Pacific Journal of Mathematics

THE L_4 NORM OF LITTLEWOOD POLYNOMIALS DERIVED FROM THE JACOBI SYMBOL

JONATHAN JEDWAB AND KAI-UWE SCHMIDT

Volume 257 No. 2 June 2012

PACIFIC JOURNAL OF MATHEMATICS
Vol. 257, No. 2, 2012

THE L_4 NORM OF LITTLEWOOD POLYNOMIALS DERIVED FROM THE JACOBI SYMBOL

JONATHAN JEDWAB AND KAI-UWE SCHMIDT

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 normalized 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 normalized 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 normalized 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

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

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. Littlewood [1966, Section 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 [1968, page 199] in a different context. Littlewood's question is closely related to other classical problems involving norms of Littlewood polynomials [Newman

J. Jedwab is supported by NSERC of Canada. K.-U. Schmidt is supported by the German Research Foundation.
MSC2010: primary 11B83, 11C08; secondary 94A55.
Keywords: Littlewood polynomial, norm, asymptotic, multiplicative character, merit factor.

1960; Erdős 1962; Littlewood 1968; Newman and Byrnes 1990; Beck 1991; Borwein 2002].

For a polynomial $A \in \mathbb{C}[z]$, a small L_4 norm corresponds to a large *merit factor*, defined as

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

provided that the denominator is nonzero. This normalized 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 [Beenker et al. 1985], and in theoretical physics, where Littlewood polynomials with the largest merit factors correspond to the ground states of Bernasconi's Ising spin model [Bernasconi 1987].

If A is drawn uniformly from the set of Littlewood polynomials of degree $n-1$, then $F(A) \to 1$ in probability as $n \to \infty$ [Borwein and Lockhart 2001]. Littlewood [1968] 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 [Jedwab 2005] 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 $(\cdot \mid n)$ be the Jacobi symbol (see [Apostol 1976], for example), and call

$$J(z) := \sum_{j=1}^{n-1} (j \mid n) z^j$$

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 [Montgomery 1980; Høholdt and Jensen 1988; Conrey et al. 2000; Borwein et al. 2001; Borwein and Choi 2002].

Indeed, defining

$$f(r) := \begin{cases} \dfrac{1}{\frac{1}{6}+8(|r|-\frac{1}{4})^2} & \text{for } -\frac{1}{2} < r \le \frac{1}{2}, \\ f(r+1) & \text{otherwise}, \end{cases} \tag{1-2}$$

the following result is known.

Theorem 1.1 [Høholdt and Jensen 1988]. *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 [2002] 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 $2p-1$ [Xiong and Hall 2008] and $4p-1$ [Schmidt et al. 2009] 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 [1988] conjectured that no larger value is possible, although there are various contradicting opinions [Littlewood 1968, page 29; Golay 1982; Borwein et al. 2004]. 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 [Littlewood 1966, Section 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 $(j \mid n) = 0$ 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 maximizes 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 maximizes 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*

$$\frac{(\log n)^3}{p_n} \to 0 \tag{2-1}$$

as $n \to \infty$, 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 us to question 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*

$$\frac{(\log n)^7}{p_n} \to 0 \tag{2-3}$$

as $n \to \infty$, and let r be real. Let J be the character polynomial of degree $n-1$. Then

$$\limsup_{n\to\infty} \max_{V \in \mathcal{V}_n} F(J_r + V_r) \le f(r).$$

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, we have $F(J_r + V_r) \sim f(r)$ for almost all choices of V.

Theorem 2.4. *Let n take values only in an infinite set of odd square-free integers greater than* 1, *where*

$$\frac{(\log n)^7}{p_n} \to 0 \tag{2-4}$$

as $n \to \infty$, 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 $n \to \infty$,

$$F(J_r + V_r) \to f(r)$$

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*

$$\frac{(\log n)^7}{p_n} \to 0 \tag{2-5}$$

as $n \to \infty$, and let r be real. Let J be the character polynomial of degree $n-1$, and define

$$V(z) = \sum_{\substack{j=0 \\ \gcd(j,n)>1}}^{n-1} \left(j \mid \frac{n}{\gcd(j,n)} \right) z^j. \tag{2-6}$$

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*

$$\frac{n^{1/3}}{p_n} \to 0 \tag{2-7}$$

as $n \to \infty$, 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: 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 2.1–2.6 in Sections 4–9, 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 [Jensen et al. 1991] 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 [Jensen et al. 1991] for both of these Littlewood completions are special cases of Theorem 2.6. Jensen et al. [1991] 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 [Jensen et al. 1991], Borwein and Choi [2001] 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 $\epsilon > 0$. Borwein and Choi remarked that the merit factors of the polynomials $J_{1/4}$ as $n \to \infty$ “approach 6 which is conjectured by some” (referring to [Golay 1983]) “to be best possible”. They also say that their result

> “should be compared with the results of T. Høholdt, H. Jensen and J. Jensen [who, in [Jensen et al. 1991]] showed that the same asymptotic formula but a weaker error term $O\big(((p+q)^5 \log^4 N)/N^3\big)$ for the special case $N = pq$. So we generalize their result to $N = p_1 p_2 \ldots p_r$ and also improve the error term.”

However, Borwein and Choi 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 [Borwein and Choi 2001] cannot be considered a generalization of those of [Jensen et al. 1991], and the comparison given by Borwein and Choi with the conjecture of [Golay 1983] (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 [Xiong and Hall 2011], they obtained 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 [Xiong and Hall 2010], 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

We now introduce some notation and give some auxiliary results. Throughout the paper, ζ_m denotes the primitive m-th 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

$$\omega(n) \le \log n \tag{3-1}$$

for $n > 2$ and $n \neq 6$. 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

$$\frac{\phi(n)}{n} \ge \Big(1 - \frac{1}{p_n}\Big)^{\omega(n)} \ge 1 - \frac{\omega(n)}{p_n} \ge 1 - \frac{\log n}{p_n}$$

for $n > 2$ and $n \neq 6$, so we can estimate its growth rate as

$$\phi(n) = n(1 + O(p_n^{-1} \log n)) \tag{3-2}$$

as $n \to \infty$. For convenience, we define the *cototient function* to be

$$\psi(n) := n - \phi(n).$$

It follows that

$$\frac{\psi(n)}{n} \le \frac{\omega(n)}{p_n} \tag{3-3}$$

$$\le \frac{\log n}{p_n} \tag{3-4}$$

for $n > 2$ and $n \neq 6$, and therefore

$$\psi(n) = O(p_n^{-1} n \log n) \tag{3-5}$$

as $n \to \infty$. We shall need the following evaluation of Ramanujan's sum [Hardy and Wright 1954, Theorem 272].

Lemma 3.1. *For integer u and positive square-free integer n, we have*

$$\sum_{\substack{j=0 \\ \gcd(j,n)=1}}^{n-1} \zeta_n^{ju} = \mu\Big(\frac{n}{\gcd(u,n)}\Big)\phi(\gcd(u,n)),$$

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,*

$$\sum_{\ell=0}^{m-1} (\ell \mid m)\zeta_m^{j\ell} = i^{(m-1)^2/4}(j \mid m)m^{1/2}.$$

The case $\gcd(j,m) = 1$ of Lemma 3.2 is given, for example, by [Berndt et al. 1998, Theorem 1.5.2 and Chapter 1, Problem 24]. 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,

$$J(\zeta_n^j) = i^{(n-1)^2/4}(j \mid n)n^{1/2}. \tag{3-6}$$

Given a polynomial A of degree $n-1$, 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

$$J_r(\zeta_n^j) = i^{(n-1)^2/4}\zeta_n^{-j\lfloor nr \rfloor}(j \mid n)n^{1/2}. \tag{3-8}$$

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 n-th roots of unity.

Lemma 3.3. *Let $A \in \mathbb{C}[z]$ have degree at most $n-1$ for $n > 2$. Then*

$$\max_{|z|=1}|A(z)| \leq (2\log n) \max_{0\leq k<n} |A(\zeta_n^k)|.$$

Proof. By bounding the coefficients that occur in the Lagrange interpolation of A from its evaluations at the n-th roots of unity, it can be shown that

$$\max_{|z|=1}|A(z)| \leq c(n) \max_{0\leq k<n} |A(\zeta_n^k)|,$$

where $c(n) = 1 + (1/n)\sum_{j=1}^{n-1} 1/\sin(\pi j/(2n))$; see [Paterson and Tarokh 2000, Appendix]. 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 $c(n) \leq 2\log n$ for $3 \leq n \leq 7$. □

Using (3-8), Lemma 3.3 gives

$$\max_{|z|=1}|J_r(z)| \leq 2n^{1/2}\log n. \tag{3-9}$$

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*

$$\left|\frac{1}{F(J_r+V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)} - \frac{\|V_r\|_4^4}{n^2}\right| < 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 + 58p_n^{-1/2}(\log n)^{7/2}.$$

In the application of Proposition 3.4 it is sometimes useful to further bound $\|V_r\|_4^4$ as

$$\|V_r\|_4^4 \leq [\psi(n)]^3, \tag{3-10}$$

which follows from $\|V_r\|_2^2 = \psi(n)$ and the simple inequality

$$\|A\|_4^4 \leq \|A\|_2^2 \max_{|z|=1}|A(z)|^2 \tag{3-11}$$

for all $A \in \mathbb{C}[z]$.

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 $\|J_r + V_r\|_2^2 = n$, by the definition of the merit factor,

$$\beta(n) = \left| \frac{1}{n^2}(\|J_r + V_r\|_4^4 - \|J_r\|_4^4 - \|V_r\|_4^4) + \left(\frac{\phi(n)}{n}\right)^2 - 1 \right|. \tag{3-12}$$

Since

$$\left| \left(\frac{\phi(n)}{n}\right)^2 - 1 \right| = \frac{1}{n^2}|(\phi(n)+n)(\phi(n)-n)| < \frac{2\psi(n)}{n}$$

by the trivial inequality $\phi(n)+n < 2n$, it follows from (3-12) that

$$\beta(n) < \left| \frac{1}{n^2}(\|J_r + V_r\|_4^4 - \|J_r\|_4^4 - \|V_r\|_4^4) \right| + \frac{2\psi(n)}{n}. \tag{3-13}$$

Now for $a, b \in \mathbb{C}$, by expanding $|a+b|^4$, we get the inequality

$$\big|\,|a+b|^4 - |a|^4 - |b|^4\big| \le 4|a|^3 \cdot |b| + 6|a|^2 \cdot |b|^2 + 4|a| \cdot |b|^3.$$

Using (3-9) and the definition of the L_α norm, we 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,

$$\|V_r\|_{m+1}^{m+1} \le \|V_r\|_2 \left(\frac{1}{2\pi}\int_0^{2\pi} |V_r(e^{i\theta})|^{2m} d\theta \right)^{1/2}.$$

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,*

$$\sum_{j=0}^{n-1} (j \mid n)(j+u \mid n) = \mu\left(\frac{n}{\gcd(u,n)}\right)\phi(\gcd(u,n)).$$

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

$$\sum_{j=0}^{n-1} (j \mid n)(j+u \mid n) = \sum_{\substack{j=0 \\ \gcd(j,n)=1}}^{n-1} \zeta_n^{ju},$$

which is Ramanujan's sum. The result now follows from Lemma 3.1. □

Høholdt and Jensen [1988] introduced a method for calculating the merit factor of a polynomial of even degree. The following result summarizes their method (and occurs as a special case of the slightly more general result of [Schmidt et al. 2009, Lemma 10]).

Lemma 4.2. *Let $A \in \mathbb{R}[z]$ be a polynomial of even degree $n-1$. Define*

$$\Lambda_A(j, k, \ell) := \sum_{a=0}^{n-1} A(\zeta_n^a) \overline{A(\zeta_n^{a+j})} A(\zeta_n^{a+k}) \overline{A(\zeta_n^{a+\ell})} \tag{4-1}$$

for integers j, k, ℓ. 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,

$$\frac{1}{F(J_r)} = \Big(\frac{n}{\phi(n)}\Big)^2 \bigg(\frac{\| J_r \|_4^4}{n^2}\bigg) - 1.$$

We claim that

$$\frac{\| J_r \|_4^4}{n^2} = 1 + \frac{1}{f(r)} + O(p_n^{-1}(\log n)^3), \tag{4-3}$$

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

$$\Lambda_{J_r}(j, k, \ell) = \zeta_n^{R(j-k+\ell)} \cdot n^2 \sum_{a=0}^{n-1} (a \mid n)(a + j \mid n)(a + k \mid n)(a + \ell \mid n). \tag{4-4}$$

The term involving $\mathbf{\Lambda_{J_r}(0, 0, 0)}$. By (4-4) we have

$$\begin{aligned}\frac{2n^2+1}{3n^5} \Lambda_{J_r}(0, 0, 0) &= \frac{2n^2+1}{3n^5} n^2 \phi(n) \\ &= \tfrac{2}{3} + O(p_n^{-1} \log n)\end{aligned} \tag{4-5}$$

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 get

$$\Lambda_{J_r}(0, k, k) = n^3 [1 + O(p_n^{-1} \log n)]$$

and, similarly,

$$\Lambda_{J_r}(k, 0, k) = \zeta_n^{2Rk} \cdot n^3 [1 + O(p_n^{-1} \log n)].$$

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

$$\sum_{k=1}^{n-1} \frac{\zeta_n^{jk}}{|1-\zeta_n^k|^2} = \frac{n^2}{2}\left(\frac{|j|}{n} - \frac{1}{2}\right)^2 - \frac{n^2+2}{24} \tag{4-7}$$

for integer j satisfying $|j| \le n$; see [Jensen et al. 1991, page 621], for example. The assumption $-\frac{1}{2} < r \le \frac{1}{2}$ 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

$$D = \frac{4}{n^2}[1 + O(p_n^{-1}\log n)]\left[\frac{n^2}{2}\left(\frac{|2R-1|}{n} - \frac{1}{2}\right)^2 + \frac{n^2-2}{8}\right].$$

By the definition of R, we have $R = nr + O(1)$. We then find that

$$D = \tfrac{1}{2} + 8(|r| - \tfrac{1}{4})^2 + O(p_n^{-1}\log n). \tag{4-8}$$

The sum B. We bound the sum B via

$$\begin{aligned} |B| &\le \frac{2}{n^5}\sum_{k=1}^{n-1} \frac{4|\Lambda_{J_r}(0,0,k)|}{|1-\zeta_n^k|^2} \\ &= \frac{8}{n^5}\sum_{k=1}^{n-1} \frac{n^2}{|1-\zeta_n^k|^2}\left|\sum_{a=0}^{n-1}(a \mid n)(a+k \mid n)\right| \end{aligned} \tag{4-9}$$

by (4-4). But from Lemma 4.1 we know that

$$\left|\sum_{a=0}^{n-1}(a \mid n)(a+k \mid n)\right| \le \phi(p_n^{-1}n) < \frac{n}{p_n} \tag{4-10}$$

for $k \not\equiv 0 \pmod{n}$. 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

$$|C| \le \frac{2}{n^5}\sum_{\substack{1\le k,\ell<n \\ k\ne\ell}} \frac{6|\Lambda_{J_r}(0,k,\ell)|}{|1-\zeta_n^k|\cdot|1-\zeta_n^\ell|}. \tag{4-12}$$

Now, from (4-4), we have

$$\begin{aligned}\frac{1}{n^2}|\Lambda_{J_r}(0,k,\ell)| &= \Bigg|\sum_{a=0}^{n-1}(a+k\mid n)(a+\ell\mid n) - \sum_{\substack{a=0\\ \gcd(a,n)>1}}^{n-1}(a+k\mid n)(a+\ell\mid n)\Bigg|\\ &\le \Bigg|\sum_{a=0}^{n-1}(a\mid n)(a+\ell-k\mid n)\Bigg| + \psi(n)\\ &< \frac{n}{p_n}+\psi(n)\end{aligned}$$

for $k \not\equiv \ell \pmod{n}$, by (4-10). Substitution in (4-12) then gives

$$\begin{aligned}|C| &< \frac{12}{n^3}\Big(\frac{n}{p_n}+\psi(n)\Big)\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}}\frac{1}{|1-\zeta_n^k|\cdot|1-\zeta_n^\ell|}\\ &< \frac{12}{n^3}\Big(\frac{n}{p_n}+\psi(n)\Big)\Bigg(\sum_{k=1}^{n-1}\frac{1}{|1-\zeta_n^k|}\Bigg)^2\\ &\le \frac{12(\log n)^2}{n}\Big(\frac{n}{p_n}+\psi(n)\Big)\end{aligned}$$

since $\sum_{k=1}^{n-1} 1/|1-\zeta_n^k| \le n\log n$ (see [Høholdt and Jensen 1988, page 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

Proof. By Proposition 3.4, we have

$$\frac{1}{F(J_r+V_r)} > \Big(\frac{\phi(n)}{n}\Big)^2\frac{1}{F(J_r)}+\delta(n),$$

where

$$\begin{aligned}\delta(n) &= \frac{1}{n^2}\|V_r\|_4^4 - 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 - 58p_n^{-1/2}(\log n)^{7/2}\\ &= \frac{1}{n^2}\|V_r\|_4^4 + O(p_n^{-2}n^{1/2}(\log n)^3) + O(p_n^{-1/2}(\log n)^{7/2}),\end{aligned} \tag{5-1}$$

using the upper bound (3-10) for $\|V_r\|_4^4$ and the upper bound (3-4) for $\psi(n)$. Thus

$$\liminf_{n\to\infty}\frac{1}{F(J_r+V_r)} \ge \liminf_{n\to\infty}\Bigg[\Big(\frac{\phi(n)}{n}\Big)^2\frac{1}{F(J_r)}\Bigg] + \liminf_{n\to\infty}\delta(n). \tag{5-2}$$

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 [Høholdt and Jensen 1988], for example), which gives the inequality

$$\frac{1}{n^2}\|V_r\|_4^4 \geq \frac{1}{2n^3}\sum_{j=0}^{n-1}|V_r(\zeta_n^j)|^4.$$

Restrict the summation to the set $U = \{n/p_n, 2n/p_n, \ldots, (p_n - 1)n/p_n\}$ and use (3-7) to obtain

$$\frac{1}{n^2}\|V_r\|_4^4 \geq \frac{1}{2n^3}\sum_{u\in U}|V(\zeta_n^u)|^4. \tag{5-3}$$

Now let $u \in U$. From the definition of V we have

$$V(\zeta_n^u) = \sum_{\substack{j=0\\ \gcd(j,n)>1}}^{n-1} \zeta_n^{ju} = \sum_{j=0}^{n-1}\zeta_n^{ju} - \sum_{\substack{j=0\\ \gcd(j,n)=1}}^{n-1} \zeta_n^{ju}.$$

The first sum evaluates to 0 because $\zeta_n^u \neq 1$. The second sum is Ramanujan's sum, and using $\gcd(u,n) = p_n^{-1}n$ in Lemma 3.1, we get

$$V(\zeta_n^u) = \phi(p_n^{-1}n) = \frac{\phi(n)}{p_n - 1}.$$

Substitution in (5-3) then gives the desired lower bound

$$\frac{1}{n^2}\|V_r\|_4^4 \geq \frac{1}{2n^3}(p_n - 1)\left(\frac{\phi(n)}{p_n - 1}\right)^4 > \frac{n}{2p_n^3}\left(\frac{\phi(n)}{n}\right)^4.$$

By substituting this lower bound in (5-1), we find that

$$\delta(n) > \frac{n}{2p_n^3}\left(\frac{\phi(n)}{n}\right)^4 + O(p_n^{-2}n^{1/2}(\log n)^3) + O(p_n^{-1/2}(\log n)^{7/2}), \tag{5-4}$$

or, equivalently,

$$\delta(n) > \frac{n}{2p_n^3}\left[\left(\frac{\phi(n)}{n}\right)^4 + O(p_n n^{-1/2}(\log n)^3) + O(p_n^{5/2}n^{-1}(\log n)^{7/2})\right]. \tag{5-5}$$

To complete the proof, partition the infinite set N, in which n takes values, into subsets N_1, N_2 defined by

$$n \in \begin{cases} N_1 & \text{if } p_n \le n^{2/7}, \\ N_2 & \text{if } p_n > n^{2/7}, \end{cases}$$

at least one of which is infinite. First suppose that N_1 is infinite and let n take values only in N_1. Then

$$p_n n^{-1/2} (\log n)^3 \le n^{-3/14} (\log n)^3 \to 0$$

and

$$p_n^{5/2} n^{-1} (\log n)^{7/2} \le n^{-2/7} (\log n)^{7/2} \to 0,$$

so that by (5-5) we obtain

$$\liminf_{n\to\infty} \delta(n) \ge \liminf_{n\to\infty} \left[\frac{n}{2p_n^3} \left(\frac{\phi(n)}{n} \right)^4 \right].$$

Choose some ϵ satisfying $0 < \epsilon < 1/28$. Since $\phi(n)/n^{1-\epsilon} \to \infty$ [Hardy and Wright 1954, Theorem 327], we have

$$\liminf_{n\to\infty} \delta(n) \ge \liminf_{n\to\infty} \frac{n^{1-4\epsilon}}{2p_n^3} \ge \tfrac{1}{2} \liminf_{n\to\infty} n^{1/7-4\epsilon} = \infty,$$

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 $p_n \le n^{2/7}$ 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

$$\liminf_{n\to\infty} \delta(n) \ge \liminf_{n\to\infty} \left[\frac{n}{2p_n^3} \left(\frac{\phi(n)}{n} \right)^4 \right].$$

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. $\square$

6. Proof of Theorem 2.3

Proof. 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

$$\delta(n) = \frac{1}{n^2}\|V_r\|_4^4 - 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 - 58p_n^{-1/2}(\log n)^{7/2}. \tag{6-1}$$

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 using Theorem 2.1 and the condition (2-3), we 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), from (6-1) we obtain

$$\liminf_{n\to\infty} \delta(n) = \liminf_{n\to\infty}\left[\frac{1}{n^2}\|V_r\|_4^4 - 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2\right] \tag{6-4}$$

$$= \liminf_{n\to\infty}\left[\frac{1}{n^2}\|V_r\|_4^4\left(1 - \frac{8p_n^{-1/2}n(\log n)^{3/2}}{\|V_r\|_4^2}\right)\right]. \tag{6-5}$$

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

$$8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 \leq 8p_n^{-1}(\log n)^4,$$

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 have established the claim (6-3). $\square$

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 [Alon and Spencer 2008, Theorem A.1.16].

Lemma 7.1. *Let $X_1, X_2, \ldots, X_m$ 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* $a \ge 0$,

$$\Pr\biggl(\biggl|\sum_{j=1}^{m} X_j\biggr|^2 \ge a\biggr) \le 2e^{-a/(2m)}.$$

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 $n \to \infty$,*

$$\Pr(\|V_r\|_4^4 < 288[\psi(n)]^2 \log n) \to 1.$$

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 [Spencer 1985, page 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

$$\begin{aligned}\Pr\big(\max_{0 \le j < 4n} |V_r(\zeta_{4n}^j)|^2 \ge a(n)\big) &\le \sum_{j=0}^{4n-1} \Pr(|V_r(\zeta_{4n}^j)|^2 \ge a(n)) \\ &\le \sum_{j=0}^{4n-1} \Bigl[\Pr\bigl(|\mathrm{Re}(V_r(\zeta_{4n}^j))|^2 \ge \tfrac{1}{2}a(n)\bigr) + \Pr\bigl(|\mathrm{Im}(V_r(\zeta_{4n}^j))|^2 \ge \tfrac{1}{2}a(n)\bigr)\Bigr].\end{aligned} \tag{7-2}$$

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, 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

$$\begin{aligned}\Pr(|\mathrm{Re}(V_r(\lambda))|^2 \ge \tfrac{1}{2}a(n)) &= \Pr\biggl(\Bigl| \sum_{\substack{\ell=0 \\ \gcd(\ell,n)>1}}^{n-1} v_\ell \mathrm{Re}(\lambda^{k(\ell)}) \Bigr|^2 \ge \tfrac{1}{2}a(n)\biggr) \\ &\le 2e^{-(1/(2\psi(n)))\cdot(a(n)/2)}\end{aligned}$$

by application of Lemma 7.1. By the definition of $a(n)$ we then obtain

$$\Pr\bigl(|\mathrm{Re}(V_r(\lambda))|^2 \ge \tfrac{1}{2}a(n)\bigr) \le 2n^{-2},$$

and, by similar reasoning,

$$\Pr\bigl(|\mathrm{Im}(V_r(\lambda))|^2 \ge \tfrac{1}{2}a(n)\bigr) \le 2n^{-2}.$$

Substitution in (7-2) then gives

$$\Pr\Bigl(\max_{0\le j<4n} |V_r(\zeta_{4n}^j)|^2 \ge a(n)\Bigr) \le 16n^{-1},$$

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

$$\mathcal{U}_n := \{V \in \mathcal{V}_n : \|V_r\|_4^4 < 288 p_n^{-2} n^2 (\log n)^3\}. \tag{7-3}$$

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,

$$\begin{aligned}&\Bigl|\frac{1}{F(J_r+V_r)} - \frac{1}{f(r)}\Bigr| \\ &\qquad\le \Bigl|\frac{1}{F(J_r+V_r)} - \Bigl(\frac{\phi(n)}{n}\Bigr)^2 \frac{1}{F(J_r)}\Bigr| + \Bigl|\Bigl(\frac{\phi(n)}{n}\Bigr)^2 \frac{1}{F(J_r)} - \frac{1}{f(r)}\Bigr|.\end{aligned} \tag{7-5}$$

Using the condition (2-4) and the growth rate (3-2) of $\phi(n)$, from Theorem 2.1, we find that

$$\Bigl|\Bigl(\frac{\phi(n)}{n}\Bigr)^2 \frac{1}{F(J_r)} - \frac{1}{f(r)}\Bigr| \to 0. \tag{7-6}$$

From Proposition 3.4 we have

$$\left|\frac{1}{F(J_r+V_r)} - \left(\frac{\phi(n)}{n}\right)^2 \frac{1}{F(J_r)}\right| < \gamma(n) \tag{7-7}$$

for $V \in \mathcal{U}_n$, 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

$$\left|\frac{1}{F(J_r+V_r)} - \frac{1}{f(r)}\right| \to 0$$

in probability. Since $f(r)$ takes values only in a finite interval bounded away from 0, we then have

$$|F(J_r + V_r) - f(r)| \to 0$$

in probability, which completes the proof. □

8. Proof of Theorem 2.5

Proof. 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

$$\gamma(n) = \frac{1}{n^2}\|V_r\|_4^4 + 8p_n^{-1/2}n^{-1}(\log n)^{3/2}\|V_r\|_4^2 + 58p_n^{-1/2}(\log n)^{7/2}. \tag{8-2}$$

From (3-11), Lemma 3.3, (3-7), and the upper bound (3-4) for $\psi(n)$, we also have

$$\|V_r\|_4^4 \le (2\log n)^2\big(\max_{0\le k<n}|V(\zeta_n^k)|^2\big)p_n^{-1}n\log n. \tag{8-3}$$

We now bound the term $|V(\zeta_n^k)|$. By the definition of V we have, for integer k,

$$V(\zeta_n^k) = \sum_{\substack{j=0\\ \gcd(j,n)>1}}^{n-1}\left(j \mid \frac{n}{\gcd(j,n)}\right)\zeta_n^{kj} = \sum_{\substack{0<m<n\\ m\mid n}}\ \sum_{\substack{\ell=0\\ \gcd(\ell,m)=1}}^{m-1}\left(\frac{\ell n}{m} \mid m\right)\zeta_m^{k\ell}$$

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 $(\ell \mid m) = 0$ for $\gcd(\ell, m) > 1$, we then have

$$V(\zeta_n^k) = \sum_{\substack{0<m<n \\ m \mid n}} \Big(\frac{n}{m} \mid m\Big) \sum_{\ell=0}^{m-1} (\ell \mid m) \zeta_m^{k\ell},$$

and therefore

$$|V(\zeta_n^k)| \le \sum_{\substack{0<m<n \\ m \mid n}} \left| \sum_{\ell=0}^{m-1} (\ell \mid m) \zeta_m^{k\ell} \right| \le \sum_{\substack{0<m<n \\ m \mid n}} m^{1/2}$$

by Lemma 3.2. Hence

$$|V(\zeta_n^k)| \le \sum_{j=1}^{\omega(n)} \binom{\omega(n)}{j} \Big(\frac{n}{p_n^j}\Big)^{1/2} < n^{1/2}(1 + p_n^{-1/2})^{\omega(n)} \le n^{1/2}(1 + (\log n)^{-7/2})^{\log n}$$

for all sufficiently large n, by (2-5) and (3-1). Hence $|V(\zeta_n^k)| = O(n^{1/2})$. Substitute in (8-3) to give

$$\|V_r\|_4^4 = O(p_n^{-1} n^2 (\log n)^3),$$

and then substitute in (8-2) to show that

$$\gamma(n) = O(p_n^{-1}(\log n)^3) + O(p_n^{-1}(\log n)^3) + O(p_n^{-1/2}(\log n)^{7/2}) \to 0,$$

by the condition (2-5). The desired 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

Proof. Let $V \in \mathscr{V}_n$. From Proposition 3.4 we have

$$\left| \frac{1}{F(J_r + V_r)} - \Big(\frac{\phi(n)}{n}\Big)^2 \frac{1}{F(J_r)} \right| < \gamma(n), \tag{9-1}$$

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

$$\gamma(n) = O(p_n^{-3} n) + O(p_n^{-2} n^{1/2} (\log n)^{3/2}) + O(p_n^{-1/2}(\log n)^{7/2}).$$

By the condition (2-7) we have $\gamma(n) \to 0$, and the desired result follows from (9-1) and Theorem 2.1, using the growth rate (3-2) of $\phi(n)$ and the condition (2-7). □

References

[Alon and Spencer 2008] N. Alon and J. H. Spencer, *The probabilistic method*, 3rd ed., Wiley, Hoboken, NJ, 2008. MR 2009j:60004 Zbl 1148.05001

[Apostol 1976] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976. MR 55 #7892 Zbl 0335.10001

[Beck 1991] J. Beck, "Flat polynomials on the unit circle — note on a problem of Littlewood", *Bull. London Math. Soc.* **23**:3 (1991), 269–277. MR 93b:42002 Zbl 0748.30006

[Beenker et al. 1985] 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. Zbl 0573.94005

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

[Berndt et al. 1998] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley, New York, 1998. MR 99d:11092 Zbl 0906.11001

[Borwein 2002] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics **10**, Springer, New York, 2002. MR 2003m:11045 Zbl 1020.12001

[Borwein and Choi 2001] P. Borwein and K.-K. S. Choi, "Merit factors of polynomials formed by Jacobi symbols", *Canad. J. Math.* **53**:1 (2001), 33–50. MR 2002k:11114 Zbl 0964.11020

[Borwein and Choi 2002] P. Borwein and K.-K. S. Choi, "Explicit merit factor formulae for Fekete and Turyn polynomials", *Trans. Amer. Math. Soc.* **354**:1 (2002), 219–234. MR 2002i:11065 Zbl 1010.11017

[Borwein and Lockhart 2001] P. Borwein and R. Lockhart, "The expected L_p norm of random polynomials", *Proc. Amer. Math. Soc.* **129**:5 (2001), 1463–1472. MR 2001m:60124 Zbl 0999.30004

[Borwein et al. 2001] P. Borwein, K.-K. S. Choi, and S. Yazdani, "An extremal property of Fekete polynomials", *Proc. Amer. Math. Soc.* **129**:1 (2001), 19–27. MR 2001j:11061 Zbl 0987.11010

[Borwein et al. 2004] P. Borwein, K.-K. S. Choi, and J. Jedwab, "Binary sequences with merit factor greater than 6.34", *IEEE Trans. Inform. Theory* **50**:12 (2004), 3234–3249. MR 2103494

[Conrey et al. 2000] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, "Zeros of Fekete polynomials", *Ann. Inst. Fourier* (*Grenoble*) **50**:3 (2000), 865–889. MR 2001h:11108 Zbl 1007.11053

[Erdős 1962] P. Erdős, "An inequality for the maximum of trigonometric polynomials", *Ann. Polon. Math.* **12** (1962), 151–154. MR 25 #5330 Zbl 0106.27702

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

[Golay 1983] M. J. E. Golay, "The merit factor of Legendre sequences", *IEEE Trans. Inform. Theory* **29**:6 (1983), 934–936. Zbl 0537.94009

[Hardy and Wright 1954] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3rd ed., Clarendon, Oxford, 1954. MR 16,673c Zbl 0058.03301

[Høholdt and Jensen 1988] T. Høholdt and H. E. Jensen, "Determination of the merit factor of Legendre sequences", *IEEE Trans. Inform. Theory* **34**:1 (1988), 161–164. Zbl 0652.40006

[Jedwab 2005] J. Jedwab, "A survey of the merit factor problem for binary sequences", pp. 30–55 in *Sequences and their applications – SETA 2004*, edited by T. Helleseth et al., Lecture Notes in Computer Science **3486**, Springer, New York, 2005. Zbl 1145.94419

[Jensen et al. 1991] 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 (1991), 617–626. MR 92j:94009 Zbl 0731.94011

[Littlewood 1966] 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. MR 33 #4237 Zbl 0142.32603

[Littlewood 1968] J. E. Littlewood, *Some problems in real and complex analysis*, D. C. Heath, Lexington, MA, 1968. MR 39 #5777 Zbl 0185.11502

[Montgomery 1980] H. L. Montgomery, "An exponential polynomial formed with the Legendre symbol", *Acta Arith.* **37** (1980), 375–380. MR 82a:10041 Zbl 0369.10024

[Newman 1960] D. J. Newman, "Norms of polynomials", *Amer. Math. Monthly* **67** (1960), 778–779. MR 23 #A2510 Zbl 0102.05904

[Newman and Byrnes 1990] D. J. Newman and J. S. Byrnes, "The L^4 norm of a polynomial with coefficients ± 1", *Amer. Math. Monthly* **97**:1 (1990), 42–45. MR 91d:30006

[Paterson and Tarokh 2000] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios", *IEEE Trans. Inform. Theory* **46**:6 (2000), 1974–1987. MR 2001j:94012 Zbl 0998.94006

[Schmidt et al. 2009] K.-U. Schmidt, J. Jedwab, and M. G. Parker, "Two binary sequence families with large merit factor", *Adv. Math. Commun.* **3**:2 (2009), 135–156. MR 2010b:94036 Zbl 1191.94083

[Spencer 1985] J. Spencer, "Six standard deviations suffice", *Trans. Amer. Math. Soc.* **289**:2 (1985), 679–706. MR 86k:05004 Zbl 0577.05018

[Turyn 1968] R. Turyn, "Sequences with small correlation", pp. 195–228 in *Error correcting codes* (Madison, WI, 1968), edited by H. B. Mann, Wiley, New York, 1968. MR 39 #3897 Zbl 0169.51002

[Xiong and Hall 2008] T. Xiong and J. I. Hall, "Construction of even length binary sequences with asymptotic merit factor 6", *IEEE Trans. Inform. Theory* **54**:2 (2008), 931–935. MR 2010e:94183

[Xiong and Hall 2010] T. Xiong and J. I. Hall, "Modifications on character sequences and construction of large even length binary sequences", preprint, 2010.

[Xiong and Hall 2011] T. Xiong and J. I. Hall, "Modifications of modified Jacobi sequences", *IEEE Trans. Inform. Theory* **57**:1 (2011), 493–504. MR 2012a:94145

Received August 4, 2011.

JONATHAN JEDWAB
DEPARTMENT OF MATHEMATICS
SIMON FRASER UNIVERSITY
8888 UNIVERSITY DRIVE
BURNABY, BC V5A 1S6
CANADA
jed@sfu.ca

KAI-UWE SCHMIDT
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

kaiuwe.schmidt@ovgu.de

PACIFIC JOURNAL OF MATHEMATICS

http://pacificmath.org

Founded in 1951 by
E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or pacificmath.org for submission instructions.

The subscription price for 2012 is US $420/year for the electronic version, and $485/year for print and electronic.
Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. Prior back issues are obtainable from Periodicals Service Company, 11 Main Street, Germantown, NY 12526-5635. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and the Science Citation Index.

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 969 Evans Hall, Berkeley, CA 94720-3840, is published monthly except July and August. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS
at the University of California, Berkeley 94720-3840
A NON-PROFIT CORPORATION
Typeset in LaTeX

PACIFIC JOURNAL OF MATHEMATICS

Volume 257 No. 2 June 2012

Extending triangulations of the 2-sphere to the 3-disk preserving a 4-coloring 257
RUI PEDRO CARPENTIER

Orthogonal quantum group invariants of links 267
LIN CHEN and QINGTAO CHEN

Some properties of squeezing functions on bounded domains 319
FUSHENG DENG, QIAN GUAN and LIYOU ZHANG

Representations of little q-Schur algebras 343
JIE DU, QIANG FU and JIAN-PAN WANG

Renormalized weighted volume and conformal fractional Laplacians 379
MARÍA DEL MAR GONZÁLEZ

The L_4 norm of Littlewood polynomials derived from the Jacobi symbol 395
JONATHAN JEDWAB and KAI-UWE SCHMIDT

On a conjecture of Kaneko and Ohno 419
ZHONG-HUA LI

Categories of unitary representations of Banach–Lie supergroups and restriction functors 431
STÉPHANE MERIGON, KARL-HERMANN NEEB and HADI SALMASIAN

Odd Hamiltonian superalgebras and special odd Hamiltonian superalgebras of formal vector fields 471
LI REN, QIANG MU and YONGZHENG ZHANG

Interior derivative estimates for the Kähler–Ricci flow 491
MORGAN SHERMAN and BEN WEINKOVE

Two-dimensional disjoint minimal graphs 503
LINFENG ZHOU

0030-8730(201206)257:2;1-5