L^q NORMS OF FEKETE AND RELATED POLYNOMIALS

CHRISTIAN GÜNTHER AND KAI-UWE SCHMIDT

ABSTRACT. A Littlewood polynomial is a polynomial in $\mathbb{C}[z]$ having all of its coefficients in $\{-1, 1\}$. There are various old unsolved problems, mostly due to Littlewood and Erdős, that ask for Littlewood polynomials that provide a good approximation to a function that is constant on the complex unit circle, and in particular have small L^q norm on the complex unit circle. We consider the Fekete polynomials

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

where p is an odd prime and $(\,\cdot\,|\,p)$ is the Legendre symbol (so that $z^{-1} f_p(z)$ is a Littlewood polynomial). We give explicit and recursive formulas for the limit of the ratio of L^q and L^2 norm of $f_p(z)$ when q is an even positive integer and $p \to \infty$. To our knowledge, these are the first results that give these limiting values for specific sequences of nontrivial Littlewood polynomials and infinitely many q. Similar results are given for polynomials obtained by cyclically permuting the coefficients of Fekete polynomials and for Littlewood polynomials whose coefficients are obtained from additive characters of finite fields. These results vastly generalise earlier results on the L^4 norm of these polynomials.

1. INTRODUCTION

For real $\alpha \geq 1$, the L^α norm of a polynomial $f(z)$ in $\mathbb{C}[z]$ on the complex unit circle is

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

and its supremum norm is $\|f\|_\infty = \max_{\theta \in [0,2\pi]} |f(e^{i\theta})|$. There are various extremal problems, originally raised by Erdős, Littlewood, and others, concerning the behaviour of such norms for polynomials with all coefficients in $\{-1, 1\}$, which are today called *Littlewood polynomials* (see Littlewood [29], Borwein [3], and Erdélyi [12] for surveys on selected problems). Roughly speaking, such problems ask for Littlewood polynomials $f(z)$ that provide a good approximation to a function that is constant on the unit circle. Note that this constant is necessarily $\|f\|_2 = \sqrt{1 + \deg f}$.

Several conjectures have been posed that address the question of what is the best approximation in a certain sense. For example, Golay [17] conjectured that there exists a constant c such that $\|f\|_4 / \|f\|_2 \geq 1 + c$ for every

nonconstant Littlewood polynomial f and Littlewood [28] conjectured that there is no such constant. Golay's conjecture implies another famous conjecture due to Erdős [14], [32], which states that there exists a constant c' such that $\|f\|_\infty/\|f\|_2 \geq 1 + c'$ for every nonconstant Littlewood polynomial f. All these conjectures are wide open.

Borwein and Lockhart [6] proved that, if f_n is a random polynomial of degree $n - 1$, then

$$\lim_{n\to\infty} \mathrm{E}\left(\frac{\|f_n\|_\alpha}{\sqrt{n}}\right)^\alpha = \Gamma(1 + \alpha/2)$$

and $(\|f_n\|_\alpha/\sqrt{n})^\alpha$ is asymptotically concentrated around its expectation (see also Choi and Erdélyi [8] for more results on L^α norms of random Littlewood polynomials). Littlewood [29] (and independently Newman and Byrnes [32] and Høholdt, Jensen, and Justesen [20]) determined the L^4 norm of the Rudin-Shapiro polynomials [35], [34]. More generally, a conjecture attributed in [10] to Saffari asserts that, if q is a positive integer and f_n is a Rudin-Shapiro polynomial of degree $n - 1$, then

$$\lim_{n\to\infty}\left(\frac{\|f_n\|_{2q}}{\sqrt{n}}\right)^{2q} = \frac{2^q}{q+1}.$$

This conjecture is true for $q \leq 27$ by combining results of Doche and Habsieger [10] and Taghavi and Azadi [37], but the general problem remains open.

In this paper we consider the following families of polynomials. For an odd prime p, the *Fekete polynomial* of degree $p - 1$ is

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

where $(\,\cdot\,|\,p)$ is the Legendre symbol. Note that $z^{-1} f_p(z)$ is a Littlewood polynomial, which has the same L^α norm as $f_p(z)$. For a Mersenne number $n = 2^k - 1$, a *Galois polynomial* of degree $n - 1$ is the Littlewood polynomial

$$g_n(z) = \sum_{j=0}^{n-1} \psi(\theta^j)\, z^j,$$

where θ is a primitive element of $\mathbb{F}_{2^k}$ and ψ is a nontrivial additive character of $\mathbb{F}_{2^k}$. Fekete polynomials appear frequently in the context of extremal polynomial problems [30], [19], [23], [9], [5], [4], [22], [21], [24] and have been studied extensively now for over a century [15].

Erdélyi [13] established the order of growth of the L^α norm of Fekete polynomials. Høholdt and Jensen [19] proved that, for Fekete polynomials $f_p(z)$,

$$\lim_{p\to\infty}\left(\frac{\|f_p\|_4}{\sqrt{p}}\right)^4 = \frac{5}{3}.$$

In fact Borwein and Choi [4] established exact expressions for $\|f_p\|_4$ in terms of the class number of $\mathbb{Q}(\sqrt{-p})$. Jensen, Jensen, and Høholdt [23] proved that, for Galois polynomials $g_n(z)$,

$$\lim_{n\to\infty} \left(\frac{\|g_n\|_4}{\sqrt{n}}\right)^4 = \frac{4}{3}.$$

These are in fact special cases of our main results (see Theorems 2.1 and 2.3), which provide corresponding limiting values for the L^{2q} norms of Fekete and Galois polynomials for all positive integers q. To our knowledge, these are the first results that give these limiting values for specific sequences of nontrivial Littlewood polynomials and infinitely many q.

We also consider the *shifted* Fekete polynomials

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

where r is an integer, which can depend on p. It is known [19] that, if $r/p \to R$ as $p \to \infty$, then

$$(1) \qquad \lim_{p\to\infty} \left(\frac{\|f_p^r\|_4}{\sqrt{p}}\right)^4 = \frac{7}{6} + \frac{1}{2}(4|R| - 1)^2 \quad \text{for } |R| \le \frac{1}{2}.$$

Again, this is a special case of a more general result (see Theorem 2.5). Note that a shifted Fekete polynomial is not necessarily a Littlewood polynomial since one of its first p coefficients is zero. However changing this coefficient to -1 or 1 does not affect the asymptotic behaviour of the L^α norm.

2. Results

We begin with establishing some notation that is required to state our results. For a positive integer m, let Π_m be the set of partitions of $\{1, 2, \dots, m\}$. For $\pi \in \Pi_m$, we refer to the elements of π as *blocks* and we say that π is *even* if each block of π has even cardinality.

For a positive integer n and real x, we define the *generalised Eulerian numbers* to be

$$(2) \qquad \left\langle \begin{matrix} n \\ x \end{matrix} \right\rangle = \sum_{j=0}^{\lfloor x+1 \rfloor} (-1)^j \binom{n+1}{j} (x + 1 - j)^n.$$

Note that $\left\langle \begin{smallmatrix} n \\ x \end{smallmatrix} \right\rangle$ is nonzero only for $x \in (-1, n)$. If x is integral, then $\left\langle \begin{smallmatrix} n \\ x \end{smallmatrix} \right\rangle$ is an Eulerian number in the usual sense. We refer to the book [33] for the combinatorial significance of Eulerian numbers and to [39] for a natural interpretation of generalised Eulerian numbers in terms of splines.

The *signed tangent numbers* $T(k)$ are defined by

$$(3) \qquad \log \cosh(z) = \sum_{k=1}^{\infty} \frac{T(k)}{(2k)!}\, z^{2k} \quad \text{for } |z| < \pi/2.$$

They are scaled versions of Bernoulli numbers and $|T(k)| = (-1)^{k+1}T(k)$ are known as the *tangent* or *zag* numbers, which appear in [1] as $\texttt{A000182} = [1, 2, 16, 272, 7936, 353792, \dots]$. The numbers $T(k)$ can be recursively determined via

$$T(k) = 1 - \sum_{j=1}^{k-1} \binom{2k-1}{2j-1} T(j) \quad \text{for } k \geq 1,$$

which can be deduced from Lemma 4.3.

For Fekete polynomials we have the following result.

Theorem 2.1. *Let q be a positive integer and let $f_p(z)$ be the Fekete polynomial of degree $p - 1$. Then*

$$\lim_{p \to \infty} \left(\frac{\|f_p\|_{2q}}{\sqrt{p}} \right)^{2q} = \sum_{\substack{\pi \in \Pi_{2q} \\ \pi \ even}} \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = q}} \prod_{i=1}^{\ell} \frac{T(N_i)}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ a_i - 1 \end{matrix} \right\rangle,$$

where $\pi = \{B_1, \dots, B_\ell\}$ and $N_i = |B_i|/2$ for all i.

The following corollary provides an efficient way to compute the limiting values in Theorem 2.1.

Corollary 2.2. *Set $F(0, 0) = 1$ and, for $1 \leq m \leq 2k - 1$, define the numbers $F(k, m)$ recursively by*

$$F(k, m) = \sum_{j=1}^{k} \binom{2k-1}{2j-1} \frac{T(j)}{(2j-1)!} \sum_i \left\langle \begin{matrix} 2j - 1 \\ i - 1 \end{matrix} \right\rangle F(k - j, m - i),$$

where the inner sum is over all i such that $F(k - j, m - i)$ is defined. Let q be a positive integer and let $f_p(z)$ be the Fekete polynomial of degree $p - 1$. Then

$$\lim_{p \to \infty} \left(\frac{\|f_p\|_{2q}}{\sqrt{p}} \right)^{2q} = F(q, q).$$

For $k \geq 1$, the numbers $(2k - 1)!\, F(k, m)$ identified in Corollary 2.2 define a triangular array of integers, whose first four rows are given by:

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & -2 & 10 & -2 & & \\
 & 16 & -184 & 456 & -184 & 16 & \\
-272 & 5776 & -30736 & 55504 & -30736 & 5776 & -272
\end{array}
$$

The first and last entry in row k equals $T(k)$ and the central entry in row k divided by $(2k - 1)!$ equals the limiting value in Corollary 2.2 for $k = q$. The first eight of these limiting values are:

$$1, \frac{5}{3}, \frac{19}{5}, \frac{3469}{315}, \frac{21565}{567}, \frac{7760593}{51975}, \frac{12478099}{19305}, \frac{643983856759}{212837625}.$$

We now turn to Galois polynomials. Let $J_0(z)$ be the zeroth Bessel function of the first kind and define the numbers $C(k)$ via

$$(4) \qquad \log(J_0(2\sqrt{z})) = \sum_{k=1}^{\infty} \frac{(-1)^k C(k)}{(k!)^2} z^k.$$

We call these numbers the *signed Carlitz numbers*. The corresponding unsigned numbers $|C(k)| = (-1)^{k+1}C(k)$ have been extensively studied by Carlitz [7] and appear in [1] as $\mathtt{A002190} = [0, 1, 1, 4, 33, 456, 9460, \dots]$ (which starts at $k = 0$ with $C(0) = 0$). The numbers $C(k)$ can be recursively determined via

$$C(k) = 1 - \sum_{j=1}^{k-1} \binom{k}{j}\binom{k-1}{j-1} C(j) \quad \text{for } k \geq 1,$$

which again can be deduced from Lemma 4.3.

For Galois polynomials we have the following result.

Theorem 2.3. *Let q be a positive integer and let $g_n(z)$ be a Galois polynomial of degree $n-1$. Then*

$$\lim_{n\to\infty} \left(\frac{\|g_n\|_{2q}}{\sqrt{n}} \right)^{2q} = \sum_{\pi \in \Pi_q} \binom{q}{N_1, \dots, N_\ell} \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = q}} \prod_{i=1}^{\ell} \frac{C(N_i)}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ a_i - 1 \end{matrix} \right\rangle,$$

where $\pi = \{B_1, \dots, B_\ell\}$ and $N_i = |B_i|$ for all i.

We have the following counterpart of Corollary 2.2 for Galois polynomials.

Corollary 2.4. *Set $G(0,0) = 1$ and, for $1 \leq m \leq 2k-1$, define the numbers $G(k, m)$ recursively by*

$$G(k, m) = \sum_{j=1}^{k} \binom{k}{j}\binom{k-1}{j-1} \frac{C(j)}{(2j-1)!} \sum_{i} \left\langle \begin{matrix} 2j-1 \\ i-1 \end{matrix} \right\rangle G(k-j, m-i),$$

where the inner sum is over all i such that $G(k-j, m-i)$ is defined. Let q be a positive integer and let $g_n(z)$ be a Galois polynomial of degree $n-1$. Then

$$\lim_{n\to\infty} \left(\frac{\|g_n\|_{2q}}{\sqrt{n}} \right)^{2q} = G(q, q).$$

For $k \geq 1$, the numbers $(2k-1)! \, G(k, m)$ identified in Corollary 2.4 also define a triangular array of integers, whose first four rows are given by:

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & -1 & 8 & -1 & & \\
 & 4 & -76 & 264 & -76 & 4 & \\
-33 & 1248 & -9735 & 22080 & -9735 & 1248 & -33
\end{array}
$$

The first and last entry in row k equals $C(k)$ and the central entry in row k divided by $(2k-1)!$ equals the limiting value in Corollary 2.4 for $k = q$. The first eight of these limiting values are:

$$1, \frac{4}{3}, \frac{11}{5}, \frac{92}{21}, \frac{15481}{1512}, \frac{411913}{15120}, \frac{2482927}{30888}, \frac{4181926481}{16216200}.$$

In what follows we consider the shifted Fekete polynomials.

Theorem 2.5. *Let q be a positive integer and let $f_p^r(z)$ be a shifted Fekete polynomial corresponding to the Fekete polynomial of degree $p-1$. If $r/p \to R$ as $p \to \infty$, then*

$$\lim_{p \to \infty} \left(\frac{\|f_p^r\|_{2q}}{\sqrt{p}} \right)^{2q} = \sum_{\substack{\pi \in \Pi_{2q} \\ \pi \text{ even}}} \sum_{\substack{a_1, \dots, a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = q}} \prod_{i=1}^{\ell} \frac{T(N_i)}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ 2R(N_i - P_i) + a_i - 1 \end{matrix} \right\rangle,$$

where $\pi = \{B_1, \dots, B_\ell\}$, $N_i = |B_i|/2$, and $P_i = |\{x \in B_i : x > q\}|$ for all i.

Note that, for $R = 0$, Theorem 2.5 reduces to Theorem 2.1. We are not aware of a computationally efficient version of Theorem 2.5 in a spirit similar to Corollaries 2.2 and 2.4.

It follows from Theorem 2.5 that, for each positive integer q, there exists a function $\varphi_q : \mathbb{R} \to \mathbb{R}$ such that, if $r/p \to R$, then

$$\lim_{p \to \infty} \left(\frac{\|f_p^r\|_{2q}}{\sqrt{p}} \right)^{2q} = \varphi_q(R).$$

Since the generalised Eulerian numbers $\left\langle \begin{smallmatrix} n \\ x \end{smallmatrix} \right\rangle$ are continuous piecewise polynomial functions of x, the functions φ_q are also continuous piecewise polynomial functions. It follows from Theorem 2.5 that $\varphi_q(x + 1/2) = \varphi_q(x)$ for all $x \in \mathbb{R}$. It can also be shown that $\varphi_q(-x) = \varphi_q(x)$ for all $x \in \mathbb{R}$, so that it is sufficient to know $\varphi_q(x)$ for $x \in [0, 1/2)$. We have for example

$$\varphi_2(x) = \frac{7}{6} + \frac{1}{2}(4x - 1)^2 \quad \text{for } 0 \le x \le \frac{1}{2},$$

in accordance with (1),

$$\varphi_3(x) = \frac{31}{20} + \frac{3}{4}(4x - 1)^2(16x^2 - 8x + 3) \quad \text{for } 0 \le x \le \frac{1}{2},$$

and

$$\varphi_4(x) = \begin{cases} \phi(x) & \text{for } 0 \le x \le 1/4 \\ \phi(1/2 - x) & \text{for } 1/4 \le x \le 1/2, \end{cases}$$

where

$$\phi(x) = \frac{653}{280} + \frac{1}{72}(4x - 1)^2 \big(60416x^4 - 52736x^3 + 20208x^2 - 4216x + 625 \big).$$

For $q \in \{2, 3, 4\}$, it is readily verified that the function φ_q attains its global minimum at a unique point in $[0, 1/2)$, namely at $1/4$. We could not prove that this is true for all $q > 1$, but conjecture that this is the case. For convenience, we provide the first eight values of $\varphi_q(1/4)$ (starting with $q = 1$):

$$1, \frac{7}{6}, \frac{31}{20}, \frac{653}{280}, \frac{71735}{18144}, \frac{24880549}{3326400}, \frac{72207143}{4633200}, \frac{960901090937}{27243216000}.$$

We shall prove our results for Fekete and Galois polynomials in Sections 4 and 5, respectively.

We note that it is also possible to define shifted Galois polynomials by cyclically permuting the coefficients of a Galois polynomial. However every such polynomial is again a Galois polynomial. It should also be noted that our methods can be used to establish similar results for polynomials obtained by periodically appending or truncating monomials in Fekete or Galois polynomials, as considered in [22] and [21].

3. CALCULATION OF L^{2q} NORMS

We begin with establishing some notation that will be used throughout this paper. For a positive integer n, we write $e_n(x) = \exp(2\pi i x/n)$. Let $f(z) = \sum_{j=0}^{n-1} a_j z^j$ be a polynomial of degree $n-1$ in $\mathbb{C}[z]$ and let r be an integer. Define the *shifted* polynomial

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

where we extend the definition of a_j so that $a_{j+n} = a_j$ for all $j \in \mathbb{Z}$. We shall express the L^{2q} norm of this polynomial in a form that will be convenient for us later.

To do so, we associate with f the function $L_f : (\mathbb{Z}/n\mathbb{Z})^{2q} \to \mathbb{C}$ given by

$$L_f(t_1, \ldots, t_{2q}) = \frac{1}{n^{q+1}} \sum_{m \in \mathbb{Z}/n\mathbb{Z}} \prod_{k=1}^{q} f(e_n(m + t_k))\overline{f(e_n(m + t_{q+k}))}$$

and define another function $h_{n,r} : (\mathbb{Z}/n\mathbb{Z})^{2q} \to \mathbb{C}$ by

$$h_{n,r}(t_1, \ldots, t_{2q}) = \sum_{\substack{0 \le j_1, \ldots, j_{2q} < n \\ j_1 + \cdots + j_q = j_{q+1} + \cdots + j_{2q}}} \prod_{k=1}^{q} \overline{e_n(t_k(j_k + r))} e_n(t_{q+k}(j_{q+k} + r)).$$

The following proposition will be the starting point to prove our main results.

Proposition 3.1. *Let q be a positive integer, let $f(z)$ be a polynomial in $\mathbb{C}[z]$ of degree $n - 1$, and let r be an integer. Then*

$$\|f^r\|_{2q}^{2q} = \frac{1}{n^q} \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} L_f(t)\, h_{n,r}(t).$$

Proof. Write $f(z) = \sum_{j=0}^{n-1} a_j z^j$. From

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

we obtain

$$\|f^r\|_{2q}^{2q} = \sum_{\substack{0 \le j_1,\ldots,j_{2q} < n \\ j_1+\cdots+j_q = j_{q+1}+\cdots+j_{2q}}} \prod_{k=1}^q a_{j_k+r} \, \overline{a_{j_{q+k}+r}}.$$

Now it is readily verified that

$$a_j = \frac{1}{n} \sum_{s \in \mathbb{Z}/n\mathbb{Z}} f(e_n(s)) \, e_n(-sj),$$

giving

$$\|f^r\|_{2q}^{2q} = \frac{1}{n^{2q}} \sum_{s_1,\ldots,s_{2q} \in \mathbb{Z}/n\mathbb{Z}} h_{n,r}(s_1,\ldots,s_{2q}) \prod_{k=1}^q f(e_n(s_k)) \, \overline{f(e_n(s_{q+k}))}.$$

Re-index the summation with $s_i = m + t_i$ for all i and then sum over $m \in \mathbb{Z}/n\mathbb{Z}$ to obtain the statement in the proposition. $\square$

We also need the following estimate.

Lemma 3.2. *There exists a constant C_q, depending only on q, such that*

$$\sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} |h_{n,r}(t)| \le C_q \, n^{2q} (\log n)^{2q-1}$$

for all r.

Proof. After re-indexing the summation in the definition of $h_{n,r}(t)$, the statement of the lemma is equivalent to

$$(5) \qquad \sum_{t_1,\ldots,t_{2q} \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le j_1,\ldots,j_{2q} < n \\ j_1+\cdots+j_{2q} = q(n-1)}} e_n(t_1 j_1 + \cdots + t_{2q} j_{2q}) \right| \le C_q \, n^{2q} (\log n)^{2q-1}.$$

For a positive integer d let $P \subseteq [0,1]^d$ be a polyhedron and let

$$F_n(z_1,\ldots,z_d) = \sum_{(j_1,\ldots,j_d) \in \mathbb{Z}^d \cap (n-1)P} z_1^{j_1} \cdots z_d^{j_d}$$

be a polynomial in $\mathbb{C}[z_1,\ldots,z_d]$. Write

$$S_n = \sum_{s_1,\ldots,s_d \in \mathbb{Z}/n\mathbb{Z}} \left| F_n(e^{2\pi i s_1/n},\ldots,e^{2\pi i s_d/n}) \right|.$$

We shall see at the end of the proof that the left hand side of (5) equals nS_n for a particular choice of the polyhedron P.

The L^1 norm of F_n is defined to be

$$\|F_n\|_1 = \frac{1}{(2\pi)^d} \int_0^{2\pi} \cdots \int_0^{2\pi} \left| F_n(e^{i\theta_1},\ldots,e^{i\theta_d}) \right| d\theta_1 \cdots d\theta_d.$$

It is known (see [38, 9.2.1], for example) that

(6) $$\|F_n\|_1 \le \gamma(P)(\log n)^d,$$

where $\gamma(P)$ depends only on the polyhedron P. We shall find an upper bound for S_n in terms of $\|F_n\|_1$.

Let $f(z)$ be a polynomial in $\mathbb{C}[z]$. By the mean value theorem there exist real numbers $\theta_0, \dots, \theta_{n-1}$ with $\theta_s \in [2\pi s/n, 2\pi(s+1)/n]$ for all s such that

(7) $$\|f\|_1 = \frac{1}{2\pi} \sum_{s=0}^{n-1} \int_{2\pi s/n}^{2\pi(s+1)/n} \left| f(e^{i\theta}) \right| d\theta = \frac{1}{n} \sum_{s=0}^{n-1} \left| f(e^{i\theta_s}) \right|.$$

By the triangle inequality we have

$$\left| \sum_{s=0}^{n-1} \left| f(e^{i\theta_s}) \right| - \sum_{s=0}^{n-1} \left| f(e^{2\pi i s/n}) \right| \right| \le \sum_{s=0}^{n-1} \left| f(e^{i\theta_s}) - f(e^{2\pi i s/n}) \right|$$

$$= \sum_{s=0}^{n-1} \left| \int_{2\pi s/n}^{\theta_s} f'(e^{i\theta}) \, d\theta \right|$$

$$\le \int_0^{2\pi} \left| f'(e^{i\theta}) \right| d\theta$$

(8) $$= 2\pi \|f'\|_1.$$

Now suppose that f has degree at most $n-1$. Then $\|f'\|_1 \le (n-1)\|f\|_1$ by a Bernstein-type inequality (see [3, p. 143] or [40, p. 11], for example). Combination of (7) and (8) then gives

$$\sum_{s=0}^{n-1} \left| f(e^{2\pi i s/n}) \right| \le (1 + 2\pi)n \|f\|_1.$$

Since $F_n(z_1, \dots, z_d)$ has degree at most $n-1$ in each indeterminate, we find by a straightforward induction that

$$S_n \le (1 + 2\pi)^d n^d \|F_n\|_1,$$

and then with (6),

(9) $$S_n \le (1 + 2\pi)^d \gamma(P)(n \log n)^d.$$

Now we take $d = 2q - 1$ and

$$P = \left\{ (x_1, \dots, x_{2q-1}) \in \mathbb{R}^{2q-1} : \begin{array}{l} 0 \le x_1, \dots, x_{2q-1} \le 1, \\ q - 1 \le x_1 + \cdots + x_{2q-1} \le q \end{array} \right\}.$$

Set $j_{2q} = q(n-1) - j_1 - \cdots - j_{2q-1}$ and $s_i = t_i - t_{2q}$ for all $i \in \{1, 2, \dots, 2q-1\}$ in (5) to see that the left hand side of (5) equals

$$\sum_{t_{2q} \in \mathbb{Z}/n\mathbb{Z}} S_n = n S_n,$$

so that the desired inequality (5) follows from (9). $\qquad\square$

4. Fekete polynomials

In this section we prove Theorem 2.5 (and therefore also Theorem 2.1) and Corollary 2.2.

We say that a tuple $(t_1, t_2, \ldots, t_{2q})$ is *even* if there exists a permutation σ of $\{1, 2, \ldots, 2q\}$ such that $t_{\sigma(2k-1)} = t_{\sigma(2k)}$ for all $k \in \{1, 2, \ldots, q\}$. For example, $(2, 1, 1, 3, 2, 3)$ is even, whereas $(2, 1, 1, 3, 1, 3)$ is not even. Let $\mathcal{E}_q(n)$ be the set of even tuples in $(\mathbb{Z}/n\mathbb{Z})^{2q}$.

We begin with the following lemma.

Lemma 4.1. *Let q be a positive integer and let $f_p^r(z)$ be a shifted Fekete polynomial corresponding to the Fekete polynomial of degree $p - 1$. Then*

$$\lim_{p \to \infty} \left(\frac{\|f_p^r\|_{2q}}{\sqrt{p}} \right)^{2q} = \lim_{p \to \infty} \frac{1}{p^{2q}} \sum_{t \in \mathcal{E}_q(p)} h_{p,r}(t),$$

provided that one of the limits exists.

Proof. Let $f_p(z)$ be the Fekete polynomial of degree $p - 1$. For $t \in (\mathbb{Z}/p\mathbb{Z})^{2q}$, let $J_p(t)$ be the indicator function that equals one if t is even and is zero otherwise. From Proposition 3.1 we find that

$$\left(\frac{\|f_p^r\|_{2q}}{\sqrt{p}} \right)^{2q} = \frac{1}{p^{2q}} \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^{2q}} J_p(t) h_{p,r}(t) + \frac{1}{p^{2q}} \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^{2q}} \left(L_{f_p}(t) - J_p(t) \right) h_{p,r}(t).$$

We show that the second sum on the right hand side tends to zero. This will prove the lemma since

$$\sum_{t \in (\mathbb{Z}/p\mathbb{Z})^{2q}} J_p(t) h_{p,r}(t) = \sum_{t \in \mathcal{E}_q(p)} h_{p,r}(t).$$

Notice that $f_p(e_p(k))$ is a quadratic Gauss sum, whose explicit evaluation is [2]

$$f_p(e_p(k)) = i^{(p-1)^2/4} p^{1/2} (k \,|\, p).$$

Therefore

$$L_{f_p}(t_1, \ldots, t_{2q}) = \frac{1}{p} \sum_{m=0}^{p-1} (m + t_1 \,|\, p) \cdots (m + t_{2q} \,|\, p).$$

If $(t_1, \ldots, t_{2q})$ is even, then it is readily verified that

$$1 - q/p \leq L_{f_p}(t_1, \ldots, t_{2q}) \leq 1 - 1/p.$$

On the other hand, if $(t_1, \ldots, t_{2q})$ is not even, then the Weil bound for sums over multiplicative characters [31, Lemma 9.25], [27, Theorem 5.41] gives

$$|L_{f_p}(t_1, \ldots, t_{2q})| \leq (2q - 1) p^{-1/2}.$$

Therefore

$$\left| L_{f_p}(t) - J_p(t) \right| \leq (2q - 1) p^{-1/2} \quad \text{for all } t \in (\mathbb{Z}/p\mathbb{Z})^{2q}.$$

By the triangle inequality we then find that

$$\frac{1}{p^{2q}} \left| \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^{2q}} \left(L_{f_p}(t) - J_p(t) \right) h_{p,r}(t) \right| \leq \frac{2q-1}{p^{2q+1/2}} \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^{2q}} |h_{p,r}(t)|,$$

which tends to zero as $p \to \infty$ by Lemma 3.2, as required. $\square$

In what follows, we shall evaluate the right hand side of the expression in Lemma 4.1.

Let $t = (t_1, t_2, \ldots, t_m)$ be a tuple in $(\mathbb{Z}/n\mathbb{Z})^m$ and let $\pi \in \Pi_m$. We define $t \prec \pi$ to be true if and only if $t_j = t_k$ whenever j and k belong to the same block of π. For example, if $t = (1, 2, 1)$ and $\pi = \{\{1,3\}, \{2\}\}$, then $t \prec \pi$ holds.

Lemma 4.2. *Let $h : \mathcal{E}_q(n) \to \mathbb{C}$ be an arbitrary function and let $T(k)$ be the k-th signed tangent number. Then*

$$(10) \qquad \sum_{t \in \mathcal{E}_q(n)} h(t) = \sum_{\substack{\pi \in \Pi_{2q} \\ \pi \ even}} \sum_{\substack{t \in \mathcal{E}_q(n) \\ t \prec \pi}} h(t) \prod_{B \in \pi} T(\tfrac{1}{2}|B|).$$

To prove the lemma, we shall need the following combinatorial principle (see [36, p. 5], for example), in which $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Lemma 4.3. *Let K be a field of characteristic 0, let $f : \mathbb{N} \to K$ be arbitrary, and define a new function $g : \mathbb{N} \cup \{0\} \to K$ by $g(0) = 1$ and*

$$g(k) = \sum_{\pi \in \Pi_k} \prod_{B \in \pi} f(|B|) \quad for \ k \geq 1.$$

Let $G(z) = \sum_{k \geq 0} g(k) z^k / k!$ and $F(z) = \sum_{k \geq 1} f(k) z^k / k!$ be the corresponding exponential generating functions. Then $G(z) = \exp(F(z))$. Moreover,

$$g(k) = \sum_{j=1}^{k} \binom{k-1}{j-1} f(j) g(k-j) \quad for \ k \geq 1.$$

Proof. The first part of the lemma is a consequence of Faá di Bruno's generalisation of the chain rule (see [26, Theorem 1.3.2], for example), which states that, for a formal power series $E(z)$ and $k \geq 1$, we have

$$(E \circ F)^{(k)}(z) = \sum_{\pi \in \Pi_k} (E^{(|\pi|)} \circ F)(z) \prod_{B \in \pi} F^{(|B|)}(z).$$

Take $E(z) = \exp(z)$ and set $z = 0$ to see that the right hand side equals $g(k)$, which proves the first part. The second part follows from $G'(z) = G(z) F'(z)$ by equating coefficients. $\square$

For a tuple $t \in (\mathbb{Z}/n\mathbb{Z})^m$, let $\pi \in \Pi_m$ be the coarsest partition of $\{1, 2, \ldots, m\}$ with the property $t \prec \pi$ and define $m_k(t)$ to be the number of blocks B in π such that $|B| = k$. For example, if $t = (1, 3, 2, 1, 2)$, then the coarsest partition π with $t \prec \pi$ is $\{\{1,4\}, \{3,5\}, \{2\}\}$ and we have $m_1(t) = 1$, $m_2(t) = 2$, and $m_k(t) = 0$ for $k > 2$.

We now give a proof of Lemma 4.2.

Proof of Lemma 4.2. Taking $F(z) = \log \cosh(z)$ in Lemma 4.3 (so that $G(z) = \cosh(z)$), we find with (3) and $\cosh(z) = \sum_{k \geq 0} z^{2k}/(2k)!$ that

$$(11) \qquad \sum_{\substack{\pi \in \Pi_{2k} \\ \pi \text{ even}}} \prod_{B \in \pi} T(\tfrac{1}{2}|B|) = 1 \quad \text{for each } k \geq 1.$$

Let $s \in \mathcal{E}_q(n)$ be an even tuple. By linearity, it suffices to prove the lemma for the case that $h(x) = 1$ for $x = s$ and $h(x) = 0$ otherwise. Clearly, the left hand side of (10) equals 1. On the other hand, the sum

$$\sum_{\substack{t \in \mathcal{E}_q(n) \\ t \prec \pi}} h(t)$$

is just the indicator function of the event $s \prec \pi$, so we can restrict the outer summation on the right hand side of (10) to the even partitions that are refinements of the coarsest partition $\pi \in \Pi_{2q}$ with the property $s \prec \pi$. Therefore the right hand side of (10) equals

$$\prod_{k=1}^{q} \left(\sum_{\substack{\pi \in \Pi_{2k} \\ \pi \text{ even}}} \prod_{B \in \pi} T(\tfrac{1}{2}|B|) \right)^{m_k(s)},$$

which again equals 1 by (11). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Next we evaluate the inner sums in the right hand side of (10) for $h = h_{n,r}$.

Lemma 4.4. *Let $\pi = \{B_1, \ldots, B_\ell\} \in \Pi_{2q}$ be an even partition with ℓ blocks. Write $N_i = |B_i|/2$ and $P_i = |\{x \in B_i : x > q\}|$. If $r/n \to R$ as $n \to \infty$, then*

$$\lim_{n \to \infty} \frac{1}{n^{2q}} \sum_{\substack{t \in \mathcal{E}_q(n) \\ t \prec \pi}} h_{n,r}(t) = \sum_{\substack{a_1, \ldots, a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = q}} \prod_{i=1}^{\ell} \frac{1}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ 2R(N_i - P_i) + a_i - 1 \end{matrix} \right\rangle.$$

To prove the lemma, we use the following asymptotic counting result, which follows from known results on the number of restricted integer compositions [16], [11] or, alternatively, from integration results over a simplex [18]. By $I[E]$ we denote the indicator function of an event E.

Lemma 4.5. *Let N be a positive integer and let M be real. Let (m_n) be a sequence of integers such that $m_n/n \to M$ as $n \to \infty$. Then*

$$\lim_{n \to \infty} \frac{1}{n^{N-1}} \sum_{0 \leq j_1, \ldots, j_N < n} I\big[j_1 + \cdots + j_N = m_n\big] = \frac{1}{(N-1)!} \left\langle \begin{matrix} N - 1 \\ M - 1 \end{matrix} \right\rangle.$$

Proof. It is well known (see [16, (11)] or [11, Example 33], for example) that

$$\sum_{0 \leq j_1, \ldots, j_N < n} I\big[j_1 + \cdots + j_N = m_n\big] = \sum_{j=0}^{N} (-1)^j \binom{N}{j} \binom{N + m_n - nj - 1}{N - 1}.$$

Since

$$\lim_{n\to\infty} \frac{1}{n^{N-1}} \binom{N+m_n-nj-1}{N-1} = \frac{1}{(N-1)!} \left(\max(0, M-j)\right)^{N-1},$$

the lemma follows from the definition (2) of the generalised Eulerian numbers. □

We now prove Lemma 4.4.

Proof of Lemma 4.4. Put

$$H_n = \sum_{\substack{t\in\mathcal{E}_q(n) \\ t\prec\pi}} h_{n,r}(t).$$

Let $\epsilon_k = -1$ for $k \le q$ and $\epsilon_k = 1$ for $k > q$. Since

$$h_{n,r}(t_1,\ldots,t_{2q}) = \sum_{\substack{0\le j_1,\ldots,j_{2q}<n \\ j_1+\cdots+j_q=j_{q+1}+\cdots+j_{2q}}} \prod_{i=1}^{\ell} \prod_{k\in B_i} e_n(\epsilon_k t_k(j_k+r)),$$

we can rewrite H_n as

$$H_n = \sum_{\substack{0\le j_1,\ldots,j_{2q}<n \\ j_1+\cdots+j_q=j_{q+1}+\cdots+j_{2q}}} \prod_{i=1}^{\ell} \sum_{t\in\mathbb{Z}/n\mathbb{Z}} e_n\left(t\sum_{k\in B_i} \epsilon_k(j_k+r)\right).$$

The product is either zero or equals n^ℓ and is nonzero exactly when there exist $a_1,\ldots,a_\ell \in \mathbb{Z}$ such that

$$(12) \qquad \sum_{k\in B_i} \epsilon_k(j_k+r) = a_i n$$

for all $i \in \{1,\ldots,\ell\}$. Hence

$$H_n = n^\ell \sum_{\substack{0\le j_1,\ldots,j_{2q}<n \\ j_1+\cdots+j_q=j_{q+1}+\cdots+j_{2q}}} \sum_{a_1,\ldots,a_\ell\in\mathbb{Z}} \prod_{i=1}^{\ell} I\left[\sum_{k\in B_i} \epsilon_k(j_k+r) = a_i n\right].$$

Summing both sides of (12) over $i \in \{1,\ldots,\ell\}$ gives

$$\sum_{k=1}^{q}(j_{q+k}-j_k) = n\sum_{i=1}^{\ell} a_i,$$

so that

$$H_n = n^\ell \sum_{\substack{a_1,\ldots,a_\ell\in\mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \sum_{0\le j_1,\ldots,j_{2q}<n} \prod_{i=1}^{\ell} I\left[\sum_{k\in B_i} \epsilon_k(j_k+r) = a_i n\right].$$

The i-th factor within the inner sum depends only on $|B_i| = 2N_i$ of the summation variables in the inner sum, so that we can factor the inner sum as follows

$$\prod_{i=1}^{\ell} \sum_{0 \leq j_1,\ldots,j_{2N_i}<n} I\left[\sum_{k=1}^{P_i}(j_k + r) - \sum_{k=P_i+1}^{2N_i}(j_k + r) = a_i n\right].$$

Replace j_k by $n - 1 - j_k$ for $k \in \{P_i + 1, \ldots, 2N_i\}$ to see that this expression equals

$$\prod_{i=1}^{\ell} \sum_{0 \leq j_1,\ldots,j_{2N_i}<n} I\left[\sum_{k=1}^{2N_i} j_k = (2N_i - P_i)(n - 1) + 2r(N_i - P_i) + a_i n\right].$$

Since $\sum_{i=1}^{\ell}(2N_i - 1) = 2q - \ell$, we find from Lemma 4.5 that

$$\lim_{n\to\infty} \frac{H_n}{n^{2q}} = \sum_{\substack{a_1,\ldots,a_\ell\in\mathbb{Z}\\a_1+\cdots+a_\ell=0}} \prod_{i=1}^{\ell} \frac{1}{(2N_i - 1)!}\left\langle\begin{matrix}2N_i - 1\\2N_i - P_i + 2R(N_i - P_i) + a_i - 1\end{matrix}\right\rangle,$$

since the outer sum is locally finite. The lemma follows after re-indexing and using $\sum_{i=1}^{\ell}(2N_i - P_i) = q$. □

Theorem 2.5 and therefore Theorem 2.1 now follows from Lemmas 4.1, 4.2, and 4.4. It remains to show how to deduce Corollary 2.2 from Theorem 2.1. To do so, write

$$(13) \qquad A_N(x) = \sum_{a=1}^{2N-1}\left\langle\begin{matrix}2N - 1\\a - 1\end{matrix}\right\rangle x^a,$$

which is known (after dividing by x) as an *Eulerian polynomial*. Letting $N_1,\ldots,N_\ell$ be positive integers such that $N_1 + \cdots + N_\ell = k$, we have

$$\prod_{i=1}^{\ell} A_{N_i}(x) = \sum_{m=\ell}^{2k-\ell} x^m \sum_{\substack{a_1,\ldots,a_\ell\in\mathbb{Z}\\a_1+\cdots+a_\ell=m}} \prod_{i=1}^{\ell}\left\langle\begin{matrix}2N_i - 1\\a_i - 1\end{matrix}\right\rangle.$$

Define polynomials $F_k(x)$ by $F_k(x) = 0$ for odd k, $F_0(x) = 1$, and

$$(14) \qquad F_{2k}(x) = \sum_{\substack{\pi\in\Pi_{2k}\\\pi \text{ even}}} \prod_{i=1}^{\ell} \frac{T(N_i)\,A_{N_i}(x)}{(2N_i - 1)!} \quad \text{for } k \geq 1,$$

where $\pi = \{B_1,\ldots,B_\ell\}$ and $N_i = |B_i|/2$. Then $F_{2k}(x)$ is a polynomial of degree $2k - 1$ with $F_{2k}(0) = 0$ for $k \geq 1$, so we can write

$$F_{2k}(x) = \sum_{m=1}^{2k-1} F(k, m)\, x^m \quad \text{for } k \geq 1.$$

It is readily verified that Theorem 2.1 is equivalent to

$$\lim_{p \to \infty} \left(\frac{\|f_p\|_{2q}}{\sqrt{p}} \right)^{2q} = F(q, q).$$

It remains to show that the numbers $F(k, m)$ are the same as those given in Corollary 2.2. Use $F_0(x) = 1$ and apply Lemma 4.3 to (14) to find that

$$F_{2k}(x) = \sum_{j=1}^{k} \binom{2k-1}{2j-1} \frac{T(j)A_j(x)}{(2j-1)!} F_{2k-2j}(x) \quad \text{for } k \geq 1.$$

With $F(0, 0) = 1$ (which equals $F_0(x)$), this is equivalent to the recursive definition of the numbers $F(k, m)$ given in Corollary 2.2.

5. GALOIS POLYNOMIALS

In this section we prove Theorem 2.3 and Corollary 2.4. We use the following notation throughout this section. A tuple $(t_1, t_2, \ldots, t_{2q})$ is an *abelian square* if there exists a permutation σ of $\{1, 2, \ldots, q\}$ such that $t_{\sigma(k)} = t_{q+k}$ for all $k \in \{1, 2, \ldots, q\}$, so that the second half of the tuple is a permutation of the first half. Let $\mathcal{A}_q(n)$ be the set of abelian squares in $(\mathbb{Z}/n\mathbb{Z})^{2q}$.

Lemma 5.1. *Let q be a positive integer and let $g_n(z)$ be a Galois polynomial of degree $n - 1$. Then*

$$\lim_{n \to \infty} \left(\frac{\|g_n\|_{2q}}{\sqrt{n}} \right)^{2q} = \lim_{n \to \infty} \frac{1}{n^{2q}} \sum_{t \in \mathcal{A}_q(n)} h_{n,0}(t),$$

provided that one of the limits exists.

Proof. For $t \in (\mathbb{Z}/n\mathbb{Z})^{2q}$, let $J_n(t)$ be the indicator function that equals one if t is an abelian square and is zero otherwise. From Proposition 3.1 we find that

$$\left(\frac{\|g_n\|_{2q}}{\sqrt{n}} \right)^{2q} = \frac{1}{n^{2q}} \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} J_n(t) h_{n,0}(t) + \frac{1}{n^{2q}} \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} (L_{g_n}(t) - J_n(t)) h_{n,0}(t).$$

We show that the second expression on the right hand side tends to zero, which will prove the lemma. Write $s = n + 1$, so that s is a power of two. By definition, a Galois polynomial of degree $n - 1$ can be written as

$$g_n(z) = \sum_{j=0}^{n-1} \psi(\theta^j) z^j,$$

where ψ is an additive character of $\mathbb{F}_s$ and θ is a primitive element of $\mathbb{F}_s$. For a multiplicative character ξ of $\mathbb{F}_s$, we define the Gauss sum

$$G(\xi) = \sum_{x \in \mathbb{F}_s^*} \psi(x)\xi(x).$$

Letting χ be the multiplicative character of $\mathbb{F}_s$ given by $\chi(\theta) = e_n(1)$, we see that $g_n(e_n(k)) = G(\chi^k)$ for all $k \in \mathbb{Z}/n\mathbb{Z}$. Therefore

$$L_{g_n}(t_1, \ldots, t_{2q}) = \frac{1}{n^{q+1}} \sum_{m \in \mathbb{Z}/n\mathbb{Z}} \prod_{k=1}^{q} G(\chi^{m+t_k}) \overline{G(\chi^{m+t_{q+k}})}.$$

Since $|G(\xi)|^2$ equals 1 if ξ is trivial and equals $n+1$ otherwise, we find that $|L_{g_n}(t_1, \ldots, t_{2q}) - 1| = O(n^{-1})$ if $(t_1, \ldots, t_{2q})$ is an abelian square. On the other hand, if $(t_1, \ldots, t_{2q})$ is not an abelian square, then a result due to Katz [25, pp. 161–162] shows that

$$|L_{g_n}(t_1, \ldots, t_{2q})| \leq \frac{q}{n^{q+1}} (n+1)^{q+1/2}.$$

Therefore, by the triangle inequality,

$$\frac{1}{n^{2q}} \left| \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} (L_{g_n}(t) - J_n(t)) h_{n,0}(t) \right| = O(n^{-2q-1/2}) \sum_{t \in (\mathbb{Z}/n\mathbb{Z})^{2q}} |h_{n,0}(t)|,$$

which tends to zero as $n \to \infty$ by Lemma 3.2, as required. $\qquad\square$

We proceed similarly as for Fekete polynomials and seek an asymptotic evaluation of the right hand side of the expression in Lemma 5.1.

The following lemma is an analogue of Lemma 4.2.

Lemma 5.2. *Let $h : \mathcal{A}_q(n) \to \mathbb{C}$ be a function that depends only on the first q entries of its input and let $C(k)$ be the k-th signed Carlitz number. Then*

$$(15) \qquad \sum_{t \in \mathcal{A}_q(n)} h(t) = q! \sum_{\pi \in \Pi_q} \sum_{\substack{u \in (\mathbb{Z}/n\mathbb{Z})^q \\ u \prec \pi}} h(u|u) \prod_{B \in \pi} \frac{C(|B|)}{|B|!},$$

where $u|u$ is the $(2q)$-tuple with the first and the second half equal to u.

Proof. Take $F(z) = \log J_0(2\sqrt{z})$ in Lemma 4.3, so that $G(z)$ equals

$$J_0(2\sqrt{z}) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(k!)^2} z^k.$$

Use (4) to find from Lemma 4.3 that

$$\sum_{\pi \in \Pi_k} \prod_{B \in \pi} \frac{(-1)^{|B|} C(|B|)}{|B|!} = \frac{(-1)^k}{k!} \quad \text{for each } k \geq 1,$$

or equivalently

$$(16) \qquad \sum_{\pi \in \Pi_k} \prod_{B \in \pi} \frac{C(|B|)}{|B|!} = \frac{1}{k!} \quad \text{for each } k \geq 1.$$

Now let $v \in (\mathbb{Z}/n\mathbb{Z})^q$ and let V be the set of abelian squares in $(\mathbb{Z}/n\mathbb{Z})^{2q}$ whose first q entries equal those of v. By linearity, it suffices to prove the

lemma for the case that $h(x) = 1$ for $x \in V$ and $h(x) = 0$ otherwise. Then the left hand side of (15) equals

$$(17) \qquad |V| = \frac{q!}{\prod_{k=1}^{q}(k!)^{m_k(v)}}$$

(where $m_k(v)$ was defined before the proof of Lemma 4.2). On the other hand, the right hand side of (15) equals

$$q! \prod_{k=1}^{q}\left(\sum_{\pi \in \Pi_k}\prod_{B \in \pi}\frac{C(|B|)}{|B|!}\right)^{m_k(v)},$$

which by (16) equals (17) again. $\qquad \square$

Next we evaluate the inner sums in the right hand side of (15) for $h = h_{n,0}$.

Lemma 5.3. *Let* $\pi = \{B_1, \ldots, B_\ell\} \in \Pi_q$ *be a partition with* ℓ *blocks and write* $N_i = |B_i|$. *Then*

$$\lim_{n \to \infty}\frac{1}{n^{2q}}\sum_{\substack{u \in (\mathbb{Z}/n\mathbb{Z})^q \\ u \prec \pi}}h_{n,0}(u|u) = \sum_{\substack{a_1,\ldots,a_\ell \in \mathbb{Z} \\ a_1+\cdots+a_\ell=q}}\prod_{i=1}^{\ell}\frac{1}{(2N_i-1)!}\left\langle\begin{matrix}2N_i-1 \\ a_i-1\end{matrix}\right\rangle,$$

where $u|u$ *is the* $(2q)$-*tuple with the first and the second half equal to* u.

Proof. The proof is similar to that of Lemma 4.4, and so is presented in slightly less detail. Put

$$H_n = \sum_{\substack{u \in (\mathbb{Z}/n\mathbb{Z})^q \\ u \prec \pi}}h_{n,0}(u|u),$$

which we can rewrite as

$$H_n = \sum_{\substack{0 \leq j_1,\ldots,j_{2q}<n \\ j_1+\cdots+j_q=j_{q+1}+\cdots+j_{2q}}}\prod_{i=1}^{\ell}\sum_{u \in \mathbb{Z}/n\mathbb{Z}}e_n\left(u\sum_{k \in B_i}(j_{q+k}-j_k)\right).$$

The product is either zero or equals n^ℓ and is nonzero exactly when there exist $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that

$$(18) \qquad \sum_{k \in B_i}(j_{q+k}-j_k) = a_i n$$

for all $i \in \{1, \ldots, \ell\}$. Hence

$$H_n = n^\ell\sum_{\substack{0 \leq j_1,\ldots,j_{2q}<n \\ j_1+\cdots+j_q=j_{q+1}+\cdots+j_{2q}}}\sum_{a_1,\ldots,a_\ell \in \mathbb{Z}}\prod_{i=1}^{\ell}I\left[\sum_{k \in B_i}(j_{q+k}-j_k) = a_i n\right].$$

Summing both sides of (18) over $i \in \{1, \ldots, \ell\}$ gives

$$\sum_{k=1}^{q} (j_{q+k} - j_k) = n \sum_{i=1}^{\ell} a_i,$$

so that

$$H_n = n^\ell \sum_{\substack{a_1, \ldots, a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = 0}} \sum_{0 \leq j_1, \ldots, j_{2q} < n} \prod_{i=1}^{\ell} I\left[\sum_{k \in B_i} (j_{q+k} - j_k) = a_i n \right]$$

or equivalently

$$H_n = n^\ell \sum_{\substack{a_1, \ldots, a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = 0}} \sum_{0 \leq j_1, \ldots, j_{2q} < n} \prod_{i=1}^{\ell} I\left[\sum_{k \in B_i} (j_{q+k} + j_k) = a_i n + N_i(n-1) \right].$$

We can factor the inner sum as follows

$$\prod_{i=1}^{\ell} \sum_{0 \leq j_1, \ldots, j_{2N_i} < n} I\left[\sum_{k=1}^{2N_i} j_k = a_i n + N_i(n-1) \right].$$

Since $\sum_{i=1}^{\ell} (2N_i - 1) = 2q - \ell$, we find from Lemma 4.5 that

$$\lim_{n \to \infty} \frac{H_n}{n^{2q}} = \sum_{\substack{a_1, \ldots, a_\ell \in \mathbb{Z} \\ a_1 + \cdots + a_\ell = 0}} \prod_{i=1}^{\ell} \frac{1}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ N_i + a_i - 1 \end{matrix} \right\rangle,$$

since the outer sum is locally finite. The lemma follows after re-indexing the summation. $\qquad\square$

Theorem 2.3 now follows from Lemmas 5.1, 5.2, and 5.3, upon noting that $h_{n,0}$ has the required property in Lemma 5.2.

Next we deduce Corollary 2.4 from Theorem 2.3. This is again broadly similar to the proof of Corollary 2.2. Recall the definition of the Eulerian polynomials $A_N(x)$ from (13) and define polynomials $G_k(x)$ by $G_0(x) = 1$, and

$$(19) \qquad \frac{G_k(x)}{k!} = \sum_{\pi \in \Pi_k} \prod_{i=1}^{\ell} \frac{C(N_i) \, A_{N_i}(x)}{(2N_i - 1)! N_i!} \quad \text{for } k \geq 1,$$

where $\pi = \{B_1, \ldots, B_\ell\}$ and $N_i = |B_i|$. Then $G_k(x)$ is a polynomial of degree $2k - 1$ with $G_k(0) = 0$ for $k \geq 1$, so we can write

$$G_k(x) = \sum_{m=1}^{2k-1} G(k, m) \, x^m \quad \text{for } k \geq 1.$$

It is readily verified that Theorem 2.3 is equivalent to

$$\lim_{n \to \infty} \left(\frac{\|g_n\|_{2q}}{\sqrt{n}} \right)^{2q} = G(q, q).$$

It remains to show that the numbers $G(k, m)$ are the same as those given in Corollary 2.4. Use $G_0(x) = 1$ and apply Lemma 4.3 to (19) to find that

$$\frac{G_k(x)}{k!} = \sum_{j=1}^{k} \binom{k-1}{j-1} \frac{C(j)A_j(x)}{(2j-1)!\,j!} \frac{G_{k-j}(x)}{(k-j)!} \quad \text{for } k \geq 1,$$

or equivalently

$$G_k(x) = \sum_{j=1}^{k} \binom{k}{j}\binom{k-1}{j-1} \frac{C(j)A_j(x)}{(2j-1)!} G_{k-j}(x) \quad \text{for } k \geq 1.$$

With $G(0,0) = 1$ (which equals $G_0(x)$), this is equivalent to the recursive definition of the numbers $G(k, m)$ given in Corollary 2.4.

References

[1] The On-Line Encyclopedia of Integer Sequences, 2010. published electronically at http://oeis.org.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums.* John Wiley & Sons, Inc., New York, 1998.

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

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

[5] P. Borwein, K.-K. S. Choi, and S. Yazdani. An extremal property of Fekete polynomials. *Proc. Amer. Math. Soc.*, 129(1):19–27, 2001.

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

[7] L. Carlitz. A sequence of integers related to the Bessel functions. *Proc. Amer. Math. Soc.*, 14:1–9, 1963.

[8] S. Choi and T. Erdélyi. Average Mahler's measure and L_p norms of Littlewood polynomials. *Proc. Amer. Math. Soc. Ser. B*, 1:105–120, 2014.

[9] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan. Zeros of Fekete polynomials. *Ann. Inst. Fourier (Grenoble)*, 50(3):865–889, 2000.

[10] C. Doche and L. Habsieger. Moments of the Rudin-Shapiro polynomials. *J. Fourier Anal. Appl.*, 10(5):497–505, 2004.

[11] S. Eger. Restricted weighted integer compositions and extended binomial coefficients. *J. Integer Seq.*, 16(1):Article 13.1.3, 25, 2013.

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

[13] T. Erdélyi. Upper bounds for the L_q norm of Fekete polynomials on subarcs. *Acta Arith.*, 153(1):81–91, 2012.

[14] P. Erdős. Some old and new problems in approximation theory: research problems 95-1. *Constr. Approx.*, 11(3):419–421, 1995.

[15] M. Fekete and G. Pólya. Über ein Problem von Laguerre. *Rend. Circ. Mat. Palermo*, 34(1):89–120, 1912.

[16] D. C. Fielder and C. O. Alford. Pascal's triangle: top gun or just one of the gang? In *Applications of Fibonacci numbers, Vol. 4 (Winston-Salem, NC, 1990)*, pages 77–90. Kluwer Acad. Publ., Dordrecht, 1991.

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

[18] I. J. Good and T. N. Tideman. Integration over a simplex, truncated cubes, and Eulerian numbers. *Numer. Math.*, 30(4):355–367, 1978.

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

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

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

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

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

[24] D. J. Katz. Asymptotic L^4 norm of polynomials derived from characters. *Pacific J. Math.*, 263(2):373–398, 2013.

[25] N. M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[26] S. G. Krantz and H. R. Parks. *A primer of real analytic functions*. Birkhäuser Boston, Inc., Boston, MA, second edition, 2002.

[27] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2nd edition, 1997.

[28] J. E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$. *J. London Math. Soc.*, 41(1):367–376, 1966.

[29] J. E. Littlewood. *Some Problems in Real and Complex Analysis*. Heath Mathematical Monographs. D. C. Heath and Company, Lexington, MA, 1968.

[30] H. L. Montgomery. An exponential polynomial formed with the Legendre symbol. *Acta Arith.*, 37:375–380, 1980.

[31] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

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

[33] T. K. Petersen. *Eulerian numbers*. Birkhäuser Advanced Texts. Springer, New York, 2015.

[34] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.

[35] H. S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, MIT, 1951.

[36] R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999.

[37] M. Taghavi and H. K. Azadi. Some new results on the Rudin-Shapiro polynomials. *J. Appl. Math. Inform.*, 26(3-4):583–590, 2008.

[38] R. M. Trigub and E. S. Bellinsky. *Fourier analysis and approximation of functions*. Kluwer Academic Publishers, Dordrecht, 2004.

[39] R.-H. Wang, Y. Xu, and Z.-Q. Xu. Eulerian numbers: a spline perspective. *J. Math. Anal. Appl.*, 370(2):486–490, 2010.

[40] A. Zygmund. *Trigonometric series. Vol. II*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, third edition, 2002.

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany.

E-mail address, Ch. Günther: `chriguen@math.upb.de`

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany.

E-mail address, K.-U. Schmidt: `kus@math.upb.de`