Canad. J. Math. Vol. **53** (1), 2001 pp. 33–50

# Merit Factors of Polynomials Formed by Jacobi Symbols

Peter Borwein and Kwok-Kwong Stephen Choi

*Abstract.* We give explicit formulas for the $L_4$ norm (or equivalently for the merit factors) of various sequences of polynomials related to the polynomials

$$f(z) := \sum_{n=0}^{N-1} \left(\frac{n}{N}\right) z^n.$$

and

$$f_t(z) = \sum_{n=0}^{N-1} \left(\frac{n+t}{N}\right) z^n.$$

where $(\frac{\cdot}{N})$ is the Jacobi symbol.

Two cases of particular interest are when $N = pq$ is a product of two primes and $p = q + 2$ or $p = q + 4$. This extends work of Høholdt, Jensen and Jensen and of the authors.

This study arises from a number of conjectures of Erdős, Littlewood and others that concern the norms of polynomials with $-1, 1$ coefficients on the disc. The current best examples are of the above form when $N$ is prime and it is natural to see what happens for composite $N$.

## 1 Introduction

There are a number of old conjectures of Erdős, Littlewood, Turyn and others that concern the norms of polynomials with $-1, 1$ coefficients. See [BC-98], [BC-99], [E-57], [E-62], [L-68], [NB-90], [S-90], [M-94].

Littlewood's conjecture is that it is possible to find $p$ a polynomial of degree $n$ with coefficients $-1, 1$ so that

$$C_1\sqrt{n} \le |p(z)| \le C_2\sqrt{n}$$

for all $z$ of modulus 1 and for two constants $C_1, C_2$ independent of $n$. This is complemented by a conjecture of Erdős that says that the constant $C_2$ above cannot be arbitrarily close to 1. The most significant related results may be found in [K-80] and [B-95].

This latter conjecture of Erdős would be proved by showing that the $L_4$ norm of such polynomials is bounded below by $C_3\sqrt{n}$ for some $C_3 > 1$. The $L_4$ norm is attractive to work with because it computationally far more tractable than the sup

Received by the editors August 19, 1999; revised March 30, 2000.

Research of P. Borwein is supported, in part, by NSERC of Canada. K. K. Choi was a Pacific Institute of Mathematics Postdoctoral Fellow and the Institute's support is gratefully acknowledged.

AMS subject classification: 11J54, 11B83, 12-04.

Keywords: Character polynomial, Class Number, $-1, 1$ coefficients, Merit factor, Fekete polynomials, Turyn Polynomials, Littlewood polynomials, Twin Primes, Jacobi Symbols.





https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

norm. These problems arose separately in the mathematics community and the engineering community. In the engineering community the problems arose as signal processing questions and here again the $L_4$ norm is natural to consider [G-83].

The example, due to Turyn and proved by Høholdt and Jensen [HJ-88], that gives the smallest asymptotic $L_4$ norm is of the form

$$f_p(z) = \sum_{n=0}^{p-1} \left( \frac{n + [p/4]}{p} \right) z^n$$

where $(\frac{\cdot}{p})$ is the Legendre symbol and $p$ is prime. (Recall that the Legendre symbol $(\frac{n}{p})$ is 1 if $n$ is a quadratic residue mod $p$ and is $-1$ otherwise.) This is discussed in [BC-98] where explicit formulae for these $L_4$ norms are given. In the above case the $L_4$ norm is asymptotic to $(7/6)^{1/4} p^{1/2}$.

In this paper we extend the analysis to the non-prime case.

Suppose $N$ is odd. Let $\chi(n)$ be a real primitive character modulo $N$. Then $N$ is a product of distinct primes $p_1 p_2 \cdots p_r$ with $p_1 < p_2 < \cdots p_r$ and

$$\chi(n) = \left( \frac{n}{p_1 p_2 \cdots p_r} \right) \tag{1.1}$$

where $\left(\frac{n}{N}\right)$ is the Jacobi symbol. We consider the polynomial formed by $\chi(n)$ as

$$f(z) := \sum_{n=0}^{N-1} \chi(n) z^n = \sum_{n=0}^{N-1} \left( \frac{n}{N} \right) z^n. \tag{1.2}$$

Then $f(z)$ is a polynomial having coefficients either 0 or $\pm 1$. We also consider the shifted polynomial $f_t(z)$ by shifting the coefficients of $f(z)$ to the left by $t$. Thus, if $1 \le t \le N$, then

$$f_t(z) = \sum_{n=0}^{N-1} \left( \frac{n+t}{N} \right) z^n. \tag{1.3}$$

In particular, $f_N(z) = f(z)$.

We are particularly interested in the behavior of the growth of the $L_4$ norm of these polynomials. For the case that $N$ is a product of twin primes, we are able to derive an exact formula for the $L_4$ norm of the unshifted polynomial $f(z)$. A similar formula for the case when $N = pq$ with odd primes $p$, $q$, $p = q + 4$ and $p \equiv 3 \pmod 4$ can also be derived. We have the following theorem.

***Theorem 1.1*** *Let $N = pq$ and $f(z)$ be the polynomial defined in (1.2). If $p = q + 2$, then*

$$\begin{aligned} \|f\|_4^4 = {} & \frac{1}{3}\big(5N^2 + 9N + 4 - (8N+1)(p+q)\big) \\ & + 24\frac{q^3}{N^2}\left(2 - \left(\frac{2}{p}\right)\right) h_p^2 - 24\frac{p^3}{N^2}\left(1 - \left(\frac{2}{q}\right)\right) h_q^2 + \frac{12}{N^2} h_N^2 \end{aligned}$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

*and if* $p = q + 4$ *and* $q \equiv 3 \pmod 4$ *then*

$$\|f\|_4^4 = \frac{1}{3}\big(5N^2 + 9N + 4 - (8N+1)(p+q)\big) + 12\frac{q^3}{N^2}\left(5 - 3\left(\frac{2}{p}\right)\right)h_p^2 - 36\frac{p^3}{N^2}\left(1 - \left(\frac{2}{q}\right)\right)h_q^2 + \frac{12}{N^2}h_N^2$$

*where* $h_l := \sum_{n=1}^{l-1} n\left(\frac{n}{l}\right)$ *for odd integer* $l$*.*

For the general case, we obtain an asymptotic estimation for the $L_4$ norm and prove

***Theorem 1.2*** *Let* $N = p_1 p_2 \cdots p_r$ *with* $p_1 < p_2 < \cdots < p_r$ *and* $f_t(z)$ *is defined in (1.3) with* $1 \le t \le N$*. Then*

$$\|f_t\|_4^4 = \frac{5}{3}N^2 - 4Nt + 8t^2 + O\left(\frac{N^{2+\epsilon}}{p_1}\right). \tag{1.4}$$

Theorem 1.2 immediately implies that if we define the merit factor of a sequence $\{x_n\}_{n=0}^{N-1}$ by

$$MF = \frac{\|F\|_2^4}{\|F\|_4^4 - \|F\|_2^4}$$

where $F(z) := \sum_{n=0}^{N-1} x_n z^n$, then from (1.4), we have the merit factor $MF$ of the Jacobi sequence satisfying

$$\frac{1}{MF} = \frac{2}{3} - 4\frac{t}{N} + 8\left(\frac{t}{N}\right)^2 + O(N^\epsilon p_1^{-1}).$$

It follows that if $N^\epsilon p_1^{-1} \longrightarrow 0$ when $N \longrightarrow \infty$, then

$$\frac{1}{MF} \longrightarrow \frac{2}{3} - 4\frac{t}{N} + 8\left(\frac{t}{N}\right)^2.$$

In particular for $t$ approximately $N/4$ the merit factors approach 6 which is conjectured by some to be best possible [G-83].

This should be compared with the result of T. Høholdt, H. Jensen and J. Jensen in [HJJ-91]. They showed that the same asymptotic formula but a weaker error term $O(\frac{(p+q)^5 \log^4 N}{N^3})$ for the special case $N = pq$. So we generalize their result to $N = p_1 p_2 \cdots p_r$ and also improve the error term.

Additional history of this problem is outlined in [BC-98] and [BC-99].

## 2 $L_4$ Norm for Character Polynomial

Let $\chi$ be a non-principal primitive character mod $N$. Let

$$f(z) := \sum_{n=0}^{N-1} \chi(n) z^n$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

be the character polynomial associated to $\chi$. Let $\omega := e^{2\pi i/N}$ and $\tau(\chi)$ be the Gaussian sum defined by

$$\tau(\chi) := \sum_{n=0}^{N-1} \chi(n)\omega^n.$$

Since $\chi$ is primitive,

$$f(\omega^k) = \tau(\chi)\overline{\chi}(k). \tag{2.1}$$

for $k = 0, 1, \ldots, N-1$. Also we have $|\tau(\chi)|^2 = N$ and $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$ (see Chapter 8 in [A-80]). The shifted polynomial $f_t(z)$ by shifting the coefficients of $f(z)$ to the left by $t$ is defined as

$$f_t(z) := \sum_{n=0}^{N-1} \chi(n+t) z^n$$

for $1 \le t \le N$ and $f_N(z) = f(z)$. It is easy to see that

$$f_t(\omega^k) = \omega^{-tk} f(\omega^k) \tag{2.2}$$

for any $0 \le k \le N-1$. We are interested in estimating the $L_4$ norm of $f_t(z)$. It can be shown (see [HJ-88], [BC-98]) that

$$\|f_t\|_4^4 = \frac{1}{2N}\left\{ \sum_{k=0}^{N-1} |f_t(\omega^k)|^4 + \sum_{k=0}^{N-1} |f_t(-\omega^k)|^4 \right\}. \tag{2.3}$$

Using (2.1) and (2.2), the first summation above is $N^2\phi(N)$. It remains to evaluate the second summation

$$\sum_{k=0}^{N-1} |f_t(-\omega^k)|^4.$$

For $1 \le t \le N$ and $0 \le k \le N-1$, we have

$$f_{N-t+1}(-\omega^k) = \omega^{-k}\chi(-1) f_t(-\omega^{-k}).$$

In particular, we have $|f_t(-\omega^k)| = |f_{N-t+1}(-\omega^{-k})|$ for $0 \le k \le N-1$ and hence from now on we may assume $1 \le t \le (N+1)/2$.

We employ an interpolation formula as in [HJ-88], [BC-98] and by (2.8), (2.9) and (2.10) in [BC-99] which is

$$\sum_{k=0}^{N-1} |f_t(-\omega^k)|^4 = \frac{16}{N^4}(A + B + C) \tag{2.4}$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

where

(2.5)

$$A = \frac{1}{48}N^2(N^2+2)\sum_{a=0}^{N-1}|f_t(\omega^a)|^4$$

$$B = -\frac{N^2}{2}\Re\left\{\sum_{a=0}^{N-1}|f_t(\omega^a)|^2 f_t(\omega^a)\sum_{k=1}^{N-1}\frac{\overline{f_t(\omega^{a-k})}(\omega^k+1)}{|\omega^k-1|^2}\right\}$$

$$C = N^2\sum_{a=0}^{N-1}|f_t(\omega^a)|^2\left|\sum_{k=1}^{N-1}\frac{f_t(\omega^{a-k})}{\omega^k-1}\right|^2 - \frac{N^2}{2}\Re\left\{\sum_{a=0}^{N-1}\overline{f_t(\omega^a)^2}\left(\sum_{k=1}^{N-1}\frac{f_t(\omega^{a-k})}{\omega^k-1}\right)^2\right\}.$$

In this section, we will simplify the terms $A$, $B$ and $C$ by using (2.1) and evaluate them in the next section. Using (2.1) and (2.2), we have

$$A = \frac{N^4(N^2+2)\phi(N)}{48}. \tag{2.6}$$

Using (2.1) and (2.2) again, we have

$$\begin{aligned} B &= -\frac{N^4}{2}\Re\left\{\sum_{k=1}^{N-1}\frac{\omega^{-tk}(\omega^k+1)}{|\omega^k-1|^2}\sum_{n=0}^{N-1}\overline{\chi(n)}\chi(n-k)\right\} \\ &= \frac{N^4}{2}\Re\left\{\sum_{k=1}^{N-1}\frac{\omega^{tk}(\omega^k+1)}{(\omega^k-1)^2}\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\right\} \\ &= \frac{N^2}{2}\Re\Big\{\sum_{a,b=1}^{N-1}ab\sum_{k=1}^{N-1}\omega^{k(t+a+b)}(\omega^k+1)\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\Big\} \\ &= \frac{N^2}{2}\Re\Big\{\sum_{a,b=1}^{N-1}ab\sum_{k=0}^{N-1}(\omega^{k(1+t+a+b)}+\omega^{k(t+a+b)})\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\Big\} \\ &\quad -\frac{N^4(N-1)^2\phi(N)}{4}, \end{aligned} \tag{2.7}$$

because

$$\frac{1}{\omega^j-1} = \frac{1}{N}\sum_{n=1}^{N-1}n\omega^{jn} \tag{2.8}$$

for $j = 1, 2, \ldots, N-1$.

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

For the term $C$, the second term in (2.5) equals

$$= -\frac{N^2}{2}\Re\left\{\sum_{a=0}^{N-1}\overline{f_t(\omega^a)^2}\left(\sum_{k=1}^{N-1}\frac{f_t(\omega^{a-k})}{\omega^k-1}\right)^2\right\}$$

$$= -\frac{N^4}{2}\Re\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\sum_{k=1}^{N-1}\frac{\omega^{kt}\overline{\chi(a-k)}}{\omega^k-1}\right)^2\right\}$$

$$= -\frac{N^4}{2}\Re\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\frac{1}{N}\sum_{n=1}^{N-1}n\sum_{k=1}^{N-1}\overline{\chi(a-k)}\omega^{k(t+n)}\right)^2\right\}$$

from (2.1) and (2.8). Using (2.1) again, this is equal to

$$= -\frac{N^4}{2}\Re\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\frac{\overline{\tau(\chi)}}{N}\sum_{n=1}^{N-1}n\chi(n+t)\omega^{a(t+n)}-\frac{N-1}{2}\overline{\chi(a)}\right)^2\right\}$$

$$= -\frac{N^4}{2}\Re\left\{\frac{\overline{\tau(\chi)}^2}{N^2}\sum_{n,m=1}^{N-1}nm\chi(n+t)\chi(m+t)\sum_{a=0}^{N-1}\chi^2(a)\omega^{a(n+m+2t)}\right\}$$

$$-\frac{N^4}{2}\left(\frac{N-1}{2}\right)^2\phi(N)+\frac{N^4(N-1)}{2}\Re\left\{\frac{\overline{\tau(\chi)}}{N}\sum_{n=1}^{N-1}n\chi(n+t)f(\omega^{t+n})\right\} \tag{2.9}$$

$$= -\frac{N^2}{2}\Re\left\{\overline{\tau(\chi)}^2\sum_{n,m=1}^{N-1}nm\chi(n+t)\chi(m+t)\sum_{a=0}^{N-1}\chi^2(a)\omega^{a(n+m+2t)}\right\}$$

$$-\frac{N^4(N-1)^2\phi(N)}{8}+\frac{N^4(N-1)}{2}\sum_{\substack{n=1\\(n+t,N)=1}}^{N-1}n.$$

Similarly, the first term in (2.5) equals

$$= N^2\sum_{a=0}^{N-1}|f_t(\omega^a)|^2\left|\sum_{k=1}^{N-1}\frac{f_t(\omega^{a-k})}{\omega^k-1}\right|^2$$

$$= N^4\sum_{a=0}^{N-1}|\chi^2(a)|\left|\sum_{k=1}^{N-1}\frac{\omega^{kt}\overline{\chi(a-k)}}{\omega^k-1}\right|^2$$

$$= N^3\sum_{nm=1}^{N-1}nm\chi(n+t)\overline{\chi(m+t)}\sum_{a=0}^{N-1}|\chi^2(a)|\omega^{a(n-m)} \tag{2.10}$$

$$+\frac{N^4(N-1)^2\phi(N)}{4}-N^4(N-1)\sum_{\substack{n=1\\(n+t,N)=1}}^{N-1}n$$

and hence from (2.5), (2.9) and (2.10)

$$
\begin{aligned}
C = &-\frac{N^2}{2}\Re\Big\{\overline{\tau(\chi)}^2\sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)\sum_{a=0}^{N-1}\chi^2(a)\omega^{a(n+m+2t)}\Big\}\\
&+\frac{N^4(N-1)^2\phi(N)}{8}+N^3\sum_{nm=1}^{N-1} nm\chi(n+t)\overline{\chi(m+t)}C_N(n-m)\\
&-\frac{N^4(N-1)}{2}\sum_{\substack{n=1\\(n+t,N)=1}}^{N-1} n
\end{aligned}
\tag{2.11}
$$

where $C_k(l)$ is the usual Ramanujan sum defined as

$$
C_k(l)=\sum_{\substack{n=0\\(n,k)=1}}^{k-1} e^{\frac{2\pi inl}{k}}.
$$

We remark that formulas (2.3), (2.4), (2.6), (2.7) and (2.11) hold for any non-principal primitive character. In the next section, we will confine our consideration to the Jacobi symbol.

## 3 Real Primitive Character Modulo $pq$

***Lemma 3.1*** *If $1\le k\le N$, then*

$$
\sum_{\substack{n,m=1\\k+n+m\equiv 0 \pmod N}}^{N-1} nm=\frac{N}{6}(N^2-6N-1+6k+3Nk-3k^2).
$$

**Proof** This is Lemma 2 in [BC-98]. ■

***Lemma 3.2*** *Let $p_1,p_2,\dots,p_r$ be distinct primes and $\chi=\chi_1\chi_2\cdots\chi_r$ where $\chi_j$ are non-principal characters modulo $p_j$. Let $N=p_1p_2\cdots p_r$. Then*

$$
\sum_{k=0}^{N-1}\omega^{kl}\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}=\begin{cases}N & \text{if } (l,N)=1,\\ 0 & \text{otherwise.}\end{cases}
\tag{3.1}
$$

**Proof** Let $\omega_q=e^{\frac{2\pi i}{q}}$. Then

$$
\begin{aligned}
&\sum_{k_1=0}^{p_1-1}\cdots\sum_{k_r=0}^{p_r-1}\omega_{p_1}^{k_1 l}\cdots\omega_{p_r}^{k_r l}\sum_{n_1=0}^{p_1-1}\cdots\sum_{n_r=0}^{p_r-1}\chi_1(n_1)\overline{\chi_1(n_1-k_1)}\cdots\chi_r(n_r)\overline{\chi_r(n_r-k_r)}\\
&=\prod_{j=1}^{r}\sum_{k_j=0}^{p_j-1}\omega_{p_j}^{k_j l}\sum_{n_j=0}^{p_j-1}\chi_j(n_j)\overline{\chi_j(n_j-k_j)}\\
&=\prod_{j=1}^{r}\Big\{p_j-\sum_{k_j=0}^{p_j-1}\omega_{p_j}^{k_j l}\Big\}
\end{aligned}
$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

because

$$\sum_{n_j=0}^{p_j-1} \chi_j(n_j)\overline{\chi_j(n_j-k_j)} = \begin{cases} p_j - 1 & \text{if } p_j | k_j, \\ 0 & \text{otherwise.} \end{cases}$$

Hence the summation in (3.1) equals $N$ if $(l, N) = 1$ and 0 otherwise. ■

From (2.7), we have if $p_1, p_2, \ldots, p_r$ are distinct primes and $\chi = \chi_1\chi_2\cdots\chi_r$ with non-principal characters $\chi_j$ modulo $p_j$, then

$$B = \frac{N^3}{2} \sum_{\substack{a,b=1 \\ (a+b+t+1,N)=1}}^{N-1} ab + \frac{N^3}{2} \sum_{\substack{a,b=1 \\ (a+b+t,N)=1}}^{N-1} ab - \frac{N^4(N-1)^2\phi(N)}{4} \tag{3.2}$$

by Lemma 3.2.

***Lemma 3.3*** *If $N = pq$ then we have*

$$\sum_{\substack{a,b=1 \\ (a+b,N)=1}}^{N-1} ab = \frac{1}{12} N(3N^2 - 7N - 2)\phi(N) \tag{3.3}$$

*and*

$$\sum_{\substack{a,b=1 \\ (a+b+1,N)=1}}^{N-1} ab = \frac{1}{12} N(N-1)(3N-4)\phi(N) \tag{3.4}$$

**Proof** Write

(3.5)
$$\sum_{\substack{a,b=1 \\ (a+b,N)=1}}^{N-1} ab = \sum_{a,b=1}^{N-1} ab - \sum_{\substack{a,b=1 \\ a+b\equiv 0 \pmod p}}^{N-1} ab - \sum_{\substack{a,b=1 \\ a+b\equiv 0 \pmod q}}^{N-1} ab + \sum_{\substack{a,b=1 \\ a+b\equiv 0 \pmod N}}^{N-1} ab.$$

We then apply Lemma 3.1 to the last three summations. Formula (3.4) can be proved in the same way. ■

Now from (3.2)–(3.4), if $t = N$ and $N = pq$, then we have

$$B = -\frac{1}{12} N^4(N+2)\phi(N). \tag{3.6}$$

***Lemma 3.4*** *If $N = pq$, then we have*

$$\sum_{\substack{a=1 \\ (a,N)=1}}^{N-1} a = \frac{1}{2} N\phi(N) \tag{3.7}$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

*and*

$$\sum_{\substack{a=1\\(a,N)=1}}^{N-1} a^2 = \frac{1}{6}N(2N+1)\phi(N). \tag{3.8}$$

**Proof** The proof is similar to Lemma 3.3. ∎

It remains to compute the term $C$ using (2.11). Suppose $\chi$ is real and $t = N$. Then the first term in (2.11) equals

$$\begin{aligned}
&= -\left(\frac{-1}{N}\right)\frac{N^3}{2}\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n+m)\\
&= -\left(\frac{-1}{N}\right)\frac{N^3}{2}\sum_{n,m=1}^{N-1} n(N-m)\left(\frac{n(-m)}{N}\right)C_N(n-m)\\
&= -\frac{N^4}{2}\sum_{n=1}^{N-1} n\left(\frac{n}{N}\right)\sum_{m=1}^{N-1}\left(\frac{m}{N}\right)C_N(n-m) + \frac{N^3}{2}\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n-m)\\
&= -\frac{N^5}{2}\sum_{n=1}^{N-1} n\left(\frac{n}{N}\right)\left(\frac{n}{N}\right) + \frac{N^3}{2}\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n-m)\\
&= -\frac{N^5}{2}\sum_{\substack{n=1\\(n,N)=1}}^{N-1} n + \frac{N^3}{2}\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n-m).
\end{aligned}$$

Hence from this together with (2.11) and (3.7), we have

$$\begin{aligned}
C = {}&\frac{3}{2}N^3\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n-m)\\
&+\frac{N^4}{16}\left(N(N-1)^2\phi^2(N) - 4N^2\phi(N) - 8(N-1)\right).
\end{aligned} \tag{3.9}$$

The last step is to evaluate the summation

$$\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right)C_N(n-m).$$

Since $C_N(l)$ is a multiplicative function of $N$ (see Section 8.3 of [A-80]) and also if $p$ is a prime, then

$$C_p(k) = \begin{cases} -1 & \text{if } (p,k) = 1 \\ p-1 & \text{if } (p,k) \neq 1 \end{cases}$$

so if $N = pq$, then

$$\begin{aligned} \sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right) C_N(n-m) &= \sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right) C_p(n-m)C_q(n-m) \\ &= N \sum_{\substack{n=1 \\ (n,N)=1}}^{N-1} n^2 - p \sum_{\substack{n,m=0 \\ n-m\equiv 0 \pmod p}}^{N-1} nm\left(\frac{nm}{N}\right) \\ &\quad - q \sum_{\substack{n,m=0 \\ n-m\equiv 0 \pmod q}}^{N-1} nm\left(\frac{nm}{N}\right) + h_N^2. \end{aligned} \tag{3.10}$$

***Lemma 3.5*** *Let $p$ and $q$ be primes greater than 3 and $N = pq$. If $p = q+2$ then*

$$\sum_{\substack{n,m=0 \\ n\equiv m \pmod p}}^{N-1} nm\left(\frac{nm}{N}\right) = \frac{1}{12}N^2(q^2-1) + 2p^2\left(1 - \left(\frac{2}{q}\right)\right) h_q^2 \tag{3.11}$$

*and*

$$\sum_{\substack{n,m=0 \\ n\equiv m \pmod q}}^{N-1} nm\left(\frac{nm}{N}\right) = \frac{1}{12}N^2(p^2-1) - 2q^2\left(2 - \left(\frac{2}{p}\right)\right) h_p^2. \tag{3.12}$$

*If $p = q+4$ and $q \equiv 3 \pmod 4$ then*

$$\sum_{\substack{n,m=0 \\ n\equiv m \pmod p}}^{N-1} nm\left(\frac{nm}{N}\right) = \frac{1}{12}N^2(q^2-1) + 3p^2\left(1 - \left(\frac{2}{q}\right)\right) h_q \tag{3.13}$$

*and*

$$\sum_{\substack{n,m=0 \\ n\equiv m \pmod q}}^{N-1} nm\left(\frac{nm}{N}\right) = \frac{1}{12}N^2(p^2-1) - q^2\left(5 - 3\left(\frac{2}{p}\right)\right) h_p^2. \tag{3.14}$$

**Proof** We only give a proof for (3.11). The proof for (3.12)–(3.14) is similar.

(3.15)

$$\begin{aligned}
\sum_{\substack{n,m=0\\ n-m\equiv 0 \pmod p}}^{N-1} nm\left(\frac{nm}{N}\right)
&= \sum_{a,b=0}^{q-1}\sum_{\substack{n,m=0\\ n-m\equiv 0 \pmod p}}^{p-1} (n+pa)(m+pb)\left(\frac{n+pa}{pq}\right)\left(\frac{m+pb}{pq}\right)\\
&= \sum_{\substack{n,m=0\\ n-m\equiv 0 \pmod p}}^{p-1}\left(\frac{nm}{p}\right)\sum_{a,b=0}^{q-1}(n+pa)(m+pb)\left(\frac{n+pa}{q}\right)\left(\frac{m+pb}{q}\right)\\
&= p^2\sum_{\substack{n,m=0\\ n-m\equiv 0 \pmod p}}^{p-1}\left(\frac{nm}{p}\right)\sum_{a,b=0}^{q-1}ab\left(\frac{n+pa}{q}\right)\left(\frac{m+pb}{q}\right)\\
&= p^2\sum_{a,b=0}^{q-1}ab\sum_{n=1}^{p-1}\left(\frac{n+pa}{q}\right)\left(\frac{n+pb}{q}\right)\\
&= p^2\left\{\sum_{a,b=0}^{q-1}ab\sum_{n=0}^{p-1}\left(\frac{n+pa}{q}\right)\left(\frac{n+pb}{q}\right)-\sum_{a,b=0}^{q-1}ab\left(\frac{pa}{q}\right)\left(\frac{pb}{q}\right)\right\}\\
&= p^2\sum_{a,b=0}^{q-1}ab\sum_{n=0}^{p-1}\left(\frac{n+pa}{q}\right)\left(\frac{n+pb}{q}\right)-p^2h_q^2.
\end{aligned}$$

If $p = q + 2$ then

$$\begin{aligned}
\sum_{n=0}^{p-1}\left(\frac{n+pa}{q}\right)\left(\frac{n+pb}{q}\right) &= \sum_{n=0}^{q+1}\left(\frac{n+2a}{q}\right)\left(\frac{n+2b}{q}\right)\\
&= \sum_{n=0}^{q-1}\left(\frac{(n+2a)(n+2b)}{q}\right)\\
&\quad + \left(\frac{ab}{q}\right)+\left(\frac{(2a+1)(2b+1)}{q}\right).
\end{aligned} \tag{3.16}$$

The first summation on the right hand side of (3.16) (see [BEW-98, p. 58]) is

$$= \begin{cases} q-1 & \text{if } a \equiv b \pmod q\\ -1 & \text{otherwise}. \end{cases}$$

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

Hence, the first term in (3.15) is

$$
\begin{aligned}
&= p^2\Biggl\{ -\sum_{a,b=0}^{q-1} ab + q \sum_{\substack{a,b=0\\ a\equiv b \pmod q}}^{q-1} ab + \sum_{a,b=0}^{q-1} ab\left(\frac{ab}{q}\right) \\
&\qquad + \sum_{a,b=0}^{q-1} ab\left(\frac{(2a+1)(2b+1)}{q}\right)\Biggr\} \\
&= p^2\Biggl\{ -\Bigl(\frac{q(q-1)}{2}\Bigr)^2 + q\sum_{a=0}^{q-1} a^2 + h_q^2 + \Bigl(\sum_{a=0}^{q-1} a\Bigl(\frac{2a+1}{q}\Bigr)\Bigr)^2 \Biggr\} \\
&= \frac{N^2}{12}(q^2-1) + p^2\left(3 - 2\Bigl(\frac{2}{q}\Bigr)\right) h_q^2.
\end{aligned}
$$

This proves (3.11). ■

So, if $p = q + 2$, then

$$
\begin{aligned}
&\sum_{n,m=1}^{N-1} nm\left(\frac{nm}{N}\right) C_N(n-m) \\
&\qquad = \frac{N^2}{12}\bigl(4N^2 - 5N(p+q) + 6N - (p+q) + 2\bigr) \\
&\qquad\qquad - 2p^3\left(1 - \Bigl(\frac{2}{q}\Bigr)\right) h_q^2 + 2q^3\left(2 - \Bigl(\frac{2}{p}\Bigr)\right) h_p^2 + h_N^2.
\end{aligned}
$$

From (3.9), we obtain

$$
\begin{aligned}
C &= \frac{N^4}{8}\bigl(N^3 + 3N^2 + 3N + 1 - (2N^2 + N + 1)(p+q)\bigr) \\
&\qquad - 3N^3p^3\left(1 - \Bigl(\frac{2}{q}\Bigr)\right) h_q^2 + 3N^3q^3\Bigl(2 - \frac{2}{p}\Bigr) h_p^2 + \frac{3}{2}N^3 h_N^2.
\end{aligned}
$$

Therefore, using this, (2.4), (2.6) and (3.6), we have if $p = q + 2$, then

$$
\begin{aligned}
\sum_{k=0}^{N-1} |f(-\omega^k)|^4 &= \frac{N}{3}\bigl(7N^2 + 15N + 8 - (13N + 2)(p+q)\bigr) \\
&\qquad + 48\frac{q^3}{N}\left(2 - \Bigl(\frac{2}{p}\Bigr)\right) h_p^2 - 48\frac{p^3}{N}\left(1 - \Bigl(\frac{2}{q}\Bigr)\right) h_q^2 + \frac{24}{N} h_N^2
\end{aligned}
$$

and

$$
\begin{aligned}
\|f\|_4^4 &= \frac{1}{3}\bigl(5N^2 + 9N + 4 - (8N+1)(p+q)\bigr) \\
&\qquad + 24\frac{q^3}{N^2}\left(2 - \Bigl(\frac{2}{p}\Bigr)\right) h_p^2 - 24\frac{p^3}{N^2}\left(1 - \Bigl(\frac{2}{q}\Bigr)\right) h_q^2 + \frac{12}{N^2} h_N^2.
\end{aligned}
$$

Similarly, if $p = q + 4$ and $q \equiv 3 \pmod 4$ and instead of using (3.11) and (3.12) in Lemma 3.5, we employ (3.13) and (3.14), then we obtain

$$\sum_{k=0}^{N-1} |f(-\omega^k)|^4 = \frac{N}{3}\big(7N^2 + 15N + 8 - (13N + 2)(p + q)\big) + 24\frac{q^3}{N}\left(5 - 3\left(\frac{2}{p}\right)\right) h_p^2 - 72\frac{p^3}{N}\left(1 - \left(\frac{2}{q}\right)\right) h_q^2 + \frac{24}{N} h_N^2$$

and

$$\|f\|_4^4 = \frac{1}{3}\big(5N^2 + 9N + 4 - (8N + 1)(p + q)\big) + 12\frac{q^3}{N^2}\left(5 - 3\left(\frac{2}{p}\right)\right) h_p^2 - 36\frac{p^3}{N^2}\left(1 - \left(\frac{2}{q}\right)\right) h_q^2 + \frac{12}{N^2} h_N^2.$$

This proves Theorem 1.1.

## 4 Asymptotic Estimate for Real Primitive Character

Let $\chi$ be a real primitive character modulo $N$ with odd $N$. Then $N = p_1 p_2 \cdots p_r$ with $p_1 < p_2 < \cdots < p_r$ and

$$\chi(n) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right).$$

In view of (2.4), we need to estimate the term $A$, $B$ and $C$. The term $A$ has been evaluated in (2.6). We now consider the term $B$ using formula (3.2). We first prove the following lemma.

***Lemma 4.1*** *For any $1 \le t \le N$, we have*

$$\sum_{\substack{a,b=1 \\ (a+b+t,N)=1}}^{N-1} ab = \frac{1}{4}N^3\phi(N) + O(N^{3+\epsilon}). \tag{4.1}$$

*For any $1 \le t \le N$, then*

$$\sum_{\substack{n \le N \\ (n+t,N)=1}} n = \frac{1}{2}N\phi(N) + O(N^{1+\epsilon}) \tag{4.2}$$

*and*

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

$$\sum_{\substack{n\le N\\(n+t,N)=1}} n^2 = \frac{1}{3}N^2\phi(N) + O(N^{2+\epsilon}). \tag{4.3}$$

*Here all the implicit constants are independent of t and N.*

**Proof** The summation in (4.1) is

$$\begin{aligned}(4.4)\qquad &= \sum_{a,b=1}^{N-1} ab \sum_{\substack{d\mid N\\ d\mid a+b+t}} \mu(d)\\ &= \sum_{d\mid N}\mu(d) \sum_{\substack{a,b=1\\ a+b+t\equiv 0 \pmod d}}^{N-1} ab.\end{aligned}$$

Using Lemma 3.1, we have

$$\begin{aligned}\sum_{\substack{a,b=1\\ a+b+t\equiv 0 \pmod d}}^{N-1} ab &= \sum_{n,m=0}^{\frac{N}{d}-1} \sum_{\substack{a,b=0\\ a+b+t\equiv 0 \pmod d}}^{d-1} (a+dn)(b+dm)\\ &= d^2 \sum_{n,m=0}^{\frac{N}{d}-1} nm \sum_{\substack{a,b=0\\ a+b+t\equiv 0 \pmod d}}^{d-1} 1 + \frac{N^2}{d^2} \sum_{\substack{a,b=0\\ a+b+t\equiv 0 \pmod d}}^{d-1} ab\\ &\quad + 2d \sum_{n,m=0}^{\frac{N}{d}-1} n \sum_{\substack{a,b=0\\ a+b+t\equiv 0 \pmod d}}^{d-1} b\\ &= \frac{N^4}{4d} - \frac{N^3}{2d} + O(N^2 d).\end{aligned}$$

It follows now from (4.4) that

$$\begin{aligned}\sum_{\substack{a,b=1\\ (a+b+t,N)=1}}^{N-1} ab &= \frac{N^4}{4}\sum_{d\mid N}\frac{\mu(d)}{d} - \frac{1}{2}N^3\sum_{d\mid N}\frac{\mu(d)}{d} + O\Big(N^2\sum_{d\mid N}\mu^2(d)d\Big)\\ &= \frac{1}{4}N^3\phi(N) + O(N^{3+\epsilon}).\end{aligned}$$

The proofs of (4.2) and (4.3) are similar. ■

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

Therefore, using (3.2) and Lemma 4.1,

$$B \ll N^{6+\epsilon}. \tag{4.5}$$

We next estimate the term $C$ using formula (2.11). The summation in the first term of (2.11) is

$$\begin{aligned}
&= \sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)C_N(n+m+2t) \\
&= \sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t) \sum_{\substack{d\mid n+m+2t\\ d\mid N}} d\mu\Big(\frac{N}{d}\Big) \\
&= N \sum_{\substack{n,m=1\\ n+m+2t\equiv 0 \pmod N}}^{N-1} nm\left(\frac{n+t}{N}\right)\left(\frac{m+t}{N}\right) \\
&\quad + O\Big(\sum_{\substack{d\mid N\\ d<N}} d \Big| \sum_{\substack{n,m=1\\ n+m+2t\equiv 0 \pmod d}}^{N-1} nm\Big(\frac{n+t}{N}\Big)\Big(\frac{m+t}{N}\Big)\Big|\Big)
\end{aligned} \tag{4.6}$$

because $c_k(l) = \sum_{d\mid k, d\mid l} d\mu(k/d)$ (see Section 8.3 in [A-80]).

The error term in (4.6) is

$$\begin{aligned}
&\ll \sum_{\substack{d\mid N\\ d<N}} d \Big| \sum_{a,b=0}^{\frac{N}{d}-1} \sum_{\substack{n,m=0\\ n+m+2t\equiv 0 \pmod d}}^{d-1} (n+ad)(m+bd)\Big(\frac{n+ad+t}{N}\Big)\Big(\frac{m+bd+t}{N}\Big)\Big| \\
&\ll \sum_{\substack{d\mid N\\ d<N}} d^3 \Big| \sum_{\substack{n,m=0\\ n+m+2t\equiv 0 \pmod d}}^{d-1} \Big(\frac{n+t}{d}\Big)\Big(\frac{m+t}{d}\Big) \sum_{a,b=0}^{\frac{N}{d}-1} ab\Big(\frac{n+ad+t}{N/d}\Big)\Big(\frac{m+bd+t}{N/d}\Big)\Big| \\
&\ll \sum_{\substack{d\mid N\\ d<N}} d^3 \sum_{\substack{n,m=0\\ n+m+2t\equiv 0 \pmod d}}^{d-1} \Big|\sum_{a=0}^{\frac{N}{d}-1} a\Big(\frac{n+ad+t}{N/d}\Big)\Big| \times \Big|\sum_{b=0}^{\frac{N}{d}-1} b\Big(\frac{m+bd+t}{N/d}\Big)\Big|.
\end{aligned}$$

We next employ Polya's inequality for character sums (see Theorem 13.15 in [A-80]), namely, if $\psi$ is any nonprincipal character modulo $k$, then for all $x \geq 2$ we have

$$\sum_{m\leq x} \psi(m) \ll k^{\frac{1}{2}} \log k.$$

Using this inequality and the partial summation formula, we have for any square-free odd integer $k$ and any integer $l$,

$$\Big|\sum_{a=0}^{k-1} a\Big(\frac{a+l}{k}\Big)\Big| \ll k^{\frac{3}{2}}\log k$$

and hence the error term in (4.6) becomes

$$\begin{aligned}
&\ll \sum_{\substack{d|N\\ d<N}} d^3 \sum_{\substack{n,m=0\\ n+m+2t\equiv 0 \pmod{d}}}^{d-1} \frac{N^3}{d^3}\log^2(N/d)\\
&\ll N^3 \sum_{\substack{d|N\\ d<N}} d\log^2(N/d)\\
&\ll \frac{N^{4+\epsilon}}{p_1}.
\end{aligned}$$

Thus

$$\begin{aligned}
&\sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)C_N(n+m+2t)\\
&\quad = N \sum_{\substack{n,m=1\\ n+m+2t\equiv 0 \pmod{N}}}^{N-1} nm\Big(\frac{n+t}{N}\Big)\Big(\frac{m+t}{N}\Big) + O\Big(\frac{N^{4+\epsilon}}{p_1}\Big).
\end{aligned}\tag{4.7}$$

In the same manner, we can prove that the summation in the third term of (2.11) is

$$\begin{aligned}
&= \sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)C_N(n-m)\\
&= N \sum_{\substack{n,m=1\\ n\equiv m \pmod{N}}}^{N-1} nm\Big(\frac{n+t}{N}\Big)\Big(\frac{m+t}{N}\Big) + O\Big(\frac{N^{4+\epsilon}}{p_1}\Big)\\
&= N \sum_{\substack{n=1\\ (n+t,N)=1}}^{N-1} n^2 + O\Big(\frac{N^{4+\epsilon}}{p_1}\Big)\\
&= \frac{1}{3}N^3\phi(N) + O\Big(\frac{N^{4+\epsilon}}{p_1}\Big)
\end{aligned}\tag{4.8}$$

using (4.3) in Lemma 4.1. Now it remains to consider the main terms in (4.7). If

https://doi.org/10.4153/CJM-2001-002-6 Published online by Cambridge University Press

$1 \le t \le \frac{N-1}{2}$, then

$$\begin{aligned}
&\sum_{\substack{n,m=1 \\ n+m+2t\equiv 0 \pmod N}}^{N-1} nm \left(\frac{n+t}{N}\right)\left(\frac{m+t}{N}\right) \\
&= \left(\frac{-1}{N}\right) \sum_{\substack{n,m=1 \\ n+m+2t\equiv 0 \pmod N \\ (n+t,N)=1}}^{N-1} nm \\
&= \left(\frac{-1}{N}\right)\Big\{ \sum_{\substack{n=1 \\ (n+t,N)=1}}^{N-2t} n(N-n-2t) + \sum_{\substack{n=N-2t+1 \\ (n+t,N)=1}}^{N-1} n(2N-n-2t)\Big\} \\
&= \left(\frac{-1}{N}\right)\frac{1}{6}\phi(N)(N^2+6Nt-12t^2) + O(N^{2+\epsilon})
\end{aligned} \tag{4.9}$$

by (4.2) and (4.3). It can be easily verified that (4.9) is also true for $t = \frac{N+1}{2}$. Thus, from (2.11), (4.2), (4.7), (4.8) and (4.9), the term $C$ is

$$C = \frac{1}{8}N^7 - \frac{1}{2}N^6 t + N^5 t^2 + O(N^{7+\epsilon}/p_1)$$

and hence

$$\sum_{k=0}^{N-1} |f(-\omega^k)|^4 = \frac{7}{3}N^3 - 8N^2 t + 16Nt^2 + O(N^{3+\epsilon}/p_1)$$

from (2.4), (2.6) and (4.5). Finally, Theorem 1.2 follows from this and (2.1) and (2.3).

## References


[A-80] T. M. Apostol, *Introduction to Analytic Number Theory.* Springer-Verlag, Berlin, 1980.

[B-95] J. Beck, *Flat polynomials on the unit circle—note on a problem of Littlewood.* Bull. London Math. Soc. **23**(1991), 269–277

[BEW-98] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums.* In: Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley-Interscience, New York, 1998.

[BC-98] P. Borwein and K. K. Choi, *Explicit Merit Factor Formulae for Fekete and Turyn Polynomials.* Under submission.

[BC-99] ———, *Merit Factors of Character Polynomials.* J. London Math. Soc., to appear.

[E-57] P. Erdős, *Some unsolved problems.* Michigan Math. J. **4**(1957), 291–300.

[E-62] P. Erdős, *An inequality for the maximum of trigonometric polynomials.* Ann. Polon. Math. **12**(1962), 151–154.

[CGP-98] B. Conrey, A. Granville and B. Poonen, *Zeros of Fekete polynomials.* In press.

[G-83] M. J. Golay, *The merit factor of Legendre sequences.* IEEE Trans. Inform. Theory **29**(1983), 934–936.

[HJ-88] T. Høholdt and H. Jensen, *Determination of the merit factor of Legendre sequences.* IEEE Trans. Inform. Theory **34**(1988), 161–164.

[HJJ-91] T. Høholdt, H. Jensen and J. Jensen, *The merit factor of binary sequences related to difference sets.* IEEE Trans. Inform. Theory **37**(1991), 617–626.

[K-80] J-P. Kahane, *Sur les polynômes à coefficients unimodulaires.* Bull. London Math. Soc. **12**(1980), 321–342.

[L-68] J. E. Littlewood, *Some Problems in Real and Complex Analysis.* Heath Mathematical Monographs, Lexington, Massachusetts, 1968.

[M-94] H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis.* CBMS **84**, Amer. Math. Soc., Providence, RI, 1994.

[NB-90] D. J. Newman and J. S. Byrnes, *The $L^4$ norm of a polynomial with coefficients* $\pm 1$. Amer. Math. Monthly **97**(1990), 42–45.

[S-90] B. Saffari, *Barker sequences and Littlewood's "two-sided conjectures" on polynomials with* $\pm 1$ *coefficients.* Séminaire d'Analyse Harmonique. Année 1989/90, Univ. Paris XI, Orsay, 1990, 139–151.

*Department of Mathematics and Statistics*
*Simon Fraser University*
*Burnaby, BC*
*V5A 1S6*

*Department of Mathematics*
*The University of Hong Kong*
*Pokfulam Road*
*Hong Kong*