi(n)}{n}\right)^4 + O\big(p_n^{-2}n^{1/2}(\log n)^3\big) + O\big(p_n^{-1/2}(\log n)^{7/2}\big), \tag{5.4}$$

or equivalently

$$\delta(n) > \frac{n}{2p_n^3}\left[\left(\frac{\phi(n)}{n}\right)^4 + O\big(p_n n^{-1/2}(\log n)^3\big) + O\big(p_n^{5/2}n^{-1}(\log n)^{7/2}\big)\right]. \tag{5.5}$$

To complete the proof, partition the infinite set N, in which n takes values, into subsets N_1, N_2 defined by

$$n \in \begin{cases} N_1 & \text{if } p_n \leq n^{2/7}\\ N_2 & \text{if } p_n > n^{2/7},\end{cases}$$

at least one of which is infinite. First suppose that N_1 is infinite and let n take values only in N_1. Then

$$p_n n^{-1/2}(\log n)^3 \leq n^{-3/14}(\log n)^3 \to 0$$

and

$$p_n^{5/2}n^{-1}(\log n)^{7/2} \leq n^{-2/7}(\log n)^{7/2} \to 0,$$

so that by (5.5) we obtain

$$\liminf_{n\to\infty}\delta(n) \geq \liminf_{n\to\infty}\left[\frac{n}{2p_n^3}\left(\frac{\phi(n)}{n}\right)^4\right].$$

Choose some ϵ satisfying $0<\epsilon<1/28$. Since $\phi(n)/n^{1-\epsilon}\to\infty$ (see [17, Thm. 327], for example), we have

$$\liminf_{n\to\infty}\delta(n) \geq \liminf_{n\to\infty}\frac{n^{1-4\epsilon}}{2p_n^3} \geq \frac{1}{2}\liminf_{n\to\infty}\,n^{1/7-4\epsilon} = \infty,$$

so that by (5.2),

$$\liminf_{n\to\infty}\frac{1}{F(J_r+V_r)} = \infty.$$

This verifies the claim (2.2) of the theorem when $n\in N_1$ since $p_n\leq n^{2/7}$ for all $n\in N_1$.

Now suppose that N_2 is infinite and let n take values only in N_2. Then

$$p_n^{-2}n^{1/2}(\log n)^3 < n^{-1/14}(\log n)^3 \to 0$$

and

$$p_n^{-1/2}(\log n)^{7/2} < n^{-1/7}(\log n)^{7/2} \to 0,$$

so that by (5.4) we obtain

$$\liminf_{n\to\infty} \delta(n) \geq \liminf_{n\to\infty} \left[\frac{n}{2p_n^3} \left(\frac{\phi(n)}{n} \right)^4 \right].$$

From the growth rate (3.2) of $\phi(n)$ and (5.2) we then conclude that the claim (2.2) of the theorem holds when $n \in N_2$. Therefore it holds when $n \in N_1 \cup N_2 = N$, which completes the proof. □

6. Proof of Theorem 2.3

The structure of the proof is broadly similar to that of Theorem 2.2, except that we now use the condition (2.3) to control the term $\|V_r\|_4^4$ for $V \in \mathcal{V}_n$. Application of Proposition 3.4 gives, for each $V \in \mathcal{V}_n$,

$$\frac{1}{F(J_r + V_r)} > \left(\frac{\phi(n)}{n} \right)^2 \frac{1}{F(J_r)} + \delta(n),$$

where

$$\delta(n) = \frac{1}{n^2} \|V_r\|_4^4 - 8p_n^{-1/2} n^{-1} (\log n)^{3/2} \|V_r\|_4^2 - 58 p_n^{-1/2} (\log n)^{7/2}. \tag{6.1}$$

We then find from the growth rate (3.2) of $\phi(n)$, using the condition (2.3), that

$$\liminf_{n\to\infty} \min_{V\in\mathcal{V}_n} \frac{1}{F(J_r + V_r)} \geq \liminf_{n\to\infty} \frac{1}{F(J_r)} + \liminf_{n\to\infty} \delta(n). \tag{6.2}$$

We claim that

$$\liminf_{n\to\infty} \delta(n) = \liminf_{n\to\infty} \frac{1}{n^2} \|V_r\|_4^4, \tag{6.3}$$

and then, since $\|V_r\|_4^4 \geq 0$, we have from (6.2)

$$\limsup_{n\to\infty} \max_{V\in\mathcal{V}_n} F(J_r + V_r) \leq \limsup_{n\to\infty} F(J_r).$$

Now use Theorem 2.1 and the condition (2.3) to replace $\limsup_{n\to\infty} F(J_r)$ by $f(r)$, proving the theorem.

It remains to prove the claim (6.3). By the condition (2.3), we obtain from (6.1) that

$$\liminf_{n\to\infty} \delta(n) = \liminf_{n\to\infty} \left[\frac{1}{n^2} \|V_r\|_4^4 - 8p_n^{-1/2} n^{-1} (\log n)^{3/2} \|V_r\|_4^2 \right] \tag{6.4}$$

$$= \liminf_{n\to\infty} \left[\frac{1}{n^2} \|V_r\|_4^4 \left(1 - \frac{8p_n^{-1/2} n (\log n)^{3/2}}{\|V_r\|_4^2} \right) \right]. \tag{6.5}$$

Partition the infinite set N, in which n takes values, into subsets N_1, N_2 defined by

$$n \in \begin{cases} N_1 & \text{if } \|V_r\|_4^4 > p_n^{-1} n^2 (\log n)^5 \\ N_2 & \text{if } \|V_r\|_4^4 \leq p_n^{-1} n^2 (\log n)^5, \end{cases}$$

at least one of which is infinite. If N_1 is infinite, then for $n \in N_1$ we have

$$\frac{8p_n^{-1/2} n (\log n)^{3/2}}{\|V_r\|_4^2} < \frac{8}{\log n} \to 0,$$

so that by (6.5), the claim (6.3) holds when n takes values only in N_1. On the other hand, if N_2 is infinite, then for $n \in N_2$ we have

$$8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 \le 8p_n^{-1}(\log n)^4,$$

so that by using the condition (2.3) and substituting in (6.4) we conclude that (6.3) holds when n takes values only in N_2. Since $n \in N_1 \cup N_2 = N$, we therefore have established the claim (6.3). □

7. Proof of Theorem 2.4

The method of the proof is to apply Proposition 3.4 and bound $\|V_r\|_4$ for almost all choices $V \in \mathcal{V}_n$, for which we require the following large deviation result (see [1, Thm. A.1.16], for example).

Lemma 7.1. *Let $X_1, X_2, \dots, X_m$ be mutually independent random variables satisfying $\mathrm{E}(X_j) = 0$ and $|X_j| \le 1$ for $1 \le j \le m$. Then, for real $a \ge 0$,*

$$\Pr\left(\left|\sum_{j=1}^m X_j\right|^2 \ge a\right) \le 2\,e^{-\frac{a}{2m}}.$$

We next use Lemma 7.1 to give an upper bound for $\|V_r\|_4$ for almost all $V \in \mathcal{V}_n$.

Lemma 7.2. *Let V be drawn uniformly from $\mathcal{V}_n$ and let r be real. Then, as $n \to \infty$,*

$$\Pr\left(\|V_r\|_4^4 < 288[\psi(n)]^2 \log n\right) \to 1.$$

Proof. Given a polynomial $A \in \mathbb{C}[z]$ of degree at most $n-1$, it is a simple consequence of Bernstein's inequality that

$$\max_{|z|=1} |A(z)| \le 6 \max_{0\le j<4n} |A(\zeta_{4n}^j)|$$

(see [28, p. 691]). Therefore, by (3.11),

$$\|V_r\|_4^4 \le 36\psi(n) \max_{0\le j<4n} |V_r(\zeta_{4n}^j)|^2.$$

Hence, it is sufficient to show that

$$\Pr\Big(\max_{0\le j<4n} |V_r(\zeta_{4n}^j)|^2 < 8\psi(n)\log n\Big) \to 1. \tag{7.1}$$

Write $a(n) = 8\psi(n)\log n$. A crude estimate gives

$$\Pr\Big(\max_{0\le j<4n} |V_r(\zeta_{4n}^j)|^2 \ge a(n)\Big) \le \sum_{j=0}^{4n-1} \Pr\Big(|V_r(\zeta_{4n}^j)|^2 \ge a(n)\Big)$$

$$\le \sum_{j=0}^{4n-1} \left[\Pr\Big(\big|\mathrm{Re}\big(V_r(\zeta_{4n}^j)\big)\big|^2 \ge \tfrac{1}{2}a(n)\Big) + \Pr\Big(\big|\mathrm{Im}\big(V_r(\zeta_{4n}^j)\big)\big|^2 \ge \tfrac{1}{2}a(n)\Big)\right]. \tag{7.2}$$

Write $V \in \mathcal{V}_n$ as $V(z) = \sum_{k=0}^{n-1} v_k z^k$ and note that $v_k = 0$ if and only if $\gcd(k,n) = 1$. Then we have by the definition of the rotation V_r,

$$V_r(z) = \sum_{\substack{\ell=0 \\ \gcd(\ell,n)>1}}^{n-1} v_\ell \, z^{k(\ell)},$$

where $k(\ell) = (\ell - \lfloor nr \rfloor) \bmod n$. Let $\lambda \in \mathbb{C}$ be such that $|\lambda| \le 1$. Then

$$\begin{aligned}\Pr\left(\left|\mathrm{Re}\big(V_r(\lambda)\big)\right|^2 \ge \tfrac{1}{2}a(n)\right) &= \Pr\left(\left|\sum_{\substack{\ell=0 \\ \gcd(\ell,n)>1}}^{n-1} v_\ell \,\mathrm{Re}(\lambda^{k(\ell)})\right|^2 \ge \tfrac{1}{2}a(n)\right) \\ &\le 2e^{-\frac{1}{2\psi(n)}\cdot\frac{a(n)}{2}}\end{aligned}$$

by application of Lemma 7.1. By definition of $a(n)$ we then obtain

$$\Pr\left(\left|\mathrm{Re}\big(V_r(\lambda)\big)\right|^2 \ge \tfrac{1}{2}a(n)\right) \le 2n^{-2},$$

and by similar reasoning

$$\Pr\left(\left|\mathrm{Im}\big(V_r(\lambda)\big)\right|^2 \ge \tfrac{1}{2}a(n)\right) \le 2n^{-2}.$$

Substitution in (7.2) then gives

$$\Pr\left(\max_{0\le j<4n} |V_r(\zeta_{4n}^j)|^2 \ge a(n)\right) \le 16n^{-1},$$

which implies (7.1), as required. □

We now use Lemma 7.2 to prove Theorem 2.4.

Proof of Theorem 2.4. Define a subset $\mathcal{U}_n$ of $\mathcal{V}_n$ by

$$\mathcal{U}_n := \left\{V \in \mathcal{V}_n : \|V_r\|_4^4 < 288 p_n^{-2} n^2 (\log n)^3\right\}. \tag{7.3}$$

Using the upper bound (3.4) for $\psi(n)$, Lemma 7.2 implies that

$$\frac{|\mathcal{U}_n|}{|\mathcal{V}_n|} \to 1. \tag{7.4}$$

By the triangle inequality,

$$\left|\frac{1}{F(J_r+V_r)} - \frac{1}{f(r)}\right| \le \left|\frac{1}{F(J_r+V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)}\right| + \left|\left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} - \frac{1}{f(r)}\right|. \tag{7.5}$$

Using the condition (2.4) and the growth rate (3.2) of $\phi(n)$, we find from Theorem 2.1 that

$$\left|\left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} - \frac{1}{f(r)}\right| \to 0. \tag{7.6}$$

From Proposition 3.4 we have

$$\left|\frac{1}{F(J_r+V_r)}-\left(\frac{\phi(n)}{n}\right)^2\frac{1}{F(J_r)}\right|<\gamma(n)\quad\text{for } V\in\mathcal{U}_n, \tag{7.7}$$

where

$$\begin{aligned}\gamma(n)&=\max_{V\in\mathcal{U}_n}\left(\frac{1}{n^2}\,\|V_r\|_4^4+8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2+58p_n^{-1/2}(\log n)^{7/2}\right)\\&<8p_n^{-2}(\log n)^3+\sqrt{512}\,p_n^{-3/2}(\log n)^3+58p_n^{-1/2}(\log n)^{7/2},\end{aligned}$$

by the definition (7.3) of $\mathcal{U}_n$. Using the condition (2.4), we have $\gamma(n)\to 0$. Since $\mathcal{U}_n$ forms a set of measure 1 within $\mathcal{V}_n$ by (7.4), we find by substitution of (7.6) and (7.7) into (7.5) that

$$\left|\frac{1}{F(J_r+V_r)}-\frac{1}{f(r)}\right|\to 0\quad\text{in probability.}$$

Since $f(r)$ takes values only in a finite interval bounded away from 0, we then have

$$|F(J_r+V_r)-f(r)|\to 0\quad\text{in probability,}$$

which completes the proof. □

8. Proof of Theorem 2.5

From Proposition 3.4 we have

$$\left|\frac{1}{F(J_r+V_r)}-\left(\frac{\phi(n)}{n}\right)^2\frac{1}{F(J_r)}\right|<\gamma(n), \tag{8.1}$$

where

$$\gamma(n)=\frac{1}{n^2}\,\|V_r\|_4^4+8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2+58p_n^{-1/2}(\log n)^{7/2}. \tag{8.2}$$

We also have from (3.11), Lemma 3.3, (3.7), and the upper bound (3.4) for $\psi(n)$,

$$\|V_r\|_4^4\le(2\log n)^2\Big(\max_{0\le k<n}\big|V(\zeta_n^k)\big|^2\Big)p_n^{-1}n\log n. \tag{8.3}$$

We now bound the term $|V(\zeta_n^k)|$. By definition of V, we have for integer k,

$$\begin{aligned}V(\zeta_n^k)&=\sum_{\substack{j=0\\ \gcd(j,n)>1}}^{n-1}\big(j\,\big|\,\tfrac{n}{\gcd(j,n)}\big)\,\zeta_n^{kj}\\&=\sum_{\substack{0<m<n\\ m\mid n}}\ \sum_{\substack{\ell=0\\ \gcd(\ell,m)=1}}^{m-1}\big(\tfrac{\ell n}{m}\,\big|\,m\big)\,\zeta_m^{k\ell}\end{aligned}$$

by putting $m = n/\gcd(j,n)$, so that we must have $j = \ell n/m$ where, since n is square-free, $0 \le \ell < m$ and $\gcd(\ell, m) = 1$. Since the Jacobi symbol is multiplicative, and $(\ell\,|\,m) = 0$ for $\gcd(\ell, m) > 1$, we then have

$$V(\zeta_n^k) = \sum_{\substack{0<m<n\\ m|n}} \left(\tfrac{n}{m}\,\middle|\, m\right) \sum_{\ell=0}^{m-1} (\ell\,|\,m)\,\zeta_m^{k\ell},$$

and therefore

$$\begin{aligned} |V(\zeta_n^k)| &\le \sum_{\substack{0<m<n\\ m|n}} \left| \sum_{\ell=0}^{m-1} (\ell\,|\,m)\,\zeta_m^{k\ell} \right| \\ &\le \sum_{\substack{0<m<n\\ m|n}} m^{1/2} \end{aligned}$$

by Lemma 3.2. Hence,

$$\begin{aligned} \big|V(\zeta_n^k)\big| &\le \sum_{j=1}^{\omega(n)} \binom{\omega(n)}{j} \left(\frac{n}{p_n^j}\right)^{1/2} \\ &< n^{1/2}\big(1 + p_n^{-1/2}\big)^{\omega(n)} \\ &\le n^{1/2}\big(1 + (\log n)^{-7/2}\big)^{\log n} \end{aligned}$$

for all sufficiently large n, by (2.5) and (3.1). Therefore

$$|V(\zeta_n^k)| = O(n^{1/2}).$$

Substitute in (8.3) to give

$$\|V_r\|_4^4 = O\big(p_n^{-1} n^2 (\log n)^3\big),$$

and then substitute in (8.2) to show that

$$\gamma(n) = O\big(p_n^{-1}(\log n)^3\big) + O\big(p_n^{-1}(\log n)^3\big) + O\big(p_n^{-1/2}(\log n)^{7/2}\big) \to 0,$$

by the condition (2.5). The required result then follows from (8.1) and Theorem 2.1, using the growth rate (3.2) of $\phi(n)$ and the condition (2.5). □

9. Proof of Theorem 2.6

Let $V \in \mathcal{V}_n$. From Proposition 3.4 we have

$$\left| \frac{1}{F(J_r + V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} \right| < \gamma(n), \tag{9.1}$$

where

$$\gamma(n) = \frac{1}{n^2}\,\|V_r\|_4^4 + 8p_n^{-1/2} n^{-1} (\log n)^{3/2} \|V_r\|_4^2 + 58 p_n^{-1/2} (\log n)^{7/2}.$$

From the upper bound (3.10) for $\|V_r\|_4^4$ and the upper bound (3.3) for $\psi(n)$ we have $\|V_r\|_4^4 \le (2n/p_n)^3$ for all sufficiently large n since the condition (2.7) forces $\omega(n) \le 2$ for all sufficiently large n. Hence

$$\gamma(n) = O\big(p_n^{-3}n\big) + O\big(p_n^{-2}n^{1/2}(\log n)^{3/2}\big) + O\big(p_n^{-1/2}(\log n)^{7/2}\big).$$

By the condition (2.7) we then have $\gamma(n) \to 0$, and the required result follows from (9.1) and Theorem 2.1, using the growth rate (3.2) of $\phi(n)$ and the condition (2.7). □

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 3rd ed., Wiley, Hoboken, New Jersey, 2008.

[2] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976.

[3] J. Beck, *Flat polynomials on the unit circle—note on a problem of Littlewood*, Bull. London Math. Soc. **23** (1991), no. 3, 269–277.

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

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

[6] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, John Wiley & Sons, New York, NY, 1998.

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

[8] P. Borwein and K.-K. S. Choi, *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math. **53** (2001), no. 1, 33–50.

[9] ———, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), no. 1, 219–234.

[10] P. Borwein, K.-K. S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than 6.34*, IEEE Trans. Inf. Theory **50** (2004), no. 12, 3234–3249.

[11] P. Borwein, K.-K. S. Choi, and S. Yazdani, *An extremal property of Fekete polynomials*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 19–27.

[12] P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, Proc. Amer. Math. Soc. **129** (2001), no. 5, 1463–1472.

[13] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 865–889.

[14] P. Erdős, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.

[15] M. J. E. Golay, *The merit factor of long low autocorrelation binary sequences*, IEEE Trans. Inf. Theory **IT-28** (1982), no. 3, 543–549.

[16] ———, *The merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **29** (1983), no. 6, 934–936.

[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Science Publications, Oxford, 1979.

[18] T. Høholdt and H. E. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **34** (1988), no. 1, 161–164.

[19] J. Jedwab, *A survey of the merit factor problem for binary sequences*, Proc. of Sequences and Their Applications (SETA), Lecture Notes in Computer Science, vol. 3486, New York: Springer Verlag, 2005, pp. 30–55.

[20] J. M. Jensen, H. E. Jensen, and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inf. Theory **37** (1991), no. 3, 617–626.

[21] J. E. Littlewood, *On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$*, J. London Math. Soc. **41** (1966), 367–376.

[22] ———, *Some problems in real and complex analysis*, Heath Mathematical Monographs, D. C. Heath and Company, Lexington, MA, 1968.
[23] H. L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.
[24] D. J. Newman, *Norms of polynomials*, Amer. Math. Monthly **67** (1960), 778–779.
[25] D. J. Newman and J. S. Byrnes, *The L^4 norm of a polynomial with coeffiecients ± 1*, Amer. Math. Monthly **97** (1990), no. 1, 42–45.
[26] K. G. Paterson and V. Tarokh, *On the existence and construction of good codes with low peak-to-average power ratios*, IEEE Trans. Inf. Theory **46** (2000), no. 6, 1974–1987.
[27] K.-U. Schmidt, J. Jedwab, and M. G. Parker, *Two binary sequence families with large merit factor*, Adv. Math. Commun. **3** (2009), no. 2, 135–156.
[28] Joel Spencer, *Six standard deviations suffice*, Trans. Amer. Math. Soc. **289** (1985), no. 2, 679–706.
[29] R. J. Turyn, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968, pp. 195–228.
[30] T. Xiong and J. I. Hall, *Construction of even length binary sequences with asymptotic merit factor 6*, IEEE Trans. Inf. Theory **54** (2008), no. 2, 931–935.
[31] ———, *Modifications on character sequences and construction of large even length binary sequences*, Preprint (2010).
[32] ———, *Modifications of modified Jacobi sequences*, IEEE Trans. Inf. Theory **57** (2011), no. 1, 493–504.

The final copy-edited version is published in J. Fourier Anal. Appl. 19(3), pp. 457-466, 2013.
(http://dx.doi.org/10.1007/s00041-013-9265-6)

ON A PROBLEM DUE TO LITTLEWOOD CONCERNING POLYNOMIALS WITH UNIMODULAR COEFFICIENTS

KAI-UWE SCHMIDT

Abstract. Littlewood raised the question of how slowly $\|f_n\|_4^4 - \|f_n\|_2^4$ (where $\|.\|_r$ denotes the L^r norm on the unit circle) can grow for a sequence of polynomials f_n with unimodular coefficients and increasing degree. The results of this paper are the following. For

$$g_n(z) = \sum_{k=0}^{n-1} e^{\pi i k^2/n}\, z^k$$

the limit of $(\|g_n\|_4^4 - \|g_n\|_2^4)/\|g_n\|_2^3$ is $2/\pi$, which resolves a mystery due to Littlewood. This is however not the best answer to Littlewood's question: for the polynomials

$$h_n(z) = \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} e^{2\pi i jk/n}\, z^{nj+k}$$

the limit of $(\|h_n\|_4^4 - \|h_n\|_2^4)/\|h_n\|_2^3$ is shown to be $4/\pi^2$. No sequence of polynomials with unimodular coefficients is known that gives a better answer to Littlewood's question. It is an open question as to whether such a sequence of polynomials exists.

1. Introduction

For real $r \geq 1$, the L^r norm of a polynomial $f \in \mathbb{C}[z]$ on the unit circle is

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

There is sustained interest in the L^r norm of polynomials with restricted coefficients (see, for example, Littlewood [14], Borwein [2], and Erdélyi [5] for surveys on selected problems). Littlewood raised the question of how slowly $\|f_n\|_4^4 - \|f_n\|_2^4$ can grow for a sequence of polynomials f_n with restricted coefficients and increasing degree. This problem is also of interest in the theory of communications, because $\|f\|_4^4$ equals the sum of squares of the aperiodic autocorrelations of the sequence formed from the coefficients of f [2, p. 122]; in this context one considers the *merit factor* $\|f\|_2^4/(\|f\|_4^4 - \|f\|_2^4)$. Much work on Littlewood's question has been done when the coefficients are -1 or 1; see [8] for recent advances. In the situation where the coefficients are

Date: 13 September 2012 (revised 12 February 2013).
2010 *Mathematics Subject Classification.* Primary: 42A05, 11B83; Secondary: 94A55.

restricted to have unit magnitude, the polynomials

$$g_n(z) = \sum_{k=0}^{n-1} e^{\pi i k^2/n}\, z^k \quad \text{for integral } n \geq 1$$

are of particular interest [11], [12], [13], [14].[1] These polynomials are also the main ingredient in Kahane's celebrated semi-probabilistic construction of ultra-flat polynomials [9], which disproves a conjecture due to Erdős [6]. Write

$$\alpha_n = \frac{\|g_n\|_4^4 - \|g_n\|_2^4}{\|g_n\|_2^3}$$

(note that $\|f\|_2 = \sqrt{n}$ for every polynomial f of degree $n-1$ with unimodular coefficients). Based on the work in [11] and [12] and calculations carried out by Swinnerton-Dyer, Littlewood concluded in [13] that

$$\lim_{n\to\infty} \alpha_n = \sqrt{2} - \frac{2}{\pi}(\sqrt{2}-1) = 1.15051\ldots, \tag{1}$$

but expressed doubt in his own conclusion. He knew that

$$0.604 \leq \alpha_n \leq 0.656 \quad \text{for } 18 \leq n \leq 41 \tag{2}$$

and noted [13, Appendix] "There is a considerable mystery here. I have checked my calculations at least six times, and they have been checked also in great detail by Dr. Flett." Littlewood raised this issue again in his book [14, p. 27] and asked for a resolution of this puzzle.

Borwein and Choi [3] conjectured

$$\|g_n\|_4^4 = n^2 + \frac{2}{\pi} n^{3/2} + \delta_n n^{1/2} + O(n^{-1/2}),$$

where $\delta_n = -2$ for $n \equiv 0, 1 \pmod 4$ and $\delta_n = 1$ for $n \equiv 2, 3 \pmod 4$ (this was not stated explicitly as a conjecture in [3], but was confirmed by the authors [4] to be a tentative conclusion based on numerical evidence). This conjecture implies in particular

$$\lim_{n\to\infty} \alpha_n = \frac{2}{\pi} = 0.63661\ldots. \tag{3}$$

Independently, Antweiler and Bömer [1] made observations similar to (2), while Stańczak and Boche [17] and Mercer [15] derived bounds for α_n. In particular, Mercer [15] showed that

$$\limsup_{n\to\infty} \alpha_n < \frac{16}{3\pi^{3/2}} = 0.95779\ldots,$$

and thereby confirming Littlewood's suspicion (although Mercer was apparently unaware of Littlewood's work).

We shall resolve Littlewood's puzzle by proving that (1) is incorrect and the conjecture (3) is true.

[1] Some authors consider $g_n(e^{\pm\pi i/n} z)$, which however has the same L^r norm as $g_n(z)$.

Theorem 1. *We have*

$$\lim_{n\to\infty} \frac{\|g_n\|_4^4 - \|g_n\|_2^4}{\|g_n\|_2^3} = \frac{2}{\pi}.$$

We shall also show that this is not the best possible answer to Littlewood's question. To do so, we consider the polynomials

$$h_n(z) = \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} e^{2\pi ijk/n}\, z^{nj+k} \quad \text{for integral } n \geq 1$$

of degree n^2-1, which have been studied by Turyn [18], among others.

Theorem 2. *We have*

$$\lim_{n\to\infty} \frac{\|h_n\|_4^4 - \|h_n\|_2^4}{\|h_n\|_2^3} = \frac{4}{\pi^2}.$$

This is the best known answer to Littlewood's question: there is no sequence of polynomials f_n with unimodular coefficients for which the limit of $(\|f_n\|_4^4 - \|f_n\|_2^4)/\|f_n\|_2^3$ is known to be less than $4/\pi^2$. It is an open question as to whether such a sequence of polynomials exists.

In the radar literature [10, Ch. 6], the sequences formed from the coefficients of g_n and h_n are called *Chu* and *Frank sequences*, respectively. Our results show that their merit factors grow like $(\pi/2)\sqrt{n}$ and $(\pi^2/4)\sqrt{n}$, respectively, which explains numerical results reported in [1].

2. Proof of Theorem 1

We begin with summarising known results (see [13, p. 371], for example). For a polynomial $f \in \mathbb{C}[z]$ with $f(z) = \sum_{k=0}^{d-1} a_k z^k$, we readily verify that

$$f(z)\overline{f(z^{-1})} = \sum_{u=-(d-1)}^{d-1} c_u z^u,$$

where

$$c_u = \sum_{0\leq j, j+u<d} a_j \overline{a_{j+u}}. \tag{4}$$

The numbers c_u satisfy $c_u = \overline{c_{-u}}$. Hence

$$\|f\|_4^4 = \frac{1}{2\pi}\int_0^{2\pi} \left(f(e^{i\theta})\overline{f(e^{i\theta})}\right)^2 d\theta = c_0^2 + 2\sum_{u=1}^{d-1}|c_u|^2. \tag{5}$$

Lemma 3. *For each $n \geq 1$, we have*

$$\|g_n\|_4^4 = n^2 - \epsilon_n + 4\sum_{1\leq u\leq n/2}\left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right)^2, \tag{6}$$

where $\epsilon_n = 2$ for $n \equiv 2 \pmod 4$ and $\epsilon_n = 0$ otherwise.

Proof. For $f = g_n$, elementary manipulations reveal that the numbers c_u in (4) satisfy

$$|c_u| = \left|\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right|$$

for $1 \le u \le n-1$. The desired result then follows from (5) after noting that $c_0 = n$ and $|c_u| = |c_{n-u}|$ for $1 \le u \le n-1$ and $2|c_{n/2}| = \epsilon_n$ for even n. □

We now prove Theorem 1 by finding an asymptotic evaluation of the sum on the right hand side of (6).

Let x be a real number satisfying $0 < x \le \pi/2$. From the inequality $x - x^3/6 \le \sin x \le x$ we see that

$$0 < \frac{1}{(\sin x)^2} - \frac{1}{x^2} < 1,$$

and therefore

$$\left|\sum_{1\le u\le n/2}\left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right)^2 - \sum_{1\le u\le n/2}\left(\frac{\sin(\pi u^2/n)}{\pi u/n}\right)^2\right| < \frac{n}{2}.$$

Thus, defining the function $r : \mathbb{R} \to \mathbb{R}$ by

$$r(x) = \left(\frac{\sin(\pi x^2/n)}{\pi x/n}\right)^2,$$

the theorem is proved by showing that

$$\lim_{n\to\infty}\frac{1}{n^{3/2}}\sum_{1\le u\le n/2} r(u) = \frac{1}{2\pi}. \tag{7}$$

It is consequence of the Euler-Maclaurin formula [16, Theorem B.5] that, for real numbers a and b with $a < b$, the expression

$$\left|\sum_{a<u\le b} r(u) - \int_a^b r(x)\,dx\right|$$

is at most

$$\frac{1}{2}\Big(|r(a)| + |r(b)|\Big) + \frac{1}{12}\left(|r'(a)| + |r'(b)| + \int_a^b |r''(x)|\,dx\right).$$

We take $b = n/2$ and let a tend to zero. Elementary calculus shows that

$$|r(n/2)| \le \frac{4}{\pi^2}, \quad |r'(n/2)| \le \frac{8}{\pi} + \frac{16}{n\pi^2}, \quad \lim_{a\to 0} r(a) = \lim_{a\to 0} r'(a) = 0,$$

and $|r''(x)| \le 34$ for all real x. Therefore

$$\left|\sum_{1\le u\le n/2} r(u) - \int_0^{n/2} r(x)\,dx\right| \le \frac{2}{\pi^2} + \frac{2}{3\pi} + \frac{4}{3n\pi^2} + \frac{17n}{12},$$

and so

$$\lim_{n\to\infty}\frac{1}{n^{3/2}}\sum_{1\le u\le n/2} r(u) = \lim_{n\to\infty}\frac{1}{n^{3/2}}\int_0^{n/2} r(x)\,dx,$$

provided that both limits exist. Substituting $y = \pi x^2/n$, we see that this last expression equals

$$\lim_{n\to\infty}\frac{1}{2\pi^{3/2}}\int_0^{\pi n/4}\frac{(\sin y)^2}{y^{3/2}}\,dy = \frac{1}{2\pi^{3/2}}\int_0^{\infty}\frac{(\sin y)^2}{y^{3/2}}\,dy.$$

This establishes (7), and so completes the proof, since

$$\int_0^{\infty}\frac{(\sin y)^2}{y^{3/2}}\,dy = \sqrt{\pi} \tag{8}$$

(see Gradshteyn and Ryzhik [7, 3.823]).

For completeness, we sketch a proof of the identity (8). To do so, we readily verify that

$$\frac{\Gamma(3/2)}{y^{3/2}} = \int_0^{\infty} e^{-yt}\sqrt{t}\,dt \quad \text{for } y > 0,$$

which together with $\Gamma(3/2) = \sqrt{\pi}/2$ yields

$$\int_0^{\infty}\frac{(\sin y)^2}{y^{3/2}}\,dy = \frac{2}{\sqrt{\pi}}\int_0^{\infty}\int_0^{\infty} e^{-yt}\sqrt{t}\,(\sin y)^2\,dt\,dy.$$

Since the integrand on the right hand side is nonnegative, we can interchange the order of integration by Tonelli's theorem. The integral therefore equals

$$\frac{2}{\sqrt{\pi}}\int_0^{\infty}\sqrt{t}\int_0^{\infty} e^{-yt}\,(\sin y)^2\,dy\,dt = \frac{2}{\sqrt{\pi}}\int_0^{\infty}\frac{2\sqrt{t}}{t^3+4t}\,dt = \sqrt{\pi}.$$

The inner integral on the left hand side is just the Laplace transform of $(\sin y)^2$, while the integral on the right hand side can be evaluated by first substituting $t = x^2$ (which makes the integrand rational) and then using standard techniques.

3. Proof of Theorem 2

We begin with proving a counterpart of Lemma 3 for the polynomials h_n.

Lemma 4. *For each $n \ge 1$, we have*

$$\|h_n\|_4^4 = n^4 - \gamma_n + 8n\sum_{1\le v\le n/2}\sum_{1\le k\le v}\left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)}\right)^2,$$

where

$$\gamma_n = \begin{cases} 3n^2 & \text{for even } n \\ 2n^2 - 2n & \text{for odd } n. \end{cases}$$

Proof. Write $\zeta = e^{2\pi i/n}$. Then, for $f = h_n$, the numbers c_u in (4) are given by (see also Turyn [18])

$$c_{nu+v} = \sum_{j=0}^{n-u-1} \sum_{k=0}^{n-v-1} \zeta^{jk-(j+u)(k+v)} + \sum_{j=0}^{n-u-2} \sum_{k=n-v}^{n-1} \zeta^{jk-(j+u+1)(k+v)}$$

for $0 \le u, v < n$. Rearrange and use $\sum_{k=0}^{n-1} \zeta^{k(u+1)} = 0$ for $n \nmid u+1$ (note that the second term is zero for $u+1 = n$) to see that

$$\overline{c_{nu+v}} = \zeta^{uv} \sum_{k=0}^{n-v-1} \zeta^{ku} \sum_{j=0}^{n-u-1} \zeta^{jv} - \zeta^{(u+1)v} \sum_{k=0}^{n-v-1} \zeta^{k(u+1)} \sum_{j=0}^{n-u-2} \zeta^{jv} \tag{9}$$

for $0 \le u, v < n$. Evaluation of the sums over j gives, for $0 \le u < n$ and $0 < v < n$,

$$\begin{aligned} \overline{c_{nu+v}} &= \frac{1}{\zeta^v - 1} \sum_{k=0}^{n-v-1} \big(\zeta^{ku}(1-\zeta^{uv}) - \zeta^{k(u+1)}(1-\zeta^{(u+1)v})\big) \\ &= \frac{1}{\zeta^v - 1} \sum_{k=0}^{n-v-1} \big[\zeta^{(k+v)u}(\zeta^{k+v}-1) - \zeta^{ku}(\zeta^k - 1)\big]. \end{aligned}$$

We can write this as

$$\left(\sum_{k=v}^{n-1} - \sum_{k=0}^{n-v-1}\right) \zeta^{ku} \frac{\zeta^k - 1}{\zeta^v - 1},$$

from which we see that

$$\sum_{u=0}^{n-1} |c_{nu+v}|^2 = n\left(\sum_{k=v}^{n-1} + \sum_{k=0}^{n-v-1} - \sum_{k=v}^{n-v-1} - \sum_{k=v}^{n-v-1}\right) \left|\frac{\zeta^k - 1}{\zeta^v - 1}\right|^2 \tag{10}$$

for $0 < v < n$. For $0 < v < n/2$ all of these sums are nonempty, so that after grouping them together we have, for $0 < v < n/2$,

$$\begin{aligned} \sum_{u=0}^{n-1} |c_{nu+v}|^2 &= n\left(\sum_{k=n-v}^{n-1} + \sum_{k=0}^{v-1}\right) \left|\frac{\zeta^k - 1}{\zeta^v - 1}\right|^2 \\ &= 2n \sum_{k=0}^{v} \left|\frac{\zeta^k - 1}{\zeta^v - 1}\right|^2 - n \\ &= 2n \sum_{k=1}^{v} \left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)}\right)^2 - n. \end{aligned} \tag{11}$$

Using (9) we readily verify that $c_{nu} = 0$ for $u \ne 0$. Therefore, since $c_0 = n^2$ trivially, we have from (5)

$$\|h_n\|_4^4 = n^4 + 2 \sum_{v=1}^{n-1} \sum_{u=0}^{n-1} |c_{nu+v}|^2. \tag{12}$$

We also have

$$c_{nu+v} = -\zeta^v \, c_{nu+n-v} \quad \text{for } (u,v) \neq (0,0), \tag{13}$$

which also follows from (9) using the identities

$$\sum_{k=0}^{v-1} \zeta^{kw} = -\zeta^{wv} \sum_{k=0}^{n-v-1} \zeta^{kw}$$

for integers w and v satisfying $n \nmid w$ and $0 \le v < n$ and

$$\sum_{j=0}^{n-w-1} \zeta^{-jv} = \zeta^{(w+1)v} \sum_{j=0}^{n-w-1} \zeta^{jv}$$

for integers w and v.

Now, for odd n, we have from (12) and (13)

$$\|h_n\|_4^4 = n^4 + 4 \sum_{v=1}^{(n-1)/2} \sum_{u=0}^{n-1} |c_{nu+v}|^2$$

and the desired result follows from (11). Similarly, for even n, we have

$$\|h_n\|_4^4 = n^4 + 4 \sum_{v=1}^{n/2-1} \sum_{u=0}^{n-1} |c_{nu+v}|^2 + 2 \sum_{u=0}^{n-1} |c_{nu+n/2}|^2.$$

Using (10), we find that

$$2 \sum_{u=0}^{n-1} |c_{nu+n/2}|^2 = \frac{n}{2} \sum_{k=0}^{n-1} |\zeta^k - 1|^2 = n^2,$$

and therefore, by (11),

$$\|h_n\|_4^4 = n^4 - n^2 + 4n + 8n \sum_{v=1}^{n/2-1} \sum_{k=1}^{v} \left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)} \right)^2.$$

To obtain the desired expression in the lemma for even n, we extend the summation over v to $n/2$ and subtract the correction term

$$8n \sum_{k=1}^{n/2} \big(\sin(\pi k/n) \big)^2 = n \sum_{k=0}^{n-1} |\zeta^k - 1|^2 + 4n = 2n^2 + 4n. \qquad \square$$

In order to prove Theorem 2, we invoke Lemma 4 and show that

$$8n \sum_{1 \le v \le n/2} \sum_{1 \le k \le v} \left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)} \right)^2 = \frac{4}{\pi^2} n^3 + O(n^2). \tag{14}$$

To do so, we make repeated use of the following elementary bound, which is also a simple consequence of the Euler-Maclaurin formula [16, Theorem B.5].

Let $r : \mathbb{R} \to \mathbb{R}$ be a differentiable function and let a and b be real numbers with $a < b$. Then

$$\left| \sum_{a<k\le b} r(k) - \int_a^b r(x)\,dx \right| \le \frac{1}{2}\Big(|r(a)| + |r(b)| + \int_a^b \big|r'(x)\big|\,dx \Big). \tag{15}$$

We first take $r(x) = (\sin(\pi x/n))^2$ and $(a, b) = (0, v)$, so that for $1 \le v \le n/2$, we have

$$\begin{aligned}\sum_{k=1}^{v} (\sin(\pi k/n))^2 &= \int_0^v (\sin(\pi x/n))^2 dx + O(1)\\ &= \frac{n}{\pi}\int_0^{\pi v/n} (\sin y)^2\,dy + O(1)\\ &= \frac{n}{2\pi}\Big(\pi v/n - \sin(\pi v/n)\cos(\pi v/n)\Big) + O(1).\end{aligned}$$

Letting

$$p(y) = \frac{y - \sin y \cos y}{(\sin y)^2},$$

we then have

$$\sum_{1\le v\le n/2} \sum_{1\le k\le v} \left(\frac{\sin(\pi k/n)}{\sin(\pi v/n)}\right)^2 = \frac{n}{2\pi} \sum_{1\le v\le n/2} p(\pi v/n) + O(n). \tag{16}$$

We now apply (15) with $r(x) = p(\pi x/n)$ and $b = n/2$ and let a tend to zero. We have

$$p'(y) = 2 - \frac{2(y - \sin y \cos y)\cos y}{(\sin y)^3}$$

from which, using $x - x^3/6 \le \sin x \le x$ and $1 - x^2/2 \le \cos x \le 1$ together with elementary calculus, we find that

$$-3 < p'(y) \le 2 \quad \text{for } 0 < y \le \pi/2.$$

Hence $|r'(x)| < 3\pi/n$ for $0 < x \le n/2$. Since we also have $r(n/2) = \pi/2$ and $\lim_{a\to 0} r(a) = 0$, we find from (15) that (16) equals

$$\frac{n}{2\pi}\int_0^{n/2} p(\pi x/n)dx + O(n) = \frac{n^2}{2\pi^2}\int_0^{\pi/2} p(y)dy + O(n).$$

The desired result (14) is then established by showing that

$$\int_0^{\pi/2} p(y)dy = 1. \tag{17}$$

By differentiation we readily verify that

$$\int \frac{y - \sin y \cos y}{(\sin y)^2}\,dy = -\frac{y}{\tan y} + C$$

for some arbitrary constant C and (17) follows by application of l'Hôpital's rule.

References

[1] M. Antweiler and L. Bömer. Merit factor of Chu and Frank sequences. *IEE Electron. Lett.*, 46(25):2068–2070, 1990.

[2] P. Borwein. *Computational Excursions in Analysis and Number Theory*. CMS Books in Mathematics. Springer-Verlag, New York, NY, 2002.

[3] P. Borwein and K.-K. S. Choi. Merit factors of character polynomials. *J. London Math. Soc.*, 61:706–720, 2000.

[4] P. Borwein and K.-K. S. Choi. Personal communication, 2012.

[5] T. Erdélyi. Polynomials with Littlewood-type coefficient constraints. In *Approximation theory, X (St. Louis, MO, 2001)*, Innov. Appl. Math., pages 153–196. Vanderbilt Univ. Press, Nashville, TN, 2002.

[6] P. Erdős. An inequality for the maximum of trigonometric polynomials. *Ann. Polon. Math.*, 12:151–154, 1962.

[7] I. S. Gradshteyn and I. M. Ryzhik. *Table of integrals, series, and products*. Elsevier/Academic Press, Amsterdam, 7th edition, 2007.

[8] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Littlewood polynomials with small L^4 norm, 2012. arXiv:1205.0260v1 [math.NT].

[9] J. P. Kahane. Sur les polynômes à coefficients unimodulaires. *Bull. London Math. Soc.*, 12:321–342, 1980.

[10] N. Levanon and E. Mozeson. *Radar signals*. Wiley-Interscience, 1st edition, 2004.

[11] J. E. Littlewood. On the mean values of certain trigonometric polynomials. *J. London Math. Soc.*, 36:307–334, 1961.

[12] J. E. Littlewood. On the mean values of certain trigonometric polynomials II. *Illinois J. Math.*, 6:1–39, 1962.

[13] J. E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$. *J. London Math. Soc.*, 41:367–376, 1966.

[14] J. E. Littlewood. *Some Problems in Real and Complex Analysis*. Heath Mathematical Monographs. D. C. Heath and Company, Lexington, MA, 1968.

[15] I. D. Mercer. Bounds on asymptotic merit factor of Chu sequences, 2012. `http://www.math.udel.edu/∼idmercer/publications.html`.

[16] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[17] 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 International Zurich Seminar on Broadband Communications*, pages 279–286. IEEE, 2000.

[18] R. Turyn. The correlation function of a sequences of roots of 1. *IEEE Trans. Inf. Theory*, 13(3):524–525, 1967.

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany.

E-mail address: `kaiuwe.schmidt@ovgu.de`

THE CORRELATION MEASURES OF FINITE SEQUENCES: LIMITING DISTRIBUTIONS AND MINIMUM VALUES

KAI-UWE SCHMIDT

Abstract. Three measures of pseudorandomness of finite binary sequences were introduced by Mauduit and Sárközy in 1997 and have been studied extensively since then: the normality measure, the well-distribution measure, and the correlation measure of order r. Our main result is that the correlation measure of order r for random binary sequences converges strongly, and so has a limiting distribution. This solves a problem due to Alon, Kohayakawa, Mauduit, Moreira, and Rödl. We also show that the best known lower bounds for the minimum values of the correlation measures are simple consequences of a celebrated result due to Welch, concerning the maximum nontrivial scalar products over a set of vectors.

1. Introduction and main results

We consider finite binary sequences, namely elements A_n of $\{-1,1\}^n$. Mauduit and Sárközy [11] introduced three measures of pseudorandomness for finite binary sequences: the *well distribution measure* $W(A_n)$, the *normality measure* $\mathcal{N}(A_n)$, and the *r-th order correlation measure* $C_r(A_n)$. These measures have been studied extensively (see [11], [8], [4], [5], [1], [3], [2], for example). Finite binary sequences for which these measures are small are considered to possess a high 'level of randomness'.

In this paper, we are concerned with the correlation measures of finite binary sequences. Let $A_n = (a_1, a_2, \dots, a_n)$ be an element of $\{-1,1\}^n$. For $2 \le r \le n$, the *r-th order correlation measure* of A_n is defined as

$$C_r(A_n) = \max_{0\le u_1<u_2<\cdots<u_r<n} \max_{1\le m\le n-u_r} \left| \sum_{j=1}^{m} a_{j+u_1} a_{j+u_2} \cdots a_{j+u_r} \right|.$$

Following earlier work by Cassaigne, Mauduit, and Sárközy [8], Alon, Kohayakawa, Mauduit, Moreira, and Rödl [5] studied the behaviour of $W(A_n)$, $\mathcal{N}(A_n)$, and $C_r(A_n)$ when A_n is drawn at random from $\{-1,1\}^n$, equipped with the uniform probability measure. They posed the following problem.

Date: 10 January 2014.

2010 *Mathematics Subject Classification.* Primary: 11K45; Secondary 60C05, 68R15.

Problem A ([5, Problem 33])**.** Investigate the existence of the limiting distributions of

$$\left\{\frac{W(A_n)}{\sqrt{n}}\right\}_{n\ge 1} \quad \text{and} \quad \left\{\frac{\mathcal{N}(A_n)}{\sqrt{n}}\right\}_{n\ge 1}$$

and

$$\left\{\frac{C_r(A_n)}{\sqrt{n\log\binom{n}{r}}}\right\}_{n\ge r}. \tag{1}$$

Investigate these distributions.

The first two instances of Problem A have been solved recently: Aistleitner [3], [2] proved that the limiting distributions of $W(A_n)/\sqrt{n}$ and of $\mathcal{N}(A_n)/\sqrt{n}$ exist. Moreover, a tail characterisation of the limiting distribution of $W(A_n)/\sqrt{n}$ is provided in [3]. It is known that, if (1) has a limiting distribution, then it is a Dirac measure [5, Theorem 3]. We shall resolve the third instance of Problem A by proving strong convergence of (1). To do so, we consider the set Ω of infinite sequences of elements -1 or 1 and endow Ω in the standard way with the probability measure defined by

$$\Pr\big[(a_1,a_2,\dots)\in\Omega : a_1=c_1,a_2=c_2,\dots,a_n=c_n\big]=2^{-n} \tag{2}$$

for all $(c_1,c_2,\dots,c_n)\in\{-1,1\}^n$.

Theorem 1.1. *Let $(a_1,a_2,\dots)$ be drawn from Ω, equipped with the probability measure defined by* (2)*, and write $A_n=(a_1,a_2,\dots,a_n)$. Then, as $n\to\infty$,*

$$\frac{C_r(A_n)}{\sqrt{2n\log\binom{n}{r-1}}}\to 1 \quad \textit{almost surely.}$$

Alon, Kohayakawa, Mauduit, Moreira, and Rödl [5] also proved a result on the asymptotic order of $C_r(A_n)$ that holds uniformly for a large range of r.

Theorem B ([5, Theorem 2])**.** Let A_n be drawn uniformly at random from $\{-1,1\}^n$. Then the probability that

$$\frac{2}{5}\sqrt{n\log\binom{n}{r}}<C_r(A_n)<\sqrt{\left(2+\frac{\log\log n}{\log n}\right)n\log\left(n\binom{n}{r}\right)}$$

holds for all r satisfying $2\le r\le n/4$ tends to 1 as $n\to\infty$.

We improve the upper bound in Theorem B as follows.

Theorem 1.2. *Let A_n be drawn uniformly at random from $\{-1,1\}^n$ and let $\epsilon>0$ be real. Then, as $n\to\infty$,*

$$\Pr\left[C_r(A_n)\le(1+\epsilon)\sqrt{2n\log\tbinom{n}{r-1}} \quad \textit{for all } r \textit{ satisfying } 2\le r\le n\right]\to 1.$$

In view of Theorem 1.1, the bound in Theorem 1.2 is essentially best possible. We also note that Theorem 1.2 gives the currently strongest existence result. (The computation of the asymptotic behaviour of the correlation measures of individual binary sequences is a notoriously difficult problem and, in the light of Theorem 1.1, the currently known results tend to be unsatisfying, see for example [11, Theorem 1].)

We shall prove Theorem 1.2 in Section 2. In Section 3, we shall determine the limit of the expected value of (1) (Proposition 3.1). We shall then use this result in Section 4 to deduce Theorem 1.1.

We now turn to lower bounds for $C_r(A_n)$. It is known that

$$\min_{A_n \in \{-1,1\}^n} C_r(A_n) = 1 \quad \text{for odd } r,$$

which arises from the alternating sequence $(1, -1, 1, -1, \dots)$. Therefore, interesting results can only be expected for even r. Indeed the following result was established by Alon, Kohayakawa, Mauduit, Moreira, and Rödl [4].

Theorem C ([4, Theorem 1.1])**.** Let r and n be positive integers with $r \le n/2$. Then

$$C_{2r}(A_n) > \sqrt{\frac{1}{2}\left\lfloor \frac{n}{2r+1} \right\rfloor}$$

for all $A_n \in \{-1, 1\}^n$.

Theorem C gives an affirmative answer to a problem due to Cassaigne, Mauduit, and Sárközy [8, Problem 2], which was suspected to be 'really difficult' in [8, p. 109]. While the proof of Theorem C in [4] is quite involved, we shall show that Theorem C is a simple consequence of the so-called Welch bound [16]. This bound is an elementary result on the maximum nontrivial scalar products over a set of vectors.

We also establish, as another consequence of the Welch bound, the following result, which was proved in [4] without an explicit lower bound for c_k.

Theorem 1.3. *There exists a sequence of real numbers c_k, satisfying $c_k > 1/9$ for each $k \ge 3$ and $c_k \to 1/\sqrt{6e}$ as $k \to \infty$, such that for all positive integers s and n with $s \le n/3$, we have*

$$\max\left\{C_2(A_n), C_4(A_n), \dots, C_{2s}(A_n)\right\} > c_n\sqrt{sn}$$

for all $A_n \in \{-1, 1\}^n$.

Theorems C and 1.3 will be proved in Section 5.

2. Typical upper bound

In this section, we shall prove Theorem 1.2. The key ingredient in the proof will be an estimate for the range of a random walk. Let $X_1, \dots, X_n$

be independent random variables, each taking the values -1 or 1, each with probability 1/2. Define the random variable

$$R_n = \max_{1\le m_1\le m_2\le n} \left| \sum_{j=m_1}^{m_2} X_j \right|, \tag{3}$$

which is called the *range* of the random walk with steps $X_1, X_2, \ldots$.

We begin with a minor generalisation of a lemma due to Aistleitner [3, Lemma 2.3].

Lemma 2.1. *Let p be a nonnegative integer and let n be an integer of the form*

$$j2^m, \text{ where } j, m \in \mathbb{Z},\ 2^p < j \le 2^{p+1}, \text{ and } m \ge 1.$$

Then, for $\lambda > 2\sqrt{n}$,

$$\Pr\Big[R_n > \lambda(1 + 12\cdot 2^{-p/2})\Big] \le 2^{2p+4} \exp\bigg(-\frac{\lambda^2}{2n}\bigg).$$

Aistleitner's lemma [3, Lemma 2.3] is obtained by setting $p = 10$ in Lemma 2.1. The general version can be proved by applying obvious modifications to the proof of [3, Lemma 2.3], which is proved using a dyadic decomposition technique. (Aistleitner's lemma has the additional assumption that n is sufficiently large, which however is not required in the proof.)

We now proceed similarly as in [3] and prove the following lemma, which holds for general n.

Lemma 2.2. *Let $\delta > 0$ be real. Then, there exists a constant $n_0 = n_0(\delta)$, such that for all $n \ge n_0$ and all $\lambda > 2\sqrt{n}$,*

$$\Pr\Big[R_n > \lambda(1+\delta)\Big] \le (\log n) \exp\bigg(-\frac{\lambda^2}{2n}\bigg).$$

Proof. Let p be a positive integer and let $\hat{n}$ be the smallest integer that satisfies $\hat{n} \ge n$ and is of the form

$$j2^m, \text{ where } j, m \in \mathbb{Z},\ 2^p < j \le 2^{p+1}, \text{ and } m \ge 1.$$

We readily verify that

$$\frac{\hat{n}}{n} \le 1 + \frac{1}{2^p} \quad \text{for } n \ge 2^{p+1}. \tag{4}$$

Let $n \ge 2^{p+1}$ and $\lambda > 2\sqrt{n}$, so that $\lambda\sqrt{1+2^{-p}} > 2\sqrt{\hat{n}}$. Then

$$\begin{aligned}
\Pr\Big[R_n > \lambda(1 + 12\cdot 2^{-p/2})\sqrt{1+2^{-p}}\Big] &\le \Pr\Big[R_{\hat{n}} > \lambda(1 + 12\cdot 2^{-p/2})\sqrt{1+2^{-p}}\Big] \\
&\le 2^{2p+4} \exp\bigg(-\frac{\lambda^2(1+2^{-p})}{2\hat{n}}\bigg) \\
&\le 2^{2p+4} \exp\bigg(-\frac{\lambda^2}{2n}\bigg),
\end{aligned}$$

by Lemma 2.1 and (4). For $n > 2$, we take $p = p(n) = \lfloor \frac{1}{2} \log\log n \rfloor$, so that $n \geq 2^{p+1}$. Moreover

$$(1 + 12 \cdot 2^{-p/2})\sqrt{1 + 2^{-p}} \leq 1 + \delta$$

and $2^{2p+4} \leq \log n$ for all $n \geq n_0$, where n_0 depends only on δ. This completes the proof. □

Before proving Theorem 1.2, we record the following elementary, albeit very useful, fact.

Lemma 2.3. *Let $X_1, X_2, \ldots, X_n$ be mutually independent random variables, each taking each of the values -1 and 1 with probability $1/2$ and let $u_1, \ldots, u_r$ be integers satisfying*

$$0 \leq u_1 < u_2 < \cdots < u_r < n.$$

Then the $n - u_r$ products

$$X_{1+u_1}X_{1+u_2}\cdots X_{1+u_r}, \ldots, X_{n-u_r+u_1}X_{n-u_r+u_2}\cdots X_n$$

are mutually independent.

For $r = 2$, a formal proof of Lemma 2.3 is provided by Mercer [13, Proposition 1.1].

We now give a proof of Theorem 1.2, in which and the remainder of this paper we make repeated use of the elementary bound

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k \quad \text{for } k, n \in \mathbb{Z} \text{ satisfying } 1 \leq k \leq n. \tag{5}$$

Proof of Theorem 1.2. Write $A_n = (a_1, a_2, \ldots, a_n)$ and notice that $C_r(A_n)$ can be rewritten as

$$C_r(A_n) = \max_{0<u_2<\cdots<u_r<n} \max_{1\leq m_1\leq m_2\leq n-u_r} \left| \sum_{j=m_1}^{m_2} a_j a_{j+u_2}\cdots a_{j+u_r} \right|. \tag{6}$$

Let r be an integer satisfying $2 \leq r \leq n$ and let $u_2, u_3, \ldots, u_r$ be integers satisfying

$$0 < u_2 < \cdots < u_r < n. \tag{7}$$

Write

$$\lambda = \sqrt{2n \log \tbinom{n}{r-1}}.$$

Then, in view of Lemma 2.3, the probability

$$\Pr\left[\max_{1\leq m_1\leq m_2\leq n-u_r} \left| \sum_{j=m_1}^{m_2} a_j a_{j+u_2}\cdots a_{j+u_r} \right| > \lambda(1+\epsilon) \right] \tag{8}$$

is at most $\Pr[R_n > \lambda(1+\epsilon)]$ with R_n defined as in (3). Write $1 + \epsilon = \sqrt{1+\gamma}(1+\delta)$ for some $\gamma, \delta > 0$. By Lemma 2.2, there is a constant n_0,

depending only on δ, such that for all $n \geq n_0$, the probability (8) is at most

$$(\log n) \exp\left(- \frac{\lambda^2(1+\gamma)}{2n} \right) = \frac{\log n}{\binom{n}{r-1}^{1+\gamma}}.$$

Summing over all possible tuples $(u_2, u_3, \dots, u_r)$ satisfying (7), we see from (6) that, for all $n \geq n_0$,

$$\begin{aligned} \Pr\left[C_r(A_n) > \lambda(1+\epsilon)\right] &\leq \frac{(\log n)\binom{n-1}{r-1}}{\binom{n}{r-1}^{1+\gamma}} \\ &< \frac{\log n}{\binom{n}{r-1}^{\gamma}}. \end{aligned} \tag{9}$$

To prove the theorem, it is enough to show that, as $n \to \infty$,

$$\sum_{r=2}^{n} \Pr\left[C_r(A_n) > \lambda(1+\epsilon)\right] \to 0.$$

From (9), for $n \geq n_0$, the left hand side is at most

$$\sum_{k=1}^{n-1} \frac{\log n}{\binom{n}{k}^{\gamma}}.$$

Let m be an integer such that $m\gamma > 1$. Then, for $n \geq m$, this last expression is at most

$$\begin{aligned} 2\sum_{k=1}^{m-1} \frac{\log n}{\binom{n}{k}^{\gamma}} + 2\sum_{k=m}^{\lfloor n/2 \rfloor} \frac{\log n}{\binom{n}{k}^{\gamma}} &\leq \frac{2m\log n}{n^{\gamma}} + \frac{n\log n}{\binom{n}{m}^{\gamma}} \\ &\leq \frac{2m\log n}{n^{\gamma}} + \frac{m^{m\gamma}\log n}{n^{m\gamma-1}}, \end{aligned}$$

using (5). Since $\gamma > 0$ and $m\gamma > 1$, the right hand side tends to zero as $n \to \infty$, as required. □

3. Asymptotic expected value

In this section, we prove the following result, which is a key step in the proof of Theorem 1.1.

Proposition 3.1. *Let A_n be drawn uniformly at random from $\{-1,1\}^n$. Then, as $n \to \infty$,*

$$\frac{\mathrm{E}\left[C_r(A_n)\right]}{\sqrt{2n\log\binom{n}{r-1}}} \to 1.$$

To prove this proposition, we make repeated use of the following lemma, which follows from well known results on concentration of probability measures (see McDiarmid [12], for example).

Lemma 3.2 ([5, Inequality (99)])**.** *Let A_n be drawn uniformly at random from $\{-1,1\}^n$. Then, for $\theta \geq 0$,*

$$\Pr\Big[\big|C_r(A_n) - \mathrm{E}[C_r(A_n)]\big| \geq \theta\Big] \leq 2\exp\bigg(-\frac{\theta^2}{2r^2n}\bigg).$$

By combining Lemma 3.2 and Theorem 1.2, it is readily verified that

$$\limsup_{n\to\infty} \frac{\mathrm{E}\left[C_r(A_n)\right]}{\sqrt{2n\log\binom{n}{r-1}}} \leq 1. \tag{10}$$

In studying a problem that is related to the second order correlation measure of finite binary sequences, the author proved in [14] that

$$\liminf_{n\to\infty} \frac{\mathrm{E}\left[C_2(A_n)\right]}{\sqrt{2n\log n}} \geq 1,$$

which proves Proposition 3.1 for $r = 2$. Our proof of the general case is also based on the approach of [14].

Let $A_n = (a_1, a_2 \ldots, a_n)$ be an element of $\{-1,1\}^n$ and, for integers $u_2, \ldots, u_r$ satisfying

$$0 < u_2 < u_3 < \cdots < u_r < n,$$

define

$$S_{u_2,\ldots,u_r}(A_n) = \sum_{j=1}^{n-u_r} a_j a_{j+u_2} \cdots a_{j+u_r}.$$

The key ingredients to the proof of Proposition 3.1 are the following two lemmas on $S_{u_2,\ldots,u_r}(A_n)$, which generalise [14, Proposition 2.1] and [14, Proposition 2.7], respectively, from $r = 2$ to general $r \geq 2$. These lemmas can be proved by modifying the arguments used in [14]. As the modifications are not always obvious, we include proofs at the end of this section.

Lemma 3.3. *Let A_n be drawn uniformly at random from $\{-1,1\}^n$ and let $r \geq 2$ be an integer. Then there exists a constant $n_0 = n_0(r)$, such that for all $n \geq n_0$ and all*

$$0 < u_2 < u_3 < \cdots < u_r \leq \frac{n}{\log n},$$

we have

$$\Pr\Big[|S_{u_2,\ldots,u_r}(A_n)| \geq \sqrt{2n\log\tbinom{n}{r-1}}\Big] \geq \frac{1}{5e^{r-2}\binom{n}{r-1}\sqrt{\log\binom{n}{r-1}}}. \tag{11}$$

Lemma 3.4. *Let A_n be drawn uniformly at random from $\{-1,1\}^n$, let $r \geq 2$ be an integer, and write*

$$\lambda = \sqrt{2n\log\tbinom{n}{r-1}}.$$

Then there exists a constant $n_0 = n_0(r)$, such that for all $n \ge n_0$ and all $(u_2, \dots, u_r) \ne (v_2, \dots, v_r)$,

$$\Pr\big[|S_{u_2,\dots,u_r}(A_n)| \ge \lambda \cap |S_{v_2,\dots,v_r}(A_n)| \ge \lambda\big] \le \frac{23}{\binom{n}{r-1}^2}. \tag{12}$$

We now prove Proposition 3.1.

Proof of Proposition 3.1. Let $\delta > 0$ and define the set

$$N(\delta) = \left\{ n \ge r : \frac{\mathrm{E}\big[C_r(A_n)\big]}{\sqrt{2n \log \binom{n}{r-1}}} < 1 - \delta \right\}. \tag{13}$$

We shall show that $N(\delta)$ has finite size for all choices of $\delta > 0$, which together with (10) proves the proposition. To do so, we define the set

$$W = \left\{ (u_2, u_3, \dots, u_r) \in \mathbb{Z}^{r-1} : 0 < u_2 < u_3 < \cdots < u_r \le \frac{n}{\log n} \right\}.$$

Since

$$C_r(A_n) \ge \max_{(u_2,\dots,u_r) \in W} \big|S_{u_2,\dots,u_r}(A_n)\big|,$$

we find by the inclusion-exclusion principle that, for all real λ,

$$\Pr\big[C_r(A_n) \ge \lambda\big] \ge \sum_{(u_2,\dots,u_r) \in W} \Pr\big[|S_{u_2,\dots,u_r}(A_n)| \ge \lambda\big]$$

$$- \frac{1}{2} \sum_{\substack{(u_2,\dots,u_r),(v_2,\dots,v_r) \in W \\ (u_2,\dots,u_r) \ne (v_2,\dots,v_r)}} \Pr\big[|S_{u_2,\dots,u_r}(A_n)| \ge \lambda \cap |S_{v_2,\dots,v_r}(A_n)| \ge \lambda\big].$$

Now take

$$\lambda = \sqrt{2n \log \tbinom{n}{r-1}}$$

and apply Lemmas 3.3 and 3.4 to get, for all sufficiently large n,

$$\Pr\big[C_r(A_n) \ge \lambda\big] \ge |W| \cdot \frac{1}{5e^{r-2}\binom{n}{r-1}\sqrt{\log \binom{n}{r-1}}} - \frac{|W|^2}{2} \cdot \frac{23}{\binom{n}{r-1}^2}. \tag{14}$$

We have

$$|W| = \binom{\lfloor n/\log n \rfloor}{r-1}$$

and by the elementary bounds (5) for binomial coefficients we find that, for all sufficiently large n,

$$|W| \le \left(\frac{en}{(r-1)\log n}\right)^{r-1} \le \left(\frac{e}{\log n}\right)^{r-1} \binom{n}{r-1}$$

and

$$|W| \ge \left(\frac{n}{2(r-1)\log n}\right)^{r-1} \ge \left(\frac{1}{2e \log n}\right)^{r-1} \binom{n}{r-1}.$$

Hence, from (14) we obtain, for all sufficiently large n,

$$\Pr\big[C_r(A_n) \geq \lambda\big] \geq \frac{1}{5e^{r-2}}\left(\frac{1}{2e\log n}\right)^{r-1}\frac{1}{\sqrt{r\log n}} - 12\left(\frac{e}{\log n}\right)^{2r-2}.$$

Since $r \geq 2$, the first term on the right hand side dominates, and so a crude estimate gives

$$\Pr\big[C_r(A_n) \geq \lambda\big] \geq \frac{1}{e^{3r}\sqrt{r}}\left(\frac{1}{\log n}\right)^{r-1/2} \tag{15}$$

for all sufficiently large n. By the definition (13) of $N(\delta)$, we have $\lambda > \mathrm{E}[C_r(A_n)]$ for all $n \in N(\delta)$, and thus find from Lemma 3.2 with $\theta = \lambda - \mathrm{E}[C_r(A_n)]$ that, for all $n \in N(\delta)$,

$$\Pr\big[C_r(A_n) \geq \lambda\big] \leq 2\exp\left(-\frac{(\lambda - \mathrm{E}[C_r(A_n)])^2}{2r^2 n}\right).$$

Comparison with (15) then gives, for all sufficiently large $n \in N(\delta)$,

$$\frac{1}{e^{3r}\sqrt{r}}\left(\frac{1}{\log n}\right)^{r-1/2} \leq 2\exp\left(-\frac{(\lambda - \mathrm{E}[C_r(A_n)])^2}{2r^2 n}\right),$$

or equivalently, since $\lambda > \mathrm{E}[C_r(A_n)]$ for all $n \in N(\delta)$,

$$\frac{\mathrm{E}[C_r(A_n)]}{\sqrt{2n\log\binom{n}{r-1}}} \geq 1 - \sqrt{\frac{r^2(r-1/2)\log\log n + r^2\log(2e^{3r}\sqrt{r})}{\log\binom{n}{r-1}}}.$$

Hence, by the definition (13) of $N(\delta)$, we see that $N(\delta)$ has finite size for all choices of $\delta > 0$, as required. □

In the remainder of this section, we provide proofs of Lemmas 3.3 and 3.4.

Proof of Lemma 3.3. We adopt the standard notation $x_n \sim y_n$ to mean that $x_n = y_n(1+o(1))$ as $n \to \infty$. By Lemma 2.3, $S_{u_2,\ldots,u_r}(A_n)$ is a sum of $n-u_r$ mutually independent random variables, each taking each of the values -1 and $+1$ with probability $1/2$. We use a normal approximation to estimate the tail of the distribution of $|S_{u_2,\ldots,u_r}(A_n)|$ (see Feller [9, Chapter VII, (6.7)], for example): If $\xi_n \to \infty$ in such a way that $\xi_n^3/\sqrt{n} \to 0$ as $n \to \infty$, then

$$\Pr\Big[\big|S_{u_2,\ldots,u_r}(A_n)\big| \geq \xi_n\sqrt{n-u_r}\Big] \sim \sqrt{\frac{2}{\pi}}\cdot\frac{1}{\xi_n}\,\exp\left(\frac{\xi_n^2}{2}\right).$$

Taking

$$\xi_n = \sqrt{\frac{2n}{n-u_r}\,\log\binom{n}{r-1}}$$

gives, since $\frac{n}{n-u_r} \sim 1$,

$$\Pr\Big[\big|S_{u_2,\dots,u_r}(A_n)\big| \ge \sqrt{2n\log\tbinom{n}{r-1}}\Big] \sim \frac{1}{\sqrt{\pi\log\tbinom{n}{r-1}}}\exp\bigg(-\frac{n}{n-u_r}\log\binom{n}{r-1}\bigg). \tag{16}$$

Using $u_r \le \frac{n}{\log n}$, we have

$$\exp\bigg(-\frac{n}{n-u_r}\log\binom{n}{r-1}\bigg) \ge \exp\bigg(-\frac{\log n}{\log n-1}\log\binom{n}{r-1}\bigg),$$

and then, since

$$\exp\bigg(-\frac{\log n}{\log n-1}\log\binom{n}{r-1}\bigg) \sim \frac{1}{e^{r-1}\binom{n}{r-1}}$$

and $e\sqrt{\pi} < 5$, we find from (16) that

$$\Pr\Big[\big|S_{u_2,\dots,u_r}(A_n)\big| \ge \sqrt{2n\log\tbinom{n}{r-1}}\Big] \ge \frac{1}{5e^{r-2}\binom{n}{r-1}\sqrt{\log\binom{n}{r-1}}}$$

for all sufficiently large n. □

To prove Lemma 3.4, it is convenient to use the following notation.

Definition 3.5. A tuple $(x_1,\dots,x_{2m})$ is *d-even* if there exists a permutation σ of $\{1,2,\dots,2m\}$ such that $x_{\sigma(2i-1)} = x_{\sigma(2i)}$ for each $i \in \{1,2,\dots,d\}$ and d is the largest integer with this property. An m-even tuple $(x_1,\dots,x_{2m})$ is just called *even*.

For example, $(1,3,1,4,3,4)$ is even, while $(2,1,1,2,1,3)$ is 2-even. In the next two lemmas we state two results about even tuples.

Recall that, for positive integer k, the double factorial

$$(2k-1)!! = \frac{(2k)!}{k!\,2^k} = (2k-1)(2k-3)\cdots 3\cdot 1$$

is the number of ways to arrange $2k$ objects into k unordered pairs. The following lemma is immediate.

Lemma 3.6 ([14, Lemma 2.4])**.** *Let m and q be positive integers. Then the number of even tuples in $\{1,\dots,m\}^{2q}$ is at most $(2q-1)!!\,m^q$.*

The following lemma generalises [14, Lemma 2.5].

Lemma 3.7. *Let n, q, and t be positive integers satisfying $0 \le t < q$ and let $u_2,\dots,u_r$ and $v_2,\dots,v_r$ be positive integers satisfying $(u_2,\dots,u_r) \ne (v_2,\dots,v_r)$. Write $I = \{1,\dots,2q\}$ and let S be the subset of $\{1,\dots,n\}^{4rq}$ containing all even elements*

$$(x_i, x_i+u_2,\dots,x_i+u_r, y_i, y_i+v_2,\dots,y_i+v_r)_{i\in I}$$

such that $(x_i)_{i\in I}$ is d-even for some $d < q-t$. Then

$$|S| \le (4rq-1)!!\, n^{2q-(t+1)/3}.$$

Proof. We will construct a set of tuples that contains S as a subset. For convenience write $u_1 = v_1 = 0$. Arrange the $4rq$ variables

$$x_i + u_k,\ y_i + v_k \quad \text{for } i \in I \text{ and } k \in \{1,2,\dots,r\} \tag{17}$$

into $2rq$ unordered pairs $(a_1,b_1),(a_2,b_2),\dots,(a_{2rq},b_{2rq})$ such that there are at most $q-t-1$ pairs (x_i,x_j). This can be done in at most $(4rq-1)!!$ ways. We formally set $a_i = b_i$ for all $i \in \{1,2,\dots,2rq\}$. If this assignment does not yield a contradiction, then we call the arrangement of (17) into $2rq$ pairs *consistent*. For example, if there are pairs of the form (x_i,y_j), $(x_i+u_2,y_j+v_2),\dots,(x_i+u_r,y_j+v_r)$, then the arrangement is not consistent since $(u_2,\dots,u_r) \ne (v_2,\dots,v_r)$ by assumption.

In each consistent arrangement, there are at most $q-t-1$ pairs of the form (x_i,x_j) and at most q pairs of the form (y_i,y_j), and so at most

$$q-t-1+q+\tfrac{1}{3}(2t+2) = 2q-\tfrac{1}{3}(t+1)$$

of the variables $x_1,\dots,x_{2q},y_1,\dots,y_{2q}$ can be chosen independently. We assign to each of these a value of $\{1,\dots,n\}$. In this way, we construct a set of at most $(4rq-1)!!\, n^{2q-(t+1)/3}$ tuples that contains S as a subset. □

The next lemma, whose proof is modelled on that of [14, Lemma 2.6], provides the key step in the proof of Lemma 3.4.

Lemma 3.8. *Let p and h be integers satisfying $0 \le h < p$ and let A_n be drawn uniformly at random from $\{-1,1\}^n$. Then, for $(u_2,\dots,u_r) \ne (v_2,\dots,v_r)$,*

$$\mathrm{E}\Big[\big(S_{u_2,\dots,u_r}(A_n)S_{v_2,\dots,v_r}(A_n)\big)^{2p}\Big] \le n^{2p}\big[(2p-1)!!\big]^2\left(1+\frac{(4rp)^{4rh}}{n^{1/3}}+\frac{(4rp)^{2rp}}{n^{(h+1)/3}}\right). \tag{18}$$

Proof. Write $A_n = (a_1,a_2,\dots,a_n)$. Expand to see that the left hand side of (18) equals

$$\sum_{i_1,\dots,i_{2p}=1}^{n-u_r}\ \sum_{j_1,\dots,j_{2p}=1}^{n-v_r} \mathrm{E}\big[a_{i_1}a_{i_1+u_2}\cdots a_{i_1+u_r}\cdots a_{i_{2p}}a_{i_{2p}+u_2}\cdots a_{i_{2p}+u_r} a_{j_1}a_{j_1+v_2}\cdots a_{j_1+v_r}\cdots a_{j_{2p}}a_{j_{2p}+v_2}\cdots a_{j_{2p}+v_r}\big]. \tag{19}$$

Write $I = \{1,2,\dots,2p\}$ and let T be the set containing all even tuples in $\{1,\dots,n\}^{4rp}$ of the form

$$(x_i, x_i+u_2,\dots,x_i+u_r, y_i, y_i+v_2,\dots,y_i+v_r)_{i\in I}. \tag{20}$$

Since $a_1,\dots,a_n$ are mutually independent, $\mathrm{E}[a_j] = 0$, and $a_j^2 = 1$ for all $j \in \{1,\dots,n\}$, we find from (19) that the left hand side of (18) is at most $|T|$. It remains to show that $|T|$ is at most the right hand side of (18).

We define the following subsets of T.

- T_1 contains all elements (20) of T such that $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ are even.
- T_2 contains all elements (20) of T such that $(x_i)_{i\in I}$ is d_1-even and $(y_i)_{i\in I}$ is d_2-even for some d_1 and d_2 satisfying $p-h \le d_1, d_2 \le p$, at least one of them strictly less than p.
- T_3 contains all elements (20) of T such that $(x_i)_{i\in I}$ or $(y_i)_{i\in I}$ is d-even for some $d < p-h$.

It is readily verified that T_1, T_2, and T_3 partition T. We now bound the cardinalities of T_1, T_2, and T_3.

The set T_1. Using Lemma 3.6 applied with $q = p$, we have

$$|T_1| \le \big[(2p-1)!!\big]^2 n^{2p}. \tag{21}$$

The set T_2. Consider an element (20) of T_2. Then there exist $(2p-2h)$-element subsets J and K of I such that $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even and

$$(x_i)_{i\in I\setminus J} \tag{22}$$

is not even (if $(x_i)_{i\in I\setminus J}$ were even, then $(y_i)_{i\in I\setminus K}$ would also be even, which contradicts the definition of the elements of T_2). Since $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even and the tuple (20) is even, we find that

$$(x_i, x_i+u_2, \dots, x_i+u_r, y_j, y_j+v_2, \dots, y_j+v_r)_{i\in I\setminus J,\, j\in I\setminus K} \tag{23}$$

is also even. There are $\binom{2p}{2h}$ subsets J and $\binom{2p}{2h}$ subsets K. By Lemma 3.6 applied with $q = p-h$, for each such J and K, there are at most $(2p-2h-1)!!\, n^{p-h}$ even tuples $(x_i)_{i\in J}$ satisfying $0 \le x_i < n$ for each $i \in J$ and at most $(2p-2h-1)!!\, n^{p-h}$ even tuples $(y_i)_{i\in K}$ satisfying $0 \le y_i < n$ for each $i \in K$. By Lemma 3.7 applied with $q = h$ and $t = 0$, the number of even tuples in $\{1,\dots,n\}^{4rh}$ of the form (23) such that the tuple in (22) is not even is at most $(4rh-1)!!\, n^{2h-1/3}$. Therefore,

$$\begin{aligned} |T_2| &\le (4rh-1)!!\, n^{2h-1/3} \Big[\tbinom{2p}{2h}(2p-2h-1)!!\, n^{p-h}\Big]^2 \\ &\le n^{2p-1/3}\big[(2p-1)!!\big]^2 (4rp)^{4rh}. \end{aligned} \tag{24}$$

The set T_3. By Lemma 3.7 applied with $q = p$ and $t = h$ and by symmetry, we have

$$|T_3| \le 2(4rp-1)!!\, n^{2p-(h+1)/3} \le n^{2p-(h+1)/3}(4rp)^{2rp}. \tag{25}$$

Now from (21), (24), and (25) we get an upper bound for $|T|$, from which we can deduce (18). □

We now prove Lemma 3.4.

Proof of Lemma 3.4. Let X_1 and X_2 be a random variables and let p be a positive integer. Then by Markov's inequality, for $\theta_1, \theta_2 > 0$,

$$\Pr\big[|X_1| \ge \theta_1 \cap |X_2| \ge \theta_2\big] \le \frac{\mathrm{E}\big[(X_1X_2)^{2p}\big]}{(\theta_1\theta_2)^{2p}}.$$

Let h be an integer satisfying $0 \le h < p$. Lemma 3.8 shows that the left hand side of (12) is at most

$$\frac{\big[(2p-1)!!\big]^2}{(2\log\binom{n}{r-1})^{2p}}\big[1 + K_1(n,p,h) + K_2(n,p,h)\big], \tag{26}$$

where

$$K_1(n,p,h) = n^{-1/3}\,(4rp)^{4rh},$$
$$K_2(n,p,h) = n^{-(h+1)/3}\,(4rp)^{2rp}.$$

We take $p = \lfloor \log\binom{n}{r-1}\rfloor$ and $h = \lfloor \alpha \log\log n\rfloor$ for some $\alpha > 0$, to be determined later, and show that (26) is at most $23/\binom{n}{r-1}^2$ for all sufficiently large n. Notice that $h < p$ for all sufficiently large n, as assumed. By Stirling's approximation

$$\sqrt{2\pi k}\,k^k e^{-k} \le k! \le \sqrt{3\pi k}\,k^k e^{-k},$$

we have

$$\frac{\big[(2p-1)!!\big]^2}{(2\log\binom{n}{r-1})^{2p}} \le \frac{3p^{2p}e^{-2p}}{(\log\binom{n}{r-1})^{2p}} \le \frac{3e^2}{\binom{n}{r-1}^2}.$$

Moreover

$$\begin{aligned} K_1(n,p,h) &\le K_1(n, r\log n, \alpha\log\log n)\\ &= n^{-\frac{1}{3}}\,n^{\frac{2\alpha\log\log n(\log r+\log\log n)}{\log n}}\\ &= O(n^{-\frac{1}{4}}) \end{aligned}$$

and

$$\begin{aligned} K_2(n,p,h) &\le K_2(n, r\log n, (\alpha-1)\log\log n)\\ &= n^{-\frac{1}{3}-(\frac{\alpha-1}{3}-2r^2)\log\log n+2r^2\log(4r^2)}\\ &= O(n^{-\log\log n}) \end{aligned}$$

by taking $\alpha = 10r^2$, say. □

4. Almost sure convergence

In this section we prove Theorem 1.1. We begin with the following standard result (see [6, Theorem A.1.1], for example).

Lemma 4.1. *Let $X_1, \dots, X_n$ be independent random variables, each taking the values -1 and 1, each with probability $1/2$. Then, for $\lambda \ge 0$,*

$$\Pr\left[\left|\sum_{j=1}^{n} X_j\right| > \lambda\right] \le 2\exp\left(-\frac{\lambda^2}{2n}\right).$$

Lemma 4.1 is used to deduce the following result.

Lemma 4.2. *Let $(a_1, a_2, \dots)$ be drawn from Ω, equipped with the probability measure defined by (2), and write $A_n = (a_1, a_2, \dots, a_n)$. Let $n_1, n_2, \dots$ be a strictly increasing sequence of integers greater than or equal to r. Then, almost surely,*

$$C_r(A_{n_{k+1}}) - C_r(A_{n_k}) \le \sqrt{10(n_{k+1}-n_k)\log\tbinom{n_{k+1}}{r-1}}$$

for all sufficiently large k.

Proof. Write

$$\lambda = \sqrt{10(n_{k+1}-n_k)\log\tbinom{n_{k+1}}{r-1}}. \tag{27}$$

If

$$C_r(A_{n_{k+1}}) - C_r(A_{n_k}) > \lambda, \tag{28}$$

then

$$\left| \sum_{j=\max(1,n_k-u_r+1)}^{m} a_{j+u_1} a_{j+u_2} \cdots a_{j+u_r} \right| > \lambda \tag{29}$$

for at least one tuple $(u_1, u_2, \dots, u_r)$ satisfying

$$0 \le u_1 < u_2 < \cdots < u_r < n_{k+1} \tag{30}$$

and at least one m satisfying

$$n_k - u_r + 1 \le m \le n_{k+1} - u_r. \tag{31}$$

Let $(u_1, u_2, \dots, u_r)$ be a tuple of integers satisfying (30) and let m be an integer satisfying (31). By Lemma 2.3, the sum in (29) is a sum of at most $n_{k+1} - n_k$ independent random variables, each taking each of the values 1 and -1 with probability $1/2$. Thus, by Lemma 4.1, the probability of (29) is at most

$$2\exp\left(-\frac{\lambda^2}{2(n_{k+1}-n_k)}\right) = 2\binom{n_{k+1}}{r-1}^{-5},$$

after substituting (27). Summing over all possible tuples $(u_1, u_2, \dots, u_r)$ and all possible m, the probability that (29) happens for some $(u_1, u_2, \dots, u_r)$ satisfying (30) and some integer m satisfying (31) is at most

$$2(n_{k+1}-n_k)\binom{n_{k+1}}{r}\binom{n_{k+1}}{r-1}^{-5}.$$

This is also an upper bound for the probability of (28), and so

$$\Pr\left[C_r(A_{n_{k+1}}) - C_r(A_{n_k}) > \lambda\right] \le 2(n_{k+1})^2\binom{n_{k+1}}{r-1}^{-4} \le \frac{2}{(n_{k+1})^2}.$$

Thus,

$$\sum_{k=1}^{\infty} \Pr\left[C_r(A_{n_{k+1}}) - C_r(A_{n_k}) > \lambda\right] \le \sum_{k=1}^{\infty} \frac{2}{(n_{k+1})^2} < \infty,$$

and the result follows from the Borel-Cantelli Lemma. □

We now prove Theorem 1.1.

Proof of Theorem 1.1. Write

$$\vartheta_n = \sqrt{2n \log \binom{n}{r-1}}$$

and let n_k be the smallest integer that is at least $e^{k^{1/2}}$. We first show that the theorem holds for the subsequence n_k, namely that, as $k \to \infty$,

$$\frac{C_r(A_{n_k})}{\vartheta_{n_k}} \to 1 \quad \text{almost surely.} \tag{32}$$

To do so, choose an $\epsilon > 0$ and observe that by the triangle inequality, the probability

$$\Pr\left[\left|\frac{C_r(A_n)}{\vartheta_n} - 1\right| > \epsilon\right]$$

is bounded from above by

$$\Pr\left[\left|\frac{C_r(A_n)}{\vartheta_n} - \frac{\mathrm{E}[C_r(A_n)]}{\vartheta_n}\right| > \tfrac{1}{2}\epsilon\right] + \Pr\left[\left|\frac{\mathrm{E}[C_r(A_n)]}{\vartheta_n} - 1\right| > \tfrac{1}{2}\epsilon\right].$$

By Proposition 3.1, the second probability equals zero for all sufficiently large n. The first probability can be bounded using Lemma 3.2, showing that

$$\Pr\left[\left|\frac{C_r(A_n)}{\vartheta_n} - 1\right| > \tfrac{1}{2}\epsilon\right] \le 2\exp\left(-\frac{\epsilon^2}{4r^2}\log\binom{n}{r-1}\right)$$

for all sufficiently large n. We can further bound this expression very crudely by $1/(\log n)^3$, say, for all sufficiently large n. Thus, since $n_k \ge e^{k^{1/2}}$, we have for sufficiently large k_0,

$$\sum_{k=k_0}^{\infty} \Pr\left[\left|\frac{C_r(A_{n_k})}{\vartheta_{n_k}} - 1\right| > \tfrac{1}{2}\epsilon\right] \le \sum_{k=k_0}^{\infty} \frac{1}{(\log n_k)^3} \le \sum_{k=k_0}^{\infty} \frac{1}{k^{3/2}} < \infty$$

and (32) follows from the Borel-Cantelli Lemma.

We shall now complete the proof by showing that, as $k \to \infty$,

$$\max_{n_k \le n \le n_{k+1}} \left|\frac{C_r(A_n)}{\vartheta_n} - 1\right| \to 0 \quad \text{almost surely.} \tag{33}$$

We apply the triangle inequality to find that

$$\begin{aligned}\max_{n_k \le n \le n_{k+1}} \left|\frac{C_r(A_n)}{\vartheta_n} - 1\right| &\le \left|1 - \frac{C_r(A_{n_{k+1}})}{\vartheta_{n_{k+1}}}\right| \\ &+ \max_{n_k \le n \le n_{k+1}} \left|\frac{C_r(A_{n_{k+1}})}{\vartheta_{n_{k+1}}} - \frac{C_r(A_n)}{\vartheta_{n_{k+1}}}\right| + \max_{n_k \le n \le n_{k+1}} \left|\frac{C_r(A_n)}{\vartheta_{n_{k+1}}} - \frac{C_r(A_n)}{\vartheta_n}\right|.\end{aligned} \tag{34}$$

Since $C_r(A_n)$ is non-decreasing, we find from Lemma 4.2 that

$$\max_{n_k\le n\le n_{k+1}}\left|\frac{C_r(A_{n_{k+1}})}{\vartheta_{n_{k+1}}}-\frac{C_r(A_n)}{\vartheta_{n_{k+1}}}\right|\le\sqrt{\frac{5(n_{k+1}-n_k)}{n_{k+1}}}$$

almost surely for all sufficiently large k. From

$$\lim_{k\to\infty}\frac{n_{k+1}}{n_k}=\lim_{k\to\infty}e^{(k+1)^{1/2}-k^{1/2}}=1 \tag{35}$$

we conclude that, as $k\to\infty$,

$$\max_{n_k\le n\le n_{k+1}}\left|\frac{C_r(A_{n_{k+1}})}{\vartheta_{n_{k+1}}}-\frac{C_r(A_n)}{\vartheta_{n_{k+1}}}\right|\to 0\quad\text{almost surely.} \tag{36}$$

The third term on the right hand side of (34) can be bounded as

$$\max_{n_k\le n\le n_{k+1}}\left|\frac{C_r(A_n)}{\vartheta_{n_{k+1}}}-\frac{C_r(A_n)}{\vartheta_n}\right|\le\frac{C_r(A_{n_{k+1}})}{\vartheta_{n_{k+1}}}\left|1-\frac{\vartheta_{n_{k+1}}}{\vartheta_{n_k}}\right|.$$

Using (35), it is readily verified that

$$\lim_{k\to\infty}\frac{\vartheta_{n_{k+1}}}{\vartheta_{n_k}}=1$$

and, after combination with (32), we conclude that, as $k\to\infty$,

$$\max_{n_k\le n\le n_{k+1}}\left|\frac{C_r(A_n)}{\vartheta_{n_{k+1}}}-\frac{C_r(A_n)}{\vartheta_n}\right|\to 0\quad\text{almost surely.} \tag{37}$$

The required convergence (33) follows by combining (34), (32), (36), and (37). □

5. Minimum values

Recall that the *scalar product* between two vectors $x=(x_1,\dots,x_\ell)$ and $y=(y_1,\dots,y_\ell)$ in $\mathbb{C}^\ell$ is $\langle x,y\rangle=\sum_{j=1}^{\ell}x_j\overline{y_j}$, where bar means complex conjugation. We shall see that Theorems C and 1.3 follow from well known results on the maximum magnitude of the nontrivial scalar products over a set of vectors in $\mathbb{C}^\ell$; a good overview is given by Kumar and Liu [10]. The most famous such result is the following bound due to Welch [16].

Lemma 5.1 (Welch [16])**.** *For positive integers ℓ and $m\ge 2$, let $v_1,\dots,v_m$ be elements of $\mathbb{C}^\ell$ satisfying $\|v_j\|_2^2=\ell$ for each j. Then, for integral $k\ge 1$,*

$$\max_{i\ne j}\left|\langle v_i,v_j\rangle\right|\ge\left[\frac{\ell^{2k}}{m-1}\left(\frac{m}{\binom{\ell+k-1}{k}}-1\right)\right]^{1/2k}.$$

This lemma can be proved by observing

$$m\ell^{2k}+m(m-1)\max_{i\ne j}\left|\langle v_i,v_j\rangle\right|^{2k}\ge\sum_{i,j}\left|\langle v_i,v_j\rangle\right|^{2k}$$

and deriving a lower bound for the right hand side. We remark that, for $k>1$ and when the vectors have entries in $\{-1,1\}$, the bound in Lemma 5.1

can be slightly improved by a bound due to Sidelnikov [15]. Lemma 5.1 is now used to give a straightforward proof of Theorem C.

Proof of Theorem C. Let $A_n = (a_1, a_2, \ldots, a_n)$ be an element of $\{-1, 1\}^n$. Write $\ell = \lfloor n/(2r+1) \rfloor$. For $\ell = 0$, the theorem is trivial, so assume that $\ell \geq 1$. Let $S_1, S_2, \ldots, S_m$ be $m = \lfloor (n - \ell + 1)/r \rfloor$ pairwise disjoint r-element subsets of $\{0, \ldots, n - \ell\}$. For each such set S_i, define the vector $v_i = (v_{i,1}, \ldots, v_{i,\ell})$ by

$$v_{i,j} = \prod_{x \in S_i} a_{j+x} \quad \text{for each } j \in \{1, \ldots, \ell\}.$$

Since all of the sets $S_1, \ldots, S_m$ have size r and are pairwise disjoint, we have

$$C_{2r}(A_n) \geq \max_{i \neq j} \big|\langle v_i, v_j \rangle\big|. \tag{38}$$

Observe that

$$m = \left\lfloor \frac{n - \lfloor n/(2r+1) \rfloor + 1}{r} \right\rfloor \geq \left\lfloor \frac{2n}{2r+1} \right\rfloor \geq 2\ell.$$

Hence, $m \geq 2$ and we can apply Lemma 5.1 with $k = 1$ to (38) to conclude

$$\big[C_{2r}(A_n)\big]^2 \geq \frac{\ell^2}{m-1}\Big(\frac{m}{\ell} - 1\Big) > \ell\Big(1 - \frac{\ell}{m}\Big) \geq \frac{\ell}{2},$$

as required. □

Slight improvements of Theorem C are possible for particular values r, by choosing ℓ more carefully in the proof (see Anantharam [7] for $r = 2$).

We now prove Theorem 1.3.

Proof of Theorem 1.3. Let $A_n = (a_1, a_2, \ldots, a_n)$ be an element of $\{-1, 1\}^n$. We have $n \geq 3$. Let $\ell = \lfloor n/3 \rfloor$ and $S_1, S_2, \ldots, S_m$ be all $m = \binom{n-\ell+1}{s}$ s-element subsets of $\{0, 1, \ldots, n - \ell\}$. For each such set S_i, define the vector $v_i = (v_{i,1}, \ldots, v_{i,\ell})$ by

$$v_{i,j} = \prod_{x \in S_i} a_{j+x} \quad \text{for each } j \in \{1, \ldots, \ell\}.$$

Then

$$\max\big\{C_2(A_n), C_4(A_n), \ldots, C_{2s}(A_n)\big\} \geq \max_{i \neq j} \big|\langle v_i, v_j \rangle\big|.$$

We apply Lemma 5.1 with $k = s$ to get

$$\Big[\max\big\{C_2(A_n), C_4(A_n), \ldots, C_{2s}(A_n)\big\}\Big]^{2s} \geq \frac{\ell^{2s}}{m-1}\left(\frac{m}{\binom{\ell+s-1}{s}} - 1\right).$$

Write $n = 3\ell + \delta$ for some $\delta \in \{0, 1, 2\}$. Then, using (5), the leading term on the right hand side is

$$\frac{\ell^{2s}}{m-1} \geq \frac{\ell^{2s}}{m} = \frac{(\frac{n-\delta}{3})^{2s}}{\binom{(2n+\delta+3)/3}{s}} \geq \left(\frac{s(n-\delta)^2}{3e(2n+\delta+3)}\right)^s > \left(\frac{sn}{9^2}\right)^s$$

since $n \geq 3$.

We complete the proof by showing that $m/\binom{\ell+s-1}{s} - 1$ is greater than 1. Define $f : \{1, 2, \ldots, \lfloor n/3 \rfloor\} \to \mathbb{Q}$ by

$$f(s) = \frac{\binom{n-\ell+1}{s}}{\binom{\ell+s-1}{s}}.$$

A standard calculation shows that f is monotonically increasing for $s \le (n - 2\ell + 2)/2$ and is monotonically decreasing for $s \ge (n - 2\ell + 2)/2$. Therefore, the minimum value of $f(s)$ is either $f(1)$ or $f(\lfloor n/3 \rfloor) = f(\ell)$. Moreover, we readily verify that $f(1) > 2$ and

$$f(\ell) \ge \frac{\binom{2\ell+1}{\ell}}{\binom{2\ell-1}{\ell}} = \frac{2(2\ell+1)}{\ell+1} \ge 3.$$

Hence f satisfies $f(s) > 2$ on its entire domain, as required. □

References

[1] R. Ahlswede, J. Cassaigne, and A. Sárközy, *On the correlation of binary sequences*, Discrete Appl. Math. **156** (2008), no. 9, 1478–1487.

[2] C. Aistleitner, *On the limit distribution of the normality measure of random binary sequences*, 2013, arXiv:1301.6454v1 [math.CO].

[3] ———, *On the limit distribution of the well-distribution measure of random binary sequences*, J. Theor. Nombres Bordeaux **25** (2013), no. 2, 245–259.

[4] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness: Minimal values*, Combin. Probab. Comput. **15** (2006), no. 1-2, 1–29.

[5] ———, *Measures of pseudorandomness: Typical values*, Proc. London Math. Soc. **95** (2007), no. 3, 778–812.

[6] N. Alon and J. H. Spencer, *The probabilistic method*, 3rd ed., Wiley, Hoboken, New Jersey, 2008.

[7] V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. **308** (2008), no. 24, 6203–6209.

[8] J. Cassaigne, C. Mauduit, and A. Sárközy, *On finite pseudorandom binary sequences. VII. The measures pseudorandomness*, Acta Arith. **103** (2002), no. 2, 97–118.

[9] W. Feller, *An introduction to probability theory and its applications. Vol. I*, Third edition, John Wiley & Sons Inc., New York, 1968.

[10] P. V. Kumar and C. M. Liu, *On lower bounds to the maximum correlation of complex roots-of-unity sequences*, IEEE Trans. Inf. Theory **36** (1990), no. 3, 633–640.

[11] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), no. 4, 265–377.

[12] C. McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics (J. Siemons, ed.), London Math. Soc. Lectures Notes Ser. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188.

[13] I. D. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), no. 5, 663–671.

[14] K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, arXiv:1105.5178 [math.CO] (to appear in Bull. London Math. Soc.).

[15] V. M. Sidel′nikov, *On mutual correlation of sequences*, Soviet Math. Dokl. **12** (1971), 197–201.

[16] L. R. Welch, *Lower bounds on the maximum cross correlation of signals*, IEEE Trans. Inf. Theory **IT-20** (1974), no. 3, 397–399.

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany.
E-mail address: kaiuwe.schmidt@ovgu.de

NONLINEARITY MEASURES OF RANDOM BOOLEAN FUNCTIONS

KAI-UWE SCHMIDT

Abstract. The r-th order nonlinearity of a Boolean function is the minimum number of elements that have to be changed in its truth table to arrive at a Boolean function of degree at most r. It is shown that the (suitably normalised) r-th order nonlinearity of a random Boolean function converges strongly for all $r \geq 1$. This extends results by Rodier for $r = 1$ and by Dib for $r = 2$. The methods in the present paper are mostly of elementary combinatorial nature and also lead to simpler proofs in the cases that $r = 1$ or 2.

1. Introduction and Results

Let $\mathbb{F}_2$ be a field with two elements. A *Boolean function* f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and its *truth table* is the list of values $f(x)$ as x ranges over $\mathbb{F}_2^n$ in some fixed order. Let $\mathfrak{B}_n$ be the space of Boolean functions on $\mathbb{F}_2^n$. Every $f \in \mathfrak{B}_n$ can be written uniquely in the form

$$f(x_1, \dots, x_n) = \sum_{k_1,\dots,k_n \in \{0,1\}} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n},$$

where $a_{k_1,\dots,k_n} \in \mathbb{F}_2$. The *degree* of f is defined to be the algebraic degree of this polynomial.

The *r-th order nonlinearity* $N_r(f)$ of a Boolean function f is the minimum number of elements that have to be changed in its truth table to arrive at the truth table of a Boolean function of degree at most r. We state this definition more formally as follows. Let $\mathrm{RM}(r, n)$ be the set of Boolean functions in $\mathfrak{B}_n$ of degree at most r (which is known as the *Reed-Muller code* of length 2^n and order r; see [10, Chapters 13–15], for example) and define the *Hamming distance* between $f, g \in \mathfrak{B}_n$ to be

$$d(f, g) = \big|\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}\big|.$$

Then the r-th order nonlinearity of f is

$$N_r(f) = \min_{g \in \mathrm{RM}(r,n)} d(f, g).$$

The nonlinearity of Boolean functions is of significant relevance in cryptography since it measures the resistance of a Boolean function against low-degree

Date: 14 August 2013.

2010 *Mathematics Subject Classification.* Primary: 06E30, 60B10; Secondary: 11T71.

approximation attacks (see [8], for example, and [3] for more background on the role of Boolean functions in cryptography and error-correcting codes).

Our interest is the distribution of the nonlinearity of Boolean functions. To this end, let Ω be the set of infinite sequences of elements from $\mathbb{F}_2$ and let $\mathfrak{B}$ be the space of functions from Ω to $\mathbb{F}_2$. For $f \in \mathfrak{B}$, we denote the restriction of f to its first n coordinates by f_n, which is in $\mathfrak{B}_n$. We endow $\mathfrak{B}$ with a probability measure defined by

$$\Pr\big[f \in \mathfrak{B} : f_n = g\big] = 2^{-2^n} \quad \text{for all } g \in \mathfrak{B}_n \text{ and all } n \in \mathbb{N}. \tag{1}$$

A basic probabilistic method can be used to show that, if f is drawn from $\mathfrak{B}$, equipped with the probability measure defined by (1), then

$$\limsup_{n\to\infty} \frac{2^{n-1} - N_r(f_n)}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \le 1 \quad \text{almost surely.} \tag{2}$$

This was proved with a weaker convergence mode by Carlet [2, Theorem 1]. The aim of this paper is to prove strong convergence of the normalised r-th order nonlinearity, which shows that the bound (2) is best possible.

Theorem 1. *Let f be drawn at random from $\mathfrak{B}$, equipped with the probability measure defined by* (1)*. Then for all $r \ge 1$, as $n \to \infty$,*

$$\frac{2^{n-1} - N_r(f_n)}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \to 1 \quad \textit{almost surely} \tag{3}$$

and

$$\frac{2^{n-1} - \mathrm{E}[N_r(f_n)]}{\sqrt{2^{n-1}\binom{n}{r}\log 2}} \to 1. \tag{4}$$

Using Fourier analytic methods due to Halász [6], Rodier [12] proved (3) for $r = 1$. More precise estimates on the rate of convergence in this case were given by Litsyn and Shpunt [9], using different methods. Dib [4] used a more combinatorial approach to prove (3) with a weaker convergence mode for $r = 2$. The methods in this paper are mostly of elementary combinatorial nature and also lead to simpler proofs of (3) in the cases that $r = 1$ or 2.

With the notation as in Theorem 1, write $Y_{n,g} = 2^n - 2d(f_n, g)$ for $g \in \mathfrak{B}_n$. In Section 2, we show that most pairs of functions in $\mathrm{RM}(r, n)$ have Hamming distance close to 2^{n-1}. Combining this with some large deviation estimates in Section 3 then shows that the events

$$Y_{n,g} \ge \sqrt{2^{n+1}\binom{n}{r}\log 2}$$

are pairwise nearly independent for all g from a large subset of $\mathrm{RM}(r, n)$. This will be the key ingredient for the proof of Theorem 1, which will be completed in Section 4.

2. Some results on Reed-Muller codes

In this section, we show that most pairs of functions in $\mathrm{RM}(r,n)$ have Hamming distance close to 2^{n-1}.

The *weight* of a Boolean function f, denoted by $\mathrm{wt}(f)$, is defined to be its Hamming distance to the zero function. For real x, write

$$A_{r,n}(x) = \big|\{g \in \mathrm{RM}(r,n) : \mathrm{wt}(g) \le 2^n x\}\big|.$$

Our starting point is the following asymptotic characterisation of $A_{r,n}(x)$, which is a special case of a result due to Kaufman, Lovett, and Porat [7].

Lemma 2 ([7, Theorem 3.1])**.** *For all $r \ge 1$, there exists a constant K_r such that*

$$A_{r,n}\left(\frac{1-\delta}{2}\right) \le \left(\frac{1}{\delta}\right)^{K_r n^{r-1}}$$

for all real δ satisfying $0 < \delta \le 1/2$.

It should be noted that the case $r = 1$ is not covered in [7, Theorem 3.1]. Lemma 2 however holds trivially in this case, since all but two functions in $\mathrm{RM}(1,n)$ have weight 2^{n-1}.

We now apply Lemma 2 to prove the main result of this section.

Lemma 3. *Let $\alpha > 0$ be real and let $r \ge 1$ be integral. Then, for all sufficiently large n, there exists a subset $S \subset \mathrm{RM}(r,n)$ of cardinality at least $2^{(1-\alpha)\binom{n}{r}}$ such that*

$$\big|d(g,h) - 2^{n-1}\big| \le 2^{n-1}/\tbinom{n}{r} \quad \text{for all } g,h \in S \text{ with } g \ne h. \tag{5}$$

Proof. Let $B_{r,n}$ be the number of functions g in $\mathrm{RM}(r,n)$ satisfying

$$\big|\,\mathrm{wt}(g) - 2^{n-1}\big| \ge 2^{n-1}/\tbinom{n}{r}.$$

Since $\mathrm{RM}(r,n)$ contains the nonzero constant function, there is a bijection between the functions in $\mathrm{RM}(r,n)$ of weight w and the functions in $\mathrm{RM}(r,n)$ of weight $2^n - w$. Therefore,

$$B_{r,n} = 2A_{r,n}\left(\frac{1 - 1/\binom{n}{r}}{2}\right)$$

and so by Lemma 2,

$$\log_2\left(\frac{B_{r,n}}{2}\right) \le K_r n^{r-1} \log_2 \binom{n}{r} \le K_r \binom{n}{r} \frac{r^r}{n} \log_2 \binom{n}{r},$$

where K_r is the same constant as in Lemma 2. Therefore,

$$B_{r,n} \le 2^{\alpha\binom{n}{r}} \tag{6}$$

for all sufficiently large n.

Next we construct the set S iteratively as follows. We take n large enough, so that the bound (6) for $B_{r,n}$ holds. Choose a $g \in \mathrm{RM}(r,n)$ to be in S and delete all $u \in \mathrm{RM}(r,n)$ satisfying

$$\big|d(g,u) - 2^{n-1}\big| \ge 2^{n-1}/\tbinom{n}{r}.$$

From (6) it is readily verified that the number of deleted functions is at most $2^{\alpha\binom{n}{r}}$. We can continue in this way to choose functions of $\mathrm{RM}(r,n)$ to be in S, while maintaining the property (5), as long as the number of chosen functions times $1+2^{\alpha\binom{n}{r}}$ is less than the cardinality of $\mathrm{RM}(r,n)$, namely $2^{1+\binom{n}{1}+\cdots+\binom{n}{r}}$. We can therefore obtain a set S satisfying (5) and

$$|S| \ge \frac{2^{1+\binom{n}{1}+\cdots+\binom{n}{r}}}{1+2^{\alpha\binom{n}{r}}} \ge \frac{2^{\binom{n}{r}}}{2^{\alpha\binom{n}{r}}}$$

for all sufficiently large n. □

3. Some large deviation estimates

In this section, we give some estimates for tail probabilities of sums of independent identically distributed random variables. For $\mathbf{a},\mathbf{b}\in\mathbb{R}^m$, we denote their scalar product by $\langle\mathbf{a},\mathbf{b}\rangle$.

Lemma 4. *Let* $\mathbf{g}$ *and* $\mathbf{h}$ *be elements of* $\{-1,1\}^N$ *and let* X *be drawn at random from* $\{-1,1\}^N$*, equipped with the uniform probability measure. Write* $Y_g=\langle X,\mathbf{g}\rangle$ *and* $Y_h=\langle X,\mathbf{h}\rangle$*. Then, for all* $t_1,t_2\in\mathbb{R}$*,*

$$\mathrm{E}\big[\exp(t_1Y_g+t_2Y_h)\big]\le\exp\big(\tfrac12N\big(t_1^2+t_2^2\big)+t_1t_2\langle\mathbf{g},\mathbf{h}\rangle\big).$$

Proof. Write $X=(X_1,\dots,X_N)$, $\mathbf{g}=(g_1,\dots,g_N)$, and $\mathbf{h}=(h_1,\dots,h_N)$. Then

$$\begin{aligned}\mathrm{E}\big[\exp(t_1Y_g+t_2Y_h)\big]&=\mathrm{E}\left[\prod_{j=1}^N\exp\big(X_j(t_1g_j+t_2h_j)\big)\right]\\&=\prod_{j=1}^N\mathrm{E}\big[\exp\big(X_j(t_1g_j+t_2h_j)\big)\big]\end{aligned}$$

using that the X_j's are independent. Since the X_j's take on each of the values 1 and -1 with probability $1/2$, we see that

$$\mathrm{E}\big[\exp(t_1Y_g+t_2Y_h)\big]=\prod_{j=1}^N\cosh(t_1g_j+t_2h_j).$$

By comparing the Maclaurin series of $\cosh(x)$ and $\exp(x^2/2)$, we find that $\cosh(x)\le\exp(x^2/2)$. Thus

$$\begin{aligned}\mathrm{E}\big[\exp(t_1Y_g+t_2Y_h)\big]&\le\prod_{j=1}^N\exp\big(\tfrac12(t_1g_j+t_2h_j)^2\big)\\&=\exp\left(\frac12\sum_{j=1}^N(t_1g_j+t_2h_j)^2\right),\end{aligned}$$

from which the desired bound easily follows. □

We next apply Lemma 4 to vectors $\mathbf{g}$ and $\mathbf{h}$ whose scalar product is sufficiently small.

Lemma 5. *Let $r \geq 0$ be an integer and let $\mathbf{g}$ and $\mathbf{h}$ be elements of $\{-1,1\}^{2^n}$ satisfying $|\langle \mathbf{g}, \mathbf{h}\rangle| \leq 2^n/\binom{n}{r}$. Let X be drawn at random from $\{-1,1\}^{2^n}$, equipped with the uniform probability measure. Write $Y_g = \langle X, \mathbf{g}\rangle$ and $Y_h = \langle X, \mathbf{h}\rangle$. Then*

$$\Pr\Big[Y_g \geq \sqrt{2^{n+1}\tbinom{n}{r}\log 2} \cap Y_h \geq \sqrt{2^{n+1}\tbinom{n}{r}\log 2}\Big] \leq 4/4^{\binom{n}{r}}.$$

Proof. Write

$$\lambda = \sqrt{2^{n+1}\tbinom{n}{r}\log 2}$$

and $s = \lambda/2^n$. Application of Markov's inequality gives

$$\begin{aligned}\Pr\big[Y_g \geq \lambda \cap Y_h \geq \lambda\big] &= \Pr\big[\exp(sY_g) \geq \exp(s\lambda) \cap \exp(sY_h) \geq \exp(s\lambda)\big] \\ &\leq \frac{\mathrm{E}\big[\exp(sY_g)\exp(sY_h))\big]}{[\exp(s\lambda)]^2} \\ &\leq \frac{\exp(2^n s^2(1+1/\binom{n}{r}))}{[\exp(s\lambda)]^2}\end{aligned}$$

by Lemma 4. This last expression equals $4/4^{\binom{n}{r}}$, as required. □

We also need the following estimate.

Lemma 6. *Let $X_1, \ldots, X_{2^n}$ be independent random variables taking on each of -1 and 1 with probability $1/2$. Then, for all $r \geq 1$ and all sufficiently large n,*

$$\Pr\Big[X_1 + \cdots + X_{2^n} \geq \sqrt{2^{n+1}\tbinom{n}{r}\log 2}\Big] \geq \frac{1}{3\cdot 2^{\binom{n}{r}}\sqrt{\binom{n}{r}}}.$$

Proof. A normal tail approximation of the distribution of $X_1 + \cdots + X_{2^n}$ gives (see Feller [5, Chapter VII, (6.7)], for example)

$$\lim_{n\to\infty} 2^{\binom{n}{r}}\sqrt{4\pi\tbinom{n}{r}\log 2}\,\Pr\Big[X_1 + \cdots + X_{2^n} \geq \sqrt{2^{n+1}\tbinom{n}{r}\log 2}\Big] = 1,$$

from which the lemma can be deduced since $\sqrt{4\pi\log 2} < 3$. □

4. Proof of Theorem 1

For $g \in \mathrm{RM}(r,n)$, write $Y_{n,g} = 2^n - 2d(f_n, g)$ and

$$Y_n = \max_{g\in\mathrm{RM}(r,n)} Y_{n,g},$$

so that $Y_n = 2^n - 2N_r(f_n)$. Notice that

$$Y_{n,g} = \sum_{x\in\mathbb{F}_2^n} (-1)^{f_n(x)+g(x)}, \tag{7}$$

from which we see that $Y_{n,g}$ is a sum of 2^n random variables, each taking each of the values -1 and 1 with probability $1/2$.

We make repeated use of the inequality

$$\Pr\big[\big|Y_n - \mathrm{E}[Y_n]\big| \ge \theta\big] \le 2\exp\left(-\frac{\theta^2}{2^{n+1}}\right) \quad \text{for } \theta \ge 0, \tag{8}$$

which follows from well known results on concentration of probability measures (see McDiarmid [11, Lemma 1.2], for example).

First, we derive an upper bound for $\mathrm{E}[Y_n]$. Letting $s \in \mathbb{R}$, we have by Jensen's inequality,

$$\begin{aligned}\exp(s\,\mathrm{E}[Y_n]) &\le \mathrm{E}\big[\exp(sY_n)\big]\\ &= \mathrm{E}\Big[\max_{g\in\mathrm{RM}(r,n)} \exp(sY_{n,g})\Big]\\ &\le \sum_{g\in\mathrm{RM}(r,n)} \mathrm{E}\big[\exp(sY_{n,g})\big]\\ &\le 2^{1+\binom{n}{1}+\cdots+\binom{n}{r}}\exp(2^{n-1}s^2)\end{aligned}$$

by Lemma 4 with $t_1 = s$ and $t_2 = 0$ using (7). Hence

$$\mathrm{E}[Y_n] \le \frac{1}{s}\big(1+\tbinom{n}{1}+\cdots+\tbinom{n}{r}\big)\log 2 + 2^{n-1}s.$$

Now choose s such that both summands are equal. This gives

$$\mathrm{E}[Y_n] \le \sqrt{2^{n+1}\big(1+\tbinom{n}{1}+\cdots+\tbinom{n}{r}\big)\log 2}. \tag{9}$$

Write

$$\lambda_n = \sqrt{2^{n+1}\tbinom{n}{r}\log 2} \tag{10}$$

and, for $\delta \in (0,1)$, define the set

$$M(\delta) = \big\{n \in \mathbb{N} : \mathrm{E}[Y_n] < (1-\delta)\lambda_n\big\}. \tag{11}$$

We claim that the cardinality of $M(\delta)$ is finite for all choices of $\delta > 0$, which together with (9) will prove

$$\lim_{n\to\infty} \mathrm{E}[Y_n]/\lambda_n = 1, \tag{12}$$

which in turn proves (4). The proof of the claim is based on an idea in [1].

Let $\alpha \in (0,1)$ be a real number, to be determined later. By Lemma 3, for all sufficiently large n, there exists a subset $S \subset \mathrm{RM}(r,n)$ satisfying

$$2^{(1-\alpha)\binom{n}{r}} \le |S| \le 2\cdot 2^{(1-\alpha)\binom{n}{r}}, \tag{13}$$

say, such that

$$\left|\sum_{x\in\mathbb{F}_2^n} (-1)^{g(x)+h(x)}\right| \le 2^n/\tbinom{n}{r} \quad \text{for all } g,h \in S \text{ with } g \ne h. \tag{14}$$

We have

$$\Pr\big[Y_n \geq \lambda_n\big] \geq \Pr\big[\max_{g\in S} Y_{n,g} \geq \lambda_n\big]$$
$$\geq \sum_{g\in S} \Pr\big[Y_{n,g} \geq \lambda_n\big] - \frac{1}{2} \sum_{\substack{g,h\in S \\ g\neq h}} \Pr\big[Y_{n,g} \geq \lambda_n \cap Y_{n,h} \geq \lambda_n\big]$$

by the Bonferroni inequality. Lemma 6 gives a lower bound for the probabilities in the first sum and, using (7) and (14), Lemma 5 gives an upper bound for the probabilities in the second sum. Applying these bounds gives, for all sufficiently large n,

$$\Pr\big[Y_n \geq \lambda_n\big] \geq |S| \cdot \frac{1}{3\cdot 2^{\binom{n}{r}}\sqrt{\binom{n}{r}}} - \frac{|S|^2}{2}\cdot\frac{4}{4^{\binom{n}{r}}}$$
$$\geq \frac{1}{3\cdot 2^{\alpha\binom{n}{r}}\sqrt{\binom{n}{r}}} - \frac{8}{4^{\alpha\binom{n}{r}}},$$

using (13). The first term dominates the second term, so that, for all sufficiently large n,

$$\Pr\big[Y_n \geq \lambda_n\big] \geq \frac{1}{4^{\alpha\binom{n}{r}}}, \tag{15}$$

say. By the definition (11) of $M(\delta)$, we have $\lambda_n > \mathrm{E}[Y_n]$ for all $n \in M(\delta)$. We therefore find from (8) with $\theta = \lambda_n - \mathrm{E}[Y_n]$ that, for all $n \in M(\delta)$,

$$\Pr\big[Y_n \geq \lambda_n\big] \leq 2\exp\left(-\frac{(\lambda_n - \mathrm{E}[Y_n])^2}{2^{n+1}}\right).$$

Comparison with (15) gives, for all sufficiently large $n \in M(\delta)$,

$$\frac{1}{4^{\alpha\binom{n}{r}}} \leq 2\exp\left(-\frac{(\lambda_n - \mathrm{E}[Y_n])^2}{2^{n+1}}\right),$$

which, after rearranging and using (10), implies

$$\mathrm{E}[Y_n]/\lambda_n \geq 1 - \sqrt{1/\tbinom{n}{r} + 2\alpha},$$

By taking $\alpha = \delta^2/4$, say, we see from the definition (11) of $M(\delta)$ that $M(\delta)$ has finite cardinality for all $\delta \in (0,1)$, which proves (12), and so proves (4).

To prove (3), we let $\epsilon > 0$ and invoke the triangle inequality to obtain

$$\Pr\big[|Y_n/\lambda_n - 1| > \epsilon\big] \leq \Pr\big[|Y_n - \mathrm{E}[Y_n]|/\lambda_n > \tfrac{1}{2}\epsilon\big] + \Pr\big[|\mathrm{E}[Y_n]/\lambda_n - 1| > \tfrac{1}{2}\epsilon\big].$$

By (12), the second probability on the right hand side equals zero for all sufficiently large n, and by (8), the first probability on the right hand side is at most $2\cdot 2^{-(\epsilon^2/4)\binom{n}{r}}$. Hence,

$$\sum_{n=1}^{\infty} \Pr\big[|Y_n/\lambda_n - 1| > \epsilon\big] < \infty,$$

from which and the Borel-Cantelli Lemma we conclude that

$$\lim_{n\to\infty} Y_n/\lambda_n = 1 \quad \text{almost surely.}$$

This proves (3). □

Acknowledgement

I thank Claude Carlet for some careful comments on a draft of this paper.

References

[1] N. Alon, S. Litsyn, and A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inform. Theory **56** (2010), no. 1, 545–554.
[2] C. Carlet, *The complexity of Boolean functions from cryptographic viewpoint*, Complexity of Boolean Functions (Dagstuhl, Germany), Dagstuhl Seminar Proceedings, no. 06111, 2006.
[3] ———, *Boolean functions for cryptography and error-correcting codes.*, Boolean models and methods in mathematics, computer science, and engineering (Y. Crama and P. L. Hammer, eds.), Cambridge University Press, 2010, pp. 257–397.
[4] S. Dib, *Distribution of Boolean functions according to the second-order nonlinearity*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 6087, Springer, Berlin, 2010, pp. 86–96.
[5] W. Feller, *An introduction to probability theory and its applications. Vol. I*, Third edition, John Wiley & Sons Inc., New York, 1968.
[6] G. Halász, *On a result of Salem and Zygmund concerning random polynomials*, Studia Sci. Math. Hungar. **8** (1973), 369–377.
[7] T. Kaufman, S. Lovett, and E. Porat, *Weight distribution and list-decoding size of Reed-Muller codes*, IEEE Trans. Inform. Theory **58** (2012), no. 5, 2689–2696.
[8] L. R. Knudsen and M. J. B. Robshaw, *Non-linear approximations in linear cryptanalysis*, Proceedings Eurocrypt'96, Lecture Notes Comput. Sci., vol. 1070, 1996, pp. 224–236.
[9] S. Litsyn and A. Shpunt, *On the distribution of Boolean function nonlinearity*, SIAM J. Discrete Math. **23** (2008/09), no. 1, 79–95.
[10] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam, The Netherlands: North Holland, 1977.
[11] C. McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics (J. Siemons, ed.), London Math. Soc. Lectures Notes Ser. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188.
[12] F. Rodier, *Asymptotic nonlinearity of Boolean functions*, Des. Codes Cryptogr. **40** (2006), no. 1, 59–70.

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany.
E-mail address: kaiuwe.schmidt@ovgu.de