

On the distribution of runners on a circle

Pavel Hrubeš*

January 11, 2021

Abstract

Consider n runners running on a circular track of unit length with constant speeds such that k of the speeds are distinct. We show that, at some time, there will exist a sector S which contains at least $|S|n + \Omega(\sqrt{k})$ runners. The bound is asymptotically tight up to a logarithmic factor. The result can be generalized as follows. Let $f(x, y)$ be a complex bivariate polynomial whose Newton polytope has k vertices. Then there exists $a \in \mathbb{C} \setminus \{0\}$ and a complex sector $S = \{re^{i\theta} : r > 0, \alpha \leq \theta \leq \beta\}$ such that the univariate polynomial $f(x, a)$ contains at least $\frac{\beta-\alpha}{2\pi}n + \Omega(\sqrt{k})$ non-zero roots in S (where n is the total number of such roots and $0 \leq (\beta-\alpha) \leq 2\pi$). This shows that the Real τ -Conjecture of Koiran [9] implies the conjecture on Newton polytopes of Koiran et al. [10].

1 Introduction

Consider n runners running on a circular track with constant and distinct speeds. Does it have to be the case that, at some point in time, they concentrate in some non-trivial sector? If the speeds are sufficiently independent, Kronecker's approximation theorem [11] implies that the runners will all meet in an arbitrarily small sector. On the other hand, if the speeds are $1, 2, \dots, n$, it is easy to set the starting positions so that the runners never meet in a common half-circle, or any constant fraction of the circle. A similar construction can also be deduced from the approximation theorem of Dirichlet [2]. Furthermore, if the starting positions are chosen randomly, the runners will be almost uniformly distributed at any point in time (see Section 4 below). Nevertheless, we will show that some deviation from uniformity must occur:

Theorem. *Assume that n runners run on a circle of unit length with constant speeds such that k of the speeds are distinct. Then there exists a time and a sector S such that S contains at least $|S|n + c\sqrt{k}$ runners, where $c > 0$ is an absolute constant.*

*Institute of Mathematics of ASCR, Prague, pahrubes@gmail.com. Supported by the GACR grant 19-27871X.

Observe that $|S|n$ is the expected number of runners in S , had they been distributed uniformly, and the theorem asserts that at some time, the true distribution of runners is $c\sqrt{k}$ -far from uniform. We will also show that the bound is asymptotically tight up to a logarithmic factor.

The problem of runners has an interesting application to distribution of roots of complex polynomials. Take a bivariate polynomial $f(x, y)$ such that its Newton polytope has k vertices: $\sum_{i=0}^{k-1} x^i y^{i^2}$ is an iconic example. Given $a \in \mathbb{C} \setminus \{0\}$, consider the univariate polynomial $f(x, a)$. Then the Theorem can be generalized as follows: there exists $a \in \mathbb{C} \setminus \{0\}$ so that if $r_1 e^{2i\pi\alpha_1}, \dots, r_n e^{2i\pi\alpha_n}$ are the non-zero roots of $f(x, a)$, the distribution of $\alpha_1, \dots, \alpha_n$ is $c\sqrt{k}$ -far from uniform.

In the iconic example, a stronger and simpler result follows from a theorem of Hutchinson [7], see Section 2 for a detailed discussion. This also gives one motivation for this problem. A different motivation comes from the complexity of algebraic computations. In [9], Koiran has conjectured the following: if a *univariate* polynomial $f(x)$ is sufficiently easy to compute then $f(x)$ has a small number of distinct real roots. This is called the Real τ -Conjecture; it is rooted partly in Valiant's VP vs. VNP problem [18, 1], partly in the τ -Conjecture of Shub and Smale [15]. Later, Koiran et al. [10] conjectured that a similar statement holds for a *bivariate* polynomial and the number of vertices of its Newton polytope. While the two conjectures seem related, and they share the crucial consequence that $\text{VP} \neq \text{VNP}$, no implication between them was previously known. We can now conclude that in fact, the Real τ -Conjecture implies the conjecture on Newton polytopes.

2 Statement and discussion of main results

We first give the usual definition of the *discrepancy* of a sequence. For $r_1, \dots, r_n \in [0, 1]$,

$$D(r_1, \dots, r_n) := \sup_{0 \leq a \leq b \leq 1} \frac{1}{n} |N_{a,b}(r_1, \dots, r_n) - n(b - a)|,$$

where $N_{a,b} := |\{i : r_i \in [a, b]\}|$ is the number of r_i 's in $[a, b]$. For general $r_1, \dots, r_n \in \mathbb{R}$, we let $D(r_1, \dots, r_n) := D(\{r_1\}, \dots, \{r_n\})$, where $\{r\} := r - \lfloor r \rfloor$ is the fractional part of r . In our setting, the normalization factor $\frac{1}{n}$ in D is rather inconvenient, and we define the *bias* of r_1, \dots, r_n as

$$B(r_1, \dots, r_n) := nD(r_1, \dots, r_n).$$

Our main theorem about runners can be formally restated¹ as follows:

Theorem 1. *Let $s_1, \dots, s_n \in [0, 1]$. Let $v_1, \dots, v_n \in \mathbb{R}$ and $k := |\{v_1, \dots, v_n\}|$ be the number of distinct v_i 's. Then there exists $t \in \mathbb{R}$ such that $B(s_1 + v_1 t, \dots, s_n + v_n t) \geq \sqrt{k/12}$.*

¹In the Introduction, we asserted that there is a sector which contains *more* than the expected number of runners, whereas here we claim the existence of a sector containing *more or less* than the expected number. But if a sector contains few runners, its complement must contain many; and we can keep it closed by enlarging it by ϵ .

The theorem will be proved in Section 3, where we also give a stronger result for $k = n$. In Section 4, we show that the bound in Theorem 1 is tight up to a factor of $\sqrt{\log k}$.

Let $f(x) \in \mathbb{C}[x]$ be a complex univariate polynomial. Assume that f has n (not necessarily distinct) *non-zero* roots $r_1 e^{i\phi_1}, \dots, r_n e^{i\phi_n}$, where $r_1, \dots, r_n > 0$ and $\phi_1, \dots, \phi_n \in [0, 2\pi)$. We define the *bias* of f

$$B(f) := B\left(\frac{\phi_1}{2\pi}, \dots, \frac{\phi_n}{2\pi}\right).$$

Denoting $N_{\alpha, \beta}(f)$ the number of roots of f in the complex sector $\{re^{i\theta} : r > 0, \theta \in [\alpha, \beta]\}$, one can also write

$$B(f) = \sup_{0 \leq \alpha \leq \beta \leq 2\pi} \left| N_{\alpha, \beta}(f) - \frac{n(\beta - \alpha)}{2\pi} \right|.$$

We remark that $B(f)$ has been studied already in the classical paper of Erdős and Turán [5].

Let $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ be a *bivariate* complex polynomial. Let $\text{supp}(f) := \{(i, j) : a_{i,j} \neq 0\} \subseteq \mathbb{Z}^2$ be the set of exponents of monomials with a non-zero coefficient. The *Newton polytope* of f , $\text{Newt}(f) \subseteq \mathbb{R}^2$, is defined as the convex hull of $\text{supp}(f)$. In Section 5.2, we will prove:

Theorem 2. *Let $f(x, y)$ be a bivariate complex polynomial such that $\text{Newt}(f)$ has k vertices. Then there exists $a \in \mathbb{C} \setminus \{0\}$ such that the univariate polynomial $f(x, a)$ satisfies² $B(f(x, a)) \geq \Omega(\sqrt{k})$.*

The theorem can be motivated by the following example. Take a real polynomial $f(x) = \sum_{i=0}^n a_i x^i$. A theorem of Hutchinson [7], which appears more explicitly in [12], gives the following: if a_i are positive and

$$a_i^2 > 4a_{i-1}a_{i+1} \tag{1}$$

for every $i \in \{1, \dots, n-1\}$ then all the roots of $f(x)$ are distinct, real and negative. Now consider the bivariate polynomial $g(x, y) = \sum_{i=0}^n b_i x^i y^{i^2}$ with $b_i > 0$. Then we can set $a > 0$ small enough, so that the coefficients of the univariate polynomial $g(x, a)$ satisfy (1), and hence all the roots are real and negative. In the language of Theorem 2, $B(g(x, a)) = n$. In this argument, i^2 could be replaced by any strictly convex function (or strictly concave, letting $a \rightarrow \infty$). Furthermore, using a result of Karpenko and Vishnyakova [8], we can also assume that $b_i \in \mathbb{R}$ are non-zero (rather than positive), giving that the roots are real (rather than negative). However, things get more complicated if some coefficients are zero. In this case, we can no longer expect all the roots of $g(x, a)$ to be real, or lie on the same line $re^{i\phi}$, $r \in \mathbb{R}$. Theorem 2 nevertheless tells us that for some $a \in \mathbb{C} \setminus \{0\}$, the roots of $g(x, a)$ non-trivially concentrate in some complex sector.

²In this paper, $g(k) \geq \Omega(h(k))$ means that $g(k) \geq c \cdot h(k)$ holds for some constant $c > 0$ and every sufficiently large k .

It is easy to see that Theorem 2 does not hold if $f(x, y)$ and a are required to be real. Furthermore, as noted in Proposition 12, the bound in Theorem 2 is tight up to $\sqrt{\log k}$ factor.

We shall also give the following modification of Theorem 2. For a univariate complex polynomial $f(x) = \sum a_i x^i$, let $\Re(f)$ denote the real polynomial $\sum_i \Re(a_i) x^i$ (where $\Re(a_i)$ is the real part of a_i).

Theorem 3. *Let $f(x, y)$ be a complex polynomial such that its Newton polytope has k vertices. Then there exists $a \in \mathbb{C} \setminus \{0\}$ such that $\Re(f(x, a))$ has $\Omega(k)$ distinct real roots.*

This is proved in Section 5.3. We remark that a weaker bound of $\Omega(\sqrt{k})$ follows from Theorem 2 and Cauchy's argument principle.

An application to Real τ -Conjectures The Real τ -Conjecture of Koiran [9] asserts the following: let $f \in \mathbb{R}[x]$ be a real univariate polynomial which can be written as

$$f = \sum_{i=1}^p \prod_{j=1}^q f_{i,j}, \quad \text{where } |\text{supp}(f_{i,j})| \leq r, \quad (2)$$

then f has at most $(pqr)^c$ distinct real roots (for some absolute constant c). In [10], Koiran et al. have made a similar conjecture (called the τ -Conjecture for Newton Polygons): let $f(x, y)$ be a real *bivariate* polynomial as in (2), then $\text{Newt}(f(x, y))$ has at most $(pqr)^{c'}$ vertices. Using Theorem 2, we can conclude the two conjectures are related:

Proposition 4. *The Real τ -Conjecture implies the τ -Conjecture for Newton Polygons.*

Proof. In [6], it was shown that the Real τ -Conjecture implies the following: given a *complex* univariate polynomial f as in (2), its bias can also be bounded as $B(f) \leq (pqr)^{c''}$ (where $c'' > 0$ is a new absolute constant). Assume now that $f(x, y)$ is a (real or complex) polynomial of the form (2) such that $\text{Newt}(f(x, y))$ has k vertices. By Theorem 2, we can find $a \in \mathbb{C} \setminus \{0\}$ so that $B(f(x, a)) \geq C\sqrt{k}$, with a constant $C > 0$. Assuming the Real τ -Conjecture, the result in [6] gives that $C\sqrt{k} \leq (pqr)^{c''}$ and hence $k \leq C^2(pqr)^{2c''}$ – as required³ by the conjecture on Newton polytopes. \square

We point out that the same could be concluded from Theorem 3 and a lemma from [6] relating the complexity of f with that of $\Re(f)$.

Some notation For $n \in \mathbb{N}$, let $[n] := \{1, \dots, n\}$. For $r \in \mathbb{R}$, $\{r\} := r - \lfloor r \rfloor$ is the fractional part of r . $\log(x)$ is the logarithm in base two.

³As the non-trivial case is $pqr \geq 2$, the constant C^2 can be subsumed in the exponent.

3 Lower bounds on the discrepancy of runners

In this section, we prove Theorem 1, as well as give a stronger bound in the special case $k = n$. We point out that the special case can be easily proved by estimating $\max_{t \in [0,1]} \left| \sum_{j=1}^n e^{2\pi i(s_j + v_j t)} \right|$ and then using some well-known properties of discrepancy, such as the Koksma inequality (see, e.g., the monograph [14]). In the case of non-distinct speeds, this approach seems hard to implement and leads to Turán style problems on power-sums [17, 13]. The strategy of our proof is therefore different. We directly estimate the expectation of the square of the number of runners in S , for a random time t and a random sector S . It is more convenient to first analyze the case when the speeds are integers: at time $t = 1$ the runners return to their original positions and it is enough to understand the system in the interval $t \in [0, 1]$.

Given $0 \leq \gamma \leq 1$ and $\alpha \in \mathbb{R}$, let

$$S_{\alpha, \alpha + \gamma} := \{x \in [0, 1] : \{x - \alpha\} \leq \gamma\}.$$

When $[0, 1]$ is viewed as a circle, $S_{\alpha, \alpha + \gamma}$ is the closed sector which starts at α and continues clockwise for distance γ . γ will be called the *aperture* of $S_{\alpha, \alpha + \gamma}$ and denoted $|S_{\alpha, \alpha + \gamma}|$. Given a sector S and $x \in \mathbb{R}$, we define

$$\chi_S(x) = \begin{cases} 1, & \{x\} \in S \\ 0, & \{x\} \notin S \end{cases}.$$

Let $N_S(x_1, \dots, x_n) := \sum_{i=1}^n \chi_S(x_i)$ and $\chi_{\alpha, \gamma}(x) := \chi_{S_{\alpha, \alpha + \gamma}}(x)$.

Remark.

$$B(r_1, \dots, r_n) = \sup_{0 \leq \alpha, \gamma \leq 1} |N_{S_{\alpha, \alpha + \gamma}}(r_1, \dots, r_n) - \gamma n|.$$

Moreover, it does not matter whether the sectors are closed, open, or half-open.

In the following, $\mathbb{E}_x h(x)$ will stand for $\int_0^1 h(x) dx$, the expectation of $h(x)$ on $[0, 1]$. Similarly, $\mathbb{E}_{x,y} h(x, y)$ stands for $\int_0^1 \int_0^1 h(x, y) dy dx$ etc. In the cases considered below, Fubini's theorem is applicable and we have $\mathbb{E}_{x,y} = \mathbb{E}_{y,x}$.

Lemma 5. *Let $s_1, s_2 \in \mathbb{R}$, let v_1, v_2 be distinct integers and $\gamma \in [0, 1]$. Then*

$$\mathbb{E}_{t, \alpha} \chi_{\alpha, \gamma}(s_1 + v_1 t) = \gamma, \tag{3}$$

$$\mathbb{E}_{t, \alpha} \chi_{\alpha, \gamma}(s_1 + v_1 t) \chi_{\alpha, \gamma}(s_2 + v_2 t) = \gamma^2. \tag{4}$$

Proof. (3) is rather obvious. In fact, we already have

$$\mathbb{E}_{\alpha} \chi_{\alpha, \gamma}(s + vt) = \gamma, \quad \mathbb{E}_t \chi_{\alpha, \gamma}(s + vt) = \gamma,$$

where the latter holds if⁴ $v \in \mathbb{Z} \setminus \{0\}$.

⁴The assumption $v \in \mathbb{Z}$ makes $\chi_{\alpha, \gamma}(s + vt)$ 1-periodic in t , and $v \neq 0$ guarantees the runner spends γ -fraction of time in $S_{\alpha, \alpha + \gamma}$.

To prove (4), note that $\chi_{\alpha,\gamma}(x+z) = \chi_{\alpha-z,\gamma}(x)$ and the left-hand side of (4) equals $A := \int_0^1 \int_0^1 \chi_{\alpha-v_1t,\gamma}(s_1)\chi_{\alpha-v_2t,\gamma}(s_2)d\alpha dt$. We have

$$\begin{aligned} \int_0^1 \chi_{\alpha-v_1t,\gamma}(s_1)\chi_{\alpha-v_2t,\gamma}(s_2)d\alpha &= \int_{-v_1t}^{1-v_1t} \chi_{\alpha',\gamma}(s_1)\chi_{\alpha'+(v_1-v_2)t,\gamma}(s_2)d\alpha' = \\ &= \int_0^1 \chi_{\alpha',\gamma}(s_1)\chi_{\alpha'+(v_1-v_2)t,\gamma}(s_2)d\alpha', \end{aligned}$$

where we have used the substitution $\alpha' = \alpha - v_1t$ and the fact that $\chi_{\alpha,\gamma}$ is 1-periodic in the first argument. Exchanging the order of integration, we have

$$\begin{aligned} A &= \int_0^1 \int_0^1 \chi_{\alpha,\gamma}(s_1)\chi_{\alpha+(v_1-v_2)t,\gamma}(s_2)d\alpha dt = \\ &= \int_0^1 \left(\chi_{\alpha,\gamma}(s_1) \int_0^1 \chi_{\alpha+(v_1-v_2)t,\gamma}(s_2)dt \right) d\alpha = \int_0^1 (\chi_{\alpha,\gamma}(s_1)\gamma) d\alpha = \gamma^2. \end{aligned}$$

□

As a warm-up for Theorem 1, we first consider the case of runners with distinct speeds. In this case, the obtained result is stronger.

Theorem 6. *Let v_1, \dots, v_n be distinct real numbers and $s_1, \dots, s_n \in [0, 1]$. Let $\gamma \in [0, 1]$. Then there exists $t \in \mathbb{R}$ and a sector $S = S_{\alpha, \alpha+\gamma}$ of aperture γ such that*

$$|N_S(s_1 + v_1t, \dots, s_n + v_nt) - \gamma n| \geq \sqrt{(\gamma - \gamma^2)n}.$$

In particular, there exists $t \in \mathbb{R}$ such that $B(s_1 + v_1t, \dots, s_n + v_nt) \geq \sqrt{n}/2$.

Proof. Assume first that v_1, \dots, v_n are distinct integers. Define $N(\alpha, t) := \sum_{i=1}^n \chi_{\alpha,\gamma}(s_i + v_it)$; the number of runners in $S_{\alpha, \alpha+\gamma}$ at time t . We shall abbreviate $\mathbb{E}_{\alpha,t}$ by \mathbb{E} . We want to estimate $\mathbb{E}((N(\alpha, t) - \gamma n)^2)$. By the previous lemma, we obtain $\mathbb{E}(N(\alpha, t)) = \gamma n$. This implies $\mathbb{E}((N(\alpha, t) - \gamma n)^2) = \mathbb{E}((N(\alpha, t))^2) - \gamma^2 n^2$. Moreover, the lemma also gives

$$\begin{aligned} \mathbb{E}(\chi_{\alpha,\gamma}(s_i + v_it)\chi_{\alpha,\gamma}(s_j + v_jt)) &= \gamma, \text{ if } i = j, \\ &= \gamma^2, \text{ if } i \neq j. \end{aligned}$$

This means that

$$\begin{aligned} \mathbb{E}(N(\alpha, t)^2) &= \sum_{i=1}^n \mathbb{E}(\chi_{\alpha,\gamma}(s_i + v_it)^2) + \sum_{i \neq j} \mathbb{E}(\chi_{\alpha,\gamma}(s_i + v_it)\chi_{\alpha,\gamma}(s_j + v_jt)) = \\ &= \gamma n + \gamma^2 n(n-1) = (\gamma - \gamma^2)n + \gamma^2 n^2. \end{aligned}$$

Altogether, we obtain

$$\mathbb{E}((N(\alpha, t) - \gamma n)^2) = (\gamma - \gamma^2)n + \gamma^2 n^2 - \gamma^2 n^2 = (\gamma - \gamma^2)n.$$

This means that for some α and t , $|N(\alpha, t) - \gamma n| \geq \sqrt{(\gamma - \gamma^2)n}$ which proves the special case of the theorem.

For non-integer speeds, we will apply Dirichlet's approximation theorem. If v'_1, \dots, v'_n are distinct real numbers and $\epsilon > 0$, the theorem gives a positive integer q and integers v_1, \dots, v_n such that $|v'_i q - v_i| \leq \epsilon$ for every i . Let $N'(\alpha, t) := \sum_{i=1}^n \chi_{\alpha, \gamma}(s_i + v'_i t)$ and $N(\alpha, t)$ be as above. We again want to estimate $|N'(\alpha, t) - \gamma n|$. Since we can scale the time by a factor of q , we can assume that in fact $q = 1$ and so $|v'_i - v_i| \leq \epsilon$ for every i . We observe that

$$\mathbb{E}((N'(\alpha, t) - \gamma n)^2) \geq \mathbb{E}((N(\alpha, t) - \gamma n)^2) - \epsilon c_n,$$

where c_n is a constant depending only on n . This is because $N(\alpha, t)$ and $N'(\alpha, t)$ differ on at most an $2\epsilon n$ -fraction of $\alpha \in [0, 1]$. Hence we conclude that there exists α and time t with $|N'(\alpha, t) - \gamma n| \geq \sqrt{(\gamma - \gamma^2)n} - \epsilon c'_n$. Since we can pick ϵ arbitrarily small and $N'(\alpha, t)$ is an integer, we conclude $|N'(\alpha, t) - \gamma n| \geq \sqrt{(\gamma - \gamma^2)n}$ for some α, t . \square

We remark that the main part of Theorem 6 fails miserably if the runners have non-distinct speeds. Consider $n = 2k$ runners with k distinct speeds running in pairs such that in a given pair, the two runners maintain distance $1/2$. Then we can set the starting positions so that for every sector S of aperture $\gamma = 1/2$ and every time, the number of runners in the sector is at least k and at most⁵ $k + 4$.

To prove Theorem 1, we need one more lemma:

Lemma 7. *Let $s_1, \dots, s_m \in \mathbb{R}$ and $\alpha \in [0, 1]$. Let $N(\gamma) := \sum_{i=1}^m \chi_{\alpha, \gamma}(s_i)$. Then*

$$\mathbb{E}_{\gamma}((N(\gamma) - \gamma m)^2) \geq \frac{1}{12}.$$

Proof. The function $N(\gamma)$ is integer-valued. Hence $|N(\gamma) - \gamma m| \geq \Delta(\gamma m)$, where $\Delta(z) \in [0, 1/2]$ denotes the distance of $z \in \mathbb{R}$ from a closest integer. It is therefore enough to estimate $\int_0^1 \Delta(\gamma m)^2 d\gamma$. The function $\Delta(\gamma m)$ is $1/m$ -periodic and symmetric with respect to the point $\gamma_0 = 1/2m$. This means that $\int_0^1 \Delta(\gamma m)^2 d\gamma = 2m \int_0^{1/2m} \Delta(\gamma m)^2 d\gamma$. Furthermore, if $\gamma \in [0, 1/2m]$ then $\Delta(\gamma m) = \gamma m$ and hence

$$\int_0^{1/2m} \Delta(\gamma m)^2 d\gamma = m^2 \int_0^{1/2m} \gamma^2 d\gamma = \frac{m^2}{3(2m)^3} = \frac{1}{24m}.$$

This gives $\int_0^1 \Delta(\gamma m)^2 \geq 2m/24m = 1/12$. \square

Proof of Theorem 1. We will assume that v_1, \dots, v_n are integers; the general case proceeds in the same way as in the proof of Theorem 6. Without loss of generality, assume that already v_1, \dots, v_k are distinct. Given $j \in [k]$,

⁵This is owing to the fact that S is closed; a half-closed sector would contain precisely k runners at every time.

let $A_j := \{i \in [n] : v_i = v_j\}$ be the set of runners with speed v_j . Let $N_j(\alpha, \gamma, t) := \sum_{i \in A_j} \chi_{\alpha, \gamma}(s_i + v_i t)$ and $N(\alpha, \gamma, t) := \sum_{i=1}^n \chi_{\alpha, \gamma}(s_i + v_i t)$. Hence $N(\alpha, \gamma, t)$ denotes the number of runners in $S_{\alpha, \alpha + \gamma}$ at time t and $N(\alpha, \gamma, t) = \sum_{j=1}^k N_j(\alpha, \gamma, t)$. We want to estimate $\mathbb{E}((N(\alpha, \gamma, t) - \gamma n)^2)$, where \mathbb{E} now stands for $\mathbb{E}_{\alpha, \gamma, t}$.

Setting $g_j(\alpha, \gamma, t) := N_j(\alpha, \gamma, t) - \gamma |A_j|$, we claim that

$$\begin{aligned} \mathbb{E}(g_j^2) &\geq 1/12, \\ \mathbb{E}(g_{j_1} g_{j_2}) &= 0, \text{ if } j_1 \neq j_2. \end{aligned} \tag{5}$$

The first inequality is a consequence of Lemma 7. (5) is an application of Lemma 5 as follows. For a fixed γ , we have $\mathbb{E}_{\alpha, t} N_j(\alpha, \gamma, t) = \gamma |A_j|$ which means that

$$\mathbb{E}_{\alpha, t}(g_{j_1} g_{j_2}) = \mathbb{E}_{\alpha, t}(N_{j_1}(\alpha, \gamma, t) N_{j_2}(\alpha, \gamma, t)) - \gamma^2 |A_{j_1}| |A_{j_2}|.$$

Furthermore, by Lemma 5,

$$\begin{aligned} \mathbb{E}_{\alpha, t}(N_{j_1}(\alpha, \gamma, t) N_{j_2}(\alpha, \gamma, t)) &= \sum_{i_1 \in A_{j_1}, i_2 \in A_{j_2}} \mathbb{E}_{\alpha, t} \chi_{\alpha, \gamma}(s_{i_1} + v_{j_1} t) \chi_{\alpha, \gamma}(s_{i_2} + v_{j_2} t) = \\ &= \gamma^2 |A_{j_1}| |A_{j_2}|. \end{aligned}$$

This shows that the left-hand side of (5) indeed equals zero.

We now have

$$\mathbb{E}((N(\alpha, \gamma, t) - \gamma n)^2) = \mathbb{E}((\sum_{j=1}^k g_j)^2) = \sum_{j=1}^k \mathbb{E}(g_j^2) + \sum_{j_1 \neq j_2} \mathbb{E}(g_{j_1} g_{j_2}) \geq \frac{k}{12}.$$

This implies that for some α, t, γ , $|N(\alpha, \gamma, t) - \gamma n| \geq \sqrt{k/12}$. □

4 An upper bound on the discrepancy of runners

We now want to show that the bounds in Theorem 1 and Theorem 6 are tight up to logarithmic factors.

Theorem 8. *Let $v_1 := 1, \dots, v_n := n$. There exist $s_1, \dots, s_n \in [0, 1)$ such that for every $t \in \mathbb{R}$ and every $\gamma \in [0, 1]$, the following holds. For every sector S of aperture γ , $|N_S(s_1 + v_1 t, \dots, s_n + v_n t) - \gamma n| \leq O(\sqrt{n\gamma \log n} + \log n)$. Hence $B(s_1 + v_1 t, \dots, s_n + v_n t) \leq O(\sqrt{n \log n})$.*

Clearly, this implies a similar bound in the general case of non-distinct speeds. If $k \leq n$, set v_1, \dots, v_n so that $v_1 = 1, \dots, v_k = k$ and $v_{k+1}, \dots, v_n = k$. Applying Theorem 8 and setting the starting positions of the last $n - k + 1$ runners so that they uniformly partition the circle, we have for every t

$$B(s_1 + v_1 t, \dots, s_n + v_n t) \leq O(\sqrt{k \log k}).$$

Proof of Theorem 8. Pick $s_1, \dots, s_n \in [0, 1]$ uniformly and independently at random. Let $N_S(t) := N_S(s_1 + v_1 t, \dots, s_n + v_n t)$ be the number of runners in S at time t . We claim that for every fixed t and a fixed sector S of aperture $\gamma \geq 4 \log n/n$,

$$\Pr_{s_1, \dots, s_n} \left[|N_S(t) - \gamma n| \geq 4\sqrt{n\gamma \log n} \right] \leq n^{-5}. \quad (6)$$

For if s_1, \dots, s_n are uniform and independent, so are $s_1 + v_1 t, \dots, s_n + v_n t$. The expected value of $N_S(t)$ is $\mu := \gamma n$. Chernoff bound gives that for every $0 \leq \delta \leq 1$,

$$\Pr[N_S(t) \leq (1 - \delta)\mu] \leq e^{-\delta^2 \mu/2}, \quad \Pr[N_S(t) \geq (1 + \delta)\mu] \leq e^{-\delta^2 \mu/3}.$$

If we now set $\delta := 4\sqrt{\frac{\log n}{\gamma n}}$, we have $\delta\mu = 4\sqrt{n\gamma \log n}$ and $\delta^2 \mu = 16 \log n$. Hence both the probabilities in (6) are at most $e^{-16 \log n/3} \leq n^{-5}$.

Let $m := \lfloor n/(4 \log n) \rfloor$ and $\gamma_0 := 1/m$. Let \mathcal{S} be the set of sectors of the form $S_{i\gamma_0, i\gamma_0 + j\gamma_0}$, $i, j \in \{0, \dots, m-1\}$. That is, \mathcal{S} consists of the m^2 sectors whose starting point and aperture is a multiple of γ_0 . Let \mathcal{T} be the set of times of the form k/nm , $k \in \{0, \dots, nm+1\}$. Since $m < n$, we have $|\mathcal{S}| \cdot |\mathcal{T}| \leq n^4$. Then (6) and the union bound give that, with positive probability, $|N_S - |S| \cdot n| \leq 4\sqrt{n|S| \log n}$ holds for every $S \in \mathcal{S}$ and $t \in \mathcal{T}$.

Hence there exist s_1, \dots, s_n so that

$$|N_S - |S| \cdot n| \leq 4\sqrt{n|S| \log n}, \quad \text{for all } S \in \mathcal{S}, t \in \mathcal{T}. \quad (7)$$

We first claim that this can be extended also to times not in \mathcal{T} :

$$|N_S - |S| \cdot n| \leq 4\sqrt{n|S| \log n} + O(\log n), \quad \text{for all } S \in \mathcal{S}, t \in \mathbb{R}. \quad (8)$$

For, given a "small" sector S_0 in \mathcal{S} of aperture γ_0 , (7) tells us that $N_{S_0} \leq 8 \log n + 1$. Between two consecutive times $t_1 = k/nm$ and $t_2 = (k+1)/nm$ in \mathcal{T} , the fastest runner with speed n covers distance $n/nm = \gamma_0$. This means that the runners that come to or leave from a sector S must come from, or move to, the at most two adjacent small sectors of aperture γ_0 . In a similar fashion, we can extend (8) to all sectors of aperture $\gamma \in [0, 1]$. For given such a sector S , we can find $S_1 \in \mathcal{S} \cup \{\emptyset\}$ and $S_2 \in \mathcal{S}$ with $S_1 \subseteq S \subseteq S_2$ and apertures satisfying $|S_1| \geq \gamma - 2\gamma_0$, $|S_2| \leq \gamma + 2\gamma_0$. \square

4.1 An explicit construction

It would be interesting to give an explicit construction of low-discrepancy runners, and we now make a step in this direction. We will use the Erdős-Turán inequality [4] which is a useful tool for bounding discrepancy. We also note that the inequality would somewhat simplify the proof of Theorem 8 (see also [3]), at the cost of obtaining weaker bounds.

It is convenient to interpret the discrepancy of runners in terms of norms of complex polynomials. Let $f(x) = \sum_i a_i x^i$ be a complex polynomial. Let $|f|_m :=$

$\max_{|x|=1} |f(x)|$ be its maximum on the unit complex circle. Furthermore, let $f^{(k)}(x) := \sum_i a_i^k x^i$ be the Hadamard power of f . The following lemma is a straightforward adaptation of the Erdős-Turán inequality to our setting:

Lemma 9. *Let v_1, \dots, v_n be distinct non-negative integers, $s_1, \dots, s_n \in [0, 1)$ and $f(x) := \sum_{i=1}^n e^{2\pi i s_i} x^{v_i}$. Then for every $t \in \mathbb{R}$,*

$$B(s_1 + v_1 t, \dots, s_n + v_n t) \leq c \left(1 + \sum_{k=1}^n \frac{|f^{(k)}(x)|_m}{k} \right),$$

where $c > 0$ is an absolute constant.

In order to apply Lemma 9, we want to find a polynomial $f(x)$ with unimodular coefficients such that $|f^{(k)}(x)|_m$ is small for every $k \leq n$. Our construction is a generalization of that of Shapiro polynomials, see, e.g., [16]. Shapiro's construction gives a polynomial $f(x)$ with ± 1 coefficients and degree $d = 2^n - 1$ such that $|f(x)|_m \leq 2^{(n+1)/2} = \sqrt{2(d+1)}$.

Let us fix a prime p . Let ξ be a p -th primitive root of unity. Let D be the $p \times p$ (unnormalized) discrete Fourier transform matrix, $D_{j,k} = \xi^{jk}$, $j, k \in \{0, \dots, p-1\}$. Recursively, we construct a p -tuple of polynomials $Q_{0,r}, \dots, Q_{p-1,r}$. We set $Q_{0,0} := 1, \dots, Q_{p-1,0} := 1$. If $r \geq 0$, we let

$$\begin{pmatrix} Q_{0,r+1} \\ Q_{1,r+1} \\ \vdots \\ Q_{p-1,r+1} \end{pmatrix} = D \cdot \begin{pmatrix} Q_{0,r} \\ x^{p^r} Q_{1,r} \\ \vdots \\ x^{(p-1)p^r} Q_{p-1,r} \end{pmatrix}. \quad (9)$$

The construction guarantees that every $Q_{i,r}$ has degree $d_r = p^r - 1$ and that its coefficients have absolute value one.

For example, in the case $p = 2$, we obtain the usual Shapiro polynomials. The definition is simplified to

$$Q_{0,0}, Q_{1,0} = 1, \quad \begin{pmatrix} Q_{0,r+1} \\ Q_{1,r+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} Q_{0,r} \\ x^{2^r} Q_{1,r} \end{pmatrix},$$

and gives the sequence:

$$\begin{array}{ccccccc} 1 & 1+x & 1+x+x^2-x^3 & 1+x+x^2-x^3+x^4+x^5-x^6+x^7 & & & \\ 1 & 1-x & 1+x-x^2+x^3 & 1+x+x^2-x^3-x^4-x^5+x^6-x^7 & , & \dots & \end{array}$$

We can bound $|Q_{i,r}^{(k)}|_m$ as follows.

Proposition 10. *Let $0 \leq i \leq p-1$ and k be a natural number such that p does not divide k . Then $|Q_{i,r}^{(k)}|_m \leq p^{\frac{r+1}{2}} = \sqrt{p(d_r+1)}$.*

Proof. Assume first that $k = 1$. We will prove that for every x with $|x| = 1$,

$$|Q_{0,r}(x)|^2 + \dots + |Q_{p-1,r}(x)|^2 = p^{r+1}. \quad (10)$$

This is by induction on r . If $r = 0$, the statement is clear. For the inductive step, let $Q_{r+1}(x)$ be the vector on the left-hand side of (9) and $P_r(x)$ the one on the right-hand side, so that $Q_{r+1}(x) = DP_r(x)$. For $u \in \mathbb{C}^p$ let $|u|$ be its Euclidean norm. The matrix D satisfies $D \cdot \bar{D}^t = pI_p$. This means that for every $u \in \mathbb{C}^p$, $|Du|^2 = p|u|^2$. Hence we have $|Q_{r+1}(x)|^2 = p|P_r(x)|^2$ for every $x \in \mathbb{C}$. Furthermore, if $|x| = 1$, we have $|P_r(x)|^2 = |Q_r(x)|^2$ and hence $|Q_{r+1}(x)|^2 = p|Q_r(x)|^2$. This implies (10).

Equality (10) gives $|Q_{i,r}|_m \leq p^{(r+1)/2}$ as required. Let k be such that p does not divide k . Then $Q_{i,r}^{(k)}$ satisfy the same recursive definition, except that the root ξ is replaced with ξ^k , and the same conclusion holds. \square

In order to obtain low-discrepancy runners from Proposition 10, it is enough to take the polynomial $Q_{0,r}$ for a suitable r . It turns out that $r = 3$ gives optimal parameters in this setting.⁶

Corollary 11. *Let p be a prime and $n := p^3$. Let $s_0, \dots, s_{n-1} \in [0, 1)$ be such that $Q_{0,3} = \sum_{j=0}^{n-1} e^{2\pi i s_j} x^j$. Then $B(s_0, s_1 + t, \dots, s_{n-1} + (n-1)t) \leq O(n^{2/3} \log n)$ for every $t \in \mathbb{R}$.*

Proof. By Lemma 9, it is enough to estimate $A := \sum_{k=1}^n \frac{|Q_{0,3}^{(k)}|_m}{k}$. If $p \nmid k$, we have $|Q_{0,3}^{(k)}|_m \leq p^2 = n^{2/3}$ by Proposition 10. Hence

$$\sum_{k \leq n, p \nmid k} \frac{|Q_{0,3}^{(k)}(x)|_m}{k} \leq \sum_{k=1}^n \frac{n^{2/3}}{k} \leq O(n^{2/3} \log n).$$

If p divides k , we have $|Q_{0,3}^{(k)}|_m \leq n$. Hence

$$\sum_{k \leq n, p|k} \frac{|Q_{0,3}^{(k)}(x)|_m}{k} \leq \sum_{k \leq n, p|k} \frac{n}{k} = \frac{n}{p} \sum_{a=1}^{n/p} \frac{1}{a} \leq O(n^{2/3} \log n).$$

This gives the estimate $A \leq O(n^{2/3} \log n)$. \square

5 Newton polytopes and angular distribution of zeros

In this section, we prove Theorems 2 and 3.

⁶Hence the recursion (9) is applied 3 times. Note, however, that $Q_{0,3}$ implicitly depends on the chosen prime p (and the root ξ).

5.1 The connection with runners

We start by discussing the connection between Theorem 2 and the discrepancy of runners. Let $f(x, y)$ be a polynomial of the form

$$f(x, y) = x^{m_1} y^{m_2} \prod_{i=1}^n (x - a_i y^{q_i}), \quad (11)$$

where $a_i = r_i e^{2\pi i s_i}$, $r_i > 0$, $s_i \in [0, 1)$, and $m_1, m_2, q_1, \dots, q_n \in \mathbb{Z}$ with $m_1, m_2 \geq 0$. Let $k := |\{q_1, \dots, q_n\}|$ be the number of distinct q_i 's. Then $\text{Newt}(f(x, y))$ has precisely $2k$ vertices (if $k > 0$). This is because the Newton polytope of a product $g_1 g_2$ is the Minkowski sum of Newton polytopes of the factors g_1 and g_2 (see, e.g., [10] or references within). Hence, $\text{Newt}(f(x, y))$ is the Minkowski sum of line segments (and a point) with precisely k distinct gradients, which yields $2k$ vertices. Given $a = r e^{2\pi i t}$, $r > 0$, the non-zero roots of $f(x, a)$ are of the form $r^{q_j} r_j e^{2\pi i (s_j + q_j t)}$, $j \in [n]$. Hence, as t varies, their arguments are

$$2\pi(s_1 + q_1 t), \dots, 2\pi(s_n + q_n t),$$

and they can be seen as a system of runners on a circle of length one with speeds q_1, \dots, q_n . Using Theorem 1, these observations entail:

$$B(f(x, a)) \geq \Omega(\sqrt{k}), \text{ for some } a \text{ with } |a| = 1.$$

Conversely, a system of runners $s_1 + v_1 t, \dots, s_n + v_n t$, $v_1, \dots, v_n \in \mathbb{N}$, can be associated with the bivariate polynomial

$$g(x, y) = \prod_{j=1}^n (x - e^{2\pi i s_j} y^{v_j}).$$

This and Theorem 8 implies:

Proposition 12. *For every n , there exists $g(x, y)$ whose Newton polytope has $2n$ vertices but for every $a \in \mathbb{C} \setminus \{0\}$, $B(g(x, a)) \leq O(\sqrt{n \log n})$.*

We remark that g can be assumed to have *real* coefficients by taking instead $g \cdot \bar{g} = \prod_{j=1}^n (x^2 - 2 \cos(2\pi s_j) x y^{v_j} + y^{2v_j})$. Furthermore, Theorem 8 gives more information: for example, every small sector of aperture $O(\log n/n)$ contains at most $O(\log n)$ runners. The same could be said about the roots of $g(x, a)$.

5.2 Proof of Theorem 2

Our goal is to deduce Theorem 2 from Theorem 1. The strategy is to approximate $f(x, y)$ by polynomials corresponding to edges of its Newton polytope – hence reducing the problem to the already understood case as in (11). As pointed out by an anonymous referee, the following proof is similar to the proof of Newton-Puiseux theorem (see, e.g., [19]). The theorem expresses roots of

$f(x, y) = 0$, when viewed as a polynomial in x , as Puiseux series in y . Moreover, the first approximation of the series is given by monomials on the boundary $\text{Newt}(f(x, y))$, which would lead to an alternative proof of Theorem 2 from Theorem 1.

Let $g(x, y)$ be a polynomial such that $\text{Newt}(g)$ lies on the line $\ell = \{(t, qt+m) : t \in \mathbb{R}\}$, $q \in \mathbb{Q}$. Then $g(x, y)$ can be written as

$$g(x, y) = y^m \sum_{j=n_1}^{n_2} c_j x^j y^{qj}. \quad (12)$$

Furthermore, if $q \in \mathbb{Z}$, $g(x, y)$ can be factored as

$$g(x, y) = a_0 y^m \prod_{i=1}^n (xy^q - a_i), \quad (13)$$

where $a_0, \dots, a_n \in \mathbb{C}$.

Lemma 13. *Let $g(x, y)$ be as in (13) with $a_0 \neq 0$. Let $h(x, y)$ be a polynomial such that $\text{Newt}(h)$ lies in the strict upper-half plane determined by ℓ . Then for every $\epsilon > 0$ sufficiently small, and every $a \in \mathbb{C}$ with $0 < |a|$ sufficiently small with respect to ϵ , the following holds. Let ξ be a non-zero root of $g(x, a)$ of multiplicity p . Then $g(x, a) + h(x, a)$ has precisely p roots ξ' which satisfy $|\xi' - \xi| \leq \epsilon|\xi|$, counted with multiplicity.*

Proof. This is an application of Rouché's theorem. Let $0 < \epsilon < 1$ be such that $\epsilon < |a_i - a_j|$ for every $a_i \neq a_j$. Given $a \in \mathbb{C} \setminus \{0\}$, every root of $g(x, a)$ is of the form $\xi(a) = a_k a^{-q}$ for some $a_k \neq 0$. Let us fix such an a_k . Let $\Omega(a)$ be the open ball with centre at $\xi(a)$ and radius $\epsilon|\xi(a)|$. Let M_1 be the minimum of $|g(x, 1)|$ on $\partial\Omega(1)$. Hence $M_1 > 0$ and

$$\min_{x \in \partial\Omega(a)} |g(x, a)| \geq M_1 |a|^m. \quad (14)$$

Furthermore, we claim that there exists M_2 independent on a such that whenever $|a| < 1$,

$$\max_{x \in \partial\Omega(a)} |h(x, a)| \leq M_2 |a|^{m+1}. \quad (15)$$

For let $h(x, y) = \sum_{(i,j) \in A} c_{i,j} x^i y^j$. By the assumption on h (also recall that q is an integer), we have that $j \geq qi + m + 1$ whenever $c_{i,j} \neq 0$. Furthermore, given $x \in \partial\Omega(a)$, we have $|x| \leq 2|\xi(a)| = 2|a_k||a|^{-q}$. Hence,

$$\begin{aligned} |h(x, a)| &\leq \sum_{(i,j) \in A} |c_{i,j}| |x|^i |a|^j \leq \sum_{(i,j) \in A} |c_{i,j}| |2a_k|^i |a|^{-qi+j} \\ &\leq |a|^{m+1} \sum_{(i,j) \in A} |c_{i,j}| |2a_k|^i, \end{aligned}$$

which shows that (15) holds.

Inequalities (14) and (15) imply that for every a with $|a|$ small enough, $|h(x, a)| < |g(x, a)|$ holds for every $x \in \partial\Omega(a)$. Rouché's theorem then gives that $g(x, a)$ and $g(x, a) + h(x, a)$ contain the same number of roots in $\Omega(a)$, counted with multiplicities. \square

We now make some observations about polytopes. Let $P \subseteq \mathbb{R}^2$ be a polytope with $k > 2$ vertices. Then P has k edges. An edge e will be called a *lower edge*, if P lies in the closed upper-half plane determined by the line passing through e . Similarly, an *upper edge* and the lower-half plane. Every edge e is either a lower or an upper edge, unless e is parallel to the y -axis. There can be at most two such edges, and we conclude that P has either at least $(k - 2)/2$ lower edges, or at least $(k - 2)/2$ upper edges.

Suppose that P has s lower edges e_1, \dots, e_s with gradients q_1, \dots, q_s . Then the gradients are distinct and, assuming $q_1 < \dots < q_s$, P contains vertices $(a_1, b_1), \dots, (a_{s+1}, b_{s+1})$ with $a_1 < \dots < a_{s+1}$ such that every e_i connects (a_i, b_i) and (a_{i+1}, b_{i+1}) . Furthermore, the projection of P to the x -axis is the interval $[a_1, a_{s+1}]$.

Let $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ and let $e \subseteq \mathbb{R}^2$ be an edge of $\text{Newt}(f)$ connecting vertices (a, b) and (a', b') with $a < a'$. We define

$$f_e(x, y) := \sum_{(i,j) \in e} a_{i,j} x^i y^j, \quad f_e^*(x, y) := x^{-a} f_e(x, y).$$

Lemma 14. *Let L be the set of lower edges of $\text{Newt}(f(x, y))$. Let $f^*(x, y) := \prod_{e \in L} f_e^*(x, y)$. Then for every $\phi \in [0, 2\pi)$ and every $r > 0$ sufficiently small,*

$$|B(f(x, re^{i\phi})) - B(f^*(x, e^{i\phi}))| < 1.$$

Proof. Without loss of generality, assume that x does not divide f and that the lower edges have integer gradients. Otherwise, we can divide by x and replace y by a suitable power of y . For $a \in \mathbb{C} \setminus \{0\}$, $\text{Arg}(a)$ denotes the unique $\theta \in (-\pi, \pi]$ with $a = |a|e^{i\theta}$.

Let $n := \deg(f(x, y))$, where from now on \deg will denote the degree with respect to the x -variable. Let e_1, \dots, e_s be the lower edges of $\text{Newt}(f(x, y))$ with gradients $q_1 < \dots < q_s$. As in the above discussion, we have vertices $(a_1, b_1), \dots, (a_{s+1}, b_{s+1})$ so that e_i connects (a_i, b_i) and (a_{i+1}, b_{i+1}) , and $a_1 = 0, a_{s+1} = n$. Observe that x does not divide $f_{e_i}^*$ and $\deg(f_{e_i}^*) = a_{i+1} - a_i$. Hence,

$$\deg(f^*) = \sum_{i=1}^s \deg(f_i^*) = \sum_{i=1}^s (a_{i+1} - a_i) = a_{s+1} - a_0 = n.$$

Let ϕ be given and $\epsilon > 0$ be sufficiently small. We claim the following: given r sufficiently small, there is a bijection between the roots of $f^*(x, e^{i\phi})$ and $f(x, re^{i\phi})$, so that any two corresponding roots ξ, ξ' satisfy $|\text{Arg}(\xi'/\xi)| < \epsilon$. We will call such a bijection an ϵ -*matching*. This clearly implies that $B(f(x, re^{i\phi}))$ and $B(f^*(x, e^{i\phi}))$ get arbitrarily close to each other (for our purposes, it is enough to set $\epsilon = 1/2n$).

The claim is an application of Lemma 13. Let $d_i := \deg(f_{e_i}^*)$. We can factor each $f_{e_i}^*$ as

$$f_{e_i}^*(x, y) = c_0 y^{b_i} \prod_{j=1}^{d_i} (xy^{q_i} - c_j), \quad (16)$$

This means that the roots of $f_{e_i}^*(x, re^{i\phi})$ lie in the disc

$$D_i(r) = \{z \in \mathbb{C} : m_i r^{-q_i} \leq |z| \leq m'_i r^{-q_i}\},$$

where $0 < m_i \leq m'_i$ are independent of r . By the definition of f_{e_i} , the Newton polytope of $f(x, y) - f_{e_i}(x, y)$ lies in the strict upper-half plane determined by the edge e_i . From Lemma 13, we conclude that for every $r > 0$ small enough, $f(x, re^{i\phi})$ contains at least d_i roots in the disc

$$D'_i(r) = \{z \in \mathbb{C} : m_i(1 - \epsilon)r^{-q_i} < |z| \leq m'_i(1 + \epsilon)r^{-q_i}\}$$

and, moreover, there is an ϵ -matching between d_i of these roots and the roots of $f_{e_i}^*(x, re^{i\phi})$. As r approaches zero, the discs $D'_i(r)$ and $D'_j(r)$ become disjoint for distinct i and j . Since $\deg(f) = \deg(f^*)$, this means that there is an ϵ -matching between the roots of $f(x, re^{i\phi})$ and $f^*(x, re^{i\phi})$. To conclude the claim, observe from (16) that the arguments of the roots of $f^*(x, re^{i\phi})$ do not depend on r . \square

Proof of Theorem 2. Let $f(x, y)$ be such that $\text{Newt}(f(x, y))$ has k vertices. Without loss of generality, we will assume that $\text{Newt}(f)$ has $s \geq (k - 2)/2$ lower edges. For otherwise, take the polynomial $y^m f(x, y^{-1})$ for m sufficiently large.

Using Lemma 14, it is enough to show there exists $\phi \in [0, 2\pi)$ with

$$B(f^*(x, e^{i\phi})) \geq \Omega(\sqrt{s}). \quad (17)$$

If the gradients of the lower edges are integers, we can factor f^* as (11) and conclude (17) from Theorem 1 as in the discussion in Section 5.1. If the gradients are not integers, take instead $f^*(x, y^m)$ for a suitable m . \square

5.3 Proof of Theorem 3

As already remarked, a weaker version of Theorem 3 follows from Theorem 2. However, the following proof of the full version is self-contained, though similar to that of Theorem 2.

An analogue of Lemma 13 is the following:

Lemma 15. *Let $g(x, y)$ be a real polynomial as in (12) with $c_{n_1}c_{n_2} < 0$ and $q \in \mathbb{Q}$. Let $h(x, y)$ be a real polynomial such that $\text{Newt}(h)$ lies strictly above the line ℓ . Then there exist $0 < d < d'$ such that for every $0 < r$ sufficiently small, $g(x, r) + h(x, r)$ contains a root in the interval $(dr^{-q}, d'r^{-q})$.*

Proof. The assumption $c_{n_1}c_{n_2} < 0$ guarantees the existence of $0 < d < d'$ with $g(d, 1)g(d', 1) < 0$. This means that for every $0 < r$, also $g(dr^{-q}, r)g(d'r^{-q}, r) < 0$. As in the proof of Lemma 13, it can be shown that for $r > 0$ sufficiently small,

$|h(dr^{-q}, r)| < |g(dr^{-q}, r)|$ and $|h(d'r^{-q}, r)| < |g(d'r^{-q}, r)|$. This shows that $g(x, r) + h(x, r)$ has different signs on the endpoints of the interval $[dr^{-k}, d'r^{-k}]$, and the interval must contain a real root. \square

The following lemma is a substitute for Theorem 1. Let r_1, \dots, r_k be a sequence of real numbers. We define

$$V(r_1, \dots, r_k) := |\{i \in [k-1] : r_i r_{i+1} < 0\}|,$$

the number of sign variations in the sequence.

Lemma 16. *Let $\alpha_1, \dots, \alpha_k \in [0, 2\pi)$ and let n_1, \dots, n_k be positive integers such that $n_i \neq n_{i+1}$ for every $i \in [k-1]$. Then there exists $\phi \in [0, 2\pi)$ such that⁷ $V(\cos(\alpha_1 + \phi n_1), \dots, \cos(\alpha_k + \phi n_k)) \geq (k-1)/8$.*

Proof. Pick a random $x \in [0, 1]$. Let $f_i(x) := \cos(\alpha_i + 2\pi n_i x) \cos(\alpha_{i+1} + 2\pi n_{i+1} x)$. We claim that

$$\Pr[f_i(x) < 0] \geq 1/8.$$

This can be seen as follows. An easy calculation shows that $\int_0^1 f_i(x) dx = 0$ and $\int_0^1 f_i(x)^2 dx = 1/4$. Let $A := \{x \in [0, 1] : f_i(x) < 0\}$. Then

$$\begin{aligned} \frac{1}{4} &= \int_0^1 f_i(x)^2 dx \\ &\leq \int_0^1 |f_i(x)| dx = \int_A |f_i(x)| dx + \int_{[0,1] \setminus A} |f_i(x)| dx = 2 \int_A |f_i(x)| dx \leq 2|A|, \end{aligned}$$

which shows that $|A| \geq 1/8$.

Let $\chi_i(x) \in \{0, 1\}$ be the indicator function of the event that $f_i(x) < 0$. Then the expectation of $\chi_1(x) + \dots + \chi_{k-1}(x)$ is at least $(k-1)/8$. Hence there exists $x \in [0, 1]$ so that $f_i(x) < 0$ holds for at least $(k-1)/8$ of the i 's. \square

Proof of Theorem 3. As in the proof of Theorem 2, we can assume that the polytope has $s \geq (k-2)/2$ lower edges. Let e_1, \dots, e_s be such edges with gradients q_1, \dots, q_s , where e_i connects (a_i, b_i) and (a_{i+1}, b_{i+1}) with $a_i < a_{i+1}$. Let $r_i e^{i\alpha_i}$ be the coefficient of $x^{a_i} y^{b_i}$ in f (where $r_i > 0$, $\alpha_i \in [0, 2\pi)$).

Given $a = r e^{i\phi}$, we can write $\Re(f_{e_i}(x, a))$ as

$$\cos(\alpha_i + b_i \phi) r_i r^{b_i} x^{a_i} + \cos(\alpha_{i+1} + b_{i+1} \phi) r_{i+1} r^{b_{i+1}} x^{a_{i+1}} + \Re(u_i(x, a)),$$

where $u_i(x, y)$ is a polynomial such that $\text{Newt}(u_i(x, y))$ lies on the line strictly between the points (a_i, b_i) and (a_{i+1}, b_{i+1}) . Let $T(\phi)$ be the sequence $\cos(\alpha_1 + \phi b_1), \dots, \cos(\alpha_{s+1} + \phi b_{s+1})$. Note that $b_i \neq b_{i+1}$ holds for every $i \in [s]$, with at most one exception. By the previous lemma, there exists a ϕ such that $V(T(\phi)) \geq (s-1)/8$ (this "one exception" compensated by the sequence having

⁷We are not trying to optimize the constant; a different argument would give an improvement of $(k-1)/6$.

length $s + 1$). Fix such a ϕ . Given an i with $\cos(\alpha_i + \phi b_i) \cos(\alpha_{i+1} + \phi b_{i+1}) < 0$, we can apply Lemma 15, to conclude that $\Re(f(x, re^{i\phi}))$ has a root in the interval $(d_i r^{-q_i}, d'_i r^{-q_i})$ for every r sufficiently small. As r approaches zero, the intervals corresponding to different i 's are disjoint (the gradients q_i are distinct). This gives that $\Re(f(x, re^{i\phi}))$ has at least $(s - 1)/8$ distinct real roots for r sufficiently small. \square

Acknowledgement The author thanks B. Green, P. Pudlák, M. Rojas, and the anonymous referees for their comments.

References

- [1] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and Computation in Mathematics*. Springer, 2000.
- [2] J. W. S. Cassels. *An introduction to Diophantine approximation*. Cambridge University Press, 1957.
- [3] P. Erdős and A. Rényi. A probabilistic approach to problems of Diophantine approximation. *Illinois J. Math.*, 1(3):303–315, 1957.
- [4] P. Erdős and P. Turán. On a problem in the theory of uniform distribution I. *Nederl. Akad. Wetensch. Indagationes Math.*, 10:370–378, 1948.
- [5] P. Erdős and P. Turán. On the distribution of roots of polynomials. *Annals of Mathematics*, 51:105–119, 1950.
- [6] P. Hrubeš. On the real τ -conjecture and the distribution of complex roots. *Theory of Computing*, 9(10):403–411, 2013.
- [7] J. I. Hutchinson. On a remarkable set of entire functions. *Trans. Amer. Math. Soc.*, pages 325–332, 1923.
- [8] I. Karpenko and A. Vishnyakova. On sufficient conditions for a polynomial to be sign-independently hyperbolic or to have real separated zeros. *Mathematical inequalities and applications*, 20(1):237–245, 2017.
- [9] P. Koiran. Shallow circuits with high-powered inputs. In *Symposium on Innovations in Computer Science*. Tsingua University Press, Beijing, 2011.
- [10] P. Koiran, N. Portier, S. Tavenas, and S. Thomassé. A τ -conjecture for Newton polygons. *Foundations of computational mathematics*, 15(1):187–197, 2015.
- [11] L. Kronecker. Näherungsweise ganzzahlige Auflösung linearer Gleichungen. *Berl. Ber.*, pages 1179–1193, 1884.
- [12] D. C. Kurtz. A sufficient condition for all the roots of a polynomial to be real. *The American Mathematical Monthly*, 99(3):259–263, 1992.

- [13] D. S. Mitronović, J.E. Pečarić, and A. M. Fink. Turán's inequalities from the power sum theory. In *Classical and New Inequalities in Analysis*, volume 61. Springer, 1993.
- [14] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. Society for Industrial and Applied Mathematics, 1992.
- [15] S. Smale. Mathematical problems for the next century. *Mathematical Intelligence*, 20(2):7–15, 1998.
- [16] C. C. Tseng and C. L. Liu. Complementary sets and sequences. *IEEE Trans. Information Theory*, pages 644–652, 1972.
- [17] P. Turán. *On a New Method of Analysis and its Applications*. John Wiley & Sons, 1984.
- [18] L. G. Valiant. Completeness classes in algebra. In *STOC*, pages 249–261, 1979.
- [19] R. J. Walker. *Algebraic curves*. Dover Publ., 1950.