Canad. J. Math. Vol. **67** (3), 2015 pp. 507–526
http://dx.doi.org/10.4153/CJM-2014-007-1

On Littlewood Polynomials with Prescribed Number of Zeros Inside the Unit Disk

Peter Borwein, Stephen Choi, Ron Ferguson, and Jonas Jankauskas

Abstract. We investigate the numbers of complex zeros of Littlewood polynomials $p(z)$ (polynomials with coefficients $\{-1, 1\}$) inside or on the unit circle $|z| = 1$, denoted by $N(p)$ and $U(p)$, respectively. Two types of Littlewood polynomials are considered: Littlewood polynomials with one sign change in the sequence of coefficients and Littlewood polynomials with one negative coefficient. We obtain explicit formulas for $N(p)$, $U(p)$ for polynomials $p(z)$ of these types. We show that if $n + 1$ is a prime number, then for each integer k, $0 \leqslant k \leqslant n - 1$, there exists a Littlewood polynomial $p(z)$ of degree n with $N(p) = k$ and $U(p) = 0$. Furthermore, we describe some cases where the ratios $N(p)/n$ and $U(p)/n$ have limits as $n \to \infty$ and find the corresponding limit values.

1 Introduction

Recall that a polynomial

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad a_j \in \{-1, 1\}, 0 \leqslant j \leqslant n$$

is called *Littlewood polynomial*. Such polynomials are named in honor of J. E. Littlewood [14–18] who studied various analytic properties (the mean value, the number of zeros, etc.) of polynomials and power series with restricted coefficients on the complex unit circle $|z| = 1$.

As usual, $p^*(z)$ denotes the reciprocal of $p(z)$; that is, $p^*(z) := z^{\deg p} p(1/z)$ for any polynomial $p(z) \in \mathbb{R}[z]$ (not necessary a Littlewood). Polynomial $p(z)$ is called *self-reciprocal* if $p^*(z) = \pm p(z)$. If $p^*(-z) = \pm p(z)$, then $p(z)$ is called *skew-symmetric*.

The study of complex zeros of Littlewood polynomials and $\{-1, 0, 1\}$ polynomials is an old subject. It was started by Bloch and Pólya [2] who proved that such polynomials, on average, have at most $O(\sqrt{n})$ roots on the real line $\mathbb{R}$. Later, Schur [23] and Szegő [24] proved an upper bound of the magnitude $O(\sqrt{n \log n})$ for the number of real roots. Nowadays this result is usually derived as a consequence of the theorem of Erdős and Turán [11] on the angular equidistribution of roots. More recently, it was shown that any polygon with vertices on the unit circle $|z| = 1$ contains at most $O(\sqrt{n})$ zeros of such polynomials [4], while any disk with the center on the unit circle $|z| = 1$ and the radius at least $33\pi \log n/\sqrt{n}$ contains at least $8\sqrt{n} \log n$ zeros of $p(z)$ [7].

Received by the editors November 27, 2013.
Published electronically April 5, 2014.
The first and second authors were supported by NSERC. The research of J. Jankauskas was supported by the Research Council of Lithuania grant No. MIP-068/2013/LSS-110000-740.
AMS subject classification: **11R06**, 11R09, 11C08.
Keywords: Littlewood polynomials, zeros, complex roots.

For any polynomial $p(z) \in \mathbb{C}[z]$, let $N(p)$ denote the the number of complex zeros of $p(z)$ inside the open unit disk $|z| < 1$, counted with multiplicities. In a similar way, let $U(p)$ denote the number of zeros of $p(z)$ on the unit circle $|z| = 1$ (again, counting with multiplicities). Such zeros of the absolute value $|z| = 1$ are called *unimodular*. In this paper, we consider two problems on the possible values of $N(p)$ and $U(p)$ for Littlewood polynomials $p(z)$.

Problem 1.1 *Let (n, k) be a pair of integers such that $1 \leqslant k \leqslant n-1$. For such a pair, does there always exist a Littlewood polynomial $p(z)$ of degree n with precisely k roots inside the unit disk and no unimodular roots, that is, $N(p) = k$, $U(p) = 0$?*

The values $k \in \{0, n\}$ are not included in Problem 1.1, since the answer is trivial in these cases. For a Littlewood polynomial $p(z)$, the product of absolute values of its roots is 1; hence, $p(z)$ always has at least one zero $|z| \geqslant 1$, and $N(p) = n$ is impossible. Another extreme case is $k = 0$. In this situation, $p(z)$ cannot have zeros of absolute value $|z| < 1$, so it also cannot have any zero of absolute value $|z| > 1$. Hence, all zeros of $p(z)$ must be unimodular, $U(p) = n$, so the answer to Problem 1.1 is negative again. By the theorem of Kronecker [13], Littlewood polynomials $p(z)$ with $U(p) = n$ are precisely products of cyclotomic polynomials and are described in [1,3].

For k between 1 and $n-1$, Problem 1.1 is no longer trivial. If $k = n-1$, then $p(z)$ must have precisely one zero of modulus $|z| > 1$. Polynomials $p(z)$ with this property are called *Littlewood Pisot polynomials*. Mukunda [21] proved that all such polynomials are of the form $\pm p(\pm z)$, where

$$p(z) = z^n - z^{n-1} - \cdots - z - 1.$$

Hence, the answer to Problem 1.1 in case $k = n-1$ is positive. By taking a reciprocal of a Littlewood Pisot polynomial, one also obtains a positive answer for $k = 1$. If the degree n is even, then the result of Mercer [19] on non-vanishing of skew-symmetric Littlewood polynomials on the unit circle provides a positive answer in case $k = n/2$, since a skew-symmetric polynomial has the same number of zeros inside the disk $|z| < 1$ as it has outside it. Apart from cases $k \in \{0, 1, n/2, n-1, n\}$ not much of Problem 1.1 is known, as there is no simple formula to compute $N(p)$ for any Littlewood polynomial $p(z)$. Since $p^*(z)$ is a Littlewood polynomial if $p(z)$ is Littlewood, one might guess that, on average, $N(p) \sim n/2$, as $n \to \infty$ if we make a reasonable assumption that the proportion of polynomials with unimodular roots is negligible among 2^{n+1} Littlewood polynomials of degree n.

Why is the condition $U(p) = 0$ (no unimodular roots) included in Problem 1.1? If $p(z)$ has unimodular roots, then the problem becomes extremely complicated. It is natural to expect that the majority of Littlewood polynomials with unimodular roots are irreducible for large n, hence they must be self-reciprocal. It is known that each self-reciprocal $\{-1, 0, 1\}$ polynomial has at least one unimodular root; see [6,12,19]. For self-reciprocal Littlewood polynomials $p(z)$, Mukunda proved that $U(p) \geqslant 3$ in the case where n is odd. Later, Drungilas [10] improved this to $U(p) \geqslant 4$ for $n \geqslant 14$ if n is even, $U(p) \geqslant 5$ for $n \geqslant 7$ if n is odd. If $p(z)$ is the n-th Fekete polynomial whose coefficients are $\left(\frac{j}{n}\right)$, the Legendre symbol modulo n, where n is an odd prime, then $U(p) \sim \kappa_0 n$ as $n \to \infty$. Here κ_0 is some constant lying in the interval $(0.500668, 0.500813)$, as it was established by Conrey, Granville, Poonen, and Soundararajan [9]. The question of whether the minimal number of unimodular roots of self-reciprocal $\{-1, 0, 1\}$ polynomial tends to infinity as the number of terms increases was posed in [6,7]. A partial answer to this question was obtained in [5].

One intuitive way of producing a Littlewood polynomial $p(z)$ with prescribed number $N(p) = k$ is to take a polynomial of degree n with all coefficients 1 (a geometric progression in z) and then change the signs of some coefficients. This technique was pioneered by Mossinghoff, Pinner, and Vaaler in their search of integer polynomials with small Mahler measures; see [20]. They considered the perturbation of a middle coefficient for polynomials $p(z)$ that are the products of cyclotomic polynomials (not necessary $p(z)$ being Littlewood polynomial). We also exploit this strategy. In connection with this approach, we pose the second problem.

Problem 1.2 *Suppose that $p(z)$ is a Littlewood polynomial of degree n with all roots of modulus $|z| = 1$. If the sign of the coefficient of the term z^k, where $0 \leqslant k \leqslant n$, is changed, how do the numbers $N(p)$ and $U(p)$ change?*

Two possible *measures of sensitivity* to perturbations are

$$\left|\frac{N(p)}{n} - \frac{1}{2}\right| \quad \text{or} \quad 1 - \frac{U(p)}{n},$$

for the perturbed polynomial $p(z)$. They measure the asymmetry between number of roots of modulus $|z| > 1$ and $|z| < 1$ and the number of unimodular roots lost after the perturbation.

In this paper, we attempt to give partial answers to Problems 1.1 and 1.2 for Littlewood polynomials of a simple shape. The main results are formulated as theorems in the Section 2. In our proofs, we will repeatedly use the method of Boyd [8] to count zeros of polynomials. Also, we will need some basic properties of the Dirichlet kernel $D_k(t)$. For the convenience of a reader, all results that are needed in the proofs are formulated in Section 3. Proofs of the main theorems are postponed to Section 4.

2 Main Results

2.1 Littlewood Polynomials with One Sign Change

We start with the existence of Littlewood polynomials with prescribed number of roots inside the open unit disk.

Theorem 2.1 *Suppose that n and k are two positive integers $1 \leqslant k \leqslant n-1$. We assume that*

$$\gcd(k, n+1) = 1, \quad \textit{if } n > 2k,$$

and

$$\gcd(k+1, n+1) = 1, \quad \textit{if } n < 2k.$$

Then there exists Littlewood polynomial $p(z)$ of degree n, such that $N(p) = k$ and $U(p) = 0$.

We have the following corollary.

Corollary 2.2 *Let $n+1$ be an odd prime. Then, for any k in the range $1 \leqslant k \leqslant n-1$, there exists a Littlewood polynomial $p(z)$ of degree n with $N(p) = k$ and $U(p) = 0$.*

For $n = 12$, $n+1 = 13$ is prime. Hence, it is possible to find Littlewood polynomials $p(z)$ of degree 12 with $k = 1, 2, 3, \dots, 11$, roots inside the unit disk. For $n = 11$, $n+1 = 12$ and Theorem 2.1 works in cases $k = 1, 5, 6, 10$; however, it says nothing for $k = 2, 3, 4, 7, 8, 9$. The conditions on $n+1$, k and $k+1$ being co-prime are simply the artifacts of the construction we use (as $p(z)$ vanish at roots of unity in certain cases). We hope these restrictions can be removed.

In order to prove Theorem 2.1, we will consider Littlewood polynomials with one sign change in the coefficient sequence. Up to the $\pm$ sign, they take the form

$$p(z) = z^n + z^{n-1} + \cdots + z^k \underbrace{- z^{k-1} - \cdots - z - 1}_{k \text{ negative terms}}, \tag{2.1}$$

for some integers $n \geqslant k \geqslant 1$. Alternatively, one can write these polynomials as a difference of two geometric progressions

$$p(z) = \frac{z^{n+1} - 1}{z - 1} - 2 \cdot \frac{z^k - 1}{z - 1} = \frac{z^{n+1} - 2z^k + 1}{z - 1}. \tag{2.2}$$

For $k = n - 1$, they are exactly the Littlewood Pisot polynomials considered by Mukunda [21, 22]. Theorem 2.1 is a consequence of a general formula for the numbers of roots $N(p)$ and $U(p)$ for polynomials $p(z)$ in (2.1).

Theorem 2.3 *Let $n \geqslant k$ be positive integers with $\gcd(k, n+1) = d$. A Littlewood polynomial $p(z)$ of degree n with one sign change (which occurs between terms z^k and z^{k-1}) has*

$$N(p) = \begin{cases} k & \text{if } n > 2k - 1, \\ 0 & \text{if } n = 2k - 1, \\ k - d & \text{if } n < 2k - 1, \end{cases}$$

and

$$U(p) = \begin{cases} d - 1 & \text{if } n \neq 2k - 1, \\ n & \text{if } n = 2k - 1, \end{cases}$$

roots inside and on the unit circle $|z| = 1$, respectively.

Theorems 2.1 and 2.3 provide a partial answer to Problem 1.1.

2.2 Littlewood Polynomials with One Negative Term

Now we turn to Problem 1.2. We start with a Littlewood polynomial of degree $n \geqslant 2$ with all coefficients equal to 1 (it is a geometric progression). We pick one term (say, z^k, $0 \leqslant k \leqslant n$) and make its coefficient negative. The polynomial we obtain takes the form

$$p(z) = z^n + \cdots + z^{k+1} - z^k + z^{k-1} + \cdots + 1 = \frac{z^{n+1}-1}{z-1} - 2z^k. \tag{2.3}$$

The zeros of the initial polynomial are $(n+1)$-th roots of unity, except $z = 1$. Our goal is to calculate the numbers $N(p)$ and $U(p)$ for the perturbed polynomial $p(z)$ and investigate the behavior of $N(p)$ as a function of n and k. The analysis breaks into two cases.

- Case 1: $p(z) = p^*(z)$. This occurs if and only if $n = 2k$ (that is, the central term is negative).
- Case 2: $p(z) \neq p^*(z)$. This occurs if and only if $n \neq 2k$. The analysis breaks down into two sub-cases:
  (a) $p(z)$ has no unimodular roots on the unit circle;
  (b) $p(z)$ has some unimodular roots on the unit circle.

Here is the result for Case 1 polynomials.

Theorem 2.4 *Let $p(z)$ be a self-reciprocal Littlewood polynomial of degree $n \geqslant 2$ with one negative coefficient. Then $p(z)$ has*

$$U(p) = 4\left\lfloor \frac{n-2}{12} \right\rfloor + 2$$

unimodular roots,

$$N(p) = \frac{n}{2} - 2\left\lfloor \frac{n-2}{12} \right\rfloor - 1$$

roots inside the unit disk and the same number of roots outside the unit disk. All roots of $p(z)$ have multiplicity 1. In particular, both $U(p)$ and $N(p) \sim n/3$, as $n \to \infty$.

We see that roots of geometric progression polynomials are sensitive to changing the sign of the central coefficient. Roughly $1/3$ of all roots of $p(z)$ move inside the unit disk, $1/3$ outside the unit disk; the total loss (as introduced in Section 1) is $2/3$.

Now we turn to Littlewood polynomials in Case 2. Cases 2(a) and 2(b) can be distinguished by the following proposition.

Proposition 2.5 *A nonself-reciprocal Littlewood polynomial $p(z)$ of Case 2 in (2.3) belongs to Case 2(b), if $n \equiv 2 \pmod 6$ and $k \equiv 1 \pmod 6$. Otherwise, $p(z)$ is as in Case 2(a).*

For Case 2 polynomials, the behavior of $N(p)$ as n and k varies is much more complicated. Our findings can be described as follows:

- Geometric progression polynomials are rather insensitive to perturbations close to the central term (but not for the perturbation of a central term itself). If the distance from the central term to the position of the negative term grows slower than the degree n as $n \to \infty$, then $N(p)$ behaves very nicely.
- If the position of the negative term (the number k) is fixed and n goes to ∞, then the ratio $N(p)/n$ has a limit. Asymptotic formulas can be found in this case, even if the limits are not easy to evaluate. We conclude that the geometric progression

polynomials are sensitive to the perturbations close to the leading term or the constant term.

We will formulate these results in a quantitative form. We start with polynomials in Case 2(a).

Theorem 2.6 *Let the polynomial $p(z)$ be as in Case 2(a) and $l = |n - 2k|$.*

If $n > 2k$, then

$$k + 1 \leqslant N(p) \leqslant k + 2\left\lceil \frac{n - 2k}{6} \right\rceil - 1,$$

where $\lceil x \rceil$ is the ceiling function of x. The lower bound is attained when $k \equiv 0 \pmod{l}$, and the upper bound is attained when $k \equiv 1 \pmod{l}$.

If $n < 2k$, then

$$k - 2\left\lceil \frac{2k - n}{6} \right\rceil + 1 \leqslant N(p) \leqslant k - 1.$$

The lower bound is attained when $k \equiv 1 \pmod{l}$ and the upper bound is attained when $k \equiv 0 \pmod{l}$.

Here is the corresponding result for polynomials in Case 2(b).

Theorem 2.7 *Let the polynomial $p(z)$ be as in Case 2(b) and $l = |n - 2k|$.*

If $n > 2k$, then

$$k + 1 \leqslant N(p) \leqslant \frac{n + k}{3} - 1.$$

The lower bound is attained when $k \equiv 0 \pmod{l}$, and the upper bound is attained when $k \equiv 1 \pmod{l}$.

If $n < 2k$, then

$$\frac{n + k}{3} - 1 \leqslant N(p) \leqslant k - 3.$$

The lower bound is attained when $k \equiv 1 \pmod{l}$, and the upper bound is attained when $k \equiv 0 \pmod{l}$.

We describe a situation when the negative term occurs close to the middle term.

Corollary 2.8 *Let $p(z)$ be in Case 2. We have the following:*

(i) *If $\lim_{n\to\infty} k/n = 1/2$, then $\lim_{n\to\infty} N(p)/n = 1/2$.*
(ii) *If $0 < n - 2k \leqslant 6$, then $N(p) = k + 1$.*
(iii) *If $0 < 2k - n \leqslant 6$, then*

$$N(p) = \begin{cases} k - 1 & \text{if } p(z) \text{ is in Case 2(a)}, \\ k - 3 & \text{if } p(z) \text{ is in Case 2(b)}. \end{cases}$$

For the next result we need to introduce the notation for the level set of the Dirichlet kernel function.

Definition 2.9 Let $k \in \mathbb{Z}$ and $\alpha \in \mathbb{R}$ be non-negative. Define the set $\mathcal{D}_k(\alpha)$ as the subset of the interval $[0, 1]$ where the scaled Dirichlet kernel $D_k(2\pi t)$ takes values greater than α:

$$\mathcal{D}_k(\alpha) := \{t \in [0,1] : D_k(2\pi t) > \alpha\}.$$

Here $D_k(t)$ is the Dirichlet kernel of degree k, namely,

$$D_k(t) := 1 + 2\sum_{j=1}^{k} \cos(jt) = \frac{\sin(k+1/2)t}{\sin(t/2)}. \tag{2.4}$$

A theorem of Conrey, Granville, Poonen, and Soundararajan [9] implies that, for n-th Fekete polynomial $p(z)$ (n is an odd prime), $N(p) \sim (1-\kappa_0)n/2$ as $n \to \infty$ for some (hard to evaluate) numerical constant κ_0. Since κ_0 is close to $1/2$, $N(p)$ is about $1/4$ of all roots. Our next Theorem 2.10 bears considerable similarities to the result on Fekete polynomials [9].

Theorem 2.10 *Let $p(z)$ be a Littlewood polynomial of degree n with one negative term z^k. If k is fixed, then*

$$\lim_{n\to\infty} \frac{N(p)}{n} = \operatorname{meas}(\mathcal{D}_k(2)),$$

where meas $(\mathcal{D}_k(2))$ *denotes the Lebesgue measure of the set $\mathcal{D}_k(2)$. If k and n varies in such a way that the difference $m = n - k$ is fixed, then*

$$\lim_{n\to\infty} \frac{N(p)}{n} = \operatorname{meas}(\mathcal{D}_m^c(2)).$$

Here, $\mathcal{D}_m^c(2) := [0,1] \setminus \mathcal{D}_m(2)$.

We calculated the values of $\mathcal{D}_k(2)$ for $k \leqslant 20$ in Table 1. It is tempting to ask whether the limit $\lim_{k\to\infty} \mathcal{D}_k(2)$ exists, but we will not try to answer this question in this paper.

Table 1: Table of measures of the set $\mathcal{D}_k(2)$ for $1 \leqslant k \leqslant 20$ (first 8 digits)

k	meas($\mathcal{D}_k(2)$)	k	meas($\mathcal{D}_k(2)$)	k	meas($\mathcal{D}_k(2)$)	k	meas($\mathcal{D}_k(2)$)
1	1/3	6	0.13291444	11	0.12666414	16	0.12184061
2	0.27418711	7	0.12728673	12	0.12041045	17	0.11888251
3	0.21854988	8	0.14139922	13	0.11748373	18	0.11565045
4	0.18027852	9	0.13856714	14	0.12482311	19	0.11378430
5	0.15308602	10	0.13294934	15	0.12414168	20	0.11843827

Theorems 2.6, 2.7, and 2.10 are derived from zero counting formulas that will be stated as Theorems 3.4 and 3.7 in the next section. In comparison to Theorem 2.4, they are more complicated. The value of $N(p)$ depends on the distribution of fractions $j/l \pmod 1$ with respect to solutions of the equation $D_k(2\pi t) = 2$, $t \in [0,1)$. According to Theorems 3.4 and 3.7, the number $N(p)$ is approximately equal to the distance between the negative term and the closest end term of a polynomial (either a leading term or a constant term) plus the Boyd number $E(p,q)$, which will

be discussed in the next section (that corresponds to an error term). Because of this error term, it is impossible to write $N(p)$ in a closed form for all pairs (n,k) as in Theorem 2.4.

3 Zero Counting

In this section we describe Boyd's method and some facts about Dirichlet kernel that will be useful in later proofs.

3.1 Boyd's Entry-exit Lemma

Boyd [8] developed a method to count roots of polynomials inside and outside the unit circle. Let $p(z) \in \mathbb{R}[z]$ be not self-reciprocal polynomial of degree n. Consider the auxiliary polynomial $q(z) = p(z) + \varepsilon \cdot p^*(z)$, where $\varepsilon \in \{-1, 1\}$. Suppose that all unimodular roots of $q(z)$ are simple (that is, they have multiplicities 1). The unimodular root ζ of $q(z)$ is called an *exit point* if a continuous algebraic curve $z = z(t)$, defined by the equation

$$q(z,t) := p(z) + \varepsilon \cdot t \cdot p^*(z) = 0,$$

for $t \in [0,1]$, exits the open unit disk at $z = \zeta$ when $t = 1$, while $z(t)$ remains inside the unit disk $|z(t)| < 1$ for $t \in [0,1)$. The number of exit points associated with polynomials $p(z)$ and $q(z)$ via the equation $q(z,t) = 0$ will be denoted $E(p,q)$. We call the number $E(p,q)$ *a Boyd's number* of $p(z)$ and $q(z)$. Proposition 3.1 is essentially proved in Boyd's paper [8]. We state it in the form most convenient for our applications.

Proposition 3.1 (Boyd) *Suppose that a real polynomial $p(z)$ is not self-reciprocal, $p(z) \neq \pm p^*(z)$ and that $p(z)$ has no unimodular roots. If all unimodular roots of $q(z)$ are simple, then*

$$N(p) = N(q) + E(p,q).$$

Proof Since $|p(z)| = |p^*(z)|$ if $|z| = 1$, for fixed $t \in [0,1)$, the polynomial $q(z,t)$ in z has the same number of roots z inside the open unit disk $|z| < 1$ as the polynomial $p(z)$. Roots of $q(z,t)$ in $|z| < 1$ converge to roots of $p(z)$ in $|z| < 1$ or to exit points (for each simple exit point ζ, exactly one branch of $z(t)$ exits the unit disk at $z = \zeta$) as $t \to 1^-$. By continuity,

$$N(p) = \lim_{t \to 1^-} N(q(z,t)) = N(q) + E(p,q). \qquad \blacksquare$$

Boyd also established a criterion for determining all exit points of $q(z)$; see [8, Lemma 3].

Criterion 3.2 (Boyd) Suppose that ζ is a simple unimodular root of the auxiliary polynomial $q(z)$. Then $\zeta^{1-\deg p} p(\zeta) q'(\zeta)$ is a nonzero real number. The root ζ is an exit point if and only if

$$\varepsilon \cdot \zeta^{1-\deg p} p(\zeta) q'(\zeta) < 0.$$

In the proof of Theorem 2.3, we need to identify polynomials with unimodular roots. These *bad cases* are described in Lemma 3.3 below.

Lemma 3.3 *Let $f(z) = z^v - 2z^u + 1$, $v \geqslant u > 0$, and $\gcd(v, u) = d$. All unimodular roots of $f(z)$ are roots of the polynomial $z^d - 1$. If $v \neq 2u$, then all unimodular roots of $f(z)$ are simple. If $v = 2u$, then $f(z) = (z^u - 1)^2$.*

Proof of Lemma 3.3 The equation $\zeta^v + 1 = 2\zeta^u$ and $|\zeta| = 1$ implies $|\zeta^v + 1| = 2$. That is possible only if $\zeta^v = 1$. This gives $\zeta^u = 1$, so ζ is a common root of $z^u - 1$ and $z^v - 1$, and so it is the root of $\gcd(z^u - 1, z^v - 1) = z^d - 1$. On the other hand, each root of $z^d - 1$ satisfies $\zeta^u = 1$ and $\zeta^v = 1$, so it is a root of $f(z)$. Hence, $(z^d - 1) \mid f(z)$, since the roots of $z^d - 1$ are pairwise distinct and simple. If $v \neq 2u$, the derivative $f'(z) = vz^{v-1} - 2uz^{u-1} = z^{u-1}(vz^{v-u} - 2u)$ does not have unimodular roots. For $v = 2u$, $f(z)$ is simply $(z^u - 1)^2$. ■

Proof of Theorem 2.3 In the case where $n + 1 = 2k$, $p(z) = (z^k - 1)^2/(z - 1)$ by (2.2), so one has $N(p) = 0$, $U(p) = 2k - 1 = n$. We assume that $n \neq 2k - 1$ through the rest of the proof. Write $k = du$ and $n + 1 = dv$ with coprime integers v and u, $v > u > 0$. Divide $p(z)$ in (2.2) by $(z^d - 1)/(z - 1)$ to obtain

$$p(z)\left(\frac{z^d - 1}{z - 1}\right)^{-1} = \frac{z^{n+1} - 2z^k + 1}{z^d - 1} = p_1(z^d),$$

where

$$p_1(z) =: \frac{z^v - 2z^u + 1}{z - 1}.$$

By Lemma 3.3, the numerator $z^v - 2z^u + 1$ vanishes on the unit circle only at $z = 1$ with multiplicity 1, since $\gcd(u, v) = 1$ and $v \neq 2u$ (this corresponds to $n \neq 2k - 1$). Therefore, $U(p_1) = 0$. This yields

$$N(p) = d \cdot N(p_1) \quad \text{and} \quad U(p) = d \cdot U(p_1) + (d - 1) = d - 1. \tag{3.1}$$

Since $p_1(z)$ has no unimodular roots, Proposition 3.1 is applicable. Consider

$$q_1(z) := p_1(z) + p_1^*(z) = 2 \cdot \frac{z^{v-u} - z^u}{z - 1} = \pm 2z^m \cdot \frac{z^l - 1}{z - 1}, \tag{3.2}$$

where

$$m := \min\{v - u, u\} \quad \text{and} \quad l := |v - 2u|.$$

According to Proposition 3.1, the number of roots of $p_1(z)$ inside the unit disk is $N(p_1) = N(q_1) + E(p_1, q_1) = m + E(p_1, q_1)$. By (3.2), $q_1(\zeta) = 0$ yields

$$\zeta^{v-u} = \zeta^u, \qquad \zeta^v = \zeta^{2u}, \qquad \zeta^{v-2u} = 1. \tag{3.3}$$

Hence,

$$p_1(\zeta) = \frac{\zeta^{2u} - 2\zeta^u + 1}{\zeta - 1} = \zeta^u \cdot \frac{\zeta^u + \zeta^{-u} - 2}{\zeta - 1}.$$

By (3.2), $\zeta = e^{it}$, where $t = 2\pi j/l$, $1 \leqslant j \leqslant l - 1$. Thus

$$p_1(\zeta) = e^{iut} \cdot \frac{e^{iut} + e^{-iut} - 2}{e^{it} - 1} = e^{i(u-1/2)t} \cdot \frac{\cos(ut) - 1}{i \sin(t/2)}.$$

The derivative of $q_1(z)$ is

$$q_1'(z) = 2\frac{(z^{v-u} - z^u)'(z-1) - (z^{v-u} - z^u)(z-1)'}{(z-1)^2}$$
$$= 2 \cdot \frac{z^{u-1} \cdot ((v-u)z^{v-2u} - u)}{z-1} - 2 \cdot \frac{z^{v-u} - z^u}{(z-1)^2}.$$

In view of (3.3), we have

$$q_1'(\zeta) = 2\zeta^{u-1} \cdot \frac{(v-u)\zeta^{v-2u} - u}{\zeta - 1} = 2 \cdot \zeta^{u-1} \cdot \frac{v-2u}{\zeta-1} = e^{i(u-3/2)t} \cdot \frac{v-2u}{i\sin(t/2)}.$$

Since $\deg p_1 = v - 1$, $\zeta^{1-\deg p_1} = e^{i(2-v)t}$, we obtain

$$\zeta^{1-\deg p_1} p_1(\zeta) q_1'(\zeta) = \frac{(v-2u)(1-\cos(ut))}{\sin^2(t/2)} = 2(v-2u)\frac{\sin^2(ut/2)}{\sin^2(t/2)}.$$

By Criterion 3.2 (with $\varepsilon = 1$), none of the unimodular roots of $q_1(\zeta)$ are exit points if $v > 2u$ ($v - u > u$). In this case, one has $m = u$, $E(p_1, q_1) = 0$, so that $N(p_1) = m = u$. If $v < 2u$ ($v - u < u$), then all unimodular roots of $q_1(z)$ are exit points. This case yields $m = v - u$, $l = 2u - v$, so that $E(p_1, q_1) = U(q_1) = l - 1 = 2u - v - 1$. This yields $N(p_1) = m + l - 1 = u - 1$. It remains to substitute $N(p_1)$ into (3.1). ■

The proofs of Theorems 2.6, 2.7, and 2.10 are also based on Boyd's method.

Theorem 3.4 *Let $p(z)$ be as in Case 2(a). Set*

$$m := \min\{k, n-k\} \quad \text{and} \quad l := |n - 2k|.$$

The number of roots of $p(z)$ inside the open unit disk is $N(p) = m + E(p, q)$. For $k = 0$, one has $E(p, q) = 1$; for $k = n$, $E(p, q) = n - 1$. For $1 \leqslant k \leqslant n - 1$, we have

$$E(p,q) = \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\Big(\frac{j}{l}\Big), \quad \text{if } n > 2k, \tag{3.4}$$

and

$$E(p,q) = \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k^c(2)}\Big(\frac{j}{l}\Big), \quad \text{if } n < 2k, \tag{3.5}$$

where $\mathbb{1}_A(x)$ is the characteristic function of a set A.

Proof of Theorem 3.4 If $p(z)$ is of type 2(a), in view of (2.3), define $q(z)$ by

$$q(z) := p(z) - p^*(z) = \Big(\frac{z^{n+1}-1}{z-1} - 2z^k\Big) - \Big(\frac{z^{n+1}-1}{z-1} - 2z^{n-k}\Big) = 2z^{n-k} - 2z^k.$$

Then $q(z) = \pm 2z^m(z^l - 1)$. The unimodular zeros of $q(z)$ are $\zeta = e^{2\pi i j/l}$, $0 \leqslant j \leqslant l - 1$. All roots of unity are simple zeros of $q(z)$. The polynomial $p(z)$ does not vanish at any of them, since $p(z)$ is as in Case 2(a). By Proposition 3.1, $N(p) = N(q) + E(p, q) = m + E(p, q)$. To determine $E(p, q)$ we evaluate $p(z)$ and $q'(z)$ at all roots of unity ζ of $q(z)$. The derivative of $q(z)$ is

$$q'(z) = 2(n-k)z^{n-k-1} - 2kz^{k-1} = 2z^{k-1}\big((n-k)z^{n-2k} - k\big).$$

First we consider $\zeta = 1$. One has

$$p(1) = n-1, \qquad q'(1) = 2(n-2k), \qquad p(1)q'(1) = 2(n-1)(n-2k).$$

By Criterion 3.2 (with $\varepsilon = -1$), $\zeta = 1$ is an exit point if and only if $n > 2k$.

Next we consider roots $\zeta \neq 1$. Observe that $\zeta^l = 1$ implies that $\zeta^n = \zeta^{2k}$ and $\zeta^k = \zeta^{n-k}$. Hence, for $\zeta \neq 1$,

$$p(\zeta) = \frac{\zeta^{2k+1}-1}{\zeta-1} - 2\zeta^k = \zeta^k\Big(D_k\Big(\frac{2\pi j}{l}\Big) - 2\Big), \tag{3.6}$$

where $D_k(t)$ is the Dirichlet kernel given by (3.10). The derivative $q'(z)$ at the point $z = \zeta$ takes the value $q'(\zeta) = 2(n-2k)\zeta^{k-1}$. By Proposition 3.2, ζ is the exit point if and only if

$$\zeta^{1-n} \cdot p(\zeta) \cdot q'(\zeta) = 2(n-2k)\Big(D_k\Big(\frac{2\pi j}{l}\Big) - 2\Big) > 0.$$

Suppose that $n > 2k$. It was noted earlier that $\zeta = 1$ is an exit point in this case. Other roots of unity $\zeta = e^{2\pi i j/l}$, $j = 1, 2, \dots, n$ are exit points precisely when the fraction $j/l \in \mathcal{D}_k(2)$. By the summation of the characteristic function $\mathbb{1}_{\mathcal{D}_k(2)}(x)$ over all such fractions, one obtains

$$E(p,q) = 1 + \sum_{j=1}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\Big(\frac{j}{l}\Big).$$

For $k = 0$, $D_0(t) = 1 < 2$ and $\mathcal{D}_0(2) = \varnothing$, so $E(p,q) = 1$. For $k \geqslant 1$, $\mathbb{1}_{\mathcal{D}_k(2)}(0) = 1$, so one can include the term 1 into the sum.

Suppose that $n < 2k$. Then $\zeta = 1$ is not an exit point. Other roots of unity $\zeta = e^{2\pi i j/l}$, $j = 1, 2, \dots, n$ are exit points precisely when $j/l \in \mathcal{D}_k^c(2)$. In this case,

$$E(p,q) = \sum_{j=1}^{l-1} \mathbb{1}_{\mathcal{D}_k^c(2)}\Big(\frac{j}{l}\Big) = \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k^c(2)}\Big(\frac{j}{l}\Big),$$

since $0 \notin \mathcal{D}_k^c(2)$ for every $k \geqslant 1$. If $k = n$, then $l = n$ and $D_k(2\pi j/l) = 1$ for each $j = 1, \dots, l-1$, which implies that $E(p,q) = n-1$. ■

The next lemma identifies all roots of unity that are zeros of Littlewood polynomials in Case 1.

Lemma 3.5 *The polynomial $\Phi_6(z) = z^2 - z + 1$ is the only possible cyclotomic divisor of the polynomial $p(z) = (z^{2k+1}-1)/(z-1) - 2z^k$, $k \geqslant 1$. Furthermore, $\Phi_6(z)$ divides $p(z)$ precisely when $k \equiv 1 \pmod 6$.*

Proof of Lemma 3.5 Suppose that ζ is a root of unity and let $h \in \mathbb{N}$ be the multiplicative order of ζ. Without loss of generality, we may assume $\zeta = e^{2\pi i/h}$.

First, let us show that $h \notin \{1, 2\}$. For $h = 1$, one has $\zeta = 1$. For $h = 2$, one has $\zeta = -1$. One can easily check that $p(1) = n - 1 \neq 0$ and $p(-1) = 1 - 2(-1)^k \neq 0$ from (2.3). Hence, $h \geqslant 3$.

If h is odd, then $h = 2j + 1$ for some $j \geqslant 1$. In this case, set $\eta := \zeta^j$. It is an algebraic conjugate of ζ, since $\gcd(j, 2j+1) = 1$.

If h is even, then $h = 4j$ for some $j \geqslant 1$, or $h = 4j + 2$ for some $j \geqslant 1$. In both cases, set $\eta := \zeta^{2j-1}$. This number η is an algebraic conjugate of ζ, since $\gcd(4j, 2j-1) = \gcd(4j+2, 2j-1) = 1$. Now consider inequalities

$$\frac{1}{6} \leqslant \frac{2j-1}{4j+2} < \frac{2j-1}{4j} < \frac{j}{2j+1} < \frac{1}{2}, \tag{3.7}$$

where $j \geqslant 1$. The equality in the left side of (3.7) can be attained only for $j = 1$. Inequalities (3.7) imply that $\pi/3 < \arg(\eta) < \pi$ for $j > 1$. It follows that $p(\eta) \neq 0$, since

$$p(\eta)\eta^{-k} = D_k(\arg(\eta)) - 2 \leq \frac{1}{\sin(\arg(\eta)/2)} - 2 < 0$$

by (2.4). However, this contradicts the fact that η is the algebraic conjugate of ζ, so it must be the root of $p(z)$. Moreover, we can rule out cases $h = 2j + 1$ and $h = 4j$ by the same argument using inequalities (3.7). Thus, one must have $j = 1$ and $h = 4j + 2 = 6$, so that $\zeta = e^{\pi i/3}$. Since $\zeta^6 = 1$, it suffices to check whether

$$p(\zeta) = \frac{\zeta^{2k+1} - 1}{\zeta - 1} - 2\zeta^k = 0$$

for $k = 0, 1, 2, 3, 4, 5$. We have $p(\zeta) = \zeta^2 - \zeta + 1 = 0$ for $k = 1$ and $p(\zeta) \neq 0$ for $k \in \{0, 2, 3, 4, 5\}$. Thus $\Phi_6(z)$ (the minimal polynomial of ζ) divides $p(z)$ if $k \equiv 1 \pmod 6$. ∎

At this point we already have everything that is needed to identify all unimodular zeros of polynomials in Case 2.

Lemma 3.6 *Let $p(z)$ be as in Case* 2*, and $n \geqslant 2$. Then all possible unimodular roots ζ of $p(z)$ are $\zeta = e^{\pm\pi i/3}$. The polynomial $p(z)$ vanishes at ζ (with multiplicity* 1*) if and only if $k \equiv 1 \pmod 6$ and $n \equiv 2 \pmod 6$.*

Proof of Lemma 3.6 If ζ is the unimodular root of $p(z)$, then it is also the unimodular root of $q(z) = p(z) - p^*(z) = 2z^k(z^{n-2k} - 1)$ of the same multiplicity. Since $z^{n-2k} - 1$ has no repeated factors, such unimodular roots are simple. Hence, $\zeta^n = \zeta^{2k}$ and

$$p(\zeta) = \frac{\zeta^{2k+1} - 1}{\zeta - 1} - 2\zeta^k = 0.$$

By Lemma 3.5, one has $\zeta = e^{\pm\pi i/3}$ and $k \equiv 1 \pmod 6$. The multiplicative order of ζ is $h = 6$. From $\zeta^{n-2k} = 1$ one deduces that $h \mid (n - 2k)$, hence $n \equiv 2k \equiv 2 \pmod 6$. ∎

Proof of Proposition 2.5 This is a direct consequence of Lemma 3.6. ∎

Theorem 3.7 *Let $p(z)$ be as in Case* 2(b)*. Then*

$$U(p) = 2 \quad \text{and} \quad N(p) = m + E(p, q).$$

where m and l are the same as in Theorem 3.4. In case $n > 2k$, $E(p, q)$ can be evaluated as in (3.4)*. In case $n < 2k$, we have*

$$E(p, q) = \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k^c(2)}\Big(\frac{j}{l}\Big) - 2.$$

Proof of Theorem 3.7 In order to apply Proposition 3.1, cyclotomic factors need to be eliminated from $p(z)$. By Lemma 3.6, such a cyclotomic factor is $\Phi_6(z)$. For the polynomial $p(z)$ in (2.3) and $q(z) = p(z) - p^*(z)$, define

$$p_1(z) := \frac{p(z)}{\Phi_6(z)} = \frac{z^{n+1} - 2z^{k+1} + 2z^k - 1}{(z-1)(z^2 - z + 1)}$$

and

$$q_1(z) := p_1(z) - p_1^*(z) = \frac{q(z)}{\Phi_6(z)} = \frac{2z^{n-k} - 2z^k}{z^2 - z + 1}$$
$$= \frac{2z^k(z^{n-2k} - 1)}{z^2 - z + 1} = \pm\frac{2z^m(z^l - 1)}{z^2 - z + 1}.$$

By Proposition 3.1, $N(p) = m + E(p,q)$. The equation $q_1(\zeta) = 0$ for $\zeta = e^{it}$, $t \in [0, 2\pi)$ implies $q(\zeta) = 0$ and $p(\zeta) = \zeta^k(D_k(t) - 2)$ as in (3.6). Since $\Phi_6(z)$ is factored out, we have $\zeta \neq e^{\pm\pi i/3}$ and

$$p_1(\zeta) = \frac{\zeta^k(D_k(t) - 2)}{\zeta^2 - \zeta + 1} = \zeta^{k-1}\frac{D_k(t) - 2}{2\cos t - 1}.$$

Similarly,

$$q_1'(z) = \frac{q'(z)\Phi_6(z) - q(z)\Phi_6'(z)}{\Phi_6^2(z)},$$

which leads to

$$q_1'(\zeta) = \frac{q'(\zeta)}{\Phi_6(\zeta)} = \frac{2\zeta^{k-1}(n-2k)}{\zeta^2 - \zeta + 1} = 2\zeta^{k-2}\frac{n-2k}{2\cos t - 1},$$

for any unimodular root ζ of $q_1(z)$. Hence,

$$\zeta^{1-\deg p_1} p_1(\zeta) q_1'(\zeta) = \frac{2(n-2k)(D_k(t) - 2)}{(2\cos t - 1)^2}.$$

If $n > 2k$, then $\zeta = e^{2\pi i j/l}$, $0 \leqslant j \leqslant l-1$ is an exit point if and only if the fraction $j/l \in \mathcal{D}_k(2)$. Since $D_k(\pi/3) \leqslant 2$ by the envelope inequality (3.11), $e^{\pm\pi i/3}$ is not an exit point and the indicator sum formula (3.4) for $E(p,q)$ in Theorem 3.4 holds. Similarly, formula (3.5) of Theorem 3.4 holds for $E(p,q)$ in case $n < 2k$ if one removes the points $\pi/3$, $5\pi/3$ from $\mathcal{D}_k^c(2)$ (these correspond to unimodular roots $e^{\pm\pi i/3}$ of $p(z)$), so that 2 needs to be subtracted from (3.5). ∎

To prove Theorems 2.6 and 2.7 we need sharp bounds for the Boyd numbers $E(p,q)$ (the error term). The error term essentially depends on the distance between the negative term and the middle coefficient of $p(z)$ and it does not exceed $2/3$ of that distance. The precise statement is given in the next lemma.

Lemma 3.8 *Let k and l be positive integers. Then*

$$1 \leqslant \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\left(\frac{j}{l}\right) \leqslant 2\lceil l/6\rceil - 1, \tag{3.8}$$

and

$$l - 2\lceil l/6\rceil + 1 \leqslant \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k^c(2)}\left(\frac{j}{l}\right) \leqslant l - 1. \tag{3.9}$$

If $k \equiv 0 \pmod{l}$*, we have the equality in the left side of* (3.8) *and the right side of* (3.9). *If* $k \equiv 1 \pmod{l}$*, we have the equality in the right side of* (3.8) *and the left side of* (3.9). *Moreover, if the number* l *is fixed and* k *varies, indicator sums in* (3.8) *and* (3.9) *(as functions of* k*) are periodic modulo* l*.*

Proof of Lemma 3.8 Consider fractions j/l, $j = 0, 1, \dots, l-1$. We have

$$D_k(2\pi j/l) \leqslant 1/\sin(\pi j/l) \leqslant 2$$

if $j/l \in [1/6, 5/6]$. The number of such fractions is equal to the number of integers j in the interval $[l/6, 5l/6]$, namely,

$$\begin{aligned} \lfloor 5l/6 \rfloor - \lceil l/6 \rceil + 1 &= \lfloor l - l/6 \rfloor - \lceil l/6 \rceil + 1 = l + \lfloor -l/6 \rfloor - \lceil l/6 \rceil + 1 \\ &= l - 2\lceil l/6 \rceil + 1. \end{aligned}$$

Therefore, the inequality $D_k(2\pi j/l) > 2$ holds at most at

$$l - (l - 2\lceil l/6 \rceil + 1) = 2\lceil l/6 \rceil - 1$$

points $j/l \in [0, 1)$. These numbers represent the largest possible number of fractions j/l in $\mathcal{D}_k(2)$ and the smallest possible number of fractions in $\mathcal{D}_k^c(2)$, respectively. Since $D_k(0) > 2$, $\mathcal{D}_k(2)$ contains at least one and $\mathcal{D}_k^c(2)$ contains at most $l-1$ such fraction. This proves inequalities (3.8) and (3.9).

The periodicity modulo l follows from the identity $D_{k+l}(2\pi j/l) = D_k(2\pi j/l)$ for $j \neq 0$ and from the fact that $0 \in \mathcal{D}_k(2)$ for every $k \geqslant 1$.

Suppose that $k \equiv 0 \pmod{l}$. By the periodicity, $D_k(2\pi j/l) = D_0(2\pi j/l) = 1$ for $1 \leqslant j \leqslant l-1$ and $D_k(0) = 2k+1$. Thus, only the number 0 is in $\mathcal{D}_k(2)$, but $j/l \notin \mathcal{D}_k(2)$ for $1 \leqslant j \leqslant l-1$, so that the sum in (3.8) is equal to 1. This forces the sum in (3.9) to be $l-1$.

Suppose that $k \equiv 1 \pmod{l}$. By the periodicity, $D_k(2\pi j/l) = D_1(2\pi j/l) = 1+2\cos(2\pi j/l)$. Thus, $D_k(2\pi j/l) > 2$ holds precisely for fractions j/l outside the interval $[1/6, 5/6]$. By our earlier counting, the number of such fractions is $2\lceil l/6 \rceil - 1$. That forces upper and lower bounds to be attained by sums in (3.8) and (3.9), respectively. ■

Table 2 and the periodicity property of the error term mentioned in Lemma 3.8 are very useful when evaluating $E(p, q)$ for small l and k.

Here is an example.

Example 3.9 Find $N(p)$ for the polynomial

$$p(z) = \frac{z^{52} - 1}{z - 1} - 2z^{16}.$$

Since $n = 51 \equiv 3 \pmod{6}$, $p(z)$ is of type 2(a) by Proposition 2.5. One has $k = 16$, $l = n - 2k = 19$, so $E(p, q) = 1$ according to Table 2 since $k \equiv 16 \pmod{l}$. Hence, $p(z)$ has $N(p) = k + E(p, q) = 17$ roots in the open unit disk.

Table 2: Values of $\sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}$ for small values of k and l, $k \geqslant 1$, $0 \leqslant l \leqslant 20$. Rows represent l, columns represent the remainder of $k \pmod{l}$.

l \ k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1																			
2	1	1																		
3	1	1	1																	
4	1	1	1	1																
5	1	1	1	1	1															
6	1	1	1	1	1	1														
7	1	3	1	1	1	1	1													
8	1	3	3	1	1	1	1	1												
9	1	3	3	1	1	1	1	1	1											
10	1	3	3	3	1	1	1	1	1	1										
11	1	3	3	3	1	1	1	1	1	1	1									
12	1	3	3	3	3	1	1	1	1	1	1	1								
13	1	5	3	3	3	1	1	1	3	1	1	1	1							
14	1	5	3	3	3	3	1	1	3	1	1	1	1	1						
15	1	5	5	3	3	3	1	1	1	3	1	1	1	1	1					
16	1	5	5	3	3	3	3	1	1	3	3	1	1	1	1	1				
17	1	5	5	3	3	3	3	1	1	1	3	3	1	1	1	1	1			
18	1	5	5	3	3	3	3	3	1	1	3	3	1	1	1	1	1	1		
19	1	7	5	5	3	3	3	3	1	1	1	3	3	1	3	1	1	1	1	
20	1	7	5	5	3	3	3	3	5	1	1	3	3	3	1	1	1	1	1	1

3.2 Useful Facts About Dirichlet Kernel

Recall that the Dirichlet kernel $D_k(t)$ is a trigonometric polynomial of degree k, defined by

$$D_k(t) := 1 + 2\sum_{j=1}^{k} \cos(jt) = \frac{\sin(k+1/2)t}{\sin(t/2)}. \tag{3.10}$$

Since $|\sin(k+1/2)t| \leqslant 1$, the graph of $D_k(t)$ for $0 \leqslant t \leqslant \pi$ is enveloped by

$$|D_k(t)| \leqslant \frac{1}{\sin(t/2)}. \tag{3.11}$$

The function $D_k(t)$ touches the envelope at points

$$s_j := \frac{2j+1}{2k+1}\pi, \qquad j = 0, \dots, k.$$

We will need some knowledge about the behavior of $D_k(t)$ in the interval $[0, \pi]$. The Dirichlet kernel vanishes at points

$$t_j = \frac{2\pi j}{2k+1}, \qquad j = 1, \dots, k,$$

so that the total number of zeros in the period $[0, 2\pi)$ is $2k$. In the interval $[0, \pi]$ $D_k(t)$ has extrema at the endpoints of the interval and between each of its two consecutive zeros: points of positive local maxima occur in intervals

$$[t_{2j}, s_{2j}] = \left[\frac{4j}{2k+1}\pi, \frac{4j+1}{2k+1}\pi \right], \tag{3.12}$$

while negative local minima occur in

$$(t_{2j+1}, s_{2j+1}] = \left(\frac{4j+2}{2k+1}\pi, \frac{4j+3}{2k+1}\pi \right], \tag{3.13}$$

for $j = 0, \dots, \lfloor (2k+1)/4 \rfloor$ (discard intervals which go outside $[0, \pi]$). Extremal points lie strictly inside of these intervals with the exception of the point $t = 0$, where $D_k(t)$ takes its largest absolute value $D_k(0) = 2k+1$ and the point $t = \pi$, where $D_k(\pi/2) = (-1)^{\lfloor k/2 \rfloor}$. These basic facts can be proved by tracking the sign changes of $D_k'(t)$ at the endpoints of intervals given in (3.12) and (3.13), thus we omit the details.

Proof of Theorem 2.4 Observe that $p(z)$ is self-reciprocal when $n = 2k$, thus,

$$p(z) = \frac{z^{2k+1} - 1}{z - 1} - 2z^k = \frac{z^{2k+1} - 2z^{k+1} + 2z^k - 1}{z - 1}.$$

We need to show that all zeros of $p(z)$ are simple. Consider the numerator

$$f(z) := z^{2k+1} - 2z^{k+1} + 2z^k - 1$$

as a polynomial in the finite field $\mathbb{F}_2[z]$:

$$f(z) \equiv z^{2k+1} + 1, \qquad f'(z) \equiv (2k+1)z^{2k} \pmod 2.$$

Hence $f(z)$ has no repeated factors in $\mathbb{Z}[z]$.

We proceed to find the number $U(p)$. Let $z = e^{it}$, $t \in [0, 2\pi)$. Since $n = 2k$,

$$\begin{aligned} p(e^{it}) &= \frac{e^{i(2k+1)t} - 1}{e^{it} - 1} - 2e^{ikt} = e^{ikt} \left(\frac{e^{(k+1/2)it} - e^{-(k+1/2)it}}{e^{it/2} - e^{-it/2}} - 2 \right) \\ &= e^{ikt}(D_k(t) - 2). \end{aligned}$$

Thus, the argument $\arg(\zeta)$ of a unimodular zero ζ of $p(z)$ is a solution to the equation $D_k(t) = 2$. By symmetry, the number of solutions to this equation in the interval $[0, 2\pi)$ is twice that number in the interval $(0, \pi)$, since $D_k(0)$ and $D_k(\pi)$ are not equal to 2, so assume that $t \in (0, \pi)$.

For $t > \pi/3$, $D_k(t) < 2$ by the enveloping inequality (3.11) in Subsection 3.2, since $\sin(t/2) > 1/2$. Hence, all zeros occur in the interval $(0, \pi/3]$. For any integer $k \geqslant 1$, there exists an integer $l \geqslant 0$, such that

$$\frac{(4l+1)\pi}{2k+1} \leqslant \frac{\pi}{3} < \frac{(4l+5)\pi}{2k+1}. \tag{3.14}$$

In the interval $(0, \pi/3]$, the Dirichlet kernel $D_k(t)$ has $l+1$ positive maxima, which occur at the points θ_j,

$$\theta_j \in \left[\frac{4j\pi}{2k+1}, \frac{(4j+1)\pi}{2k+1} \right), \qquad j = 0, 1, \dots l.$$

At each point θ_j,

$$D_k(\theta_j) > D_k\Big(\frac{(4j+1)\pi}{2k+1}\Big) = \Big(\sin\Big(\frac{(4j+1)\pi}{2k+1}\Big)\Big)^{-1} \geqslant \frac{1}{\sin(\pi/6)} = 2.$$

Observe that the (possibly empty) open interval

$$\Big(\theta_l,\ \frac{(4l+1)\pi}{2k+1}\Big)$$

contains no solution, since $D_k(t)$ is decreasing and greater than 2 in that interval. The kernel $D_k(t)$ has a negative minima between each two consecutive points of positive maxima, hence the equation $D_k(t) = 2$ has precisely two solutions in each of the intervals $[\theta_j, \theta_{j+1}]$, $j = 0, \dots, l-1$. In total, $D_k(t) = 2$ has exactly $2l$ solutions in the interval

$$\Big[0,\ \frac{(4l+1)\pi}{2k+1}\Big).$$

By (3.14), other possible solutions are contained in

$$\Big[\frac{(4l+1)\pi}{2k+1},\ \frac{\pi}{3}\Big]$$

(it is a singleton if the endpoints coincide). Since $D_k(t) \geqslant 2$ at the left end-point and $D_k(\pi/3) \leqslant 2$, there exists at least one such zero, say ϕ. We claim that there are no more zeros. Indeed, let us suppose that there exists another zero, say ψ. We can assume that $\phi < \psi \leqslant \pi/3$. With this assumption in mind, we want to determine more precise location of numbers ϕ, ψ, $\pi/3$ in the interval (3.14) and find the value of k in terms of l. We see that

$$\psi \notin \Big[\frac{(4l+2)\pi}{2k+1},\ \frac{(4l+4)\pi}{2k+1}\Big],$$

since $D_k(t)$ is negative there. There must be at least one critical point of $D_k'(t)$ between ϕ and ψ. According to (3.12) and (3.13), the only possibility for this to happen in (3.14) is

$$\psi \in \Big(\frac{(4l+4)\pi}{2k+1},\ \frac{(4l+5)\pi}{2k+1}\Big). \tag{3.15}$$

Since $\psi \leqslant \pi/3$,

$$\frac{(4l+4)\pi}{2k+1} < \frac{\pi}{3} < \frac{(4l+5)\pi}{2k+1} \tag{3.16}$$

by (3.14) and (3.15). This leads to $12l + 11 < 2k < 12l + 14$, hence $k = 6l + 6$.

Now we show that the existence of the second solution ψ is impossible. By (3.12), the interval (3.15) contains the point of a local maximum of $D_k(t)$ say, θ where the derivative $D_k'(t)$ changes its sign from $+$ to $-$. Since $k = 6l + 6$, $D_k'(\pi/3) = k\sqrt{3} > 0$. Together with (3.16), this implies $\pi/3 < \theta$, hence $D_k(\theta) < 2$ by the envelope inequality (3.11). Thus, we arrive at inequalities

$$D_k(\psi) \leqslant D_k(\theta) < 2,$$

which contradict the existence of the second solution ψ.

It follows that the total number of solutions in $[0, \pi]$ to the equation $D_k(t)$ is $2l+1$. The total number of solutions in $[0, 2\pi)$ is $4l + 2$. By solving inequalities (3.14), one obtains $l = \lfloor (k-1)/6 \rfloor$ with $k = n/2$. We already know that $p(z)$ has no repeated roots, so all these zeros correspond to simple unimodular roots of polynomial $p(z)$. Thus, $U(p) = 4\lfloor (n-2)/12 \rfloor + 2$. Since $p(z) = p^*(z)$, one finds $N(p)$ by using $N(p) = (n - U(p))/2$. ∎

4 Proofs of Main Theorems

Proofs of Theorem 2.1 and Corollary 2.2 If $n \geqslant 2k$, consider Littlewood polynomial $p(z)$ with one sign change among the terms z^k and z^{k-1}. By Theorem 2.3, $N(p) = k$, $U(p) = 0$, since $d = 1$ (coprimality condition is fulfilled if $n = 2k$). For $n \leqslant 2k$, consider $p(z)$ with one sign change among the terms z^{k+1} and z^k and apply Theorem 2.3 with k replaced by $k+1$. ∎

Proofs of Theorem 2.4 and Proposition 2.5 have been given in Section 3.

Proofs of Theorems 2.6 and 2.7 and Corollary 2.8 Apply formulas from Theorems 3.4 and 3.7. Use $E(p,q) = 1$ in case $k = 0$. For $k \geqslant 1$, estimate $E(p,q)$ by inequalities (3.8) and (3.9) in Lemma 3.8. In Theorem 2.7, $p(z)$ has unimodular roots only for $n \equiv 2 \pmod 6$ and $k \equiv 1 \pmod 6$ by Criterion 3.2. Thus $|n-2k|$ is divisible by 6, $2\lceil (n-2k)/6 \rceil = (2k-n)/3$ if $n > 2k$ and $2\lceil (2k-n)/6 \rceil = (2k-n)/3$ if $n < 2k$. This yields $(n+k)/3$ terms in inequalities. We note that there is no contradiction between upper and lower bounds in Theorem 2.7. Since $n \neq 2k$ and $n \equiv 2k \pmod 6$, we have $|n-2k| \geqslant 6$. This shows that the right-hand side of the first inequality (for $n > 2k$) in Theorem 2.7 is at least $k+1$, while the left-hand side of the second inequality (for $n < 2k$) is at most $k-3$.

Assume now that $k \sim n/2$, so that $l = |n-2k| = o(n)$ as $n \to \infty$. Then $m = \min\{k, n-k\} \sim n/2$. By Lemma 3.8, $E(p,q) < l/3$ and hence it is also $o(n)$. By the formulas of Theorems 3.4 and 3.7, it follows that $N(p) \sim n/2$ as $n \to \infty$.

In the case of $l = |n-2k| \leqslant 6$ in Corollary 2.8, we have $E(p,q) = 1$ for $n > 2k$, $E(p,q) = l-1$ for $n < 2k$ if $p(z)$ has no unimodular roots by Lemma 3.8. If $p(z)$ has unimodular roots, then $E(p,q) = 1$ and $E(p,q) = l-3$ for $n > 2k$ and $n < 2k$, respectively. That yields the formulas of Corollary 2.8 in the cases where $0 < n-2k \leqslant 6$ and $0 < 2k-n \leqslant 6$. ∎

Proof of Theorem 2.10 By Theorem 3.4, for $n > 2k > 0$, one has $N(p) = k + E(p,q)$, where

$$E(p,q) = \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\Big(\frac{j}{l}\Big), \quad l = n-2k.$$

If k is fixed, then $n \sim l$ as $l \to \infty$. Hence,

$$\lim_{n\to\infty} \frac{N(p)}{n} = \lim_{l\to\infty} \frac{N(p)}{l} = \lim_{l\to\infty} \frac{k}{l} + \lim_{l\to\infty} \frac{E(p,q)}{l} = \lim_{l\to\infty} \frac{1}{l} \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\Big(\frac{j}{l}\Big).$$

The last sum is the left endpoint Riemann sum of the indicator function $\mathbb{1}_{\mathcal{D}_k(2)}$ in the interval $[0,1]$. It converges to

$$\lim_{l\to\infty} \frac{1}{l} \sum_{j=0}^{l-1} \mathbb{1}_{\mathcal{D}_k(2)}\Big(\frac{j}{l}\Big) = \int_0^1 \mathbb{1}_{\mathcal{D}_k(2)}(x)\,dx = \operatorname{meas}\big(\mathcal{D}_k(2)\big).$$

For $k = 0$, one has $E(p, q) = 1$, so $N(p) = 1$ by Theorem 3.4, and $N(p)/n = 1/n \to 0$ as $n \to \infty$. Since $\mathrm{meas}(\mathcal{D}_0(2)) = 0$, the statement of Theorem 2.10 also holds in the case where $k = 0$.

For $n < 2k$, observe that $N(p) = n - N(p^*)$ or $N(p) = n - N(p^*) - 2$ for polynomials $p(z)$ in Cases 2(a) and 2(b) respectively by Lemma 3.6. By applying the first part of the proof of Theorem 2.10 to the polynomial $p^*(z)$ with k replaced by $m = n - k$ and noting that $1 - \mathrm{meas}(\mathcal{D}_m(2)) = \mathrm{meas}(\mathcal{D}_m^c(2))$, when $n - k$ is fixed, we have

$$\lim_{n\to\infty} \frac{N(p)}{n} = \mathrm{meas}\big(\mathcal{D}_m^c(2)\big).$$

This completes the proof of Theorem 2.10. ■

References

[1] S. Akhtari and S. K. K. Choi, *On the Littlewood cyclotomic polynomials.* J. Number Theory **128**(2008), no. 4, 884–894. http://dx.doi.org/10.1016/j.jnt.2007.02.010

[2] A. Bloch and G. Pólya, *On roots of certain algebraic equations*. Proc. London Math. Soc., **S2-33**(1932), 102–114. http://dx.doi.org/10.1112/plms/s2-33.1.102

[3] P. Borwein and S. K. K. Choi, *On cyclotomic polynomials with* ± 1 *coefficients.* Experiment. Math. **8**(1999), no. 4, 399–407. http://dx.doi.org/10.1080/10586458.1999.10504628

[4] P. Borwein and T. Erdélyi, *On the zeros of polynomials with restricted coefficients*. Illinois J. Math. **41**(1997), 667–675.

[5] ———, *Lower bounds for the number of zeros of cosine polynomials in the period: a problem of Littlewood*. Acta Arith. **128**(2007), no. 4, 377–384. http://dx.doi.org/10.4064/aa128-4-5

[6] P. Borwein, T. Erdélyi, R. Ferguson, and R. Lockhart, *On the zeros of cosine polynomials: solution to a problem of Littlewood*. Ann. of Math. **167**(2008), no. 3, 1109–1117. http://dx.doi.org/10.4007/annals.2008.167.1109

[7] P. Borwein, T. Erdélyi, and F. Littmann, *Polynomials with coefficients from a finite set*. Trans. Amer. Math. Soc. **360**(2008), no. 10, 5145–5154. http://dx.doi.org/10.1090/S0002-9947-08-04605-9

[8] D. W. Boyd, *Small Salem numbers*. Duke Math. J. **44**(1977), no. 2, 315–328. http://dx.doi.org/10.1215/S0012-7094-77-04413-1

[9] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*. Ann. Inst. Fourier (Grenoble) **50**(2000), no. 3, 865–889. http://dx.doi.org/10.5802/aif.1776

[10] P. Drungilas, *Unimodular roots of reciprocal Littlewood polynomials*. J. Korean Math. Soc. **45**(2008), no. 3, 835–840. http://dx.doi.org/10.4134/JKMS.2008.45.3.835

[11] P. Erdős and P. Turán, *On the distribution of roots of polynomials*. Ann. of Math. **51**(1950), 105–119. http://dx.doi.org/10.2307/1969500

[12] J. Kovanlina and V. Matache, *Palindrome-polynomials with roots in the unit circle*. C.R. Math. Acad. Sci. Soc. R. Can. **26**(2004), 39–44.

[13] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 53(1857), 173–175.

[14] J. E. Littlewood, *On the mean values of certain trigonometric polynomials*. J. London Math. Soc. **36**(1961), 307–334. http://dx.doi.org/10.1112/jlms/s1-36.1.307

[15] ———, *On the real roots of real trigonometric polynomials. II*. J. London Math. Soc. **39**(1964), 511–532. http://dx.doi.org/10.1112/jlms/s1-39.1.511

[16] ———, *On polynomials* $\sum^n \pm z^m, \sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$. J. London Math. Soc. **41**(1966), 367–376. http://dx.doi.org/10.1112/jlms/s1-41.1.367

[17] ———, *The real zeros and value distributions of real trigonometric polynomials*. J. London Math. Soc. **41**(1966), 336–342. http://dx.doi.org/10.1112/jlms/s1-41.1.336

[18] ———, *Some problems in real and complex analysis*. Heath Mathematical Monographs, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.

[19] I. D. Mercer, *Unimodular roots of special Littlewood polynomials*. Canad. Math. Bull. **49**(2006), no. 3, 438–447. http://dx.doi.org/10.4153/CMB-2006-043-x

[20] M. J. Mossinghoff, C. G. Pinner, and J. D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*. Math. Comp. **67**(1998), no. 224, 1707–1726. http://dx.doi.org/10.1090/S0025-5718-98-01007-2

[21] K. Mukunda, *Littlewood Pisot numbers*. J. Number Theory **117**(2006), no. 1, 106–121. http://dx.doi.org/10.1016/j.jnt.2005.05.009
[22] ———, *Pisot and Salem numbers from polynomials of height* 1. PhD Thesis, Simon Fraser University, 2006.
[23] I. Schur, *Unteruchungen über algebraische Gleichungen.* Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 403–428.
[24] G. Szegő, *Bemerkungen zu einem Satz von E. Schmidt über algebraische Gleichungen.* Sitz Preuss. Akad. Wiss., Phys.-Math. Kl. (1934), 86–98.

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6
e-mail: pborwein@sfu.ca schoia@sfu.ca ronf@sfu.ca

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
e-mail: jonas.jankauskas@gmail.com