EXPLICIT MERIT FACTOR FORMULAE
FOR FEKETE AND TURYN POLYNOMIALS

PETER BORWEIN AND KWOK-KWONG STEPHEN CHOI

May 3, 2001

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

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

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol. For example for q an odd prime,

$$\|f_q\|_4^4 := \frac{5q^2}{3} - 3q + \frac{4}{3} - 12(h(-q))^2$$

where $h(-q)$ is the class number of $\mathbb{Q}(\sqrt{-q})$. Similar explicit formula are given for various polynomials including an example of Turyn's that is constructed by cyclically permuting the first quarter of the coefficients of f_q. This is the sequence that has the largest known asymptotic merit factor. Explicitly,

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q}\right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfies

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

where

$$\gamma_q := \begin{cases} h(-q)(h(-q) - 4) & \text{if} \quad q \equiv 1, 5 \pmod 8, \\ 12(h(-q))^2 & \text{if} \quad q \equiv 3 \pmod 8, \\ 0 & \text{if} \quad q \equiv 7 \pmod 8. \end{cases}$$

Indeed we derive a closed form for the L_4 norm of all shifted Fekete polynomials

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k+t}{q}\right) z^k.$$

Namely

$$\|f_q^t\|_4^4 = \frac{1}{3}(5q^2 + 3q + 4) + 8t^2 - 4qt - 8t - \frac{8}{q^2}\left(1 - \frac{1}{2}\left(\frac{-1}{q}\right)\right)\left|\sum_{n=1}^{q-1} n\left(\frac{n+t}{q}\right)\right|^2,$$

and $\|f_q^{q-t+1}\|_4^4 = \|f_q^t\|_4^4$ if $1 \le t \le (q+1)/2$.

1. INTRODUCTION

The main purpose of this paper is to give explicit formulas for the L_4 norms (on the boundary of the unit disc) and hence, also the merit factors of various polynomials that are closely related to the Fekete polynomials. These allow us to explicitly recover various asymptotic results and to derive various new ones. These are all related to the old problem of constructing sequences of polynomials with coefficients in the set $\{+1, -1\}$ and with small L_4 norm [Bo-98].

As usual the L_α norm on the boundary of the unit disc is defined by

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

The L_4 norm of a polynomial is particularly easy to work with because it can be computed as the square root of the L_2 norm of $p(z)\overline{p(z)}$ and hence, computes exactly as the fourth root of the sum of the squares of the coefficients of $p(z)\overline{p(z)}$. In contrast, the supremum norm or other L_p norms, where p is not an even integer, are computationally difficult.

Let q be a prime number and let $\left(\frac{\cdot}{q} \right)$ be the Legendre symbol. We now define the particular polynomials we consider. The Fekete polynomials are defined by

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q} \right) z^k$$

and the closely related polynomials

$$F_q(z) := 1 + f_q(z) = 1 + \sum_{k=1}^{q-1} \left(\frac{k}{q} \right) z^k.$$

The half–Fekete polynomials are defined by

$$G_q(z) := \sum_{k=1}^{(q-1)/2} \left(\frac{k}{q} \right) z^k.$$

If we cyclically permute the coefficients of f_q by about $q/4$ places we get an example of Turyn's which we denote by

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, and we denote the general shifted Fekete polynomials by

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k+t}{q} \right) z^k.$$

Note that R has one coefficient that is zero (from the permutation of the constant term in f). For example

$$f_{11} := -x^{10} + x^9 - x^8 - x^7 - x^6 + x^5 + x^4 + x^3 - x^2 + x$$

and

$$R_{11} := -x^{10} + x^9 - x^7 + x^6 - x^5 - x^4 - x^3 + x^2 + x + 1.$$

The explicit formulas involve the class number of the imaginary quadratic field of $\mathbb{Q}(\sqrt{-d})$ which is denoted by $h(-d)$. For any odd prime d it can be computed as

$$(1.1) \qquad h(-d) = \lambda_q \sum_{k=1}^{(d-1)/2} \left(\frac{k}{d} \right) (-1)^k = \lambda_q G_d(-1)$$

where
$$\lambda_d := \begin{cases} 1 & \text{if } d \equiv 1, 7 \pmod 8, \\ -1/3 & \text{if } d \equiv 3 \pmod 8, \\ -1 & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

For primes $d \equiv 3 \pmod 4$ it can also be computed as

$$(1.2) \qquad h(-d) = -\frac{f'_d(1)}{d} = -\frac{1}{d} \sum_{k=1}^{d-1} \left(\frac{k}{d}\right) k$$

(this sum is 0 for $d \equiv 1 \pmod 4$).

We call a polynomial with coefficients $\{+1, -1\}$ of degree n a Littlewood polynomial of degree n and denote this class by $\mathcal{L}_n$. The above polynomials are either Littlewood polynomials or differ from Littlewood polynomials in a single coefficient.

There are two natural measures of smallness for the L_4 norm of a polynomial p. One is the ratio of the L_4 norm to the L_2 norm, $\|p\|_4/\|p\|_2$. The other (equivalent) measure is the merit factor, defined by
$$\mathrm{MF}(p) = \frac{\|p\|_2^4}{\|p\|_4^4 - \|p\|_2^4}.$$

The L_2 norm of any element of $\mathcal{L}_{n-1}$ is $\sqrt{n}$ and this is, of course, a lower bound for the L_4 norm. The expected L_4 norm of an element of $\mathcal{L}_n$ is computed in [BL-01] (see also [Ne-90]). It is $2^{1/4}\sqrt{n}$. (This corresponds to a merit factor of 1.) The L_4 norms of the Rudin-Shapiro polynomials are explicitly computed by Littlewood [Li-68] (see also [Ne-90] and [BM-00]); their merit factors tend to 3.

The $\{R_q\}$ above are a sequence with asymptotic merit factor 6. Golay [Go-83] gives a heuristic argument for this observation of Turyn's and this is proved rigorously in [Hø-88] (see also [Je-91]). The Fekete polynomials themselves have asymptotic merit factor $3/2$ and different amounts of cyclic permutations can give rise to any asymptotic merit factor between $3/2$ and 6. This result is recovered, in more generality, in Theorem 6. We also show that the half Fekete polynomials have an asymptotic merit factor of 3. Much material on the Fekete polynomials may be accessed in [CGPS-98].

Golay [Go-83] speculates that 6 may be the largest possible asymptotic merit factor. He writes "the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors." Newman and Byrnes [Ne-90], apparently independently, make a similar conjecture. As do Høholdt and Jensen [Hø-88]. Computations by a number of people (including the authors) on polynomials up to degree 200 lead us to believe that higher merit factors are likely possible. See [Go-77], [Me-96], [Re-93], and the web page of A. Reinholz at http://borneo.gmd.de/~andy/ACR.html.

The Fekete polynomial f_q has modulus $\sqrt{q}$ at each qth root of unity (as does f_q^t) and one might hope that they also satisfy the upper bound in Littlewood's conjecture but Montgomery [Mo-80] shows that this is not the case. Littlewood's conjecture is that it is possible to find $p_n \in \mathcal{L}_{n-1}$ so that
$$C_1\sqrt{n} \le |p_n(z)| \le C_2\sqrt{n}$$

for all z of modulus 1 and for two constants C_1, C_2 independent of n. Much further material on this conjecture is to be found in [Li-68], [Be-91], [Ka-80], [Sa-90] and [Bo-98].

Further research in this area has been done in [BC-00] and [BC-01].

2. RESULTS

The main result of this paper is Theorem 5 below. Theorem 1 and Theorem 4 follow immediately from Theorem 5. While Theorem 2 and Theorem 3 are sufficiently close in methodology that we skip their proofs.

Theorem 1. *For q an odd prime, the Fekete polynomial,*

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

satisfies

$$\|f_q\|_4^4 = \frac{5q^2}{3} - 3q + \frac{4}{3} - \gamma_q$$

where

$$\gamma_q := \begin{cases} 0 & if \quad q \equiv 1 \pmod 4, \\ 12(h(-q))^2 & if \quad q \equiv 3 \pmod 4. \end{cases}$$

Theorem 2. *For q an odd prime, the modified Fekete polynomial,*

$$F_q(z) := 1 + \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

satisfies

$$\|F_q\|_4^4 = \frac{5q^2}{3} + q - \frac{5}{3} - \gamma_q$$

where

$$\gamma_q := \begin{cases} 0 & if \quad q \equiv 1 \pmod 4, \\ 12h(-q)(h(-q)+1) & if \quad q \equiv 3 \pmod 4. \end{cases}$$

Theorem 3. *For q an odd prime the half–Fekete polynomials*

$$G_q(z) := \sum_{k=1}^{(q-1)/2} \left(\frac{k}{q}\right) z^k.$$

satisfy

$$\|G_q\|_4^4 = \frac{q^2}{3} - \frac{q}{2} + \frac{1}{6} - \gamma_q(h(-q))^2$$

where

$$\gamma_q := \begin{cases} 0 & if \quad q \equiv 1 \pmod 4, \\ 2 & if \quad q \equiv 7 \pmod 8, \\ 6 & if \quad q \equiv 3 \pmod 8. \end{cases}$$

The exact same formulae above hold for the polynomials $(f_q(z)+f_q(-z))/2$ and $(f_q(z)-f_q(-z))/2$.

Theorem 4. *For q an odd prime, the Turyn type polynomials*

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfy

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

and

$$\gamma_q := \begin{cases} h(-q)(h(-q) - 4) & \text{if} \quad q \equiv 1, 5 \pmod{8}, \\ 12(h(-q))^2 & \text{if} \quad q \equiv 3 \pmod{8}, \\ 0 & \text{if} \quad q \equiv 7 \pmod{8}. \end{cases}$$

Theorem 5. *For q an odd prime, the shifted Fekete polynomials*

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k + t}{q} \right) z^k$$

satisfy

$$\|f_q^t\|_4^4 = \frac{1}{3}(5q^2 + 3q + 4) + 8t^2 - 4qt - 8t - \frac{8}{q^2}\left(1 - \frac{1}{2}\left(\frac{-1}{q} \right) \right) \left| \sum_{n=1}^{q-1} n \left(\frac{n + t}{q} \right) \right|^2,$$

and $\|f_q^{q-t+1}\|_4^4 = \|f_q^t\|_4^4$ if $1 \le t \le (q + 1)/2$.

The distribution of the values of the Fekete polynomials $f_q(z)$ at the $2q$th roots of unity is of particular interest. In [Mo-86], Montgomery shows that the maximum modulus of $f_q(z)$ at the $2q$th root of unity is at least $\frac{2}{\pi}\sqrt{q}\log\log q$. More recently, Conrey, Granville and Poonen examine the distribution function of the values of $f_q(-e^{\frac{2\pi i k}{q}})$. The following result concerning the average of $f_q(-e^{\frac{2\pi i k}{q}})$ is a step in the proof of Theorem 5.

Corollary 6. *For q an odd prime, we have*

$$\sum_{j=0}^{q-1} |f_q(-e^{\frac{2\pi i k}{q}})|^4 = \frac{q}{3}(7q - 8)(q - 1) - 2q\gamma_q$$

where γ_q is the same as in Theorem 1.

Theorem 7. *For q an odd prime, the shifted Fekete polynomials*

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k + t}{q} \right) z^k$$

satisfy

$$\|f_q^t\|_4^4 = \|f_q^{q-t+1}\|_4^4 = \frac{5q^2}{3} + 8t^2 - 4qt + O(q(\log q)^2)$$

if $1 \leq t \leq (q+1)/2$.

Theorem 7 follows from Theorem 5 on observing that

$$(2.1) \qquad \frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n+k}{q}\right) = \sum_{n=1}^{k-1}\left(\frac{n}{q}\right) + \frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n}{q}\right).$$

This is coupled with the known estimate [Hu-82, p 172]

$$\left|\sum_{n=1}^{k-1}\left(\frac{n}{q}\right)\right| < q^{\frac{1}{2}}\log q$$

and the observation that

$$-\frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n}{q}\right)$$

equals the class number, $h(-q)$, for primes $q \equiv 3 \pmod 4$ and is zero for primes $q \equiv 1 \pmod 4$. The asymptotics of Turyn et al mentioned previously are the above theorem in the case where t is a constant multiple of q.

3. PROOF OF THEOREM 5

Let q be a prime number and, as before, let

$$f_q(z) := \sum_{n=1}^{q-1}\left(\frac{n}{q}\right) z^n$$

be the Fekete polynomial. Define

$$\epsilon_q := \begin{cases} 1 & \text{if } \quad q \equiv 1 \pmod 4, \\ i & \text{if } \quad q \equiv 3 \pmod 4. \end{cases}$$

Then we have the following well-known result of Gauss' [Hu-82]

$$(3.1) \qquad f_q(\omega^k) = \epsilon_q\sqrt{q}\left(\frac{k}{q}\right).$$

for $k = 0, 1, \cdots, q-1$, where $\omega := e^{2\pi i/q}$.

Lemma 1. *For any* $1 \leq t \leq q$, *we have*

$$\sum_{b=1}^{q-1}\left(\frac{b}{q}\right)\frac{\omega^{bt}}{\omega^b - 1} = \frac{\epsilon_q}{\sqrt{q}}\sum_{n=1}^{q-1} n\left(\frac{n+t}{q}\right).$$

Proof. First we note that since $\sum_{n=0}^{q-1} z^n = \frac{z^q-1}{z-1}$, we have

$$\sum_{n=1}^{q-1} n z^{n-1} = \frac{(z-1)qz^{q-1} - (z^q-1)}{(z-1)^2}.$$

Thus, we obtain

(3.2)
$$\frac{1}{\omega^j - 1} = \frac{1}{q} \sum_{n=1}^{q-1} n\omega^{jn},$$

for $j = 1, \cdots, q-1$. Using (3.2), it follows that

$$\sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{bt}}{\omega^b - 1} = \sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \omega^{bt} \frac{1}{q} \sum_{n=1}^{q-1} n\omega^{bn}$$

$$= \frac{1}{q} \sum_{n=1}^{q-1} n \sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \omega^{b(n+t)}$$

$$= \frac{1}{q} \sum_{n=1}^{q-1} n f_q(\omega^{n+t}).$$

Lemma 1 now follows from (3.1). $\square$

Lemma 2. *If* $1 \le k \le q$, *then*

(3.3)
$$\sum_{\substack{n,m=1 \\ k+n+m\equiv 0 \ (\mathrm{mod} \ q)}}^{q-1} nm = \frac{q}{6}(q^2 - 6q - 1 + 6k + 3qk - 3k^2).$$

Proof. Suppose $2 \le k \le q-2$. Then

$$\sum_{\substack{n,m=1 \\ k+n+m\equiv 0 \ (\mathrm{mod} \ q)}}^{q-1} nm = \sum_{n=1}^{q-k-1} n(q-k-n) + \sum_{n=q-k+1}^{q-1} n(2q-k-n)$$

$$= \sum_{n=1}^{q-1} n(q-k-n) + q \sum_{n=q-k+1}^{q-1} n$$

$$= \frac{q}{6}(q^2 - 6q - 1 + 6k + 3qk - 3k^2).$$

The cases $k = 1, q-1$ and q can be verified directly. $\square$

Lemma 3. *If* $1 \le k \le q$, *then*

(3.4)
$$\sum_{\substack{a,b=1 \\ a\neq b}}^{q-1} \frac{\omega^{(a-b)k}}{(\omega^{a-b} - 1)^2} = -\frac{1}{12}(q-2)(q^2 + 6q + 5 - 12k - 6qk + 6k^2).$$

Proof. The summation in (3.4) is equal to

$$= \sum_{a=1}^{q-1} \left\{ \sum_{b=1}^{a-1} + \sum_{b=a+1}^{q-1} \right\} \frac{\omega^{(a-b)k}}{(\omega^{a-b}-1)^2}$$

$$= \sum_{a=1}^{q-1} \sum_{n=1}^{a-1} \frac{\omega^{nk}}{(\omega^n-1)^2} + \sum_{a=1}^{q-1} \sum_{n=1}^{q-a-1} \frac{\omega^{-nk}}{(\omega^{-n}-1)^2}$$

$$= \sum_{a=1}^{q-1} \sum_{\substack{n=1 \\ n \neq a}}^{q-1} \frac{\omega^{nk}}{(\omega^n-1)^2}$$

(3.5)
$$= (q-2) \sum_{a=1}^{q-1} \frac{\omega^{ak}}{(\omega^a-1)^2}.$$

We now apply (3.2) and Lemma 2 to obtain

$$\sum_{a=1}^{q-1} \frac{\omega^{ak}}{(\omega^a-1)^2} = \sum_{n=1}^{q-1} \omega^{nk} \frac{1}{q^2} \sum_{a,b=1}^{q-1} ab\,\omega^{n(a+b)}$$

$$= \frac{1}{q^2} \sum_{a,b=1}^{q-1} ab \sum_{n=1}^{q-1} \omega^{n(a+b+k)}$$

$$= \frac{1}{q} \sum_{\substack{a,b=1 \\ k+a+b\equiv 0 \pmod q}}^{q-1} ab - \frac{(q-1)^2}{4}$$

(3.6)
$$= -\frac{1}{12}(q^2 + 6q + 5 - 12k - 6qk + 6k^2).$$

Lemma 3 follows from this and (3.5). □

As before let $f_q^t(z)$ be the shifted Fekete polynomial obtained by shifting the coefficients to the left by t where $1 \leq t \leq q$. So $f_q^q(z) = f_q(z)$. Then we have

(3.7)
$$f_q^t(\omega^k) = \omega^{-tk} f_q(\omega^k)$$

for any $0 \leq k \leq q-1$. We are going to evaluate the following summation

$$\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4.$$

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

$$f_q^{q-t+1}(-\omega^k) = \sum_{n=0}^{q-1} \left(\frac{n+q-t+1}{q} \right) (-\omega^k)^n$$

$$= (-\omega^k)^{-(q-t+1)} \left\{ -\sum_{n=1}^{q-t} + \sum_{n=q-t+1}^{q-1} \right\} \left(\frac{n}{q} \right) (-\omega^k)^n$$

$$= (-\omega^k)^{-(q-t+1)} \left\{ -\sum_{n=t}^{q-1} + \sum_{n=1}^{t-1} \right\} \left(\frac{q-n}{q} \right) (-\omega^k)^{q-n}$$

$$= (-\omega^k)^{-(q+1)} \left(\frac{-1}{q} \right) (-\omega^k)^t \left\{ -\sum_{n=1}^{t-1} + \sum_{n=t}^{q-1} \right\} \left(\frac{n}{q} \right) (-\omega^k)^n$$

(3.8)
$$= \omega^{-k} \left(\frac{-1}{q} \right) \overline{f_q^t(-\omega^k)}.$$

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

We use the basic approach of [Hø-88] which is by interpolation at the $2q$th roots of unity. Using the Lagrange interpolation formula at the qth roots of unity, we have

$$f_q^t(z) = \frac{1}{q} \sum_{j=0}^{q-1} \frac{z^q - 1}{z - \omega^j} \omega^j f_q^t(\omega^j).$$

It follows that

$$\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 = \frac{16}{q^4} \sum_{k=0}^{q-1} \left| \sum_{j=0}^{q-1} \frac{\omega^j}{\omega^k + \omega^j} f_q^t(\omega^j) \right|^4$$

$$= \frac{16}{q^4} \sum_{a,b,c,d=0}^{q-1} f_q^t(\omega^a) \bar{f}_q^t(\omega^b) f_q^t(\omega^c) \bar{f}_q^t(\omega^d) \omega^{a+c}$$

$$\times \sum_{k=0}^{q-1} \frac{1}{\omega^k + \omega^a} \frac{\omega^k}{\omega^k + \omega^b} \frac{1}{\omega^k + \omega^c} \frac{\omega^k}{\omega^k + \omega^d}.$$

We then group the terms in the above summation over a, b, c and d by the following cases:

    (1) $a = c$ and $a \ne b \ne d$,
    (2) $a = b = c \ne d$,
    (3) $a = b \ne c = d$,
    (4) $a = b = c = d$,
    (5) $a \ne b \ne c \ne d$,

and we obtain the following formula from [Hø-88]

(3.9)
$$\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 = \frac{16}{q^4}(A + B + C + D)$$

where

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

$$B = \frac{q^2}{4}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}|f_q^t(\omega^a)|^2(\bar{f}_q^t(\omega^a)f_q^t(\omega^b)\omega^b + f_q^t(\omega^a)\bar{f}_q^t(\omega^b)\omega^a)\left(\frac{\omega^a+\omega^b}{(\omega^a-\omega^b)^2}\right)$$

$$C = -\frac{q^2}{4}\sum_{\substack{a,b,c=0\\a\neq b\neq c}}^{q-1}2|f_q^t(\omega^a)|^2\left(\frac{f_q^t(\omega^b)\bar{f}_q^t(\omega^c)\omega^{a+b}+f_q^t(\omega^c)\bar{f}_q^t(\omega^b)\omega^{a+c}}{(\omega^b-\omega^a)(\omega^c-\omega^a)}\right)$$

$$-\frac{q^2}{4}\sum_{\substack{a,b,c=0\\a\neq b\neq c}}^{q-1}\frac{f_q^t(\omega^a)^2\bar{f}_q^t(\omega^b)\bar{f}_q^t(\omega^c)\omega^{2a}+\bar{f}_q^t(\omega^a)^2 f_q^t(\omega^b)f_q^t(\omega^c)\omega^{b+c}}{(\omega^b-\omega^a)(\omega^c-\omega^a)}$$

$$D = -\frac{q^2}{4}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}\frac{4|f_q^t(\omega^a)|^2|f_q^t(\omega^b)|^2\omega^{a+b}+f_q^t(\omega^b)^2\bar{f}_q^t(\omega^a)^2\omega^{2b}+f_q^t(\omega^a)^2\bar{f}_q^t(\omega^b)^2\omega^{2a}}{(\omega^a-\omega^b)^2}.$$

Here A, B, C and D are the sum of terms according to the above cases (1), (2), (3) and (4) respectively and the sum of terms corresponding to the case (5) is zero.

We now evaluate A, B, C and D separately. Using (3.1) and (3.7), we have

(3.10)
$$A = \frac{q^4(q-1)(q^2+2)}{48}$$

and

$$B = \frac{q^2}{4}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}q^2\left(\frac{ab}{q}\right)\frac{(\omega^{at-bt+b}+\omega^{-at+bt+a})(\omega^a+\omega^b)}{(\omega^b-\omega^a)^2}$$

$$= \frac{q^4}{2}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}\left(\frac{ab}{q}\right)\frac{\omega^{at-bt+b}(\omega^a+\omega^b)}{(\omega^b-\omega^a)^2}$$

$$= -\frac{q^4}{2}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}\left(\frac{ab}{q}\right)\frac{\omega^{(a-b)t}}{|\omega^{a-b}-1|^2}+\frac{q^4}{2}\sum_{\substack{a,b=0\\a\neq b}}^{q-1}\left(\frac{ab}{q}\right)\frac{\omega^{(a-b)t}}{(\omega^{a-b}-1)^2}$$

$$:= \frac{q^4}{2}\left\{-B_1(\omega)+B_2(\omega)\right\}.$$

It is clear that $B_1(\omega^j) = B_1(\omega)$ and $B_2(\omega^j) = B_2(\omega)$ for $1 \leq j \leq q-1$. Thus,

$$B = \frac{q^4}{2(q-1)} \left\{ -\sum_{j=1}^{q-1} B_1(\omega^j) + \sum_{j=1}^{q-1} B_2(\omega^j) \right\}$$

$$= \frac{q^4}{2(q-1)} \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \left(\frac{ab}{q}\right) \sum_{j=1}^{q-1} \omega^{j(a-b)t} \left\{ \frac{1}{(\omega^{j(a-b)} - 1)^2} - \frac{1}{|\omega^{j(a-b)} - 1|^2} \right\}$$

$$= \frac{q^4}{2(q-1)} \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \left(\frac{ab}{q}\right) \sum_{j=1}^{q-1} \omega^{jt} \left\{ \frac{1}{(\omega^j - 1)^2} - \frac{1}{|\omega^j - 1|^2} \right\}$$

$$= -\frac{q^4}{2} \left\{ \sum_{j=1}^{q-1} \frac{\omega^{jt}}{(\omega^j - 1)^2} - \sum_{j=1}^{q-1} \frac{\omega^{jt}}{|\omega^j - 1|^2} \right\}$$

$$= -\frac{q^4}{2} \left\{ \sum_{j=1}^{q-1} \frac{\omega^{jt} + \omega^{j(t+1)}}{(\omega^j - 1)^2} \right\}$$

$$(3.11) \qquad = \frac{q^4}{12}(q^2 + 3q + 2 - 6t - 6qt + 6t^2)$$

by (3.6). Here we have used the fact that

$$\sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \left(\frac{ab}{q}\right) = -(q-1).$$

For D, we have

$$D = -\frac{q^4}{4} \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \frac{4\omega^{a+b} + \omega^{-2bt+2at+2b} + \omega^{-2at+2bt+2a}}{(\omega^a - \omega^b)^2}$$

$$(3.12) \qquad = -q^4 \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \frac{\omega^{a+b}}{(\omega^a - \omega^b)^2} - \frac{q^4}{2} \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \frac{\omega^{2(a-b)t}}{(\omega^{a-b} - 1)^2},$$

from (3.1) and (3.7). The first sum in (3.12) can be evaluated as follows:

$$\sum_{a=1}^{q-1} \sum_{\substack{b=1 \\ b \neq a}}^{q-1} \frac{\omega^{a+b}}{(\omega^b - \omega^a)^2} = -\sum_{a=1}^{q-1} \sum_{\substack{b=1 \\ b \neq a}}^{q-1} \frac{1}{|\omega^{b-a} - 1|^2}$$

$$= -\sum_{a=1}^{q-1} \sum_{\substack{k=1 \\ k \neq a}}^{q-1} \frac{1}{|\omega^k - 1|^2}$$

$$= -(q-2) \sum_{k=1}^{q-1} \frac{1}{|\omega^k - 1|^2}$$

$$(3.13) \qquad = -\frac{(q^2 - 1)(q-2)}{12}.$$

To compute the second sum in (3.12), we apply Lemma 3 with $k = 2t$. Hence using (3.4) in Lemma 3, (3.12) and (3.13), we have

$$(3.14) \qquad D = \frac{q^4(q-2)}{8}(q^2 + 2q + 1 - 8t - 4qt + 8t^2).$$

Finally, we consider the term C. Using (3.1) and (3.7) again, we obtain

$$C = -\frac{q^4}{4} \sum_{\substack{a,b,c=1 \\ a \neq b \neq c}}^{q-1} \left(\frac{bc}{q}\right) \left\{ \frac{2\omega^{-bt+ct+a+b} + 2\omega^{bt-ct+a+c} + \omega^{-2at+bt+ct+2a} + \omega^{2at-bt-ct+b+c}}{(\omega^b - \omega^a)(\omega^c - \omega^a)} \right\}$$

$$= -q^4 \sum_{\substack{a,b,c=1 \\ a \neq b \neq c}}^{q-1} \left(\frac{bc}{q}\right) \frac{\omega^{-bt+ct+a+b}}{(\omega^b - \omega^a)(\omega^c - \omega^a)} - \frac{q^4}{2}\Re \left\{ \sum_{\substack{a,b,c=1 \\ a \neq b \neq c}}^{q-1} \left(\frac{bc}{q}\right) \frac{\omega^{-2at+bt+ct+2a}}{(\omega^b - \omega^a)(\omega^c - \omega^a)} \right\}$$

$$(3.15)$$

$$:= -\left(q^4 c_1 + \frac{q^4}{2}\Re(c_2)\right).$$

Both c_1 and c_2 can be evaluated in the similar way. From (3.13) and Lemma 1, we have

$$c_1 = -\sum_{a=1}^{q-1} \left| \sum_{\substack{b=1 \\ b \neq a}}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{b(1-t)}}{\omega^b - \omega^a} \right|^2 - \sum_{\substack{a,b=1 \\ a \neq b}}^{q-1} \frac{\omega^{a+b}}{(\omega^b - \omega^a)^2}$$

$$= -\sum_{a=0}^{q-1} \left| \sum_{\substack{b=1 \\ b \neq a}}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{b(1-t)}}{\omega^b - \omega^a} \right|^2 + \frac{(q^2-1)(q-2)}{12} + \left| \sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{b(1-t)}}{\omega^b - 1} \right|^2$$

$$(3.16) \qquad = -\sum_{a=0}^{q-1} \left| \sum_{\substack{b=1 \\ b \neq a}}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{b(1-t)}}{\omega^b - \omega^a} \right|^2 + \frac{(q^2-1)(q-2)}{12} + \frac{1}{q}\left| \sum_{n=1}^{q-1} n\left(\frac{t+n}{q}\right) \right|^2.$$

To evaluate c_1, it remains to consider the first summation in (3.16). Using (3.1) and (3.2)

$$
\sum_{a=0}^{q-1}\left|\sum_{\substack{b=1\\b\neq a}}^{q-1}\left(\frac{b}{q}\right)\frac{\omega^{b(1-t)}}{\omega^b-\omega^a}\right|^2 = \sum_{a=0}^{q-1}\left|\sum_{\substack{b=1\\b\neq a}}^{q-1}\left(\frac{b}{q}\right)\frac{\omega^{-bt}}{1-\omega^{a-b}}\right|^2
$$

$$
= \frac{1}{q^2}\sum_{a=0}^{q-1}\left|\sum_{n=1}^{q-1}n\omega^{an}\sum_{\substack{b=1\\b\neq a}}^{q-1}\left(\frac{b}{q}\right)\omega^{-b(n+t)}\right|^2
$$

$$
= \frac{1}{q^2}\sum_{a=0}^{q-1}\left|\sum_{n=1}^{q-1}n\omega^{an}\left\{f_p(\omega^{-(n+t)})-\left(\frac{a}{q}\right)\omega^{-a(n+t)}\right\}\right|^2
$$

$$
= \frac{1}{q^2}\sum_{a=0}^{q-1}\left|\sqrt{q}\left(\frac{-1}{q}\right)\epsilon_q\sum_{n=1}^{q-1}n\omega^{an}\left(\frac{n+t}{q}\right)-\frac{q(q-1)}{2}\left(\frac{a}{q}\right)\omega^{-at}\right|^2
$$

$$
= \frac{1}{q}\sum_{a=0}^{q-1}\left|\sum_{n=1}^{q-1}n\omega^{an}\left(\frac{n+t}{q}\right)\right|^2 + \frac{(q-1)^3}{4}
$$

(3.17)
$$
- \epsilon_q\frac{q-1}{\sqrt{q}}\left(\frac{-1}{q}\right)\sum_{n=1}^{q-1}n\left(\frac{n+t}{q}\right)f_q(\omega^{n+t}).
$$

The first term in (3.17) is equal to

$$
= \frac{1}{q}\sum_{n,m=1}^{q-1}nm\left(\frac{n+t}{q}\right)\left(\frac{m+t}{q}\right)\sum_{a=0}^{q-1}\omega^{a(n-m)}
$$

$$
= \sum_{n=1}^{q-1}n^2\left(\frac{n+t}{q}\right)^2
$$

$$
= \frac{q(q-1)(2q-1)}{6}-(q-t)^2
$$

and the last term in (3.17) is

$$
= -\epsilon_q^2\left(\frac{-1}{q}\right)(q-1)\sum_{n=1}^{q-1}n\left(\frac{n+t}{q}\right)^2
$$

$$
= -(q-1)\left(\frac{q(q-1)}{2}-(q-t)\right)
$$

because $\epsilon_q^2\left(\frac{-1}{q}\right)=1$. So this shows that

$$
\sum_{a=0}^{q-1}\left|\sum_{\substack{b=1\\b\neq a}}^{q-1}\left(\frac{b}{q}\right)\frac{\omega^{b(1-t)}}{\omega^b-\omega^a}\right|^2 = \frac{(q-1)}{12}(q^2-2q+3)-(t-1)(t-q)
$$

and hence from (3.16), we have

$$(3.18) \qquad c_1 = \frac{(q-1)(q-5)}{12} + (t-1)(t-q) + \frac{1}{q} \left| \sum_{n=1}^{q-1} n \left(\frac{n+t}{q} \right) \right|^2 .$$

Similarly, we can prove that

$$c_2 = \frac{1}{12}(-5q^2 - 6q - 13 + 24tq + 48t - 48t^2) - (t-1)(t-q) - \left(\frac{-1}{q} \right) \frac{1}{q} \left| \sum_{n=1}^{q-1} n \left(\frac{n+t}{q} \right) \right|^2$$

and therefore from (3.15) and (3.18), we have

$$(3.19) \qquad C = \frac{q^4}{8}(q^2 + 2q + 1 + 12t^2 - 4qt - 12t) - q^3 \left(1 - \frac{1}{2} \left(\frac{-1}{q} \right) \right) \left| \sum_{n=1}^{q-1} n \left(\frac{n+t}{q} \right) \right|^2 .$$

As a result, from (3.9), (3.10), (3.11), (3.14) and (3.19) we have

$$(3.20) \quad \sum_{j=0}^{q-1} |f_q^t(-\omega^j)|^4 = \frac{q}{3}(7q^2 + 9q + 8 + 48t^2 - 24qt - 48t) - \frac{16}{q} \left(1 - \frac{1}{2} \left(\frac{-1}{q} \right) \right) \left| \sum_{n=1}^{q-1} n \left(\frac{n+t}{q} \right) \right|^2 .$$

Finally, since

$$\|f_q^t\|_4^4 = \frac{1}{2q} \left\{ \sum_{k=0}^{q-1} |f_q^t(\omega^k)|^4 + \sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 \right\}$$

$$= \frac{1}{2q} \left\{ q^2(q-1) + \sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 \right\},$$

by (3.1), so from (3.7), (3.8) and (3.20), we conclude that

$$\|f_q^t\|_4^4 = \frac{1}{3}(5q^2 + 3q + 4) + 8t^2 - 4qt - 8t - \frac{8}{q^2} \left(1 - \frac{1}{2} \left(\frac{-1}{q} \right) \right) \left| \sum_{n=1}^{q-1} n \left(\frac{n+t}{q} \right) \right|^2$$

and $\|f_q^{q-t+1}\|_4^4 = \|f_q^t\|_4^4$ for $1 \le t \le (q+1)/2$. This completes the proof of our Theorem 5.

To prove Corollary 6, we put $t = 1$ into (3.20) and use the fact that

$$\sum_{n=1}^{q-1} n \left(\frac{n+1}{q} \right) = \sum_{n=1}^{q-1} n \left(\frac{n}{q} \right) .$$

We now come to the proof of Theorem 4. We first have the following lemma.

Lemma 4. *Let q be a prime and $q > 3$. Then we have*

$$\sum_{n=1}^{[\frac{q}{4}]-1} \left(\frac{n}{q}\right) = \begin{cases} \frac{1}{2}h(-q) - 1 & if \quad q \equiv 1 \pmod 4, \\ 0 & if \quad q \equiv 3 \pmod 8, \\ h(-q) & if \quad q \equiv 7 \pmod 8. \end{cases}$$

Proof. We write $q = 4k + a$ if $q \equiv a \pmod 4$ where a is either 1 or 3. Consider

$$G_q(1) + G_q(-1) = \sum_{n=1}^{\frac{q-1}{2}} \left(\frac{n}{q}\right)(1 + (-1)^n)$$

$$= 2 \sum_{\substack{n=1 \\ n \text{ is even}}}^{\frac{q-1}{2}} \left(\frac{n}{q}\right)$$

$$= 2 \sum_{n=1}^{k} \left(\frac{2n}{q}\right).$$

When $q \equiv 1 \pmod 4$, then $[\frac{q}{4}] = k$ and $G_q(1) = 0$ and hence from (1.1)

$$\sum_{n=1}^{[\frac{q}{4}]-1} \left(\frac{n}{q}\right) = \frac{1}{2}\left(\frac{2}{q}\right)G_q(-1) - \left(\frac{[\frac{q}{4}]}{q}\right)$$

$$= \frac{1}{2\lambda_q}\left(\frac{2}{q}\right)h(-q) - 1$$

$$= \frac{1}{2}h(-q) - 1$$

because

$$\left(\frac{[\frac{q}{4}]}{q}\right) = \left(\frac{k}{q}\right) = \left(\frac{4k}{q}\right) = \left(\frac{q-1}{q}\right) = \left(\frac{-1}{q}\right) = 1.$$

When $q \equiv 3 \pmod 4$, then $[\frac{q}{4}] = k + 1$ and we have

$$\sum_{n=1}^{[\frac{q}{4}]-1} \left(\frac{n}{q}\right) = \frac{1}{2}\left(\frac{2}{q}\right)\{G_q(1) + G_q(-1)\}$$

$$= \frac{1}{2}\left(\frac{2}{q}\right)\left\{\left(2 - \left(\frac{2}{q}\right)\right)h(-q) + \frac{1}{\lambda_q}h(-q)\right\}$$

$$= \frac{1}{2}\left(\frac{2}{q}\right)\left\{\left(2 - \left(\frac{2}{q}\right)\right) + \frac{1}{\lambda_q}\right\}h(-q)$$

and our result follows from this and (1.1). □

Using (2.1) we have

$$\frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n+[\frac{q}{4}]}{q}\right) = \sum_{n=1}^{[\frac{q}{4}]-1}\left(\frac{n}{q}\right) + \frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n}{q}\right).$$

Then Theorem 4 follows from this, (1.2), Lemma 4 and Theorem 5.

REFERENCES

Be-91. J. Beck, *Flat polynomials on the unit circle – note on a problem of Littlewood*, Bull. London Math. Soc. **23** (1991), 269–277.

Bo-98. P. Borwein, *Some Old Problems on Polynomials with Integer Coefficients*, Approximation theory IX **Vol. I.** (Nashville, TN, 1998), 31–50.

BC-00. P. Borwein and K.K. Choi, *Merit Factors for Character Polynomials*, Journal of the London Mathematical Society, **(2) 61** (2000), no. 3, 706-720.

BC-01. P. Borwein and K.K. Choi, *Merit Factors of Polynomials formed by Jacobi Symbols*, Canadian Journal of Mathematics **53** (2001), no. 1, 33-50.

BL-01. P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, Proc. Amer. Math. Soc. **129** (2001), 1463-1472.

BM-00. P. Borwein and M. Mossinghoff, *Rudin-Shapiro like Polynomials in L_4*, Math. Computat **69** (2000), 1157–1166.

CGPS-98. B. Conrey, A. Granville, B. Poonen and K. Soundararajan, *Zeros of Fekete polynomials*, Annales Institut Fourier (Grenoble) **50** (2000), no. 3, 865–889.

Go-77. M. J. Golay, *Sieves for low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **23** (1977), 43–51.

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

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

Hu-82. L. K. Hua, *Introduction to Number Theory*, Springer–Verlag, Berlin, 1982.

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

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

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

Me-96. S. Mertens, *Exhaustive search for low-autocorrelation binary sequences*, J. Phys. A **29** (1996), L473–L481.

Mo-80. H. L. Montgomery, *An exponential sum formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.

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

Re-93. A. Reinholz, *Ein paralleler genetische Algorithmus zur Optimierung der binären Autokorrelations-Funktion*, Diplomarbeit, Rheinische Friedrich-Wilhelms-Universität Bonn, 1993.

Saf-90. B. Saffari, *Barker sequences and Littlewood's "two-sided conjectures" on polynomials with ± 1 coefficients*, Séminaire d'Analyse Harmonique. Anneé 1989/90, 139–151, Univ. Paris XI, Orsay, 1990.

DEPARTMENT OF MATHEMATICS AND STATISTICS, SIMON FRASER UNIVERSITY, BURNABY, B.C., CANADA V5A 1S6