Norms of Cyclotomic Littlewood Polynomials

By Peter Borwein, Kwok-Kwong Stephen Choi

Department of Mathematics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6

and Ron Ferguson

Department of Mathematics, University of British Columbia, Vancouver, B.C., Canada V6T 1Z2

and

Department of Mathematics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6

(*Received* 8 *October* 2003; *revised* 9 *January* 2004)

Abstract

The main result of this paper gives an explicit computation of the L_4 norm of any cyclotomic polynomial of the form

$$f(x) = \Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}).$$

Here Φ_p is the *pth* cyclotomic polynomial and the p_i are primes that are not necessarily distinct.

A corollary of this is the following theorem.

Theorem. *If*

$$f(x) = \Phi_{p_1}(\epsilon_1 x)\Phi_{p_2}(\epsilon_2 x^{p_1}) \cdots \Phi_{p_r}(\epsilon_r x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ *and* $\epsilon_j = \pm$, *then*

$$\frac{\|f\|_4^4}{N^2} \geqslant \frac{\|\Phi_2(-x)\Phi_2(-x^2)\cdots\Phi_2(-x^{2^{r-1}})\|_4^4}{4^r}$$
$$= \frac{(\frac{1}{2}+\frac{5}{34}\sqrt{17})(1+\sqrt{17})^r - (-\frac{1}{2}+\frac{5}{34}\sqrt{17})(1-\sqrt{17})^r}{4^r}.$$

In particular the minimum possible normalized L_4 norm of any polynomial of the above form is attained by

$$\Phi_2(-x)\Phi_2(-x^2)\cdots\Phi_2(-x^{2^{r-1}}).$$

---

1. *Introduction*

For positive α, the L_α norm on the boundary of the unit disk is defined by

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

For a polynomial $p(z) := a_n z^n + \cdots + a_1 z + a_0$, the L_2 norm is also given by

$$\|p\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2}.$$

Let

$$\mathcal{L}_n := \left\{\sum_{i=0}^{n} a_i z^i : a_i \in \{-1, 1\}\right\}$$

denote the set of polynomials of degree exactly n with coefficients from $\{-1, 1\}$. In general, we will call polynomials with coefficients in $\{-1, 1\}$ Littlewood polynomials.

There are three classical conjectures concerning Littlewood polynomials. Each of these is at least 50 years old and while there are a host of interesting partial results none is solved. This is discussed in detail in [**1**] and also [**8**].

CONJECTURE 1·1. **(Littlewood)** *There exist positive constants* c_1 *and* c_2 *such that*

for any n it is possible to find $p_n \in \mathcal{L}_n$ with

$$c_1\sqrt{n+1} \leqslant |p_n(z)| \leqslant c_2\sqrt{n+1}$$

for all complex z with $|z| = 1$.

CONJECTURE 1·2. **(Erdős)** *There exists a positive constant c such that for all sufficiently large n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \geqslant (1+c)\sqrt{n+1}$.*

CONJECTURE 1·3. **(Golay)** *There exists a positive constant c such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_4 \geqslant (1+c)\sqrt{n+1}$.*

Because of the monotonicity of the L_p norms, the conjecture of Golay implies the conjecture of Erdős.

The Mahler measure of a polynomial

$$p_n(z) := a(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)$$

is, by definition, the product of all the roots of p_n that have modulus at least 1 multiplied by the leading coefficient. That is,

$$M(p_n) = |a| \prod_{|\alpha_i|\geqslant 1} |\alpha_i|.$$

It is also the L_0 norm:

$$\lim_{\alpha\to 0} \|p\|_\alpha = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|p\left(e^{i\theta}\right)\right| \, d\theta\right) =: \|p\|_0.$$

The following conjecture is proved in Borwein and Choi [1999] for N odd and for a variety of even N including $N = 2^k$. It is still open in general for N even. There are some partial results for even case. In [**5**], Conjecture 1·4 is proved when $N = 2p^l$ or when $P(x)$ is a separable polynomial.

CONJECTURE 1·4. **(Characterization of cyclotomic Littlewood polynomials)**

A Littlewood polynomial $P(z)$ of degree $N-1$ has Mahler measure 1 if and only if P can be written in the form

$$P(z) = \pm\Phi_{p_1}(\pm z)\Phi_{p_2}(\pm z^{p_1})\cdots\Phi_{p_r}(\pm z^{p_1 p_2\cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct and

$$\Phi_n(z) := \sum_{m=0}^{\phi(n)} a(m,n) z^m$$

is the nth cyclotomic polynomial.

Identifying extremal polynomials with respect to any of the above conjectures is hard. The Littlewood polynomials of measure 1 (which we call cyclotomic Littlewood polynomials) are clearly the minimal polynomials with respect to the L_0 norm and, thus one expects them to have relatively large L_p norm when $p > 2$ (because of Hölder's inequality: if $1 \leqslant \alpha < \beta \leqslant \infty$ and $\alpha^{-1} + \beta^{-1} = 1$, then $\|fg\|_1 \leqslant \|f\|_\alpha \|g\|_\beta$.)

The main purpose of this paper is to explicitly compute the L_4 norms of the type of cyclotomic polynomials that arise in the above conjecture (and hence, conjecturally, all cyclotomic Littlewood polynomials). This will show that both the L_4 norm and the supremum norm of such polynomials must be relatively large.

The size of the coefficients of general cyclotomic polynomials has been the subject of numerous investigations. Erdoš conjectured that $A(n) := \max_m |a(m,n)|$ tends to infinity for almost all n. This conjecture is proved by Maier in [**9**] (also see [**10**] and [**11**]). In general, the coefficients of $\Phi_n(z)$ can be large.

Cyclotomic Littlewood polynomials of degree $N-1$ have all coefficients of size 1 and hence have L_2 norm $\sqrt{N}$. So by monotonicity of the norms, $\|P\|_4 \geqslant \sqrt{N}$. We will prove

in Theorem 2·6 below that a considerably stronger result holds. Namely

$$\|P\|_4 \gg N^{\frac{\log_2(1+\sqrt{17})}{4}} = N^{0.589\cdots}.$$

2. *Proofs*

Consider a cyclotomic Littlewood polynomial $h(x)$ which factors in the form

$$h(x) = f(x)g(x^k)$$

where $f(x)$ and $g(x)$ are cyclotomic Littlewood polynomials of degrees $k-1$ and $l-1$. The 4th power of the 4-norm of $h(x)$ on the unit circle has the same value as the constant term of $(h(x)h(x^{-1}))^2$. If $(f(x)f(x^{-1}))^2 = a_0 + \sum_{i=1}^{2(k-1)} a_i(x^i + x^{-i})$ and $(g(x)g(x^{-1}))^2 = b_0 + \sum_{i=1}^{2(l-1)} b_i(x^i + x^{-i})$, then this constant term has value $c_0 = a_0b_0 + 2a_kb_1$. Furthermore, $h(x)$ has degree $kl-1$ and the coefficient of x^{kl}, c_{kl}, in $(h(x)h(x^{-1}))^2$ has value $a_kb_{l+1} + a_0b_l + a_kb_{l-1}$. Written in matrix form, this becomes

$$\begin{bmatrix} c_0 \\ \\ c_{kl} \end{bmatrix} = \begin{bmatrix} b_0 & 2b_1 \\ \\ b_l & b_{l-1} + b_{l+1} \end{bmatrix} \begin{bmatrix} a_0 \\ \\ a_k \end{bmatrix}.$$

Each $g(x)$ of degree $l-1$ has an associated 2×2 matrix

$$G = \begin{bmatrix} b_0/l^2 & 2b_1/l^2 \\ \\ b_l/l^2 & (b_{l-1} + b_{l+1})/l^2 \end{bmatrix}.$$

Here we normalize the matrix by dividing l^2 which is $\|g\|_2^4$. For example, $\Phi_1(x) = 1 + x$ has the associated matrix

$$G_2^+ = \begin{bmatrix} \frac{3}{2} & 2 \\ \\ \\ \frac{1}{4} & 1 \end{bmatrix}$$

and $\Phi_2(x) = 1 - x$ has the associated matrix

$$G_2^- = \begin{bmatrix} \frac{3}{2} & -2 \\ & \\ \frac{1}{4} & -1 \end{bmatrix}.$$

More generally, for odd prime p, $\Phi_p = \Phi_p(x) = 1 + x + \ldots + x^{p-1}$ is associated with

$$G_p^+ = \begin{bmatrix} \frac{2}{3}(p + \frac{1}{2p}) & \frac{4}{3}(p - \frac{1}{p}) \\ & \\ \frac{1}{6}(p - \frac{1}{p}) & \frac{1}{3}(p + \frac{2}{p}) \end{bmatrix}$$

and $\Phi_{2p} = \Phi_p(-x) = 1 - x + x^2 - \ldots + x^{p-1}$ is associated with

$$G_p^- = \begin{bmatrix} \frac{2}{3}(p + \frac{1}{2p}) & -\frac{4}{3}(p - \frac{1}{p}) \\ & \\ -\frac{1}{6}(p - \frac{1}{p}) & \frac{1}{3}(p + \frac{2}{p}) \end{bmatrix}$$

for odd prime p. This gives an inductive method for determining the 4-norms of cyclotomic Littlewood polynomials built up in the fashion (2·1).

PROPOSITION 2·1. *If*

$$f(x) = \Phi_{p_1}(\epsilon_1 x)\Phi_{p_2}(\epsilon_2 x^{p_1}) \cdots \Phi_{p_r}(\epsilon_r x^{p_1 p_2 \cdots p_{r-1}}), \tag{2·1}$$

where $N = p_1 p_2 \cdots p_r$ *and* $\epsilon_j = \pm$, *then*

$$\frac{\|f\|_4^4}{N^2} = \frac{\|f\|_4^4}{\|f\|_2^4} = [1\ 0] G_{p_r}^{\epsilon_r} \cdots G_{p_2}^{\epsilon_2} G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}.$$

For example, let $c_{n,0}$ be the 4th power of the 4-norm of the polynomial $f_n(x) = \prod_{i=1}^{n}(x^{2^{i-1}} - 1)$ of degree $2^n - 1$ and $c_{n,2^n}$ the coefficient of x^{2^n} in $(f_n(x)f_n(x^{-1}))^2$.

Then

$$\begin{bmatrix} c_{n,0} \\ \\ c_{n,2^n} \end{bmatrix} = G_2^- \begin{bmatrix} c_{n-1,0} \\ \\ c_{n-1,2^{n-1}} \end{bmatrix} = \left(G_2^-\right)^{n-1} \begin{bmatrix} 6 \\ \\ 1 \end{bmatrix}.$$

In fact, we can eliminate the coefficients of the form $c_{n,2^n}$ in the recursion. Starting from the equations

$$c_{n+1,0} = 6c_{n,0} - 8c_{n,2^n}$$

$$c_{n+1,2^{n+1}} = \ c_{n,0} - 4c_{n,2^n}$$

we eliminate $c_{n,2^n}$ to obtain $c_{n+1,2^{n+1}} = \frac{1}{2}c_{n+1,0} - 2c_{n,0}$ and thus $c_{n,2^n} = \frac{1}{2}c_{n,0} - 2c_{n-1,0}$. Substituting this in the first equation gives

$$c_{n+1,0} = 2c_{n,0} + 16c_{n-1,0},$$

a recursion involving only the 4-norms.

The eigenvalues for the matrix G_2^- are $(1 \pm \sqrt{17})/4$. The 4th power of the 4-norm will thus increase by a factor of approximately $1 + \sqrt{17}$ for each doubling of the length. The 4th power of the 4-norm divided by the 2nd power of the 2-norm will increase by a factor of approximately $(1 + \sqrt{17})/4$. For length n, this quotient will be of the order

$$\left(\frac{1+\sqrt{17}}{4}\right)^{\log_2 n} = n^{0.357\ldots}.$$

We extend the definition of the matrix $G_p^{\pm}$ by

$$G_n^+ = \begin{bmatrix} \frac{2}{3}(n + \frac{1}{2n}) & \frac{4}{3}(n - \frac{1}{n}) \\ \\ \\ \frac{1}{6}(n - \frac{1}{n}) & \frac{1}{3}(n + \frac{2}{n}) \end{bmatrix}$$

for $n = 2, 3, \cdots$ and

$$G_n^- = \begin{bmatrix} \frac{2}{3}(n+\frac{1}{2n}) & -\frac{4}{3}(n-\frac{1}{n}) \\ \\ -\frac{1}{6}(n-\frac{1}{n}) & \frac{1}{3}(n+\frac{2}{n}) \end{bmatrix}$$

for $n = 3, 4, \cdots$. The matrices $G_n^{\pm}$ satisfy the following properties.

LEMMA 2·2. *Let*

$$E = \begin{bmatrix} 1 & 0 \\ \\ 0 & -1 \end{bmatrix}.$$

Then for odd primes p and q, we have

(i) $G_p^+ = EG_p^-E$ *and* $G_p^- = EG_p^+E$;

(ii) $G_2^- = G_2^+E$ *and* $G_2^+ = G_2^-E$;

(iii) $G_p^{\pm} \cdot G_q^{\pm} = G_{pq}^{\pm} = G_q^{\pm} \cdot G_p^{\pm}$;

(iv) $G_p^+ \cdot G_2^+ = G_{2p}^+ = G_2^+ \cdot G_p^+$;

(v) $\left(G_2^+\right)^r = G_{2^r}^+$.

The aim of this article is to consider the set of the cyclotomic Littlewood polynomial of degree $N-1$ such that N is a product of r primes and to show that the normalized L_4 norm $\|f\|_4^4/\|f\|_2^4$ attains its minimal value when $f(x) = f_r(x)$, i.e., $p_1 = p_2 = \cdots = p_r = 2$ and $\epsilon_1 = \epsilon_2 = \cdots = \epsilon_r = +$ in (2·1).

LEMMA 2·3. *Let $r \geqslant 1$ and*

$$G_{p_r}^{\epsilon_r} G_{p_{r-1}}^{\epsilon_{r-1}} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ \\ B \end{bmatrix}.$$

Then $A > 4|B| > 0$. Moreover, $B < 0$ if and only if $G_{p_r}^{\epsilon_r} = G_p^-$ for odd prime $p \geqslant 3$.

Proof. We prove by induction on r. When $r = 1$,

$$G_2^- \begin{bmatrix} 1 \\ 0 \end{bmatrix} = G_2^+ \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3/2 \\ 1/4 \end{bmatrix}$$

and

$$G_p^+ \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{2}{3}(p+\frac{1}{2p}) \\ \\ \frac{1}{6}(p-\frac{1}{p}) \end{bmatrix}; \quad G_p^- \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{2}{3}(p+\frac{1}{2p}) \\ \\ -\frac{1}{6}(p-\frac{1}{p}) \end{bmatrix}.$$

Since $\frac{2}{3}(p+\frac{1}{2p}) - 4 \times (\frac{1}{6}(p-\frac{1}{p})) = \frac{1}{p} > 0$, the lemma is true for $r = 1$.

Suppose

$$G_{p_{r-1}}^{\epsilon_{r-1}} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ B \end{bmatrix}$$

with $A > 4|B| > 0$.

If $G_{p_r}^{\epsilon_r} = G_2^-$ then

$$G_{p_r}^{\epsilon_r} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = G_2^- \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 3A/2 - 2B \\ A/4 - B \end{bmatrix}$$

Since $A/4 - B \geqslant A/4 - |B| > 0$, so

$$\left(\frac{3}{2}A - 2B\right) - 4\left|\frac{1}{4}A - B\right| = \frac{1}{2}A + 2B \geqslant \frac{A - 4|B|}{2} > 0.$$

The case $G_{p_r}^{\epsilon_r} = G_2^+$ can be proved in the same way as $G_2^+ = G_2^- E$ by (ii) Lemma 2·2.

If $G_{p_r}^{\epsilon_r} = G_p^+$, then

$$G_{p_r}^{\epsilon_r} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = G_p^+ \begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \frac{2}{3}(p+\frac{1}{2p})A + \frac{4}{3}(p-\frac{1}{p})B \\ \\ \frac{1}{6}(p-\frac{1}{p})A + \frac{1}{3}(p+\frac{2}{p})B \end{bmatrix}$$

for $p \geqslant 3$. Since

$$\begin{aligned}\frac{1}{6}\left(p-\frac{1}{p}\right)A+\frac{1}{3}\left(p+\frac{2}{p}\right)B &\geqslant \frac{1}{6}\left(p-\frac{1}{p}\right)A-\frac{1}{3}\left(p+\frac{2}{p}\right)|B| \\ &> \left\{\frac{4}{6}\left(p-\frac{1}{p}\right)-\frac{1}{3}\left(p+\frac{2}{p}\right)\right\}|B| \\ &= \left(\frac{1}{3}p-\frac{4}{3p}\right)|B|>0,\end{aligned}$$

it then follows that

$$\begin{aligned}&\left(\frac{2}{3}\left(p+\frac{1}{2p}\right)A+\frac{4}{3}\left(p-\frac{1}{p}\right)B\right)-4\left|\frac{1}{6}\left(p-\frac{1}{p}\right)A+\frac{1}{3}\left(p+\frac{2}{p}\right)B\right| \\ &=\frac{2}{3}\left(p+\frac{1}{2p}\right)A+\frac{4}{3}\left(p-\frac{1}{p}\right)B-\frac{4}{6}\left(p-\frac{1}{p}\right)A-\frac{4}{3}\left(p+\frac{2}{p}\right)B \\ &=\frac{1}{p}A-\frac{4}{p}B>0.\end{aligned}$$

The case $G_{p_r}^{\epsilon_r}=G_p^-$ can be proved in the same way. □

For integer $t \geqslant 0$, we let

$$\begin{aligned}a_t &:= \frac{(\frac{1}{2}+\frac{5}{34}\sqrt{17})(1+\sqrt{17})^t-(-\frac{1}{2}+\frac{5}{34}\sqrt{17})(1-\sqrt{17})^t}{4^t} \\ b_t &:= \frac{4\sqrt{17}((1-\sqrt{17})^t-(1+\sqrt{17})^t)}{17\cdot 4^t} \\ c_t &:= \frac{\sqrt{17}((1+\sqrt{17})^t-(1-\sqrt{17})^t)}{34\cdot 4^t} \\ d_t &:= \frac{(\frac{1}{2}+\frac{5}{34}\sqrt{17})(1-\sqrt{17})^t-(-\frac{1}{2}+\frac{5}{34}\sqrt{17})(1+\sqrt{17})^t}{4^t}\end{aligned}$$

and

$$A_t := (1+\sqrt{17})^t+(1-\sqrt{17})^t \qquad \text{and} \qquad B_t := (1+\sqrt{17})^t-(1-\sqrt{17})^t.$$

Since

$$\begin{aligned}A_t &= \sum_{m=0}^{t}\binom{t}{m}(\sqrt{17})^m+\sum_{m=0}^{t}\binom{t}{m}(-\sqrt{17})^m \\ &= 2\sum_{m\equiv 0 \pmod 2}\binom{t}{m}(\sqrt{17})^m>0\end{aligned}$$

and

$$B_t = 2 \sum_{m \equiv 1 \pmod 2} \binom{t}{m} (\sqrt{17})^m > 0,$$

it then follows that

$$a_t = \frac{\frac{1}{2}A_t + \frac{5}{34}\sqrt{17}B_t}{4^t} > 0$$

$$b_t = \frac{-4\sqrt{17}B_t}{17 \cdot 4^t} < 0$$

$$c_t = \frac{\sqrt{17}B_t}{34 \cdot 4^t} > 0$$

and d_t can take positive or negative values for various t. By diagonalizing G_2^-, it can be shown that for integer $t \geqslant 0$,

$$\left(G_2^-\right)^t = \begin{bmatrix} a_t & b_t \\ c_t & d_t \end{bmatrix}. \tag{2·2}$$

LEMMA 2·4. *Let $A > 0$, $B \geqslant 0$ and $t \geqslant 0$. If $p \geqslant 3$ or if $p = 2$ and $B > 0$, then we have*

$$[1\ 0]\left(G_2^-\right)^t G_p^+ \begin{bmatrix} A \\ B \end{bmatrix} > [1\ 0]\left(G_2^-\right)^{t+1} \begin{bmatrix} A \\ B \end{bmatrix}. \tag{2·3}$$

Proof. Note that in view of (2·3), we have $[1\ 0]\left(G_2^-\right)^t = [a_t\ b_t]$. So

$$\begin{aligned} & [1\ 0]\left(G_2^-\right)^t \left(G_p^+ - G_2^-\right) \\ &= [a_t\ b_t] \begin{bmatrix} \frac{2}{3}p + \frac{1}{3p} - \frac{3}{2} & \frac{4}{3}p - \frac{4}{3p} + 2 \\ \\ \frac{1}{6}p - \frac{1}{6p} - \frac{1}{4} & \frac{1}{3}p + \frac{2}{3p} + 1 \end{bmatrix} \\ &= \begin{bmatrix} \dfrac{\lambda_t(p)}{p} & \dfrac{\mu_t(p)}{p} \end{bmatrix} \end{aligned}$$

where

$$\lambda_t(p) := \left(\frac{2}{3}a_t + \frac{1}{6}b_t\right)p^2 - \left(\frac{3}{2}a_t + \frac{1}{4}b_t\right)p + \left(\frac{1}{3}a_t - \frac{1}{6}b_t\right)$$

and

$$\mu_t(p) := \left(\frac{4}{3}a_t + \frac{1}{3}b_t\right)p^2 + (2a_t + b_t)p + \left(-\frac{4}{3}a_t + \frac{2}{3}b_t\right).$$

Note that $\frac{2}{3}a_t + \frac{1}{6}b_t = \frac{1}{4^t}\left(\frac{1}{3}A_t + \frac{\sqrt{17}}{17}B_t\right) > 0$ since $A_t, B_t > 0$ and

$$\begin{aligned}\frac{d}{dp}\lambda_t(p) = 2\left(\frac{2}{3}a_t + \frac{1}{6}b_t\right)p - \left(\frac{3}{2}a_t + \frac{1}{4}b_t\right) &\geqslant 4\left(\frac{2}{3}a_t + \frac{1}{6}b_t\right) - \left(\frac{3}{2}a_t + \frac{1}{4}b_t\right) \\ &= \frac{1}{4^t}\left(\frac{7}{12}A_t + \frac{5\sqrt{17}}{68}B_t\right) > 0.\end{aligned}$$

Thus $\lambda_t(p)$ is increasing in p. Hence $\lambda_t(p) \geqslant \lambda_t(2) = 0$ if $p \geqslant 2$ and

$$\lambda_t(p) \geqslant \lambda_t(3) = \frac{1}{4^t}\left(\frac{11}{12}A_t + \frac{9\sqrt{17}}{68}B_t\right) > 0 \tag{2·4}$$

if $p \geqslant 3$. Similarly, $\frac{4}{3}a_t + \frac{1}{3}b_t = \frac{1}{4^t}\left(\frac{2}{3}A_t + \frac{2\sqrt{17}}{17}B_t\right) > 0$ and

$$\begin{aligned}\frac{d}{dp}\mu_t(p) = 2\left(\frac{4}{3}a_t + \frac{1}{3}b_t\right)p + (2a_t + b_t) &\geqslant 4\left(\frac{4}{3}a_t + \frac{1}{3}b_t\right) + (2a_t + b_t) \\ &= \frac{1}{4^t}\left(\frac{11}{3}A_t + \frac{9\sqrt{17}}{17}B_t\right) > 0.\end{aligned}$$

So $\mu_t(p)$ is increasing in p and

$$\mu_t(p) \geqslant \mu_t(2) = \frac{1}{4^t}\left(4A_t + \frac{4\sqrt{17}}{17}B_t\right) > 0. \tag{2·5}$$

for $p \geqslant 2$. Therefore, for $p \geqslant 3$,

$$\begin{aligned}[1\ 0]\left(G_2^-\right)^t\left(G_p^+ - G_2^-\right)\begin{bmatrix}A\\B\end{bmatrix} &= \begin{bmatrix}\frac{\lambda_t(p)}{p} & \frac{\mu_t(p)}{p}\end{bmatrix}\begin{bmatrix}A\\B\end{bmatrix} \\ &= \frac{\lambda_t(p)A + \mu_t(p)B}{p} > 0\end{aligned}$$

by (2·4) and (2·5) and for $p = 2$ and $B > 0$,

$$[1\ 0]\left(G_2^-\right)^t\left(G_2^+ - G_2^-\right)\begin{bmatrix} A \\ B \end{bmatrix} = \frac{\lambda_t(2)A + \mu_t(2)B}{2}$$
$$= \frac{\mu_t(2)B}{2} > 0.$$

This proves Lemma 2·4. □

LEMMA 2·5. *If* $A > 4|B| \geqslant 0, p \geqslant 2, q \geqslant 3$ *and* $t \geqslant 0$, *then*

$$[1\ 0]\left(G_2^-\right)^t G_p^+ G_q^- \begin{bmatrix} A \\ B \end{bmatrix} > [1\ 0]\left(G_2^-\right)^{t+2}\begin{bmatrix} A \\ B \end{bmatrix}.$$

Proof. We first let

$$[1\ 0]\left(G_2^-\right)^t\left(G_p^+G_q^- - \left(G_2^-\right)^2\right) = [a\ b]$$

and claim that $a > 0$ and $b < 0$. In fact, by (2·2) we get

$$\begin{aligned} 1224 \cdot 4^t \cdot p \cdot q \cdot a \ =\ & \left((136A_t + 24\sqrt{17}B_t)q^2 + 272A_t + 48\sqrt{17}B_t\right)p^2 \\ & - \left(1071A_t + 279\sqrt{17}B_t\right)pq \\ & + \left((272A_t + 144\sqrt{17}B_t)q^2 - (68A_t + 36\sqrt{17}B_t)\right) \\ :=\ & f(p,q) \end{aligned}$$

and

$$\begin{aligned} -1224 \cdot 4^t \cdot p \cdot q \cdot b \ =\ & \left((272A_t + 48\sqrt{17}B_t)q^2 - (1088A_t + 192\sqrt{17}B_t)\right)p^2 \\ & - \left(612A_t + 324\sqrt{17}B_t\right)pq \\ & + \left((544A_t + 288\sqrt{17}B_t)q^2 + (272A_t + 144\sqrt{17}B_t)\right) \\ :=\ & g(p,q). \end{aligned}$$

Since

$$\begin{aligned}\frac{\partial f(p,q)}{\partial p} &= 2\left((136A_t + 24\sqrt{17}B_t)q^2 + 272A_t + 48\sqrt{17}B_t\right)p - (1071A_t + 279\sqrt{17}B_t)q \\ &\geqslant 4\left((136A_t + 24\sqrt{17}B_t)q^2 + 272A_t + 48\sqrt{17}B_t\right) - (1071A_t + 279\sqrt{17}B_t)q \\ &> 12(136A_t + 24\sqrt{17}B_t)q - (1071A_t + 279\sqrt{17}B_t)q \\ &= (561A_t + 9\sqrt{17}B_t)q > 0\end{aligned}$$

for $q \geqslant 3$, hence

$$\begin{aligned}f(p,q) &\geqslant f(2,q) \\ &= 4\left((136A_t + 24\sqrt{17}B_t)q^2 + 272A_t + 48\sqrt{17}B_t\right) \\ &\quad -2\left(1071A_t + 279\sqrt{17}B_t\right)q \\ &\quad +\left((272A_t + 144\sqrt{17}B_t)q^2 - (68A_t + 36\sqrt{17}B_t)\right) \\ &\geqslant 4\left((136A_t + 24\sqrt{17}B_t)3q + 272A_t + 48\sqrt{17}B_t\right) \\ &\quad -2\left(1071A_t + 279\sqrt{17}B_t\right)q \\ &\quad +\left((272A_t + 144\sqrt{17}B_t)3q - (68A_t + 36\sqrt{17}B_t)\right) \\ &= (306A_t + 162\sqrt{17}B_t)q + 1020A_t + 156\sqrt{17}B_t > 0.\end{aligned}$$

Similarly we can prove that $g(p,q)$ is increasing both in p and q. Hence $g(p,q) \geqslant g(2,3) =$

$6936A_t + 1752\sqrt{17}B_t > 0$. Therefore $a > 0$ and $b < 0$. It then follows that

$$\begin{aligned}
&[1\ 0]\left(G_2^-\right)^t\left(G_p^+G_q^- - \left(G_2^-\right)^2\right)\begin{bmatrix}A\\ \\ B\end{bmatrix}\\
&= [a\ b]\begin{bmatrix}A\\ \\ B\end{bmatrix} = aA + bB\\
&\geqslant aA - |bB| = aA + b|B|\\
&> a4|B| + b|B| = (4a+b)|B|,
\end{aligned}$$

because $A > 4|B| > 0$. It suffices to show that $4a+b > 0$ or equivalently $4f(p,q)-g(p,q) > 0$. Since

$$\begin{aligned}
&4f(p,q) - g(p,q)\\
=\ &\left((272A_t + 48\sqrt{17}B_t)q^2 + 2176A_t + 384\sqrt{17}B_t\right)p^2\\
&-\left(3672A_t + 792\sqrt{17}B_t\right)pq\\
&+\left((544A_t + 288\sqrt{17}B_t)q^2 - (544A_t + 288\sqrt{17}B_t)\right)\\
:=\ &k(p,q).
\end{aligned}$$

As before, we can show that $k(p,q)$ is increasing both in p and q. Hence

$$k(p,q) \geqslant k(2,3) = 816A_t + 816\sqrt{17}B_t > 0.$$

This completes the proof of the lemma. □

THEOREM 2·6. *If*

$$f(x) = \Phi_{p_1}(\epsilon_1 x)\Phi_{p_2}(\epsilon_2 x^{p_1})\cdots\Phi_{p_r}(\epsilon_r x^{p_1p_2\cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ *and* $\epsilon_j = \pm$, *then*

$$\frac{\|f\|_4^4}{N^2} \geqslant \frac{\|\Phi_2(-x)\Phi_2(-x^2)\cdots\Phi_2(-x^{2^{r-1}})\|_4^4}{4^r} = \frac{\|f_r\|_4^4}{\|f_r\|_2^4}$$

$$= [1\ 0]\left(G_2^-\right)^r \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}$$

$$= \frac{(\frac{1}{2} + \frac{5}{34}\sqrt{17})(1+\sqrt{17})^r - (-\frac{1}{2} + \frac{5}{34}\sqrt{17})(1-\sqrt{17})^r}{4^r}$$

Proof. We consider the set of all cyclotomic Littlewood polynomials of degree $N-1$ such that N is a product of r primes. We prove by induction on r. It is clear that for $\epsilon = \pm 1$,

$$[1\ 0]G_p^\epsilon \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} \geqslant [1\ 0]G_2^- \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} = \frac{3}{2}.$$

So the theorem is true for $r = 1$ by Proposition 2·1. Let

$$G_{p_r}^{\epsilon_r} \cdots G_{p_1}^{\epsilon_1} = \left(G_2^-\right)^t \left(G_{p_l}^{\epsilon_l} \cdots G_{p_1}^{\epsilon_1}\right)$$

be a Littlewood polynomial f with the smallest normalized L_4 norm $\|f\|_4^4/\|f\|_2^4$ of degree $N-1$ and $t \geqslant 0$ and $l = r - t$ and $G_{p_l}^{\epsilon_l} \neq G_2^-$. We will show that

$$[1\ 0]G_{p_r}^{\epsilon_r} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} \geqslant [1\ 0]\left(G_2^-\right)^r \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}.$$

If $\epsilon_l = +$, then write $G_{p_{l-1}}^{\epsilon_{l-1}} \cdots G_{p_1}^{\epsilon_1} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ \\ B \end{bmatrix}$.

If $B > 0$, then by Lemma 2·4, we have $l \geqslant 2$ and

$$\begin{aligned}
&[1\ 0]\left(G_2^-\right)^t\left(G_{p_l}^{\epsilon_l}\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix}\\
&=[1\ 0]\left(G_2^-\right)^t G_{p_l}^+\begin{bmatrix}A\\B\end{bmatrix}\\
&>[1\ 0]\left(G_2^-\right)^{t+1}\begin{bmatrix}A\\B\end{bmatrix}\\
&=[1\ 0]\left(G_2^-\right)^{t+1}\left(G_{p_{l-1}}^{\epsilon_{l-1}}\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix}
\end{aligned}$$

which contradicts the minimality of $\|f\|_4^4/\|f\|_2^4$.

If $B = 0$, by Lemma 2·3, we have $l = 1$ and by Lemma 2·4

$$[1\ 0]\left(G_{p_r}^{\epsilon_r}\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix}=[1\ 0]\left(G_2^-\right)^{r-1}G_{p_1}^+\begin{bmatrix}1\\0\end{bmatrix}\geqslant[1\ 0]\left(G_2^-\right)^r\begin{bmatrix}1\\0\end{bmatrix}$$

and the equality only holds when $p_1 = 2$. So

$$G_{p_r}^{\epsilon_r}\cdots G_{p_1}^{\epsilon_1}=\left(G_2^-\right)^{r-1}G_2^+.$$

But

$$[1\ 0]\left(G_2^-\right)^r\begin{bmatrix}1\\0\end{bmatrix}=[1\ 0]\left(G_2^-\right)^{r-1}G_2^+\begin{bmatrix}1\\0\end{bmatrix}.$$

If $B < 0$. then by Lemma 2·3, $A > 4|B| > 0$ and $\begin{bmatrix}A\\B\end{bmatrix} = G_q^-\begin{bmatrix}A'\\B'\end{bmatrix}$ with $q \geqslant 3$ and

$A' > 4|B'| \geqslant 0$. So

$$[1\ 0]\left(G_2^-\right)^t\left(G_{p_l}^{\epsilon_l}\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix} = [1\ 0]\left(G_2^-\right)^t G_{p_l}^+ G_q^-\begin{bmatrix}A'\\B'\end{bmatrix}$$

$$> [1\ 0]\left(G_2^-\right)^{t+2}\begin{bmatrix}A'\\B'\end{bmatrix}$$

$$= [1\ 0]\left(G_2^-\right)^{t+2}\left(G_{p_{l-2}}^{\epsilon_{l-2}}\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix}$$

by Lemma 2·5. This contradicts the minimality.

If $\epsilon_l = -$, then we write

$$G_{p_l}^- G_{p_{l-1}}^{\epsilon_{l-1}}\cdots G_{p_1}^{\epsilon_1}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}A\\B\end{bmatrix}$$

with $B \leqslant 0$ by Lemma 2·3. Thus

$$[1\ 0]\left(G_2^-\right)^t\left(G_{p_l}^-\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix}$$

$$= [1\ 0]\left(G_2^-\right)^t\begin{bmatrix}A\\B\end{bmatrix}$$

$$= [1\ 0]\begin{bmatrix}a_t & b_t\\c_t & d_t\end{bmatrix}\begin{bmatrix}A\\B\end{bmatrix}$$

$$= a_t A + b_t B.$$

By induction assumption,

$$A = [1\ 0]\left(G_{p_l}^-\cdots G_{p_1}^{\epsilon_1}\right)\begin{bmatrix}1\\0\end{bmatrix} \geqslant [1\ 0]\left(G_2^-\right)^l\begin{bmatrix}1\\0\end{bmatrix} = a_l = a_{r-t}.$$

Since $b_t < 0, c_{r-t} > 0$ and $B \leqslant 0$, so

$$\begin{aligned} a_t A + b_t B &\geqslant a_t A \\ &\geqslant a_t a_{r-t} \\ &\geqslant a_t a_{r-t} + b_t c_{r-t}. \end{aligned}$$

On the other hand,

$$\begin{aligned} [1\ 0] \left(G_2^-\right)^r \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} &= [1\ 0] \left(G_2^-\right)^t \left(G_2^-\right)^{r-t} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} \\ &= [1\ 0] \begin{bmatrix} a_t\ b_t \\ \\ c_t\ d_t \end{bmatrix} \begin{bmatrix} a_{r-t}\ b_{r-t} \\ \\ c_{r-t}\ d_{r-t} \end{bmatrix} \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} \\ &= [a_t\ b_t] \begin{bmatrix} a_{r-t} \\ \\ c_{r-t} \end{bmatrix} \\ &= a_t a_{r-t} + b_t c_{r-t}. \end{aligned}$$

So

$$[1\ 0] \left(G_2^-\right)^t \left(G_{p_l}^- \cdots G_{p_1}^{\epsilon_1}\right) \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} \geqslant [1\ 0] \left(G_2^-\right)^r \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix}.$$

This completes the proof of Theorem 2·6. □

Acknowledgements. Research of P. Borwein and R. Ferguson is supported by MITACS and research of P. Borwein and K-K Choi is supported by NSERC of Canada.

REFERENCES

[**1**] P. Borwein. *Computational Excursions in Analysis and Number Theory,* Springer–Verlag, 2002.

[**2**] P. Borwein and S. Choi. Explicit merit factor formulae for Fekete and Turyn Polynomials, *Trans. Amer. Math. Soc.* **3**54 (2002), 219–234.

[3] P. BORWEIN and S. CHOI. On cyclotomic polynomials with ±1 coefficients, *Experimental Math* **8** (1999), 399–407.

[4] D. BOYD. On a problem of Byrnes concerning polynomials with restricted coefficients, *Math. Comp.* **6**6 (1997), 1697–1703.

[5] S. CHOI. On cyclotomic polynomials with ±1 coefficients II, in preparation (2003).

[6] M.J. GOLAY. The merit factor of long low autocorrelation binary sequences, *IEEE Transactions on Information Theory* **2**8 (1982), 543–549.

[7] J-P. KAHANE. Sur les polynômes á coefficients unimodulaires, *Bull. London Math. Soc.* **1**2 (1980), 321–342.

[8] J.E. LITTLEWOOD. *Some Problems in Real and Complex Analysis,* Heath Mathematical Monographs, Lexington, Massachusetts, 1968.

[9] H. MAIER. The coefficients of cyclotomic polynomials, *Analytic number theory (Allerton Park, IL, 1989)*, 349–366, Progr. Math., **8**5, Birküser Boston, Boston, MA, 1990.

[10] H. MAIER. Cyclotomic polynomials with large coefficients, *Acta Arith.* **6**4 (1993), no. 3, 227–235.

[11] H. MAIER. The size of the coefficients of cyclotomic polynomials, in *Analytic number theory Vol. 2 (Allerton Park, IL, 1995)* (ed. B.C. Berndt et al.), Progr. Math., 139, Birkhäuser Boston, Boston, MA (1996), 633–639.

[12] D. J. NEWMAN and J. S. BYRNES. The L_4 norm of a polynomial with coefficients ±1, *Amer. Math. Monthly* **9**7 (1990), no. 1, 42–45.