Annals of Mathematics **192** (2020), 977–1004
https://doi.org/10.4007/annals.2020.192.3.6

Flat Littlewood polynomials exist

By Paul Balister, Béla Bollobás, Robert Morris, Julian Sahasrabudhe, and Marius Tiba

Abstract

We show that there exist absolute constants $\Delta > \delta > 0$ such that, for all $n \geqslant 2$, there exists a polynomial P of degree n, with coefficients in $\{-1, 1\}$, such that

$$\delta\sqrt{n} \leqslant |P(z)| \leqslant \Delta\sqrt{n}$$

for all $z \in \mathbb{C}$ with $|z| = 1$. This confirms a conjecture of Littlewood from 1966.

1. Introduction

We say that a polynomial $P(z)$ of degree n is a *Littlewood polynomial* if

$$P(z) = \sum_{k=0}^{n} \varepsilon_k z^k,$$

where $\varepsilon_k \in \{-1, 1\}$ for all $0 \leqslant k \leqslant n$. The aim of this paper is to prove the following theorem, which answers a question of Erdős [15, Prob. 26] from 1957, and confirms a conjecture of Littlewood [26] from 1966.

Theorem 1.1. *There exist constants $\Delta > \delta > 0$ such that, for all $n \geqslant 2$, there exists a Littlewood polynomial $P(z)$ of degree n with*

$$\delta\sqrt{n} \leqslant |P(z)| \leqslant \Delta\sqrt{n} \tag{1}$$

for all $z \in \mathbb{C}$ with $|z| = 1$.

Polynomials satisfying (1) are known as *flat polynomials*, and Theorem 1.1 can therefore be more succinctly stated as follows: "flat Littlewood polynomials exist." It turns out that our main challenge will be to prove the lower bound

Keywords: Littlewood polynomials, discrepancy theory, probabilistic methods

AMS Classification: Primary: 42A05.

The first two authors were partially supported by NSF grant DMS 1855745, the third author was partially supported by CNPq (Proc. 303275/2013-8) and FAPERJ (Proc. 201.598/2014), and the fifth author was supported by a Trinity Hall Research Studentship.

on $|P(z)|$; indeed, explicit polynomials satisfying the upper bound in (1) have been known to exist since the work of Shapiro [41] and Rudin [37] over 60 years ago (see Section 3). In the 1980s a completely different (and non-constructive) proof of the upper bound was given by Spencer [42], who used a technique that had been developed a few years earlier by Beck [2] in his study of combinatorial discrepancy. We remark that the Rudin–Shapiro construction, and also ideas from discrepancy theory (see Section 4), will play key roles in our proof.

The study of Littlewood polynomials has a long and distinguished history (see, for example, [7] or [34]). The roots of their study go back to the work of Hardy and Littlewood [18] on Diophantine approximation over 100 years ago, the work of Bloch and Pólya [5] on the maximum number of real roots of polynomials with restricted coefficients, and the work of Littlewood and Offord [29], [30], [31] and others [16], [39] on random polynomials. Two important extremal problems that arose from these early investigations are Littlewood's L_1-problem [19], which was famously resolved (up to constant factors) in 1981 by McGehee, Pigno and Smith [33] and Konyagin [22], and Chowla's cosine problem [14]; see [8], [38].

The question studied in this paper was asked in 1957, by Erdős [15], and was then taken up (and extensively studied) by Littlewood [24], [25], [27], [26] in a series of papers on the extremal properties of polynomials with restricted coefficients. In particular, Littlewood conjectured in [26] that flat Littlewood polynomials exist. This problem was given particular consideration in his well-known 1968 monograph [28], where he lays out 30 of his favourite problems, which he had curated for himself and his students for more than 30 years. In the book, he details several failed approaches to the "fascinating" question of the existence of flat Littlewood polynomials and notes that he tried in vain to construct such polynomials.

Another well-known open problem, also proposed by Erdős [15] in the same problem paper, asks whether there exists a constant $c > 0$ such that, for every polynomial $P_n(z) = \sum_{k=0}^{n} a_k z^k$ with $a_k \in \mathbb{C}$ and $|a_k| = 1$ for all $0 \leqslant k \leqslant n$, we have

$$|P_n(z)| \geqslant (1+c)\sqrt{n}$$

for some $z \in \mathbb{C}$ with $|z| = 1$. (Note that, by a simple application of Parseval's theorem, the conclusion holds with $c = 0$.) Let us write $\mathcal{F}_n$ for the family of Littlewood polynomials of degree n, and $\mathcal{G}_n$ for the (larger) family with coefficients satisfying $|a_k| = 1$. The class $\mathcal{G}_n$ is significantly richer than $\mathcal{F}_n$, and for polynomials in this richer class, significant progress was made in the years following Littlewood's work. It had been known since the work of Hardy and Littlewood [18] that the upper bound in (1) holds for the polynomial in $\mathcal{G}_n$ given by setting $a_k := k^{ik}$, and Littlewood [25] proved that the polynomial in $\mathcal{G}_n$ given by setting $a_k := \exp\big(\binom{k+1}{2}\pi i/(n+1)\big)$ satisfies the stronger upper and lower bounds

$$|P(z)| = \big(1 + o(1)\big)\sqrt{n} \tag{2}$$

for all $z \in \mathbb{C}$ with $|z| = 1$ except in a small interval around $z = 1$. Following further progress in [4], [12] and building, in particular, on work of Körner [23], the second question of Erdős [15] mentioned above was answered by Kahane [21], who proved that there exist *ultra-flat* polynomials in $\mathcal{G}_n$, i.e., polynomials that satisfy (2) for all $z \in \mathbb{C}$ with $|z| = 1$. More recently, Bombieri and Bourgain [6] improved Kahane's bounds and, moreover, gave an effective construction of an ultra-flat polynomial in $\mathcal{G}_n$.

For the more restrictive class of Littlewood polynomials, much less progress has been made over the past 50 years. The Rudin–Shapiro polynomials mentioned above satisfy the upper bound in (1) with $\Delta = \sqrt{2}$ when $n = 2^t - 1$, and with $\Delta = \sqrt{6}$ in general (see [1]). However, the previously best-known lower bound, proved by Carroll, Eustice and Figiel [13] via a simple recursive construction, states that there exist Littlewood polynomials $P_n(z) \in \mathcal{F}_n$ with $|P_n(z)| \geqslant n^{0.431}$ for all sufficiently large $n \in \mathbb{N}$. Moreover, exhaustive search for small values of n (see [35]) suggests that ultra-flat Littlewood polynomials most likely do not exist. Let us mention one final interesting result in the direction of Littlewood's conjecture, due to Beck [3], who proved that there exist flat polynomials in $\mathcal{G}_n$ with $a_k^{400} = 1$ for every k.

In the next section, we outline the general strategy that we will use to prove Theorem 1.1. Roughly speaking, our Littlewood polynomial will consist (after multiplication by a suitable negative power of z) of a real cosine polynomial that is based on the Rudin–Shapiro construction, and an imaginary sine polynomial that is designed to be large in the (few) places where the cosine polynomial is small. To be slightly more precise, we will attempt to "push" the sine polynomial far away from zero in these few dangerous places, using techniques from discrepancy theory to ensure that we can do so. In order to make this argument work, it will be important that the intervals on which the Rudin–Shapiro construction is small are "well separated" (see Definition 2.2). The properties of the cosine polynomial that we need are stated in Theorem 2.3 and proved in Section 3; the properties of the sine polynomial are stated in Theorem 2.4 and proved in Section 5.

2. Outline of the proof

We may assume that n is sufficiently large, since the polynomial $1 - z - z^2 - \cdots - z^n$ has no roots with $|z| = 1$ if $n \geqslant 2$. It will also suffice to prove Theorem 1.1 for $n \equiv 0 \pmod 4$, since the addition of a constant number of terms of the form $\pm z^k$ can at worst only change $|P(z)|$ by an additive constant. We can also multiply the polynomial by $z^{-2n'}$ so that it becomes the centred

"Laurent polynomial"

$$\sum_{k=-2n'}^{2n'} \varepsilon_k z^k,$$

where $n = 4n'$. The following theorem therefore implies Theorem 1.1.

THEOREM 2.1. *For every sufficiently large $n \in \mathbb{N}$, there exists a Littlewood polynomial $P(z) = \sum_{k=-2n}^{2n} \varepsilon_k z^k$ such that*

$$2^{-160}\sqrt{n} \leqslant |P(z)| \leqslant 2^{12}\sqrt{n}$$

for all $z \in \mathbb{C}$ with $|z| = 1$.

We remark that the constants in Theorem 2.1 could be improved somewhat, but we have instead chosen to (slightly) simplify the exposition wherever possible.

2.1. *Strategy.* Before embarking on the technical details of the proof, let us begin by giving a rough outline of the strategy that we will use to prove Theorem 2.1. The first idea is to choose a set $C \subseteq [2n] = \{1, \ldots, 2n\}$, and set $\varepsilon_{-k} = \varepsilon_k$ for each $k \in C$, and $\varepsilon_{-k} = -\varepsilon_k$ for each $k \in S := [2n] \setminus C$. Setting $z = e^{i\theta}$, the polynomial $P(z)$ then decomposes as

$$\sum_{k=-2n}^{2n} \varepsilon_k z^k = \varepsilon_0 + 2\sum_{k\in C} \varepsilon_k \cos(k\theta) + 2i \sum_{k \in S} \varepsilon_k \sin(k\theta).$$

The real part of this expression is a cosine polynomial, while the imaginary part is a sine polynomial. Our aim is to choose the sine and cosine polynomials so that both are $O(\sqrt{n})$ for all θ, and so that the sine polynomial is large whenever the cosine polynomial is small.

Let us first describe our rough strategy for choosing the sine polynomial $s(\theta)$, given a suitable cosine polynomial $c(\theta)$. For each "bad" interval $I \subseteq \mathbb{R}/2\pi\mathbb{Z}$ on which $|c(\theta)| < \delta\sqrt{n}$, we will choose a direction (positive or negative) and attempt to "push" the sine polynomial in that direction on that interval. In other words, we pick a step function that is $\pm K\sqrt{n}$ on each of the bad intervals, and zero elsewhere, where K is a large constant. We then attempt to approximate this step function with a sine polynomial, the hope being that we can do so with an error of size $O(\sqrt{n})$ on each bad interval (independent of K).

In order to carry out this plan, we will use an old result[1] of Spencer [42] on combinatorial discrepancy (in the form of Corollary 4.2), first to choose the step function, and then to show that we can approximate it sufficiently closely.

[1]We will in fact find it convenient to use a variant of Spencer's theorem, due to Lovett and Meka [32].

More precisely, the first application (see Lemma 5.3) provides us with a step function whose Fourier coefficients are all small, and the second application (see Lemmas 5.4 and 5.5) then produces a sine polynomial that does not deviate by more than $O(\sqrt{n})$ from this step function.

To make the sketch above rigorous, we will need the bad intervals to have a number of useful properties; roughly speaking, they should be "few," "small," and "well separated." In particular, we will construct (see Definition 2.2 and Theorem 2.3) a set $\mathcal{I}$ of intervals, each of size $O(1/n)$, separated by gaps of size $\Omega(1/n)$, with $|c(\theta)| \geqslant \delta\sqrt{n}$ for all $\theta \notin \bigcup_{I\in\mathcal{I}} I$. Moreover, the number of intervals in $\mathcal{I}$ will be at most γn for some small constant $\gamma > 0$.

To see that these demands are not unreasonable, note first that if $C \subseteq [\gamma n]$, then the cosine polynomial has few roots, and the "typical" value of the derivative of the cosine polynomial should be $\Theta((\gamma n)^{3/2})$. This means that, if we choose δ much smaller than γ, the polynomial should typically vary by more than $\delta\sqrt{n}$ over a distance of order $1/n$. In particular, we will show that if the set of bad intervals cannot be covered by a collection of small and well-separated intervals (in the sense described above), then several of the derivatives must be small simultaneously. For our cosine polynomial, we shall use an explicit construction based on the Rudin–Shapiro polynomials (see Section 3), and we will show (see Lemma 3.5) that the value and first three derivatives of this polynomial cannot all be simultaneously small.

2.2. *The cosine polynomial.* Let $n \in \mathbb{N}$ be sufficiently large, choose $2^{-43} < \gamma \leqslant 2^{-40}$ such that

$$\gamma n = 2^{t+11} + 2^t - 1 \tag{3}$$

for some *odd* integer t, and set

$$\delta := 2^{-8}\gamma^{7/2},$$

noting that $\delta > 2^{-160}$. Define $C \subseteq [2\gamma n]$ by setting $C = 2C'$, where

$$C' := \{2^{t+10}, \dots, 2^{t+10} + 2^t - 1\} \cup \{2^{t+11}, \dots, 2^{t+11} + 2^t - 1\},$$

so that C is a set of 2^{t+1} *even* integers. Our first aim is to construct a cosine polynomial

$$c(\theta) = \sum_{k\in C} \varepsilon_k \cos(k\theta)$$

that is only small on a few, well-separated intervals and is never too large.

To state the two main steps in the proof of Theorem 2.1, we first need to define what we mean by a "suitable" and "well-separated" family of intervals.

Definition 2.2. Let $\mathcal{I}$ be a collection of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$. We will say that $\mathcal{I}$ is *suitable* if

(a) the endpoints of each interval in $\mathcal{I}$ lie in $\frac{\pi}{n}\mathbb{Z}$;

(b) $\mathcal{I}$ is invariant under the maps $\theta \mapsto \pi \pm \theta$;
(c) $|\mathcal{I}| = 4N$ for some $N \leqslant \gamma n$.

We say that a suitable collection $\mathcal{I}$ is *well separated* if

(d) $|I| \leqslant 6\pi/n$ for each $I \in \mathcal{I}$;
(e) $d(I, J) \geqslant \pi/n$ for each $I, J \in \mathcal{I}$ with $I \neq J$;[2]
(*f*) $\bigcup_{I \in \mathcal{I}} I$ is disjoint from the set $(\pi/2)\mathbb{Z} + [-100\pi/n, 100\pi/n]$.

We will prove the following theorem about cosine polynomials.

THEOREM 2.3. *There exists a cosine polynomial*

$$c(\theta) = \sum_{k \in C} \varepsilon_k \cos(k\theta),$$

with $\varepsilon_k \in \{-1, 1\}$ *for every* $k \in C$, *and a suitable and well-separated collection* $\mathcal{I}$ *of disjoint intervals in* $\mathbb{R}/2\pi\mathbb{Z}$, *such that*

$$|c(\theta)| \geqslant \delta\sqrt{n}$$

for all $\theta \notin \bigcup_{I \in \mathcal{I}} I$ *and* $|c(\theta)| \leqslant \sqrt{n}$ *for all* $\theta \in \mathbb{R}/2\pi\mathbb{Z}$.

The cosine polynomial we will use to prove Theorem 2.3 is a slight modification of the Rudin–Shapiro polynomial. We might remark here that one would expect almost any cosine polynomial whose absolute value is $O(\sqrt{n})$ to satisfy somewhat similar conditions, but this seems difficult to prove in general.

2.3. *The sine polynomials.* There will in fact be two sine polynomials; the first,

$$s_e(\theta) = \sum_{j \in S_e} \varepsilon_j \sin(j\theta), \tag{4}$$

will just be chosen to be small everywhere, more precisely at most $6\sqrt{n}$ for all $|z| = 1$ (see Lemma 3.3). It is defined on the set $S_e = 2S_e'$, where

$$S_e' := [n] \setminus C'$$

so that S_e is the set of remaining even integers in $[2n]$.

We write $S_o := \{1, 3, \ldots, 2n - 1\}$ for the set of all the odd integers in $[2n]$, and our main task will be to construct an "odd sine polynomial"

$$s_o(\theta) = \sum_{k \in S_o} \varepsilon_k \sin(k\theta)$$

that is large on each $I \in \mathcal{I}$ and not too large elsewhere. To be precise, we shall prove the following theorem.

[2]Given two sets $I, J \subseteq \mathbb{R}/2\pi\mathbb{Z}$, let us write $d(I, J) := \inf\{d(\theta, \theta') : \theta \in I,\ \theta' \in J\}$, where $d(\theta, \theta')$ is the distance between θ and θ' mod 2π.

THEOREM 2.4. *Let $\mathcal{I}$ be a suitable and well-separated collection of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$. There exists a sine polynomial*

$$s_o(\theta) = \sum_{k \in S_o} \varepsilon_k \sin(k\theta),$$

with $\varepsilon_k \in \{-1, 1\}$ for every $k \in S_o$, such that

(i) $|s_o(\theta)| \geqslant 10\sqrt{n}$ *for all* $\theta \in \bigcup_{I \in \mathcal{I}} I$, *and*
(ii) $|s_o(\theta)| \leqslant 2^{10}\sqrt{n}$ *for all* $\theta \in \mathbb{R}$.

To deduce Theorem 2.1 from the results above, we simply set

$$P(e^{i\theta}) := \big(1 + 2c(\theta)\big) + 2i\big(s_e(\theta) + s_o(\theta)\big),$$

where $c(\theta)$ and $s_o(\theta)$ are the cosine and sine polynomials given by Theorems 2.3 and 2.4 respectively, and $s_e(\theta)$ is a sine polynomial as in (4); see Section 5 for the details.

The rest of the paper is organised as follows. First, in Section 3, we will define $c(\theta)$ and $s_e(\theta)$ and prove Theorem 2.3. In Section 4 we will recall the main lemma from [32] and deduce Corollary 4.2; this will be our main tool in the proof of Theorem 2.4, which is given in Section 5. Finally, we will conclude by completing the proof of Theorem 2.1.

3. Rudin–Shapiro polynomials

In this section we will define the cosine polynomial that we will use to prove Theorem 2.3 and the sine polynomial that we will use on the remaining even integers. In both cases, we use the so-called Rudin–Shapiro polynomials, which were introduced independently by Shapiro [41] and Rudin [37] (and whose sequence of coefficients was also previously studied by Golay [17]). These polynomials have been extensively studied over the last few decades; see, e.g., [9], [10], [11], [36]. Let us begin by recalling their definition.

Definition 3.1 (Rudin–Shapiro polynomials). Set $P_0(z) = Q_0(z) = 1$, and inductively define

$$P_{t+1}(z) = P_t(z) + z^{2^t} Q_t(z),$$
$$Q_{t+1}(z) = P_t(z) - z^{2^t} Q_t(z)$$

for each $t \geqslant 0$.

Observe that $P_t(z)$ and $Q_t(z)$ are both Littlewood polynomials of degree $2^t - 1$. A simple induction argument (see, e.g., [34]) shows that $P_t(z)P_t(1/z) + Q_t(z)Q_t(1/z) = 2^{t+1}$ for all $z \in \mathbb{C} \setminus \{0\}$. It follows that

$$|P_t(z)|^2 + |Q_t(z)|^2 = 2^{t+1}, \qquad (5)$$

and hence $|P_t(z)|, |Q_t(z)| \leqslant 2^{(t+1)/2}$, for every $z \in \mathbb{C}$ with $|z| = 1$. Observing that the first 2^t terms of P_{t+1} are the same as for P_t, let us write $P_{<n}(z)$ for the polynomial of degree $n-1$ that agrees with $P_t(z)$ on the first n terms for all sufficiently large t, and note that $P_t(z) = P_{<2^t}(z)$. The following bound, which is a straightforward consequence of (5), was proved by Shapiro [41]. (Stronger bounds are known — see [1] — but we shall not need them.)

Lemma 3.2. *We have* $|P_{<n}(z)| \leqslant 5\sqrt{n}$ *for every* $z \in \mathbb{C}$ *with* $|z| = 1$.

We now set

$$T := 2^{t+10}.$$

We define our cosine polynomial to be

$$c(\theta) := \operatorname{Re}\big(z^T P_t(z) + z^{2T} Q_t(z)\big), \tag{6}$$

and our even sine polynomial to be

$$s_e(\theta) := \operatorname{Im}\big(P_{<(n+1)}(z) - z^T P_t(z) - z^{2T} P_t(z)\big), \tag{7}$$

where in both cases $z = e^{2i\theta}$. (Note the factor of 2 in the exponent here.) We claim first that[3] $\operatorname{supp}(c) = C$ and $\operatorname{supp}(s_e) = S_e$. This is clear for c, since $C = 2C'$ and $C' = \{T, \ldots, T + 2^t - 1\} \cup \{2T, \ldots, 2T + 2^t - 1\}$; for s_e, it follows since the terms of $P_{<(n+1)}(z)$ corresponding to C' form the polynomial $z^T P_t(z) + z^{2T} P_t(z)$. (To see this, simply consider the first time that these terms appear in Definition 3.1, and note that the first 2^t terms of both P_{t+10} and Q_{t+10} are the same as for P_t.) We remark that the idea behind the definition of $c(\theta)$ is that the highly oscillatory factors z^T and z^{2T} allow us to show that c and its first three derivatives cannot all simultaneously be small (see Lemma 3.5).

The following lemma is an almost immediate consequence of Lemma 3.2 and (5).

Lemma 3.3. *We have* $|c(\theta)| \leqslant \sqrt{n}$ *and* $|s_e(\theta)| \leqslant 6\sqrt{n}$ *for every* $\theta \in \mathbb{R}$.

Proof. Observe first that, setting $z := e^{2i\theta}$, we have

$$|c(\theta)| \leqslant |P_t(z)| + |Q_t(z)| \leqslant 2^{(t+3)/2} \leqslant \sqrt{n},$$

where the first inequality follows from the definition of c, the second holds by (5), and the last holds by (3), since $\gamma \leqslant 1$. Similarly, we have

$$|s_e(\theta)| \leqslant |P_{<(n+1)}(z)| + 2|P_t(z)| \leqslant 5\sqrt{n+1} + 2^{(t+3)/2} \leqslant 6\sqrt{n},$$

where the first inequality follows from the definition of s_e, the second holds by Lemma 3.2 and (5), and the last holds by (3). □

[3] We define the *support*, $\operatorname{supp}(f)$, of a sine polynomial $f(\theta) = \sum_{k>0} \varepsilon_k \sin(k\theta)$ or cosine polynomial $f(\theta) = \sum_{k>0} \varepsilon_k \cos(k\theta)$ to be the set of k such that $\varepsilon_k \neq 0$.

In order to prove Theorem 2.3, it remains to show that $|c(\theta)| \geqslant \delta\sqrt{n}$ for all $\theta \notin \bigcup_{I\in\mathcal{I}} I$ for some suitable and well-separated collection $\mathcal{I}$ of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$. When doing so we will find it convenient to rescale the polynomial as follows: define a function $H\colon \mathbb{R} \to \mathbb{C}$ by setting

$$H(x) := e^{ix}\alpha(x) + e^{2ix}\beta(x),$$

where

$$\alpha(x) := 2^{-(t+1)/2} P_t(e^{ix/T}) \qquad \text{and} \qquad \beta(x) := 2^{-(t+1)/2} Q_t(e^{ix/T}),$$

and observe that

$$c(\theta) = 2^{(t+1)/2}\ \mathrm{Re}\big(H(2T\theta)\big).$$

Note that, by (5), we have

$$|\alpha(x)|^2 + |\beta(x)|^2 = 1.$$

We think of $\alpha(x)$ and $\beta(x)$ as being slowly varying functions, relative to the much more rapidly varying exponential factors in the definition of $H(x)$.

The key property of the polynomial $c(\theta)$ that we will need is given by the following lemma.

Lemma 3.4. *Let $0 < \eta < 2^{-11}$. Every interval $I \subseteq \mathbb{R}$ of length 7η contains a sub-interval $J \subseteq I$ of length η such that*

$$\big|\ \mathrm{Re}\big(H(x)\big)\big| \geqslant \frac{\eta^3}{2^7}$$

for every $x \in J$. Moreover, if $I = [a, a + 7\eta]$, then we can take $J = [a + j\eta, a + (j + 1)\eta]$ for some $j \in \{0, 1, \ldots, 6\}$.

To prove Lemma 3.4, we will first need to prove the following lemma.

Lemma 3.5. *For any $x \in \mathbb{R}$, there exists $k \in \{0, 1, 2, 3\}$ such that*

$$\big|\ \mathrm{Re}\big(H^{(k)}(x)\big)\big| \geqslant \frac{1}{4}.$$

The proof of Lemma 3.5 is not very difficult, but we will need to work a little. We will use Bernstein's classical inequality (see, e.g., [40]), which states that if $f(z)$ is a polynomial of degree n, then

$$\max_{|z|=1} |f'(z)| \leqslant n \cdot \max_{|z|=1} |f(z)|. \tag{8}$$

This easily implies the following bound on the derivatives of the Rudin–Shapiro polynomials.

Lemma 3.6. *Let $0 \leqslant k, t \in \mathbb{Z}$. We have*

$$\left|\frac{d^k}{d\theta^k} P_t(e^{i\theta})\right|, \left|\frac{d^k}{d\theta^k} Q_t(e^{i\theta})\right| \leqslant 2^{kt+(t+1)/2} \tag{9}$$

for every $\theta \in \mathbb{R}$. *In particular,*

$$|\alpha^{(k)}(x)|,\, |\beta^{(k)}(x)| \leqslant 2^{-10k} \tag{10}$$

for every $k \geqslant 1$ *and* $x \in \mathbb{R}$.

Note that (10) justifies our intuition that $\alpha(x)$ and $\beta(x)$ vary relatively slowly.

Proof. To prove (9) we simply apply (8) k times and (5) once. It follows from (9) that

$$\max\left\{|\alpha^{(k)}(x)|,\, |\beta^{(k)}(x)|\right\} \leqslant 2^{-(t+1)/2} \cdot T^{-k} \cdot 2^{kt+(t+1)/2} = 2^{-10k}$$

for every $k \geqslant 1$ and $x \in \mathbb{R}$, as claimed. □

We will use the following easy consequences of Lemma 3.6.

LEMMA 3.7. *For each* $0 \leqslant k \leqslant 4$, *and every* $x \in \mathbb{R}$, *we have*

$$\left|H^{(k)}(x) - \left(i^k e^{ix}\alpha(x) + (2i)^k e^{2ix}\beta(x)\right)\right| \leqslant \frac{1}{8}$$

and

$$|H^{(k)}(x)| \leqslant 2^k + 2.$$

Proof. Since $H(x) = e^{ix}\alpha(x) + e^{2ix}\beta(x)$, we have

$$H^{(k)}(x) = \sum_{j=0}^{k} \binom{k}{j} \left(i^{k-j} e^{ix}\alpha^{(j)}(x) + (2i)^{k-j} e^{2ix}\beta^{(j)}(x)\right),$$

and hence, using (10),

$$\left|H^{(k)}(x) - \left(i^k e^{ix}\alpha(x) + (2i)^k e^{2ix}\beta(x)\right)\right| \leqslant \sum_{j=1}^{k} \binom{k}{j} \left(1 + 2^{k-j}\right) 2^{-10j} \leqslant \frac{1}{8}$$

(with room to spare) since $k \leqslant 4$. Since $|i^k e^{ix}\alpha(x) + (2i)^k e^{2ix}\beta(x)| \leqslant 1 + 2^k$, it follows immediately that

$$|H^{(k)}(x)| \leqslant 2^k + 2,$$

as claimed. □

We can now easily deduce Lemma 3.5.

Proof of Lemma 3.5. Suppose that

$$\left|\operatorname{Re}\left(H^{(k)}(x)\right)\right| < \frac{1}{4}$$

for each $k \in \{0, 1, 2, 3\}$. Setting

$$E_k := \operatorname{Re}\left(i^k e^{ix}\alpha(x) + (2i)^k e^{2ix}\beta(x)\right),$$

observe that

$$\operatorname{Re}\left(e^{ix}\alpha(x)\right) = \frac{4E_0 + E_2}{3}, \qquad \operatorname{Re}\left(e^{2ix}\beta(x)\right) = -\frac{E_0 + E_2}{3},$$

$$\operatorname{Im}\left(e^{ix}\alpha(x)\right) = -\frac{4E_1 + E_3}{3}, \qquad \text{and} \qquad \operatorname{Im}\left(e^{2ix}\beta(x)\right) = \frac{E_1 + E_3}{6}.$$

Now, by Lemma 3.7, we have

$$|E_k| \leqslant \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$$

for each $k \in \{0, 1, 2, 3\}$, and therefore

$$\begin{aligned} 1 &= |\alpha(x)|^2 + |\beta(x)|^2 \\ &= \left|\operatorname{Re}\left(e^{ix}\alpha(x)\right)\right|^2 + \left|\operatorname{Im}\left(e^{ix}\alpha(x)\right)\right|^2 + \left|\operatorname{Re}\left(e^{2ix}\beta(x)\right)\right|^2 + \left|\operatorname{Im}\left(e^{2ix}\beta(x)\right)\right|^2 \\ &\leqslant \left(\frac{5^2}{3^2} + \frac{5^2}{3^2} + \frac{2^2}{3^2} + \frac{2^2}{6^2}\right) \cdot \frac{3^2}{8^2} = \frac{55}{9} \cdot \frac{9}{64} < 1, \end{aligned}$$

which is a contradiction. It follows that $|\operatorname{Re}(H^{(k)}(x_0))| \geqslant 1/4$ for some $0 \leqslant k \leqslant 3$. □

To deduce Lemma 3.4 from Lemmas 3.5 and 3.7, we shall use a generalization of Lagrange interpolation from [20, Th. 2] that bounds the higher derivatives of a function in terms of its values at certain points.

THEOREM 3.8. *Let $f\colon I \to \mathbb{R}$ be a $k+1$ times continuously differentiable function, and suppose $y_0, \ldots, y_k \in I$ with $y_0 < y_1 < \cdots < y_k$. Then*[4]

$$\left\| f^{(k)}(x) - \sum_{i=0}^{k} \frac{k!f(y_i)}{\prod_{j \neq i}(y_i - y_j)} \right\|_\infty \leqslant \left\| x - \frac{1}{k+1}\sum_{i=0}^{k} y_i \right\|_\infty \cdot \|f^{(k+1)}(x)\|_\infty.$$

Lemma 3.4 is a straightforward consequence of Lemmas 3.5 and 3.7 and Theorem 3.8.

Proof of Lemma 3.4. Let $I = [a, a+7\eta]$, and suppose (for a contradiction) that for each $0 \leqslant j \leqslant 6$, there exists a point

$$x_j \in I_j := \left[a + j\eta,\, a + (j+1)\eta\right]$$

such that $|\operatorname{Re}(H(x_j))| < 2^{-7}\eta^3$. We will show that $|\operatorname{Re}(H^{(k)}(x_0))| < 1/4$ for each $0 \leqslant k \leqslant 3$, which will contradict Lemma 3.5, and hence prove the lemma.

For $k = 0$, we have $|\operatorname{Re}(H^{(k)}(x_0))| < 2^{-7}\eta^3 < 1/4$ (by assumption), so let $k \in \{1, 2, 3\}$. By Lemma 3.7 and Theorem 3.8, applied with $f := \operatorname{Re}(H)$ and

---

[4]In the notation of [20], the sum in the first $\|\cdot\|_\infty$ expression is $L^{(k)}(x)$, where $L(x) = \sum_i f(y_i)\prod_{j\neq i}(x - y_j)/(y_i - y_j)$, and the second $\|\cdot\|_\infty$ expression is $\|\omega^{(k)}(x)/(k+1)!\|_\infty$, where $\omega(x) = \prod_i(x - y_i)$. Note that the inequality is tight when $f(x) = \omega(x)$.

$y_j := x_{2j}$ for each $0 \leqslant j \leqslant k$ (so, in particular, $|y_i - y_j| \geqslant \eta$ for all $i \neq j$), we have

$$\big|\operatorname{Re}\big(H^{(k)}(x_0)\big)\big| \leqslant \sum_{i=0}^{k} \frac{k!}{\eta^k} \cdot \frac{\eta^3}{2^7} + 7\eta \cdot \big\|\operatorname{Re}\big(H^{(k+1)}(x)\big)\big\|_\infty$$
$$\leqslant \frac{4 \cdot 3!}{2^7} + \frac{7(2^4+2)}{2^{11}} < \frac{1}{4},$$

since $\eta < 2^{-11}$, as required. □

Finally, in order to show that $\bigcup_{I \in \mathcal{I}} I$ is disjoint from the set $(\pi/2)\mathbb{Z} + [-100\pi/n, 100\pi/n]$, we will need the following simple lemma.

Lemma 3.9. *If* $|x| \leqslant 1/8$ *or* $|x - T\pi| \leqslant 1/8$, *then* $\operatorname{Re}\big(H(x)\big) \geqslant 1/2$.

Proof. We will use the following facts (cf. [10, Th. 5]), which can be easily verified by induction: for every $t \geqslant 0$,

$$P_{2t}(1) = P_{2t}(-1) = Q_{2t}(1) = -Q_{2t}(-1) = 2^t,$$

and

$$P_{2t+1}(1) = Q_{2t+1}(-1) = 2^{t+1}, \qquad P_{2t+1}(-1) = Q_{2t+1}(1) = 0.$$

Since t is odd, it follows that

$$\operatorname{Re}\big(H(0)\big) = 2^{-(t+1)/2}\big(P_t(1) + Q_t(1)\big) = 1$$

and

$$\operatorname{Re}\big(H(T\pi)\big) = 2^{-(t+1)/2}\big(P_t(-1) + Q_t(-1)\big) = 1.$$

Now, by Lemma 3.7 we have $|H'(x)| \leqslant 4$ for every $x \in \mathbb{R}$, and so

$$\operatorname{Re}\big(H(x)\big) \geqslant 1 - 4|x| \geqslant \frac{1}{2}$$

for all $x \in \mathbb{R}$ with $|x| \leqslant 1/8$. A similar argument works for those x near $T\pi$. □

Remark 3.10. Note that $x = T\pi$ corresponds to $\theta = \pi/2$ in the cosine polynomial $c(\theta)$. The reader may have noticed that we do not necessarily need the cosine polynomial to be large at this point, as the sine polynomial can be large there. However, for technical reasons, this will be useful later on, in the proof of Lemma 5.6.

We are finally ready to prove Theorem 2.3.

Proof of Theorem 2.3. Let $c(\theta)$ be the cosine polynomial defined in (6), and recall that $\operatorname{supp}(c) = C$, that $\varepsilon_k \in \{-1, 1\}$ for every $k \in C$, and that $|c(\theta)| \leqslant \sqrt{n}$ for every $\theta \in \mathbb{R}/2\pi\mathbb{Z}$, by Lemma 3.3. We will show that there exists a suitable and well-separated collection $\mathcal{I}$ of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$ such that $|c(\theta)| \geqslant \delta\sqrt{n}$ for all $\theta \notin \bigcup_{I \in \mathcal{I}} I$.

To prove this, set $\eta := 2T\pi/n$, and note that $\eta < \pi\gamma < 2^{-11}$. Partition $\mathbb{R}/4T\pi\mathbb{Z} = \mathbb{R}/2n\eta\mathbb{Z}$ into $2n$ intervals $I_j := [j\eta, (j+1)\eta]$, each of length η, and say that an interval I_j is *good* if

$$\big|\operatorname{Re}\big(H(x)\big)\big| \geqslant \frac{\eta^3}{2^7}$$

for all $x \in I_j$. Let $\mathcal{J}'$ be the collection of maximal unions of consecutive good intervals I_j, and let $\mathcal{I}'$ be the collection of remaining intervals (i.e., maximal unions of consecutive bad intervals). Thus $\mathcal{I}'$ and $\mathcal{J}'$ form interleaving collections of intervals decomposing $\mathbb{R}/4T\pi\mathbb{Z}$. Scaling from x to $\theta = x/2T$ gives corresponding collections of intervals $\mathcal{I}$ and $\mathcal{J}$; we claim that $\mathcal{I}$ is the required suitable and well-separated collection.

First, to see that $\mathcal{I}$ is suitable, note that each interval I_j (and hence each $I \in \mathcal{I}'$) starts and ends at a multiple of $\eta = 2T\pi/n$. Hence after scaling, each $I \in \mathcal{I}$ starts and ends at points of $\frac{\pi}{n}\mathbb{Z}$. The set $\mathcal{I}$ is invariant under the maps $\theta \mapsto \pi \pm \theta$ by the symmetries of the function $\cos(k\theta)$ when $k \in C \subseteq 2\mathbb{Z}$. To see that $|\mathcal{I}| \leqslant 4\gamma n$, note that since a cosine polynomial of degree d has at most $2d$ roots in its period, there are at most $4(2T + 2^t - 1) = 4\gamma n$ values of $x \in \mathbb{R}/4T\pi\mathbb{Z}$ where $\operatorname{Re}(H(x)) = 2^{-7}\eta^3$, and the same bound on the number where $\operatorname{Re}(H(x)) = -2^{-7}\eta^3$. Since each $I \in \mathcal{I}'$ must contain at least two such points (counted with multiplicity), we have $|\mathcal{I}| = |\mathcal{I}'| \leqslant 4\gamma n$, as required.

Next, let us show that $\mathcal{I}$ is well separated. Recall first that, by Lemma 3.4, any set of seven consecutive intervals I_j must contain a good interval. Thus $|I| \leqslant 6\eta$ for each $I \in \mathcal{I}'$, and so $|I| \leqslant 6\pi/n$ for each $I \in \mathcal{I}$. Now, $d(I,J) \geqslant \pi/n$ for distinct $I, J \in \mathcal{I}$ by construction, and the sets $[-100\eta, 100\eta]$ and $T\pi + [-100\eta, 100\eta]$ are each contained in an element of $\mathcal{J}'$ by Lemma 3.9, since $2^{-7}\eta^3 < 1/2$ and $100\eta < 1/8$. Scaling down, it follows that $\bigcup_{I\in\mathcal{I}} I$ is disjoint from the set $(\pi/2)\mathbb{Z} + [-100\pi/n, 100\pi/n]$, as required.

Finally, recalling that $\eta = 2T\pi/n$, $\gamma n = 2T + 2^t - 1$, $T = 2^{t+10}$, and that $|\operatorname{Re}(H(x))| \geqslant 2^{-7}\eta^3$ for each $x \in J \in \mathcal{J}'$, it follows that

$$|c(\theta)| \geqslant 2^{(t+1)/2} \cdot 2^{-7}\eta^3 = 2^{-12}\pi^3(2T)^{7/2}/n^3 \geqslant 2^{-8}\gamma^{7/2}\sqrt{n} = \delta\sqrt{n}$$

for every $\theta \notin \bigcup_{I\in\mathcal{I}} I$, as required. □

4. Minimising discrepancy

In this section we recall the main "partial colouring" lemma of Spencer [42] (whose proof, as noted in the introduction, was based on a technique of Beck [2]), which will play an important role in the proof of Theorem 2.4. In particular, we will use the results of this section both to choose in which direction we should "push" the sine polynomial on each interval $I \in \mathcal{I}$, and to show that we can choose $\varepsilon_k \in \{-1, 1\}$ so that it is pushed (roughly) the correct distance. The following convenient variant of Spencer's theorem was proved by Lovett and Meka [32, Th. 4],[5] who also gave a beautiful polynomial-time randomised algorithm for finding a colouring with small discrepancy.

THEOREM 4.1 (Main Partial Colouring Lemma). *Let* $v_1, \dots, v_m \in \mathbb{R}^n$ *and* $x_0 \in [-1,1]^n$. *If* $c_1, \dots, c_m \geqslant 0$ *are such that*

$$\sum_{j=1}^{m} \exp\big(-c_j^2/16\big) \leqslant \frac{n}{16},$$

then there exists an $x \in [-1,1]^n$ *such that*

$$|\langle x - x_0, v_j \rangle| \leqslant c_j \|v_j\|_2$$

for every $j \in [m]$ *and, moreover,* $x_i \in \{-1,1\}$ *for at least* $n/2$ *indices* $i \in [n]$.

We will in fact use the following corollary of Theorem 4.1.

COROLLARY 4.2. *Let* $v_1, \dots, v_m \in \mathbb{R}^n$ *and* $x_0 \in [-1,1]^n$. *If* $c_1, \dots, c_m \geqslant 0$ *are such that*

$$\sum_{j=1}^{m} \exp\big(-c_j^2/14^2\big) \leqslant \frac{n}{16}, \tag{11}$$

then there exists an $x \in \{-1,1\}^n$ *such that*

$$|\langle x - x_0, v_j \rangle| \leqslant (c_j + 30)\sqrt{n} \cdot \|v_j\|_\infty$$

for every $j \in [m]$.

Proof. We prove Corollary 4.2 by induction on n. Note first that the result is trivial for all $n \leqslant 900$, since we can choose $x \in \{-1,1\}^n$ with $\|x - x_0\|_\infty \leqslant 1$, and for such a vector we have $|\langle x - x_0, v_j \rangle| \leqslant n \cdot \|v_j\|_\infty \leqslant 30\sqrt{n} \cdot \|v_j\|_\infty$.

For $n > 900$, we apply Theorem 4.1 with constants $b_j := 2c_j/7$, noting that

$$\sum_{j=1}^{m} \exp\big(-b_j^2/16\big) = \sum_{j=1}^{m} \exp\big(-c_j^2/14^2\big) \leqslant \frac{n}{16}.$$

We obtain a vector $y \in [-1,1]^n$, with

$$|\langle y - x_0, v_j \rangle| \leqslant b_j \|v_j\|_2 \leqslant b_j \sqrt{n} \cdot \|v_j\|_\infty$$

for every $j \in [m]$, such that $y_i \in \{-1,1\}$ for at least $n/2$ indices $i \in [n]$.

[5] The theorem as stated in [32] only insists that $|x_i| \geqslant 1 - \delta$ for at least $n/2$ indices, due to the requirement that a fast algorithm exists. However, it is clear by continuity that we can take $\delta = 0$ if we are only interested in an "existence proof."

Now, let $U \subseteq [n]$ be a set of size $\lceil n/2 \rceil$ such that $y_i \in \{-1, 1\}$ for every $i \in U$, and set $W := [n] \setminus U$. For each $j \in [m]$, define a constant $a_j \geqslant 0$ so that

$$a_j^2 := c_j^2 + 14^2 \log\left(\frac{n}{\lfloor n/2 \rfloor}\right),$$

and observe that

$$\sum_{j=1}^{m} \exp\left(-a_j^2/14^2\right) \leqslant \frac{\lfloor n/2 \rfloor}{16} = \frac{|W|}{16},$$

and that $a_j \leqslant c_j + 12$, since $14^2 \log(n/\lfloor n/2 \rfloor) < 196 \log 2.01 < 12^2$ for $n > 900$.

Let $\pi\colon \mathbb{R}^n \to \mathbb{R}^W$ be projection onto the coordinates of W. By the induction hypothesis, we obtain a vector $z \in \{-1, 1\}^W$ with

$$|\langle z - \pi(y), \pi(v_j)\rangle| \leqslant (a_j + 30)\sqrt{|W|} \cdot \|\pi(v_j)\|_\infty \leqslant (a_j + 30)\sqrt{n/2} \cdot \|v_j\|_\infty.$$

Now, define $x \in \{-1, 1\}^n$ by setting $x_i := y_i$ for $i \in U$ and $\pi(x) = z$, and observe that

$$\begin{aligned} |\langle x - x_0, v_j\rangle| &\leqslant |\langle y - x_0, v_j\rangle| + |\langle z - \pi(y), \pi(v_j)\rangle| \\ &\leqslant \big(b_j + (a_j + 30)/\sqrt{2}\big)\sqrt{n} \cdot \|v_j\|_\infty \\ &\leqslant \left(\frac{2c_j}{7} + \frac{c_j + 42}{\sqrt{2}}\right)\sqrt{n} \cdot \|v_j\|_\infty \\ &\leqslant (c_j + 30)\sqrt{n} \cdot \|v_j\|_\infty, \end{aligned}$$

as required, since $b_j = 2c_j/7$ and $a_j \leqslant c_j + 12$. This completes the induction step. □

Remark 4.3. The result is stated in terms of the ℓ^∞-norms $\|v_j\|_\infty$ because we cannot control the decrease in $\|v_j\|_2$ when we discard half of the coordinates.

Remark 4.4. It is important for our application that m can be much larger than n, and that the only restriction on m occurs via the condition (11). In particular, we will later apply Corollary 4.2 with m very large, but with the c_j increasing sufficiently rapidly so that (11) still holds.

5. **The odd sine polynomial**

The aim of this section is to prove Theorem 2.4. Let $\mathcal{I}$ be a collection of suitable well-separated intervals, and recall from Definition 2.2 that $|\mathcal{I}| = 4N$ for some $N \leqslant \gamma n$, and that $\mathcal{I}$ is invariant under the maps $\theta \mapsto \pi \pm \theta$. The collection $\mathcal{I}$ is therefore uniquely determined by the set $\mathcal{I}_0 \subseteq \mathcal{I}$ of N intervals that lie in $[0, \pi/2]$ (since no $I \in \mathcal{I}$ contains 0 or $\pi/2$).

As described in Section 2.1, our aim is to "push" the sine polynomial away from zero (in either the positive or negative direction) on each interval in $\mathcal{I}$. Let us say that a colouring $\alpha\colon \mathcal{I} \to \{-1, 1\}$ is *symmetric* if $\alpha(I') = \alpha(I)$

whenever $I' = \pi - I$, and $\alpha(I') = -\alpha(I)$ whenever $I' = \pi + I$. Note that if α is symmetric, then it is uniquely determined by its values on the set $\mathcal{I}_0$. Finally, recall that $S_o = \{1, 3, 5, \ldots, 2n-1\}$, and set $K := 2^7$.

Definition 5.1. Given a colouring $\alpha \colon \mathcal{I} \to \{-1, 1\}$, we define $g_\alpha \colon \mathbb{R}/2\pi\mathbb{Z} \to \{-1, 0, 1\}$ by

$$g_\alpha(\theta) := \sum_{I \in \mathcal{I}} \alpha(I) \mathbb{1}[\theta \in I].$$

We also define a vector $\hat{\varepsilon} = (\hat{\varepsilon}_1, \hat{\varepsilon}_3, \ldots, \hat{\varepsilon}_{2n-1}) \in \mathbb{R}^{S_o}$ by setting

$$\hat{\varepsilon}_j := K\sqrt{n} \int_{-\pi}^{\pi} g_\alpha(\theta) \sin(j\theta)\, d\theta$$

for each $j \in S_o$.

Remark 5.2. By Fourier inversion, one would expect the function $\hat{s}_\alpha(\theta) := \sum_{j \in S_o} \hat{\varepsilon}_j \sin(j\theta)$ to approximate $\pi K \sqrt{n}\, g_\alpha(\theta)$; in particular, it should be large on the intervals $I \in \mathcal{I}$. We will prove in Lemma 5.6 that this is indeed the case.

We will use $\hat{\varepsilon}$ as the starting point of an application of Corollary 4.2, so we need $|\hat{\varepsilon}_j| \leqslant 1$ for all $j \in S_o$. The following lemma, which we also prove using Corollary 4.2, shows that, since we chose γ sufficiently small, we can choose the colouring α so that this is the case.

LEMMA 5.3. *There exists a symmetric colouring $\alpha \colon \mathcal{I} \to \{-1, 1\}$ such that $\hat{\varepsilon} \in [-1, 1]^{S_o}$.*

Proof. Write $\mathcal{I}_0 = \{I_1, \ldots, I_N\}$, and recall that this collection determines $\mathcal{I}$. Now, for each $j \in [n]$, define a vector $v_j \in \mathbb{R}^N$ by setting

$$(v_j)_i := 4K\sqrt{n} \int_{I_i} \sin\big((2j-1)\theta\big)\, d\theta$$

for each $i \in [N]$, and observe that, for each $j \in [n]$, we have

$$\hat{\varepsilon}_{2j-1} = K\sqrt{n} \int_{-\pi}^{\pi} g_\alpha(\theta) \sin\big((2j-1)\theta\big)\, d\theta = \sum_{i=1}^{N} \alpha(I_i)(v_j)_i,$$

by the symmetry conditions on both α and $\mathcal{I}$. Our task is therefore to find a vector $x \in \{-1, 1\}^N$ such that $|\langle x, v_j \rangle| \leqslant 1$ for all $j \in [n]$. Indeed, we will then be able to set $\alpha(I_i) = x_i$ for each $i \in [N]$ and deduce that $|\hat{\varepsilon}_k| \leqslant 1$ for all $k \in S_o$.

We do so by applying Corollary 4.2 with $x_0 := 0$ and $c_j := 14\sqrt{\log(16n/N)}$ for each $j \in [n]$. Noting that (11) is satisfied, it follows from Corollary 4.2 that there exists an $x \in \{-1, 1\}^N$ such that

$$|\langle x, v_j \rangle| \leqslant \big(c_j + 30\big)\sqrt{N} \cdot \|v_j\|_\infty.$$

Now, since $\mathcal{I}$ is well separated, by Definition 2.2(d) we have

$$|(v_j)_i| \leqslant 4K\sqrt{n}\cdot|I_i| \leqslant \frac{24\pi K}{\sqrt{n}}$$

for every $i \in [N]$ and $j \in [n]$. It follows that

$$|\langle x, v_j\rangle| \leqslant \big(14\sqrt{\log(16n/N)}+30\big)\sqrt{N/n}\cdot 24\pi K.$$

Note that the right-hand side is an increasing function of N for $N/n \leqslant \gamma < 1$ and so

$$|\langle x, v_j\rangle| \leqslant \big(14\sqrt{\log(16/\gamma)}+30\big)\sqrt{\gamma}\cdot 24\pi K \leqslant 1,$$

where the last inequality follows from our choice of $K = 2^7$ and the inequality $\gamma \leqslant 2^{-40}$. □

For the rest of the proof, fix this colouring α (and hence also the vector $\hat{\varepsilon}$). Recall that our aim is to choose a colouring $\varepsilon\colon S_o \to \{-1,1\}$ so that the conclusion of Theorem 2.4 holds. Given such a colouring, define

$$s_o(\theta) := \sum_{j\in S_o}\varepsilon_j \sin(j\theta) \qquad \text{and} \qquad \hat{s}_\alpha(\theta) := \sum_{j\in S_o}\hat{\varepsilon}_j \sin(j\theta).$$

Our aim is to choose the ε_j so that $|s_o(\theta) - \hat{s}_\alpha(\theta)|$ is uniformly bounded for all $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ (see Lemma 5.5). A naïve approach to controlling this difference on a sufficiently dense set of points would require imposing more constraints (with smaller values of c_j) than can be handled by Corollary 4.2. Instead we shall place constraints on the differences $|s_o^{(\ell)}(\theta) - \hat{s}_\alpha^{(\ell)}(\theta)|$ of the ℓth derivatives for each $\ell \geqslant 0$, but at many fewer values of θ, and then use Taylor's Theorem to bound $|s_o(\theta) - \hat{s}_\alpha(\theta)|$ at all other points. The advantage of this approach is that the constraints we need on the higher derivatives become rapidly weaker as ℓ increases and, in particular, can be chosen so that (11) is satisfied.

Note that it is enough to bound $|s_o(\theta) - \hat{s}_\alpha(\theta)|$ on $[0, \frac{\pi}{2}]$ as both $s_o(\theta)$ and $\hat{s}_\alpha(\theta)$ have the same symmetries under $\theta \mapsto \pi \pm \theta$. Set $M := 16n$, and let $\theta_k := \frac{(2k-1)\pi}{4M}$ for $k = 1, \dots, M$. Then for any point $\theta \in [0, \frac{\pi}{2}]$, there exists $k \in [M]$ such that $|\theta - \theta_k| \leqslant \frac{\pi}{4M} = 2^{-6}\pi/n$. By Taylor's Theorem (and the fact that all sine polynomials are entire functions so their Taylor expansions converge), we have

$$s_o(\theta) - \hat{s}_\alpha(\theta) = \sum_{\ell=0}^{\infty}\big(s_o^{(\ell)}(\theta_k) - \hat{s}_\alpha^{(\ell)}(\theta_k)\big)\frac{(\theta-\theta_k)^\ell}{\ell!}. \tag{12}$$

We will bound the absolute value of the right-hand side using Corollary 4.2.

Lemma 5.4. *There exists a colouring $\varepsilon\colon S_o \to \{-1,1\}$ such that*

$$\big|s_o^{(\ell)}(\theta_k) - \hat{s}_\alpha^{(\ell)}(\theta_k)\big| \leqslant (65+2\ell)\sqrt{n}\cdot(2n)^\ell$$

for every $k \in [M]$ and $\ell \geqslant 0$.

Proof. For each $k \in [M]$ and $\ell \geqslant 0$, define a vector $v_{(k,\ell)} \in \mathbb{R}^n$ by setting

$$(v_{(k,\ell)})_j = \frac{d^\ell}{d\theta^\ell} \sin\big((2j-1)\theta\big)\big|_{\theta=\theta_k}$$

for each $j \in [n]$, and observe that

$$s_o^{(\ell)}(\theta_k) - \hat{s}_\alpha^{(\ell)}(\theta_k) = \sum_{j=1}^{n} \big(\varepsilon_{2j-1} - \hat{\varepsilon}_{2j-1}\big)(v_{(k,\ell)})_j = \langle \varepsilon - \hat{\varepsilon}, v_{(k,\ell)} \rangle,$$

where we consider $\varepsilon - \hat{\varepsilon}$ and $v_{(k,\ell)}$ as vectors in $\mathbb{R}^{S_o}$.

We apply Corollary 4.2 with $x_0 := \hat{\varepsilon}$ and $c_{(k,\ell)} = 14\sqrt{(9+\ell)\log 2}$. Observe that

$$\sum_{k=1}^{M}\sum_{\ell=0}^{\infty} \exp\big(-c_{(k,\ell)}^2/14^2\big) = \sum_{k=1}^{M}\sum_{\ell=0}^{\infty} 2^{-(9+\ell)} = M \cdot 2^{-8} = \frac{n}{16},$$

and so (11) is satisfied. It follows[6] from Corollary 4.2 that there exists an $\varepsilon \in \{-1,1\}^n$ such that

$$|\langle \varepsilon - \hat{\varepsilon}, v_{(k,\ell)} \rangle| \leqslant \big(c_{(k,\ell)} + 30\big)\sqrt{n} \cdot \|v_{(k,\ell)}\|_\infty$$

for every $k \in [M]$ and $\ell \geqslant 0$. Now, observe that

$$\|v_{(k,\ell)}\|_\infty \leqslant (2n)^\ell,$$

and that $14^2(9+\ell)\log 2 \leqslant 35^2 + 140\ell \leqslant (35+2\ell)^2$, so

$$c_{(k,\ell)} + 30 \leqslant 65 + 2\ell.$$

Combining these bounds, we obtain

$$\big|s_o^{(\ell)}(\theta_k) - \hat{s}_\alpha^{(\ell)}(\theta_k)\big| = |\langle \varepsilon - \hat{\varepsilon}, v_{(k,\ell)} \rangle| \leqslant (65+2\ell)\sqrt{n} \cdot (2n)^\ell$$

for every $k \in [M]$ and $\ell \geqslant 0$, as required. □

The following bound on the magnitude of $s_o(\theta) - \hat{s}_\alpha(\theta)$ is a straightforward consequence.

LEMMA 5.5. *There exists a colouring $\varepsilon\colon S_o \to \{-1,1\}$ such that*

$$|s_o(\theta) - \hat{s}_\alpha(\theta)| \leqslant 72\sqrt{n}$$

for every $\theta \in \mathbb{R}$.

[6] Note that we appear to be applying Corollary 4.2 with an infinite number of constraints, but in fact only finitely many of them are needed as the constraints vacuously hold when $\ell \geqslant n$.

Proof. Let us assume (without loss of generality) that $\theta \in [0, \frac{\pi}{2}]$, and let $k \in [M]$ be such that $|\theta - \theta_k| \leqslant 2^{-6}\pi/n$. By (12) and Lemma 5.4, we have

$$\big|s_o(\theta) - \hat{s}_\alpha(\theta)\big| \leqslant \sum_{\ell=0}^{\infty} \big|s_o^{(\ell)}(\theta_k) - \hat{s}_\alpha^{(\ell)}(\theta_k)\big| \frac{(2^{-6}\pi/n)^\ell}{\ell!} \leqslant \sum_{\ell=0}^{\infty}(65+2\ell)\sqrt{n}\cdot\frac{(2^{-5}\pi)^\ell}{\ell!}.$$

Now simply observe that

$$\sum_{\ell=0}^{\infty}(65+2\ell)\frac{(2^{-5}\pi)^\ell}{\ell!} = (65 + 2^{-4}\pi)e^{2^{-5}\pi} \leqslant 72,$$

and the lemma follows. □

We will prove that the conclusion of Theorem 2.4 holds for the colouring ε given by Lemma 5.5. To deduce this, it will suffice to show that $\hat{s}_\alpha(\theta)$ approximates the step function $\pi K\sqrt{n}\cdot g_\alpha(\theta)$ sufficiently well and, in particular, that it is large on each interval $I \in \mathcal{I}$.

LEMMA 5.6. *For every* $\theta \in \bigcup_{I\in\mathcal{I}} I$, *we have*

$$|\hat{s}_\alpha(\theta)| \geqslant \frac{2K\sqrt{n}}{3}.$$

Moreover, $|\hat{s}_\alpha(\theta)| \leqslant 5K\sqrt{n}$ *for every* $\theta \in \mathbb{R}$.

The proof of Lemma 5.6 follows from a standard (but somewhat technical) calculation, and to simplify things slightly we will find it convenient to renormalise, by defining

$$\tilde{s}_\alpha(\theta) := (K\sqrt{n})^{-1}\hat{s}_\alpha(\theta).$$

Fix $\theta_0 \in \mathbb{R}$, and observe that, by the symmetry conditions on both α and $\mathcal{I}$, we have

$$\begin{aligned} \tilde{s}_\alpha(\theta_0) &= \sum_{j=0}^{n-1} \sin\big((2j+1)\theta_0\big) \int_{-\pi}^{\pi} g_\alpha(\theta)\sin\big((2j+1)\theta\big)\,d\theta \\ &= 4\int_0^{\pi/2} g_\alpha(\theta) \sum_{j=0}^{n-1} \sin\big((2j+1)\theta_0\big)\sin\big((2j+1)\theta\big)\,d\theta. \end{aligned} \tag{13}$$

We can now use the following simple trigonometric fact.

OBSERVATION 5.7.

$$4\sum_{j=0}^{n-1}\sin\big((2j+1)\theta_0\big)\sin\big((2j+1)\theta\big) = \frac{\sin\big(2n(\theta-\theta_0)\big)}{\sin(\theta-\theta_0)} - \frac{\sin\big(2n(\theta+\theta_0)\big)}{\sin(\theta+\theta_0)}.$$

Proof. Simply note that both sides are equal to

$$2\sum_{j=0}^{n-1}\Big(\cos\big((2j+1)(\theta-\theta_0)\big)-\cos\big((2j+1)(\theta+\theta_0)\big)\Big),$$

using the addition formulae for $\sin(\alpha\pm\beta)$ and $\cos(\alpha\pm\beta)$ and the telescoping series

$$\begin{aligned}\sin(2n\varphi) &= \sum_{j=0}^{n-1}\Big(\sin\big((2j+1)\varphi+\varphi\big)-\sin\big((2j+1)\varphi-\varphi\big)\Big)\\ &= \sum_{j=0}^{n-1} 2\cos\big((2j+1)\varphi\big)\sin(\varphi)\end{aligned}$$

for $\varphi = \theta \pm \theta_0$. □

Combining (13) and Observation 5.7, and recalling the definition of $g_\alpha(\theta)$, it follows that

$$\tilde{s}_\alpha(\theta_0) = \sum_{I\in\mathcal{I}_0}\alpha(I)\int_I\left(\frac{\sin\big(2n(\theta-\theta_0)\big)}{\sin(\theta-\theta_0)}-\frac{\sin\big(2n(\theta+\theta_0)\big)}{\sin(\theta+\theta_0)}\right)d\theta. \tag{14}$$

Before bounding the right-hand side of (14), let us briefly discuss what is going on. Let $\theta_0\in[0,\pi/2]$, and recall from Definition 2.2(f) that no $I\in\mathcal{I}_0$ contains any point close to 0 or $\pi/2$. It follows that the integrand in (14) behaves roughly like a point mass placed at $\theta=\theta_0$, and hence $\tilde{s}_\alpha(\theta_0)$ should be approximately $\alpha(I)$ when $\theta_0\in I$, and small otherwise.

To make this rigorous, we will show that the integral of the first term over the interval $I\in\mathcal{I}_0$ containing θ_0 (if such an interval exists) is of order 1, and that the integral over the remaining intervals (and over the second term) is smaller. This will follow via a straightforward calculation from the fact that the endpoints of each interval in $\mathcal{I}$ lie in $\frac{\pi}{n}\mathbb{Z}$.

Instead of approximating the integral for an interval close to θ_0 directly, we will instead compare it to the following standard "sine integral."

LEMMA 5.8. *Let $I\in\mathcal{I}$, and let $\theta_0\in\mathbb{R}$.*

(a) *If $\theta_0\in I$, then*

$$\frac{4}{3} \leqslant \int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta \leqslant 4.$$

(b) *If $\theta_0\notin I$ then*

$$-1 \leqslant \int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta \leqslant 2.$$

Proof. Recall from Definition 2.2 that the endpoints of I are in $\frac{\pi}{n}\mathbb{Z}$, and let $I = [a\pi/n, b\pi/n]$, where $a, b \in \mathbb{Z}$ with $a < b$. Substituting $x = 2n(\theta - \theta_0)$ gives us the integral

$$f(\theta_0) := \int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta = \int_{2a\pi-2n\theta_0}^{2b\pi-2n\theta_0} \frac{\sin x}{x}\,dx,$$

and we note that

$$\begin{aligned} f'(\theta_0) &= (-2n)\left(\frac{\sin(2b\pi-2n\theta_0)}{2b\pi-2n\theta_0} - \frac{\sin(2a\pi-2n\theta_0)}{2a\pi-2n\theta_0}\right) \\ &= \frac{4\pi n(a-b)\sin(2n\theta_0)}{(2a\pi-2n\theta_0)(2b\pi-2n\theta_0)}, \end{aligned}$$

since $a, b \in \mathbb{Z}$, so $\sin(2a\pi - 2n\theta_0) = \sin(2b\pi - 2n\theta_0) = -\sin(2n\theta_0)$. Since $a \neq b$, it follows that the extremal values of $f(\theta_0)$ can occur only when $\sin(2n\theta_0) = 0$, i.e., when $2n\theta_0 \in \pi\mathbb{Z}$. These extremal values must therefore be of the form

$$u(\ell) + u(\ell+1) + \cdots + u(\ell + 2(b-a) - 1)$$

for some $\ell \in \mathbb{Z}$, where

$$u(j) := \int_{j\pi}^{(j+1)\pi} \frac{\sin x}{x}\,d\theta.$$

We claim first that if $\theta_0 \in I$, then

$$\int_0^{2\pi} \frac{\sin x}{x}\,d\theta \leqslant f(\theta_0) \leqslant \int_{-\pi}^{\pi} \frac{\sin x}{x}\,d\theta.$$

Indeed, if $\theta_0 \in I$, then $2a\pi \leqslant 2\theta_0 n \leqslant 2b\pi$, and so $\ell \leqslant 0 \leqslant \ell + 2(b-a)$. Note also that

$$u(2j) > 0, \qquad u(2j+1) < 0 \qquad \text{and} \qquad u(-j) = u(j-1)$$

for every non-negative $j \in \mathbb{Z}$, and moreover

$$u(2j-1) + u(2j) < 0 < u(2j) + u(2j+1)$$

for every $j \geqslant 1$. It follows that the maxima of $f(\theta_0)$ are at most $u(-1) + u(0)$, and the minima are at least $u(0) + u(1)$, as claimed. Similarly, if $\theta_0 \notin I$, then without loss of generality we have $\ell \geqslant 0$, and by the same argument as above we have

$$\int_{\pi}^{2\pi} \frac{\sin x}{x}\,d\theta \leqslant f(\theta_0) \leqslant \int_0^{\pi} \frac{\sin x}{x}\,d\theta.$$

It is now straightforward to obtain the claimed bounds by numerical integration. □

We will also use the following simple lemma to bound the integrals in (14).

Lemma 5.9. *If $h\colon [a,b] \to \mathbb{R}$ is a monotonic function and $b - a \in \frac{\pi}{n}\mathbb{Z}$, then*

$$\left| \int_a^b h(\theta) \sin(2n\theta)\, d\theta \right| \leqslant \frac{|h(b) - h(a)|}{n}.$$

Proof. Assume without loss of generality that h is increasing, and suppose first that $b = a + \frac{\pi}{n}$. Since $\sin(x + \pi) = -\sin(x)$, we have

$$\int_a^{a+\frac{\pi}{n}} h(\theta) \sin(2n\theta)\, d\theta = \int_a^{a+\frac{\pi}{2n}} \big(h(\theta) - h(\theta + \tfrac{\pi}{2n}) \big) \sin(2n\theta)\, d\theta,$$

and therefore, since h is increasing,

$$\left| \int_a^{a+\frac{\pi}{n}} h(\theta) \sin(2n\theta)\, d\theta \right| \leqslant \big(h(b) - h(a) \big) \int_a^{a+\frac{\pi}{2n}} |\sin(2n\theta)|\, d\theta \,=\, \frac{h(b) - h(a)}{n},$$

as required. To deduce the general case, simply split the interval $[a,b]$ into sub-intervals of length $\frac{\pi}{n}$ and use the triangle inequality. □

We are now ready to prove Lemma 5.6.

Proof of Lemma 5.6. Recall that it is enough to prove the bounds when $\theta = \theta_0 \in [0, \pi/2]$, and that $\mathcal{I}_0 = \{ I \in \mathcal{I} : I \subseteq [0, \pi/2] \}$. By (14), we have

$$\tilde{s}_\alpha(\theta_0) = \sum_{I \in \mathcal{I}_0} \alpha(I) \int_I \left(\frac{\sin\big(2n(\theta - \theta_0)\big)}{\sin(\theta - \theta_0)} - \frac{\sin\big(2n(\theta + \theta_0)\big)}{\sin(\theta + \theta_0)} \right) d\theta \tag{15}$$

for every $\theta_0 \in [0, \pi/2]$. We will deal with the second term first.

Claim 1: $\displaystyle\sum_{I \in \mathcal{I}_0} \left| \int_I \frac{\sin(2n(\theta + \theta_0))}{\sin(\theta + \theta_0)}\, d\theta \right| \leqslant \frac{1}{50\pi} + \frac{O(1)}{n}.$

Proof of Claim 1. Let $I \in \mathcal{I}_0$, and suppose first that $\sin\theta$ is monotonic on $I + \theta_0$. By Lemma 5.9, applied with $h(\theta) = 1/\sin\theta$, we have

$$\left| \int_I \frac{\sin(2n(\theta + \theta_0))}{\sin(\theta + \theta_0)}\, d\theta \right| \leqslant \frac{1}{n} \left(\max_{\theta \in I} \frac{1}{\sin(\theta + \theta_0)} - \min_{\theta \in I} \frac{1}{\sin(\theta + \theta_0)} \right)$$

since, by Definition 2.2, the endpoints of I are in $\frac{\pi}{n}\mathbb{Z}$. If $\sin\theta$ is not monotonic on $I + \theta_0$, then we instead use the trivial bound

$$\left| \int_I \frac{\sin(2n(\theta + \theta_0))}{\sin(\theta + \theta_0)}\, d\theta \right| \leqslant |I| \cdot \max_{\theta \in I} \frac{1}{\sin(\theta + \theta_0)} \,=\, \frac{O(1)}{n},$$

where the final inequality holds since $|I| = O(1/n)$, by Definition 2.2, and hence (since $\sin\theta$ is not monotonic on $I + \theta_0 \subseteq [0, \pi]$) we have $\sin(\theta + \theta_0) > 1/2$ for all $\theta \in I$.

Now, summing over intervals $I \in \mathcal{I}_0$ and partitioning into three classes according to whether $\sin\theta$ is increasing, decreasing, or neither on $I + \theta_0$, we obtain two alternating sums that are both bounded by their maximum terms, and possibly one additional term (for which we use the trivial bound). Recalling from

Definition 2.2 that $\bigcup_{I\in\mathcal{I}} I$ is disjoint from the set $(\pi/2)\mathbb{Z}+[-100\pi/n,100\pi/n]$, we obtain

$$\sum_{I\in\mathcal{I}_0}\left|\int_I \frac{\sin(2n(\theta+\theta_0))}{\sin(\theta+\theta_0)}\,d\theta\right| \leqslant \frac{2}{n\sin(100\pi/n)}+\frac{O(1)}{n} = \frac{1}{50\pi}+\frac{O(1)}{n},$$

as claimed. □

The next claim will allow us to replace the first term in (15) by the integral in Lemma 5.8.

Claim 2: $$\sum_{I\in\mathcal{I}_0}\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\sin(\theta-\theta_0)}-\frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| = \frac{O(1)}{n}.$$

Proof of Claim 2. We again apply Lemma 5.9, this time with $h(\theta)=\frac{1}{\sin\theta}-\frac{1}{\theta}$, which is increasing on $[-\pi/2,\pi/2]$, to give

$$\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\sin(\theta-\theta_0)}-\frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| \leqslant \frac{1}{n}\Big(\max_{\theta\in I} h(\theta-\theta_0)-\min_{\theta\in I} h(\theta-\theta_0)\Big)$$

for every $I\in\mathcal{I}_0$. (Note that $\theta-\theta_0\in[-\pi/2,\pi/2]$ for $\theta\in I\in\mathcal{I}_0$.) Summing over intervals $I\in\mathcal{I}_0$, and noting that we again have an alternating sum, we obtain the bound

$$\sum_{I\in\mathcal{I}_0}\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\sin(\theta-\theta_0)}-\frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| \leqslant \frac{h(\pi/2)-h(-\pi/2)}{n} = \frac{O(1)}{n},$$

as claimed. □

It remains to bound $\int_I \frac{\sin(2n(\theta-\theta_0))}{\theta-\theta_0}\,d\theta$ for each $I\in\mathcal{I}$. When $d(\theta_0,I)<\pi/n$ we will apply Lemma 5.8 to bound this integral. However, in order to deal with the intervals that are far from θ_0 we will need the following stronger bound. Let $\mathcal{J}(\theta_0) := \big\{I\in\mathcal{I}_0 : d(\theta_0,I)\geqslant \pi/n\big\}$.

Claim 3: $$\sum_{I\in\mathcal{J}(\theta_0)}\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| \leqslant \frac{2}{\pi}.$$

Proof of Claim 3. Once again we apply Lemma 5.9, this time with $h(\theta)=1/\theta$. We obtain

$$\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| \leqslant \frac{1}{n}\bigg(\max_{\theta\in I}\frac{1}{\theta-\theta_0}-\min_{\theta\in I}\frac{1}{\theta-\theta_0}\bigg)$$

for every $I\in\mathcal{I}_0$ with $\theta_0\notin I$. Summing over intervals in $\mathcal{J}(\theta_0)$, and noting that we obtain two alternating sums (one on either side of θ_0), we obtain

$$\sum_{I\in\mathcal{J}(\theta_0)}\left|\int_I \frac{\sin\big(2n(\theta-\theta_0)\big)}{\theta-\theta_0}\,d\theta\right| \leqslant \frac{2}{n}\cdot\frac{1}{\pi/n} = \frac{2}{\pi}$$

as claimed. □

Note that $2/\pi + 1/(50\pi) + O(1/n) \leqslant 2/3$ if n is sufficiently large, and suppose first that $\theta_0 \in I$ for some $I \in \mathcal{I}_0$. Then $d(\theta_0, I') \geqslant \pi/n$ for all $I \neq I' \in \mathcal{I}_0$, by Definition 2.2. It follows, by (15), Claims 1, 2 and 3, and Lemma 5.8, that

$$\frac{2}{3} = \frac{4}{3} - \frac{2}{3} \leqslant \big|\tilde{s}_\alpha(\theta_0)\big| \leqslant 4 + \frac{2}{3} < 5,$$

as required. On the other hand, if $\theta_0 \notin \bigcup_{I \in \mathcal{I}_0} I$, then there are at most two intervals $I \in \mathcal{I}_0$ such that $d(\theta_0, I) < \pi/n$. Therefore, by (15), Claims 1, 2 and 3, and Lemma 5.8, we have

$$|\tilde{s}_\alpha(\theta_0)| \leqslant 2 \cdot 2 + \frac{2}{3} < 5.$$

Since $\hat{s}_\alpha(\theta) = K\sqrt{n}\,\tilde{s}_\alpha(\theta)$, this completes the proof of the lemma. ◻

Remark 5.10. We note that it is important that the lengths of the intervals $I \in \mathcal{I}$ are multiples of $\frac{\pi}{n}$. Without this assumption it is possible that the error term from the distant intervals $I \in \mathcal{I}_0$ in Claim 3 could be unbounded. Indeed, the reason it does not stems ultimately from the cancelation in the integrals provided by Lemma 5.9.

Theorem 2.4 is an almost immediate consequence of Lemmas 5.5 and 5.6.

Proof of Theorem 2.4. Let $\mathcal{I}$ be a suitable and well-separated collection of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$. By Lemma 5.5, there exists a colouring $\varepsilon\colon S_o \to \{-1, 1\}$ such that, if α is the function given by Lemma 5.3, then

$$|s_o(\theta) - \hat{s}_\alpha(\theta)| \leqslant 72\sqrt{n}$$

for every $\theta \in \mathbb{R}$. Now observe that, by Lemma 5.6, we have

$$|s_o(\theta)| \geqslant |\hat{s}_\alpha(\theta)| - |s_o(\theta) - \hat{s}_\alpha(\theta)| \geqslant \left(\frac{2K}{3} - 72\right)\sqrt{n} > 10\sqrt{n}$$

for all $\theta \in \bigcup_{I \in \mathcal{I}} I$, and

$$|s_o(\theta)| \leqslant |\hat{s}_\alpha(\theta)| + |s_o(\theta) - \hat{s}_\alpha(\theta)| \leqslant \big(5K + 72\big)\sqrt{n} \leqslant 2^{10}\sqrt{n}$$

for all $\theta \in \mathbb{R}$, as required. ◻

Finally, let us put together the pieces and prove Theorem 2.1.

Proof of Theorem 2.1. Let $c(\theta)$ be the cosine polynomial, and let $\mathcal{I}$ be the suitable and well-separated collection of disjoint intervals in $\mathbb{R}/2\pi\mathbb{Z}$, given by Theorem 2.3. Now, given $\mathcal{I}$, let $s_o(\theta)$ be the sine polynomial given by Theorem 2.4, and let $s_e(\theta)$ be the sine polynomial defined in (7). We claim that the polynomial

$$P(e^{i\theta}) := \big(1 + 2c(\theta)\big) + 2i\big(s_e(\theta) + s_o(\theta)\big)$$

has the properties required by the theorem.

To prove the claim, we should first observe that $P(z) = \sum_{k=-2n}^{2n} \varepsilon_k z^k$ with $\varepsilon_k \in \{-1, 1\}$ for every $k \in [-2n, 2n]$. Indeed the supports of $c(\theta)$, $s_e(\theta)$, and $s_o(\theta)$ are disjoint and cover the powers z^k with $k \in \{-2n, \ldots, -2n\} \setminus \{0\}$, and the constant 1 provides the term corresponding to $k = 0$. Now, observe that

$$\begin{aligned} |P(e^{i\theta})|^2 &\leqslant \big(2|c(\theta)| + 1\big)^2 + 4|s_e(\theta) + s_o(\theta)|^2 \\ &\leqslant \big(2\sqrt{n} + 1\big)^2 + 4\big(2^{10} + 6\big)^2 n \leqslant \big(2^{12}\sqrt{n}\big)^2 \end{aligned}$$

for every $\theta \in \mathbb{R}$, since $|c(\theta)| \leqslant \sqrt{n}$ and $|s_e(\theta)| \leqslant 6\sqrt{n}$, by Theorem 2.3 and Lemma 3.3, and $|s_o(\theta)| \leqslant 2^{10}\sqrt{n}$, by Theorem 2.4. Next, observe that if $\theta \notin \bigcup_{I \in \mathcal{I}} I$, then

$$|P(e^{i\theta})| \geqslant \big|\operatorname{Re}\big(P(e^{i\theta})\big)\big| \geqslant 2|c(\theta)| - 1 \geqslant \delta\sqrt{n}$$

for all sufficiently large n, by Theorem 2.3. Finally, if $\theta \in \bigcup_{I \in \mathcal{I}} I$, then

$$|P(e^{i\theta})| \geqslant \big|\operatorname{Im}\big(P(e^{i\theta})\big)\big| \geqslant 2\big(|s_o(\theta)| - |s_e(\theta)|\big) \geqslant 2\big(10\sqrt{n} - 6\sqrt{n}\big) = 8\sqrt{n},$$

by Theorem 2.4. Hence $|P(z)| \geqslant \delta\sqrt{n}$ for all $z \in \mathbb{C}$ with $|z| = 1$, as required. □

Acknowledgements. Much of this research was carried out during a one-month visit by the authors to IMT Lucca. We are grateful to IMT (and especially to Prof. Guido Caldarelli) for providing a wonderful working environment.

References

[1] P. Balister, Bounds on Rudin–Shapiro polynomials of arbitrary degree, 2019. arXiv 1909.08777.

[2] J. Beck, Roth's estimate of the discrepancy of integer sequences is nearly sharp, *Combinatorica* **1** no. 4 (1981), 319–325. MR 0647981. Zbl 0491.10046. https://doi.org/10.1007/BF02579452.

[3] J. Beck, Flat polynomials on the unit circle—note on a problem of Littlewood, *Bull. London Math. Soc.* **23** no. 3 (1991), 269–277. MR 1123337. Zbl 0748.30006. https://doi.org/10.1112/blms/23.3.269.

[4] E. Beller and D. J. Newman, The minimum modulus of polynomials, *Proc. Amer. Math. Soc.* **45** (1974), 463–465. MR 0355015. Zbl 0306.30001. https://doi.org/10.2307/2039981.

[5] A. Bloch and G. Pólya, On the roots of certain algebraic equations, *Proc. London Math. Soc.* (2) **33** no. 2 (1931), 102–114. MR 1576817. Zbl 0003.10501. https://doi.org/10.1112/plms/s2-33.1.102.

[6] E. Bombieri and J. Bourgain, On Kahane's ultraflat polynomials, *J. Eur. Math. Soc.* (*JEMS*) **11** no. 3 (2009), 627–703. MR 2505444. Zbl 1170.42001. https://doi.org/10.4171/jems/163.

[7] P. Borwein, *Computational Excursions in Analysis and Number Theory*, *CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC* **10**, Springer-Verlag, New York, 2002. MR 1912495. Zbl 1020.12001. https://doi.org/10.1007/978-0-387-21652-2.

[8] J. Bourgain, Sur le minimum d'une somme de cosinus, *Acta Arith.* **45** no. 4 (1986), 381–389. MR 0847298. Zbl 0615.42001. https://doi.org/10.4064/aa-45-4-381-389.

[9] J. Brillhart, On the Rudin-Shapiro polynomials, *Duke Math. J.* **40** (1973), 335–353. MR 0315096. Zbl 0263.33012. https://doi.org/10.1215/S0012-7094-73-04028-3.

[10] J. Brillhart and L. Carlitz, Note on the Shapiro polynomials, *Proc. Amer. Math. Soc.* **25** (1970), 114–118. MR 0260955. Zbl 0191.35101. https://doi.org/10.2307/2036537.

[11] J. Brillhart, J. S. Lomont, and P. Morton, Cyclotomic properties of the Rudin-Shapiro polynomials, *J. Reine Angew. Math.* **288** (1976), 37–65. MR 0498479. Zbl 0335.12003. https://doi.org/10.1515/crll.1976.288.37.

[12] J. S. Byrnes, On polynomials with coefficients of modulus one, *Bull. London Math. Soc.* **9** no. 2 (1977), 171–176. MR 0486435. Zbl 0364.30004. https://doi.org/10.1112/blms/9.2.171.

[13] F. W. Carroll, D. Eustice, and T. Figiel, The minimum modulus of polynomials with coefficients of modulus one, *J. London Math. Soc.* (2) **16** no. 1 (1977), 76–82. MR 0480955. Zbl 0365.30001. https://doi.org/10.1112/jlms/s2-16.1.76.

[14] S. Chowla, Some applications of a method of A. Selberg, *J. Reine Angew. Math.* **217** (1965), 128–132. MR 0172853. https://doi.org/10.1515/crll.1965.217.128.

[15] P. Erdős, Some unsolved problems, *Michigan Math. J.* **4** (1957), 291–300. MR 0098702. Zbl 0081.00102. https://doi.org/10.1307/mmj/1028997963.

[16] P. Erdös and A. C. Offord, On the number of real roots of a random algebraic equation, *Proc. London Math. Soc.* (3) **6** (1956), 139–160. MR 0073870. Zbl 0070.01702. https://doi.org/10.1112/plms/s3-6.1.139.

[17] M. J. E. Golay, Multi-slit spectrometry, *J. Opt. Soc. Am.* **39** no. 6 (1949), 437–444. https://doi.org/10.1364/JOSA.39.000437.

[18] G. H. Hardy and J. E. Littlewood, Some problems of Diophantine approximation: A remarkable trigonometric series, *Proc. Nat. Acad. Sci.* **2** (1916), 583–586. JFM 46.0443.02.

[19] G. H. Hardy and J. E. Littlewood, A new proof of a theorem on rearrangements, *J. London Math. Soc.* **23** (1948), 163–168. MR 0028445. Zbl 0034.04301. https://doi.org/10.1112/jlms/s1-23.3.163.

[20] G. W. Howell, Derivative error bounds for Lagrange interpolation: an extension of Cauchy's bound for the error of Lagrange interpolation, *J. Approx. Theory* **67** no. 2 (1991), 164–173. MR 1133057. Zbl 0749.41005. https://doi.org/10.1016/0021-9045(91)90015-3.

[21] J.-P. Kahane, Sur les polynômes à coefficients unimodulaires, *Bull. London Math. Soc.* **12** no. 5 (1980), 321–342. MR 0587702. Zbl 0443.30005. https://doi.org/10.1112/blms/12.5.321.

[22] S. V. Konyagin, On the problem of Littlewood, *Izv. Akad. Nauk SSSR Ser. Mat.* **45** (1981), 243–265. MR 616222. Zbl 0493.42004. https://doi.org/10.1070/IM1982v018n02ABEH001386.

[23] T. W. Körner, On a polynomial of Byrnes, *Bull. London Math. Soc.* **12** no. 3 (1980), 219–224. MR 0572106. Zbl 0435.30004. https://doi.org/10.1112/blms/12.3.219.

[24] J. E. Littlewood, On the mean values of certain trigonometric polynomials, *J. London Math. Soc.* **36** (1961), 307–334. MR 0141934. Zbl 0108.05801. https://doi.org/10.1112/jlms/s1-36.1.307.

[25] J. E. Littlewood, On the mean values of certain trigonometric polynomials. II, *Illinois J. Math.* **6** (1962), 1–39. MR 0141935. Zbl 0108.05802. https://doi.org/10.1215/ijm/1255631803.

[26] 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** (1966), 367–376. MR 0196043. Zbl 0142.32603. https://doi.org/10.1112/jlms/s1-41.1.367.

[27] J. E. Littlewood, The real zeros and value distributions of real trigonometrical polynomials, *J. London Math. Soc.* **41** (1966), 336–342. MR 0196372. Zbl 0142.31301. https://doi.org/10.1112/jlms/s1-41.1.336.

[28] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, *Heath Mathematical Monographs*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968. MR 0244463. Zbl 0185.11502.

[29] J. E. Littlewood and A. C. Offord, On the Number of Real Roots of a Random Algebraic Equation, *J. London Math. Soc.* **13** no. 4 (1938), 288–295. MR 1574980. Zbl 0020.13604. https://doi.org/10.1112/jlms/s1-13.4.288.

[30] J. E. Littlewood and A. C. Offord, On the distribution of the zeros and a-values of a random integral function. I, *J. London Math. Soc.* **20** (1945), 130–136. MR 0019123. Zbl 0060.21902. https://doi.org/10.1112/jlms/s1-20.3.130.

[31] J. E. Littlewood and A. C. Offord, On the distribution of zeros and a-values of a random integral function. II, *Ann. of Math.* (2) **49** (1948), 885–952; errata 50, 990–991 (1949). MR 0029981. https://doi.org/10.2307/1969404.

[32] S. Lovett and R. Meka, Constructive discrepancy minimization by walking on the edges, *SIAM J. Comput.* **44** no. 5 (2015), 1573–1582. MR 3416145. Zbl 1330.68343. https://doi.org/10.1137/130929400.

[33] O. C. McGehee, L. Pigno, and B. Smith, Hardy's inequality and the L^1 norm of exponential sums, *Ann. of Math.* (2) **113** no. 3 (1981), 613–618. MR 0621019. Zbl 0473.42001. https://doi.org/10.2307/2007000.

[34] H. L. Montgomery, Littlewood polynomials, in *Analytic Number Theory, Modular Forms and q-Hypergeometric Series*, *Springer Proc. Math. Stat.* **221**, Springer, Cham, 2017, pp. 533–553. MR 3773937. Zbl 1391.42004. https://doi.org/10.1007/978-3-319-68376-8_3.

[35] A. Odlyzko, Search for ultraflat polynomials with plus and minus one coefficients, in *Connections in Dscrete Mathematics*, Cambridge Univ. Press, Cambridge, 2018, pp. 39–55. MR 3821831. Zbl 1400.30005. https://doi.org/10.1017/9781316650295.004.

[36] B. Rodgers, On the distribution of Rudin-Shapiro polynomials and lacunary walks on $SU(2)$, *Adv. Math.* **320** (2017), 993–1008. MR 3709127. Zbl 1392.11070. https://doi.org/10.1016/j.aim.2017.09.022.

[37] W. Rudin, Some theorems on Fourier coefficients, *Proc. Amer. Math. Soc.* **10** (1959), 855–859. MR 0116184. Zbl 0091.05706. https://doi.org/10.2307/2033608.

[38] I. Z. Ruzsa, Negative values of cosine sums, *Acta Arith.* **111** no. 2 (2004), 179–186. MR 2039421. Zbl 1154.11312. https://doi.org/10.4064/aa111-2-6.

[39] R. Salem and A. Zygmund, Some properties of trigonometric series whose terms have random signs, *Acta Math.* **91** (1954), 245–301. MR 0065679. Zbl 0056.29001. https://doi.org/10.1007/BF02393433.

[40] A. C. Schaeffer, Inequalities of A. Markoff and S. Bernstein for polynomials and related functions, *Bull. Amer. Math. Soc.* **47** (1941), 565–579. MR 0005163. Zbl 0027.05205. https://doi.org/10.1090/S0002-9904-1941-07510-5.

[41] H. S. Shapiro, Extremal problems for polynomials and power series, 1951, thesis for S.M. degree, Massachusetts Institute of Technology, 102 pp. Available at http://hdl.handle.net/1721.1/12198.

[42] J. Spencer, Six standard deviations suffice, *Trans. Amer. Math. Soc.* **289** no. 2 (1985), 679–706. MR 0784009. Zbl 0577.05018. https://doi.org/10.2307/2000258.

(Received: July 22, 2019)
(Revised: September 16, 2020)

Mathematical Institute, University of Oxford, Oxford, UK
E-mail: Paul.Balister@maths.ox.ac.uk

Department of Pure Mathematics and Mathematical Statistics, Cambridge, UK and Department of Mathematical Sciences, University of Memphis, Memphis, TN, USA
E-mail: b.bollobas@dpmms.cam.ac.uk

IMPA, Rio de Janeiro, Brazil
E-mail: rob@impa.br

Peterhouse, University of Cambridge, Cambridge, UK
E-mail: jdrs2@cam.ac.uk

Department of Pure Mathematics and Mathematical Statistics, Cambridge, UK
E-mail: mt576@dpmms.cam.ac.uk