

AN ELEMENTARY INEQUALITY AND SOME APPLICATIONS

MICHAEL W. KOWALSKI AND JAMES WRIGHT

ABSTRACT. We establish an elementary inequality relating the coefficients of a polynomial with the separation of its roots. Applications to one dimensional oscillatory integrals with real polynomial phases and the structure of global sublevel sets for polynomials with coefficients in a general ring are discussed.

1. INTRODUCTION

Let x_1, \dots, x_d be d points so that their sum $S := |x_1 + \dots + x_d|$ is large and the other elementary symmetric functions of x_1, \dots, x_d ,

$$\left| \sum_{j < k} x_j x_k \right| \leq S, \quad \left| \sum_{j < k < \ell} x_j x_k x_\ell \right| \leq S, \quad \dots, \quad |x_1 x_2 \cdots x_d| \leq S$$

are each bounded by this sum. Then the maximal separation $\Delta := \max_{j,k} |x_j - x_k|$ of these points grows like S . More precisely, there are positive constants C_d, c_d and A_d , depending only on d so that

$$c_d S \leq \Delta := \max_{j,k} |x_j - x_k| \leq C_d S \tag{1}$$

whenever $S \geq A_d$. This inequality is easy to prove and is valid for points x_1, \dots, x_d in any commutative ring R with identity which has a nontrivial absolute value¹ $|\cdot|$; that is, a size $|x| \geq 0$ is assigned to every element $x \in R$ so that $|x| = 0$ if and only if $x = 0$, $|xy| = |x||y|$ and $|x+y| \leq |x| + |y|$ for every $x, y \in R$. The basic examples to keep in mind are $R = \mathbb{R}$ or \mathbb{C} with the usual absolute value or $R = \mathbb{Z}$ with a p -adic valuation.

Although the above inequality is simple to prove, we will establish other elementary inequalities which are slightly less trivial to prove and which examine how certain geometric quantities associated to the d points, besides the diameter Δ , grow in terms of the elementary symmetric functions of x_1, \dots, x_d . Such inequalities can be expressed in terms of polynomials of a single variable $P \in A[X]$ since the coefficients of P are simply the elementary symmetric functions of its roots. In what follows, when we discuss the polynomial ring $A[X]$, the ring of coefficients A will always be a commutative ring with an absolute value $|\cdot|$ and when we discuss a particular

1991 *Mathematics Subject Classification.* 42B15.

The second author was supported in part by an EPSRC grant.

¹The setting can be generalised to any commutative Banach algebra \mathcal{A} which is semisimple and is such that the Gelfand dual $\widehat{\mathcal{A}}$ is closed in $C(D)$ where D is the maximal ideal space of \mathcal{A} . There are in fact noncommutative versions as well but we do not pursue this here.

polynomial $P(x) = a_d \prod_j (x - x_j)$ with roots lying in some field extension K of the field of fractions of A , we take *any* extension of $|\cdot|$ in K .

A basic application of our elementary inequalities, relating the coefficients of P to various geometric quantities associated to the separation of the roots $\{x_j\}$ of P , is a precise structural statement of the global sublevel set $\{x \in A : |P(x)| \leq \delta\}$; see Corollary 2.3 below. When $A = \mathbb{R}$ or \mathbb{C} and $|\cdot|$ is the usual absolute value (that is, the archimedean case), this gives rise to global sublevel set estimates. And when $A = \mathbb{R}$ we go further and establish a global oscillatory integral estimate; see Corollary 2.2.

However, when the absolute value $|\cdot|$ is non-archimedean, the inequality $|P(x)| \leq \delta$ expresses the congruence $P(x) \equiv 0 \pmod I$ where $I := \{y \in K : |y| \leq \delta\}$ is a fractional ideal of K (recall we are assuming that $|\cdot|$ is nontrivial) and then our basic structural result for the sublevel set $\{x \in A : |P(x)| \leq \delta\}$ has number theoretic implications. In fact, in this non-archimedean context, suppose that A is a field (so that $K = A$), $P \in \mathfrak{o}[X]$ where \mathfrak{o} is a subring of the ring of integers $\{x \in A : |x| \leq 1\}$ whose field of fractions is A and $\delta \leq 1$ so that I is an integral ideal with respect to this ring of integers. Hence if $x \in A$ satisfies the congruence $P(x) \equiv 0 \pmod I$, then any member y in the coset $x + I$ also satisfies this congruence and therefore we say that the element $\bar{x} = x + I$ in the factor group A/I is a ‘global’ solution of the congruence $P \equiv 0 \pmod I$.² If we denote by $\#\{P \equiv 0 \pmod I\}$ the number of ‘global’ solutions of this congruence, then the structure of the sublevel set $\{x \in A : |P(x)| \leq \delta\}$ described in Corollary 2.3 gives a bound on $\#\{P \equiv 0 \pmod I\}$.

For example, let \mathfrak{o} be any Dedekind domain with field of fractions A and suppose \mathfrak{p} is a nonzero prime ideal of \mathfrak{o} whose residue class field $\mathfrak{o}/\mathfrak{p}$ is finite. The prime ideal \mathfrak{p} gives rise to a non-archimedean absolute value $|x| := \|\mathfrak{p}\|^{-t}$ on A where $\|\mathfrak{p}\|$ denotes the number of elements in the residue class field $\mathfrak{o}/\mathfrak{p}$ and \mathfrak{p}^t appears as the \mathfrak{p} factor in the prime ideal decomposition of the principal ideal $x\mathfrak{o}$, generated by $x \in A$. An application of the elementary inequalities is the following.

Theorem 1.1. *In the setting above, suppose that $P(x) = a_d x^d + \cdots + a_0 \in \mathfrak{o}[X]$ is normalised so that $\max |a_j| = 1$ with $|a_{d-k}| = 1$ for some $k \leq d/2$. If the characteristic q of \mathfrak{o} is positive, we assume in addition $q > d - k$. Then the number of ‘global’ solutions in the field of fractions A has the bound*

$$\#\{P \equiv 0 \pmod{\mathfrak{p}^s}\} \leq C_d \|\mathfrak{p}\|^{s-s/d}$$

whenever $s \geq 0$.

Remarks:

- We recall that the bound (in \mathfrak{o})

$$\#\{\bar{x} \in \mathfrak{o}/\mathfrak{p}^s : P(\bar{x}) \equiv 0 \pmod{\mathfrak{p}^s}\} \leq C_d \|\mathfrak{p}\|^{s(1-1/d)}$$

²For this discussion it suffices to keep in mind the basic example $A = \mathbb{Q}$ with the rational integers $\mathfrak{o} = \mathbb{Z}$ as the subring of the ring of integers with respect to some p -adic valuation. Consider the example $P(x) = 54x - 11$ which has no solutions mod 3 in \mathbb{Z} but has a ‘global’ solution $(1/27) + 3\mathbb{Z}$ in \mathbb{Q} .

when $\max |a_j| = 1$ is a well-known result and goes back to Hua [1] in the classical setting of \mathbb{Z} (see [7] for an alternative approach in the above setting); of course in this case there is no restriction on k ($\leq d/2$).

- The interesting feature of Theorem 1.1 is that the restriction $k \leq d/2$ is sharp in general. Let p be a rational prime which induces a p -adic absolute value $|\cdot|$ described above and consider $P(x) = p^{kt}x^{k-1}(x - p^{-t})^k \in \mathbb{Z}[X]$. Then $d = 2k-1$, $\gcd(a_d, \dots, a_0, p^s) = 1$, $|a_{d-j}| < 1$, $j \leq k-1$ and $|a_{d-k}| = 1$ ($p \nmid a_{d-k}$). Also the set

$$\{|x - p^{-t}| < p^t : |P(x)| = p^{-t}|x - p^{-t}|^k \leq p^{-s}\}$$

is easily seen to be contained in $\{x \in \mathbb{Q} : |P(x)| \leq p^{-s}\}$ which implies

$$\#\{P \equiv 0 \pmod{p^s}\} \geq p^{s-1-(s-t)/k} = p^{t/k}p^{s(1-1/k)-1}$$

and so the bound $\#\{P \equiv 0 \pmod{p^s}\} \leq C_d p^{s(1-1/d)}$ cannot hold since t can be large.

Along the way to establishing Theorem 1.1 we improve upon a result of Loxton and Smith [3] on the number of ‘classical’ solutions to a polynomial congruence. Again suppose we are in the non-archimedean setting where \mathfrak{o} a Dedekind domain with A its field of fractions endowed with an absolute value $|x| := \|\mathfrak{p}\|^{-\text{ord}_{\mathfrak{p}}(x)}$ arising from a nonzero prime ideal \mathfrak{p} whose residue class field is finite; here $\text{ord}_{\mathfrak{p}}(x)$ is the valuation of x defined as the unique integer t so that \mathfrak{p}^t is the factor of \mathfrak{p} in the prime ideal decomposition of principal ideal $x\mathfrak{o}$.

Let $P(x) = a_d \prod (x - z_j)^{m_j}$ be a polynomial in $\mathfrak{o}[X]$ of degree d with m distinct zeros $\{z_1, \dots, z_m\}$. Let K denote the field over A generated by $\{z_1, \dots, z_m\}$ and let $\text{ord}_{\mathfrak{p}}$ be any extension to K of the valuation $\text{ord}_{\mathfrak{p}}$. By a *root cluster* \mathcal{C} we simply mean a subset $\mathcal{C} \subset \{z_1, \dots, z_m\}$ and we denote by

$$S(\mathcal{C}) := \sum_{j: z_j \in \mathcal{C}} m_j$$

the number of roots in \mathcal{C} , counted with multiplicity. For each root z_j and root cluster \mathcal{C} containing z_j , set

$$\delta(P; \mathcal{C}, z_j) = \delta_{\mathfrak{p}}(P; \mathcal{C}, z_j) := \text{ord}_{\mathfrak{p}}\left(a_d \prod_{k: z_k \notin \mathcal{C}} (z_j - z_k)^{m_k}\right).$$

Theorem 1.2. *With $P \in \mathfrak{o}[X] = a_d \prod (x - z_j)^{m_j}$ as above,*

$$\#\{x \in \mathfrak{o}/\mathfrak{p}^{\alpha} : P(x) \equiv 0 \pmod{\mathfrak{p}^{\alpha}}\} \leq \sum_{j=1}^m \inf_{\mathcal{C}: z_j \in \mathcal{C}} \|\mathfrak{p}\|^{\alpha - \frac{(\alpha - \delta_{\mathfrak{p}}(P; \mathcal{C}, z_j))}{S(\mathcal{C})}} \#\mathcal{C} \quad (2)$$

where for each $1 \leq j$, the infimum is taken over all root clusters \mathcal{C} containing z_j .

The proof of Theorem 2 in [3] gives the bound in (2) where one only considers the singleton clusters $\mathcal{C} = \{z_j\}$; more precisely they work in the setting $\mathfrak{o} = \mathbb{Z}$ with $\mathfrak{p} = p\mathbb{Z}$ and p a rational prime and prove

$$\#\{x \in \mathbb{Z}/p^{\alpha}\mathbb{Z} : P(x) \equiv 0 \pmod{p^{\alpha}}\} \leq \sum_{j=1}^m p^{\alpha - \frac{(\alpha - \delta_p(P; z_j))}{m_j}} \quad (3)$$

where

$$\delta_p(P; z_j) = \text{ord}_p(a_d \prod_{k \neq j} (z_j - z_k)^{m_k}) = \text{ord}_p(P^{(m_j)}(z_j)/m_j!)$$

which in turn implies the bound stated in their theorem.

The bound in (2) often gives a significant improvement over the bound in (3). For instance suppose $P(x) = x(x - z_1)(x - z_2)^2$ where $z_1, z_2 \in \mathbb{Z}$ satisfy $p^s \parallel z_1, z_2$, $p^t \parallel z_1 - z_2$ where $t > s$. We will examine the congruence $P \equiv 0 \pmod{p^\alpha}$ where $4s \leq \alpha \leq t$. In this case one sees that the root cluster $\mathcal{C} = \{z_1, z_2\}$ plays an important role; the bound in (2) gives $6p^{(2/3)\alpha + (1/3)s}$ which is an improvement over the bound $3p^{s+2t}$ from (3). Note that $p^{(2/3)\alpha + (1/3)s}$ is the correct bound since

$$\{x : p^{-t} < |x - z_1| < p^{-s}, |P(x)| = p^{-s}|x - z_1|^3 \leq p^{-\alpha}\} \subset \{P(x) \equiv 0 \pmod{p^\alpha}\}$$

and the set on the left contains $\{x \in \mathbb{Z} : p^{-t} < |x - z_1| \leq p^{-(\alpha-s)/3}\}$. This gives the bound $\#\{P \equiv 0 \pmod{p^\alpha}\} \geq p^{(2/3)\alpha + (1/3)s - 1}$ since $t \geq \alpha$.

In the case when $\text{ord}_p(a_d) = 0$, considering only the maximal root cluster $\mathcal{C} = \{z_1, \dots, z_m\}$, the bound in (2) gives the classical bound of Hua

$$\#\{P \equiv 0 \pmod{p^\alpha}\} \leq m^2 \|\mathfrak{p}\|^{\alpha(1-1/d)}$$

already mentioned above.

Notation: For two positive quantities A and B we use the notation $A \lesssim B$ to mean that there is a constant C , depending only on d, k and $|\cdot|$, so that $A \leq CB$ and we use the notation $A \sim B$ to denote that both inequalities $A \lesssim B$ and $B \lesssim A$ hold. Finally we use the notation $A \ll B$ to denote that the relation $B \lesssim A$ does not hold.

Acknowledgement: We wish to thank Tony Carbery for several illuminating discussions on various aspects of this paper and for comments which have improved the content and structure of the paper.

2. STATEMENT OF MAIN RESULT AND APPLICATIONS

Often a simple scaling argument allows one to reduce certain problems involving polynomials to solving the corresponding problem for normalised polynomials; that is, if $P(x) = a_d x^d + \dots + a_0$ then one may assume $\max_j |a_j| = 1$. If the maximum occurs at the top coefficient, $|a_d| = 1$, then we are more or less looking at monic polynomials which may be an easier case but nevertheless it is the situation which should be dealt with first.

However if the coefficient $|a_d|$ is small but the next coefficient $|a_{d-1}| = 1$ is where the maximum occurs, then since $a_{d-1} = -a_d(x_1 + \dots + x_d)$, $a_{d-2} = a_d \prod_{j < k} x_j x_k$, etc... where $\{x_1, \dots, x_d\}$ are the roots of the polynomial P , lying in some field extension K of the field of fractions of A , we see that $S := |a_d|^{-1}$ is large with

$$S = |x_1 + \dots + x_d|, \quad \left| \prod_{j < k} x_j x_k \right| \leq S, \quad \dots, \quad |x_1 \cdots x_d| \leq S$$

and so the inequality (1) in the introduction can be expressed as saying that the maximal separation of the roots $\Delta = \max_{j,k} |x_j - x_k|$ grows like S in this situation; here Δ is measured with respect to *any* extension of the absolute value $|\cdot|$ to K . More precisely, there are positive constants c_d, C_d and ϵ_d so that if $P(x) = \sum_{j=0}^d a_j x^j$ with $\max_j |a_j| = |a_{d-1}| = 1$, then

$$c_d |a_d|^{-1} \leq \Delta := \max_{j,k} |x_j - x_k| \leq C_d |a_d|^{-1} \quad (4)$$

whenever $|a_d| \leq \epsilon_d$.

Now if both $|a_d|$ and $|a_{d-1}|$ are small but $|a_{d-2}| = 1$ is where the maximum occurs, the geometric quantity which arises is

$$\Delta_2 := \min_j \max_{k \neq \ell} |x_j - x_k| |x_j - x_\ell|$$

where the maximum is taken over all pairs $k, \ell \in \{1, 2, \dots, d\}$ so that $k \neq \ell$. The quantity Δ_2 can be expressed in terms of certain *clusters* of the points $\{x_1, \dots, x_d\}$; here we deviate from the notion of root cluster introduced above and define a cluster L as any subset $L \subset \{1, 2, \dots, d\}$ which we think of as labelling the points $\{x_j\}_{j \in L}$. The appropriate clusters for Δ_2 all have size $|L| = d-2$, $|L|$ denoting the cardinality of the cluster L . Hence

$$\Delta_2 = \min_j \max_{j \in L: |L|=d-2} \prod_{k \notin L} |x_j - x_k|$$

where the maximum is taken over all clusters L containing j with size $|L| = d-2$. Similarly the diameter Δ can be described in terms of clusters of size $d-1$:

$$\Delta_1 := \min_j \max_{j \in L: |L|=d-1} \prod_{k \notin L} |x_j - x_k|.$$

Strictly speaking Δ is not equal to Δ_1 but they differ only by a factor of 2; that is, $\Delta_1 \leq \Delta \leq 2\Delta_1$ (however in the non-archimedean case they are in fact equal). Informally the inequality in this case states that Δ_2 grows like $|a_d|^{-1}$ if $|a_d|$ and $|a_{d-1}|$ are small, $|a_{d-2}| = 1$ and $|a_j| \leq 1$ for all coefficients.

For the general case, corresponding to the maximum of the coefficients $|a_{d-k}| = 1$ occurring at the k th place from the top, the geometric quantity which arises is

$$\Delta_k(x_1, \dots, x_d) := \min_j \max_{j \in L: |L|=d-k} \prod_{k \notin L} |x_j - x_k|.$$

In order to state the main result below we introduce the notation

$$e_k(x_1, \dots, x_d) := \sum_{j_1 < \dots < j_k} x_{j_1} \cdots x_{j_k}$$

for $1 \leq k \leq d$, the elementary symmetric polynomials in x_1, \dots, x_d .

Theorem 2.1. *Let R be a commutative ring with an absolute value $|\cdot|$. For any integers k, d with $d \geq 2$ and $k \leq d/2$, there are small positive constants $\eta_1, \dots, \eta_{k-1}$ and c and a large positive constant A , each depending only on d, k and $|\cdot|$ so that for any collection of d points $\{x_1, \dots, x_d\} \subset R$,*

$$c |e_k(x_1, \dots, x_d)| \leq \Delta_k(x_1, \dots, x_d) \quad (5)$$

holds whenever $|e_k| \geq A$, each $|e_j| \leq |e_k|$ and in addition, when $1 \leq j \leq k-1$, $|e_j| \leq \eta_j |e_k|$. Furthermore if the characteristic q of R is positive, we assume $q > d-k$.

Remarks:

- The restriction $k \leq d/2$ is sharp in any ring R containing an element with absolute value strictly bigger than 1 (taking powers we can then find elements with arbitrarily large absolute values); simply consider $x_1 = \dots = x_{k-1} = 0$ and $x_k = \dots = x_{2k-1} = y$ where $|y|$ is large. Here $d = 2k-1$, $e_k = y^k$, $e_j = 0$ for every $j \geq k+1$ and $e_j = c_j y^j = c_j y^{-(k-j)} e_k$ for $1 \leq j \leq k-1$ **but** $\Delta_k = 0$. The fact that (5) does not hold for $k > d/2$ (together with the applications discussed below) is the interesting feature of Theorem 2.1. As we will see, the proof itself is not very difficult.
- The additional conditions $|e_j| \leq \eta_j |e_k|$ for some small η_j when $j \leq k-1$ is necessary in general. For instance if $d=4, k=2, x_1 = x_2 = x_3 = 1$ and x_4 is large (take, say, $R = \mathbb{R}$ with the usual absolute value), then $|e_2| \sim |x_4|$ yet $\Delta_2 = 0$; note that in this case, $|e_1| \sim |x_4|$ is not small compared to $|e_2|$.
- The reverse inequality in (5) holds under less restrictive conditions; in fact $\Delta_k(x_1, \dots, x_d) \leq C |e_k(x_1, \dots, x_d)|$ holds for some large positive constant $C = C_{d,k,|\cdot|}$ whenever $|e_j| \leq |e_k|$ for all $j \geq 1$. In particular there is no restriction on k . The proof is easy and elementary. If the points are ordered in size $|x_1| \leq |x_2| \leq \dots \leq |x_d|$, it suffices to show that $|x_{d-k+1} \dots x_d| \lesssim |e_k|$ and this can be established by contradiction: if $|x_{d-k+1} \dots x_d| \gg |e_k|$, then one can reason inductively that for each $1 \leq j \leq d-k+1$, the inequality $|x_j x_{d-k+2} \dots x_d| \lesssim |e_k|$ cannot hold. Interlaced in this inductive argument, one runs a complementary inductive argument showing that for each $2 \leq \ell \leq d-k+1$, we have $|x_\ell| \gg 1$. At the final step we arrive at the conclusion that

$$|x_1 \dots x_d| = |x_1 x_{d-k+2} \dots x_d \cdot x_2 \dots x_{d-k+1}| \gg |e_k| \cdot 1$$

which contradicts our hypothesis $|x_1 \dots x_d| := |e_d| \leq |e_k|$.

- In terms of polynomials $P \in A[X]$, Theorem 2.1 can be expressed in the following way: there are positive constants $\epsilon_1, \dots, \epsilon_{k-1}, c, C$ and A so that if $P(x) = a_d x^d + \dots + a_0 = a_d \prod_j (x - x_j)$ is normalised so that $\max_j |a_j| = |a_{d-k}| = 1$ for some $k \leq d/2$ and $|a_{d-j}| \leq \epsilon_j, 0 \leq j \leq k-1$, then

$$c |a_d|^{-1} \leq \Delta_k(x_1, \dots, x_d) \leq C |a_d|^{-1}. \quad (6)$$

Here we see that Theorem 2.1 expresses a certain curious discontinuous behaviour; if $k > d/2$ (so the theorem is false in general) but nevertheless the conditions on the coefficients are satisfied, in particular the top coefficients are small, then allowing some of these top coefficients to vanish so that now k is less than half the degree, the inequality (6) suddenly becomes true.

One application of Theorem 2.1 is the following observation for one dimensional global oscillatory integrals with real polynomial phases $P(x) \in \mathbb{R}[X]$.

Corollary 2.2. *For every $d \geq 2$, there is a positive constant C_d so that if $P(x) = a_d x^d + \dots + a_1 x \in \mathbb{R}[X]$ with $\|\vec{a}\| := \max_j |a_j| = |a_{d-k}| \geq 1$ and $k \leq (d-1)/2$, then*

$$\left| \int_{\mathbb{R}} e^{2\pi i(a_d x^d + \dots + a_1 x)} dx \right| \leq C_d \|\vec{a}\|^{-1/d}. \quad (7)$$

Since the degree d is at least 2, the integral in (7) makes sense as a limit $\int_{x \in \mathbb{R}} \exp(\dots) dx = \lim_{R \rightarrow \infty} \int_{|x| \leq R} \exp(\dots) dx$. If there is a uniform bound of some derivative of P from below, $|P^{(j)}(x)| \geq c_d \|\vec{a}\|$, then the estimate (7) follows immediately from an application of van der Corput's lemma; see for instance [6]. This is indeed the case when $k = 0$ (or if x is restricted to a compact interval), however it is not the case for larger values of k . Furthermore the estimate in (7) is false when $k > (d-1)/2$ as shown for instance by the example $P \in \mathbb{R}[X]$ with

$$P'(x) = \epsilon x^{k-1} (x - \epsilon^{-1/k})^k \quad \text{and} \quad \epsilon \ll 1.$$

For this example, the corresponding oscillatory integral in (7) is bounded below by $c_d \epsilon^{-1/k(k+1)}$ for some $c_d > 0$. There are analogues of Corollary 2.2 in non-archimedean settings in which case the oscillatory integral in (7) becomes related to a character sum.

Another application of Theorem 2.1 is the following structural statement about global sublevel sets for polynomials $P \in A[X]$ with coefficients in any commutative ring A with an absolute value $|\cdot|$.

Corollary 2.3. *For every $d \geq 1$, there is a positive constant A_d so that if $P(x) = a_d x^d + \dots + a_0 \in A[X]$ with $\|\vec{a}\| := \max_j |a_j| = |a_{d-k}| = 1$ and $k \leq d/2$, then*

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{z \in \mathcal{R}_P} [B_{A_d \delta^{1/d} \min(1, \delta^{1/d})}(z) \cap A] \quad (8)$$

holds whenever the characteristic of the ring A , if positive, is larger than $d - k$. Here $\mathcal{R}_P \subset K$ denotes the set of roots of P lying in some field extension K and $B_r(z) = \{y \in K : |y - z| \leq r\}$ is the ball centred at $z \in K$ with radius r , measured with respect to any extension of the absolute value $|\cdot|$ to K .

Two examples to keep in mind are $A = \mathbb{R}$ and $A = \mathbb{C}$ with the usual absolute value; in these cases we take $K = \mathbb{C}$. If $A = \mathbb{R}$, then $B_r(z) \cap \mathbb{R}$ is contained in the interval $\{x \in \mathbb{R} : |x - \text{Re}(z)| \leq r\}$ where $\text{Re}(z)$ denotes the real part of $z \in \mathbb{C}$ and so in this case Corollary 2.3 implies the global sublevel set estimate

$$|\{x \in \mathbb{R} : |P(x)| \leq \delta\}| \leq 2d A_d \delta^{1/d}; \quad (9)$$

whereas in the case $A = \mathbb{C}$, Corollary 2.3 implies the global sublevel set estimate

$$|\{x \in \mathbb{C} : |P(x)| \leq \delta\}| \leq \pi d A_d^2 \delta^{2/d} \quad (10)$$

whenever $\delta \leq 1$ and P satisfies the hypotheses of Corollary 2.3. Local versions of both (9) and (10) are well known and then no restriction on $k (\leq d/2)$ is needed.

When $A = \mathbb{R}$ or $A = \mathbb{C}$, the same example illustrating the sharpness of Corollary 2.2 shows that the sublevel set inclusion (8) is false for any $k > d/2$; in fact the sublevel set estimates (9) and (10) are also false when $k > d/2$. Note that when

$A = \mathbb{R}$ the sublevel set estimate follows by a standard argument when $k = 0$ but the set inclusion (8) is not so trivial in this case.

Let us see now how Corollary 2.3 gives a proof of Theorem 1.1. Recall that we are counting the ‘global’ solutions to a congruence $P \equiv 0 \pmod{\mathfrak{p}^s}$, $s \geq 0$ in the field of fractions A of a Dedekind domain \mathfrak{o} with a nonzero prime ideal \mathfrak{p} whose residue class field $\mathfrak{o}/\mathfrak{p}$ is finite. Here $P(x) = a_d x^d + \cdots + a_0$ lies in $\mathfrak{o}[X]$ and is normalised so that $\max |a_j| = |a_{d-k}| = 1$ with $k \leq d/2$ where $|\cdot|$ is induced from the prime ideal \mathfrak{p} . Hence Corollary 2.3 applies and implies

$$\{x \in A : P(x) \equiv 0 \pmod{\mathfrak{p}^s}\} \subset \bigcup_{z \in \mathcal{R}_P} [B_{A_d \|\mathfrak{p}\|^{-s/d}}(z) \cap A]$$

where we note $B_{A_d \|\mathfrak{p}\|^{-s/d}}(z) \cap A = \{x \in A : |x - y| \leq A_d \|\mathfrak{p}\|^{-s/d}\}$ for some $y \in A$ if $B_{A_d \|\mathfrak{p}\|^{-s/d}}(z) \cap A$ is nonempty. Therefore the number of solutions (in A)

$$\#\{P \equiv 0 \pmod{\mathfrak{p}^s}\} \leq dN$$

where N is an upper bound of the number disjoint balls $\{x \in A : |x - c| \leq \|\mathfrak{p}\|^{-s}\}$, $c \in A$ which fit inside some fixed ball $\{x \in A : |x - y| \leq A_d \|\mathfrak{p}\|^{-s/d}\}$, again $y \in A$. A simple computation shows $N \leq A_d \|\mathfrak{p}\|^{s-s/d}$ and so we have the following bound on the number of ‘global’ solutions

$$\#\{P \equiv 0 \pmod{\mathfrak{p}^s}\} \leq dA_d \|\mathfrak{p}\|^{s(1-1/d)} \quad (11)$$

which establishes Theorem 1.1.

The original interest in Corollary 2.3 was to explore certain implications of oscillatory integral estimates for corresponding sublevel set estimates. It is well known that if $\phi : E \rightarrow \mathbb{R}$ is a real-valued phase on some compact set $E \subset \mathbb{R}^n$, then an oscillatory integral estimate

$$\left| \int_E e^{2\pi i \lambda \phi(x)} dx \right| \leq A |\lambda|^{-a} \quad (12)$$

(or more generally a multilinear oscillatory integral form where ϕ defines the underlying oscillatory kernel) implies the corresponding sublevel set (or more generally the corresponding multilinear sublevel set operator) estimate $|\{x \in E : |\phi(x)| \leq \delta\}| \leq C_n A \delta^a$ as long as $a < 1$. However since (12) is invariant when $\phi(x)$ is replaced by a translate $\phi(x) + c$ where $c \in \mathbb{R}$, Corollary 2.3 immediately shows, via the usual argument of passing from oscillatory integrals to sublevel sets by the Fourier inversion formula, that (12) implies

$$|\{x \in E : |P(\phi(x))| \leq \delta\}| \leq C_{n,d,a} A \delta^{a/d}$$

whenever the real polynomial P satisfies the hypothesis of Corollary 2.3. Since the real values of ϕ on $E \subset \mathbb{R}^n$ are unrestricted one is naturally led to examining *global* sublevel sets of P on \mathbb{R} . Of course establishing oscillatory integral estimates for polynomial changes of the phase, $P(\phi(x))$ from (12) is another matter altogether. The discussion and conclusions made above hold for general multilinear oscillatory integrals.

3. PROOF OF THEOREM 2.1

Here we present most of the details of how one can establish (5) in Theorem 2.1. The reader can consult [2] for a more detailed proof.

Recall that we are considering d points $\{x_1, \dots, x_d\}$ in a commutative ring R with an absolute value $|\cdot|$ and our goal is to establish the inequality $\Delta_k(x_1, \dots, x_d) \gtrsim |e_k(x_1, \dots, x_d)|$ under certain conditions on the elementary symmetric polynomials e_j of these points. More precisely for any fixed k with $k \leq d/2$, we will show the existence of positive constants $c_{k,d}, A_{k,d}, \eta_1, \dots, \eta_{k-1}$ so that

$$\Delta_k := \min_j \max_{j \in L: |L|=d-k} \prod_{k \notin L} |x_j - x_k| \geq c_{d,k} |e_k(x_1, \dots, x_d)| \quad (13)$$

holds whenever $|e_k| \geq A_{k,d}$, each $|e_j| \leq |e_k|$ and when $1 \leq j \leq k-1$, we have the additional hypothesis $|e_j| \leq \eta_j |e_k|$.

Without loss of generality assume that the minimum in Δ_k occurs when $j = 1$ and assume the points are ordered so that $|x_1 - x_2| \leq |x_1 - x_3| \leq \dots \leq |x_1 - x_d|$. Then $\Delta_k = |x_1 - x_{d-k+1}| \cdots |x_1 - x_d|$. The basic idea of the argument is to find a symmetric polynomial Q in d variables of degree $2k$ so that when Q is evaluated at the d given points we have $|Q(x_1, \dots, x_d)| \lesssim \Delta_k(x_1, \dots, x_d)^2$. Next one uses the fundamental lemma representing symmetric polynomials as a polynomial of the elementary symmetric polynomials $Q(t_1, \dots, t_d) = P(e_1, \dots, e_d)$ and observes that the coefficient of e_k^2 is nonzero and various troublesome terms in fact do not arise, leading to a bound from below $|P(e_1, \dots, e_d)| \gtrsim |e_k|^2$ when the elementary symmetric polynomials e_j are evaluated at (x_1, \dots, x_d) .

The following symmetric polynomial works; $Q(t_1, \dots, t_d) :=$

$$\sum_{j_1 < \dots < j_{2k}} \sum_{\sigma \in \mathcal{S}_{2k}} (t_{j_{\sigma(1)}} - t_{j_{\sigma(2)}})^2 (t_{j_{\sigma(3)}} - t_{j_{\sigma(4)}})^2 \cdots (t_{j_{\sigma(2k-1)}} - t_{j_{\sigma(2k)}})^2$$

where \mathcal{S}_{2k} denotes the symmetric group of permutations on the set $\{1, 2, \dots, 2k\}$ and the first sum is over all $2k$ -tuples (j_1, \dots, j_{2k}) of increasing elements in $\{1, \dots, d\}$. Here we are assuming that $d \geq 2k$. One easily checks that Q is a symmetric polynomial of degree $2k$.

Claim: Given the above ordering of the points $\{x_j\}$, we have

$$|Q(x_1, \dots, x_d)| \leq C |x_1 - x_{d-k+1}|^2 \cdots |x_1 - x_d|^2 = C \Delta_k^2$$

for some constant C depending only on k and d . In fact consider a fixed summand

$$(x_{j_{\sigma(1)}} - x_{j_{\sigma(2)}})(x_{j_{\sigma(3)}} - x_{j_{\sigma(4)}}) \cdots (x_{j_{\sigma(2k-1)}} - x_{j_{\sigma(2k)}})$$

for some permutation σ and $2k$ -tuple (j_1, \dots, j_{2k}) . We first observe that there exists a pair $(\sigma(r), \sigma(r+1))$ with r odd and $1 \leq r \leq 2k-1$ so that $\max(j_{\sigma(r)}, j_{\sigma(r+1)}) \leq d-k+1$. If not we can then find k distinct integers $\{j_{r_1}, \dots, j_{r_k}\}$ in the integer interval $[d-k+2, d]$ which is clearly impossible. For such a pair $(\sigma(r), \sigma(r+1))$ we have

$$|x_{j_{\sigma(r)}} - x_{j_{\sigma(r+1)}}| \leq 2|x_1 - x_{d-k+1}|.$$

We eliminate this pair and proceed to find another pair $(\sigma(r'), \sigma(r' + 1))$ so that $\max(j_{\sigma(r')}, j_{\sigma(r'+1)}) \leq d - k + 2$ which gives

$$|x_{j_{\sigma(r')}} - x_{j_{\sigma(r'+1)}}| \leq 2|x_1 - x_{d-k+2}|.$$

And so on by induction which gives the claim.

By the fundamental theorem for symmetric polynomials we can find a *unique* polynomial

$$P(e_1, \dots, e_d) = \sum_{\substack{\alpha=(\alpha_1, \dots, \alpha_d) \\ \alpha_1+2\alpha_2+\dots+d\alpha_d \leq 2k}} c_\alpha e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d}$$

where $P(e_1, \dots, e_d) = Q(t_1, \dots, t_d)$ and the e_j are the elementary symmetric polynomials of the variables t_1, \dots, t_d . Since Q is a homogeneous polynomial of degree $2k$ and since each monomial $e_1^{\alpha_1} \dots e_d^{\alpha_d}$ is a homogeneous polynomial (in t_1, \dots, t_d) of degree $\alpha_1 + 2\alpha_2 + \dots + d\alpha_d$, we see that

$$P(e_1, \dots, e_d) = \sum_{\substack{\alpha=(\alpha_1, \dots, \alpha_d) \\ \alpha_1+2\alpha_2+\dots+d\alpha_d=2k}} c_\alpha e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d}.$$

If we set $t_{k+1} = \dots = t_d = 0$, then $Q(t_1, \dots, t_k, 0, \dots, 0) = c[t_1 \dots t_k]^2$ for some $c > 0$. In fact a computation shows that

$$c = c_{k,d} = 2k \binom{d-k}{k} k!^2$$

and our assumption that the characteristic of the ring R , if positive, is larger than $d - k$ guarantees that $|cx| = a|x|$ where $a = |c \cdot \mathbf{1}| > 0$. Here $\mathbf{1}$ is the identity element in our ring R and $c \cdot \mathbf{1} = \mathbf{1} + \dots + \mathbf{1}$, c times.

Hence

$$P(s_1, \dots, s_k, 0, \dots, 0) = c[t_1 \dots t_k]^2 = c[s_k]^2$$

where $s_1 = t_1 + \dots + t_k, \dots, s_k = t_1 \dots t_k$ are the first k elementary symmetric functions of the variables t_1, \dots, t_k . By the uniqueness part of the fundamental theorem representing symmetric polynomials by polynomials of elementary symmetric polynomials, we have $c_\alpha = 0$ for all $\alpha = (\alpha_1, \dots, \alpha_k, 0, \dots, 0)$ satisfying $\alpha_1 + 2\alpha_2 + \dots + k\alpha_k = 2k$ except when $\alpha = (\alpha_1, \dots, \alpha_d)$ with $\alpha_k = 2$ and all other entries equal to zero, in which case $c_\alpha = c > 0$.

Our goal now is to show that $|e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d}|$ is small compared to $|e_k|^2$ (when the e_j are evaluated at our points x_1, \dots, x_d) for all $\alpha = (\alpha_1, \dots, \alpha_d)$ with $c_\alpha \neq 0$ except for the one with $\alpha_k = 2$ and all other entries zero where of course the above expression is equal to $|e_k|^2$. Let us look at a general monomial $c_\alpha e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d}$ of the symmetric polynomial P . Of course $\alpha_{2k+1} = \dots = \alpha_d = 0$ but furthermore there can be at most one nonzero α_j for $j \geq k + 1$ and if this is the case, it must have value equal to one. If $j = 2k$ then $e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d} = e_{2k}$ and $|e_{2k}|$ is clearly small compared to $|e_k|^2$ by hypothesis (in fact $|e_{2k}| \leq |e_k| \leq A^{-1}|e_k|^2$). If $j = 2k - 1$ then $e_1^{\alpha_1} e_2^{\alpha_2} \dots e_d^{\alpha_d} = e_1 e_{2k-1}$ and $|e_1 e_{2k-1}|$ is also small compared to $|e_k|^2$; in fact, $|e_1 e_{2k-1}| \leq \eta_1 |e_k|^2$.

But we now run into some trouble since there are terms when $j \leq 2k - 2$ which will not be small compared to $|e_k|^2$ and we must show that such troublesome terms in fact do not arise; that is, the corresponding coefficients c_α are in fact zero. To see this write

$$P(e_1, \dots, e_d) = ce_k^2 + e_{k+1}P_1(e_1, \dots, e_k) + \dots + e_{2k}P_k(e_1, \dots, e_k)$$

where $c > 0$ and for each $1 \leq j \leq k$,

$$P_j(e_1, \dots, e_k) = \sum_{\substack{\alpha=(\alpha_1, \dots, \alpha_k) \\ \alpha_1+2\alpha_2+\dots+k\alpha_k=k-j}} b_\alpha^j e_1^{\alpha_1} e_2^{\alpha_2} \dots e_k^{\alpha_k}$$

For the moment let us concentrate on P_1 and here the goal is to show that $b_\alpha^1 = 0$ for all $\alpha = (\alpha_1, \dots, \alpha_k)$, $\alpha_1 + \dots + k\alpha_k = k - 1$ except for that α with all entries equal to zero save $\alpha_{k-1} = 1$ (note that this is the only non-offending monomial in P_1 since $|e_{k-1}e_{k+1}|$ can be made small compared to $|e_k|^2$ by our hypotheses). We impose the following *total* ordering on k -tuples arising in the sum defining P_1 : if $\alpha = (\alpha_1, \dots, \alpha_k)$ and $\beta = (\beta_1, \dots, \beta_k)$ are two such k -tuples then we say $\alpha < \beta$ if there is an ℓ , $1 \leq \ell \leq k$ so that $\alpha_1 + \dots + \alpha_k = \beta_1 + \dots + \beta_k$, $\alpha_2 + \dots + \alpha_k = \beta_2 + \dots + \beta_k$, \dots , $\alpha_{\ell-1} + \dots + \alpha_k = \beta_{\ell-1} + \dots + \beta_k$ but $\alpha_\ell + \dots + \alpha_k < \beta_\ell + \dots + \beta_k$. Of course, given any two distinct k -tuples α and β it is a trivial matter to check that either $\alpha < \beta$ or $\beta < \alpha$.

We now proceed to eliminate each b_α^1 (that is, showing they are zero) one by one starting with the maximal α in this total ordering which by the way is $\alpha = (k - 1, 0, \dots, 0)$ since all other $\alpha = (\alpha_1, \dots, \alpha_k)$ satisfy $\alpha_2 + 2\alpha_3 + \dots + (k-1)\alpha_k \geq 1$ and so $\alpha_1 + \dots + \alpha_k < k - 1 = \alpha_1 + 2\alpha_2 + \dots + k\alpha_k$. To do this we set $t_{k+2} = \dots = t_d = 0$ and thus

$$Q(t_1, \dots, t_{k+1}, 0, \dots, 0) = cs_k^2 + s_{k+1}P_1(s_1, \dots, s_k)$$

where now (changing notation a bit) s_1, \dots, s_{k+1} denote the elementary symmetric polynomials in the variables t_1, \dots, t_{k+1} . We simply note that the monomial $t_1^k t_2 \dots t_{k+1}$ which arises in $s_1^{k-1} s_{k+1}$ does not arise in any other term $s_1^{\alpha_1} \dots s_k^{\alpha_k} s_{k+1}$ appearing in $s_{k+1}P_1(s_1, \dots, s_k)$ as well as not arising in $Q(t_1, \dots, t_{k+1}, 0, \dots, 0)$ (strictly speaking we are assuming $k \geq 3$ but the arguments for the cases $k = 1$ and $k = 2$ are completed by this point). Hence $b_{(k-1, 0, \dots, 0)}^1 = 0$.

If $\beta \neq (0, \dots, 0, 1, 0)$, we want to show $b_\beta^1 = 0$. By induction assume we have shown that $b_\alpha^1 = 0$ for all $\alpha > \beta$. Therefore

$$Q(t_1, \dots, t_{k+1}, 0, \dots, 0) = cs_k^2 + s_{k+1} \sum_{\alpha \leq \beta} b_\alpha^1 s_1^{\alpha_1} \dots s_k^{\alpha_k}$$

and we note that if $\alpha_0 < \beta$ is the predecessor of β in this total ordering, then there is an ℓ , $1 \leq \ell \leq k$ so that $\alpha_{0,1} + \dots + \alpha_{0,k} = \beta_1 + \dots + \beta_k$, \dots , $\alpha_{0,\ell-1} + \dots + \alpha_{0,k} = \beta_{\ell-1} + \dots + \beta_k$ but $\alpha_{0,\ell} + \dots + \alpha_{0,k} < \beta_\ell + \dots + \beta_k$. We observe that the monomial

$$t_1^{\beta_1 + \dots + \beta_k + 1} t_2^{\beta_2 + \dots + \beta_k + 1} \dots t_\ell^{\beta_\ell + \dots + \beta_k + 1} t_{\ell+1}^{\theta_1} \dots t_{k+1}^{\theta_{k+1} - \ell}$$

which arises in $s_{k+1} s_1^{\beta_1} \dots s_k^{\beta_k}$ does not arise in $s_{k+1} s_1^{\alpha_1} \dots s_k^{\alpha_k}$ for any $\alpha < \beta$ and also does not arise in $Q(t_1, \dots, t_{k+1}, 0, \dots, 0)$ when $\beta \neq (0, \dots, 0, 1, 0)$. Therefore $b_\beta^1 = 0$ as desired.

When we move on to the polynomial P_2 and set $t_{k+3} = \dots = t_d = 0$, we have

$$Q(t_1, \dots, t_{k+2}, 0, \dots, 0) = cs_k^2 + ds_{k-1}s_{k+1} + s_{k+2}P_2(s_1, \dots, s_k)$$

where we continue to abuse notation and denote by s_1, \dots, s_{k+2} , the elementary symmetric polynomials in the variables t_1, \dots, t_{k+2} . In a similar way one shows $P_2(s_1, \dots, s_k) = es_{k-2}$ and so on and so forth by induction, arriving finally at

$$P(e_1, \dots, e_d) = ce_k^2 + b_1e_{k-1}e_{k+1} + b_2e_{k-2}e_{k+2} + \dots + b_ke_{2k}$$

where $c > 0$ is given explicitly above (full details can be found in [2]). Therefore when we evaluate the e_j at our given points x_1, \dots, x_d , we have

$$|P(e_1, \dots, e_d)| \geq |ce_k|^2 - Mk \max(\eta_1, \dots, \eta_{k-1}, A^{-1})|e_k|^2$$

where M is the maximum of the integer coefficients $b_j, 1 \leq j \leq k$. And together with the **Claim** above establishes the desired inequality (13).

4. FURTHER APPLICATIONS

In this section we prove Corollary 2.2 and Corollary 2.3. We begin with the proof of Corollary 2.3 which depends on the following proposition that gives a structural statement for sublevel sets of polynomials in terms of root clusters defined in the introduction. Recall that if $\{z_1, \dots, z_m\}$ denotes the set of distinct roots of a polynomial $P(x) = a_d \prod_j (x - z_j)^{m_j}$ of degree $d = \sum_j m_j$ in $A[X]$, then we define a root cluster as some subset $\mathcal{C} \subset \{z_1, z_2, \dots, z_m\}$. The following is a slight extension of a result of Phong and Stein in [5].

Proposition 4.1. *Suppose A is a commutative ring with a nontrivial absolute value $|\cdot|$ and let $P(x) = a_d \prod (x - z_j)^{m_j}$ be a polynomial in $A[X]$ (the roots $\mathcal{R}_P = \{z_1, \dots, z_m\}$ of P lying in some field extension K). Then ³*

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{j=1}^m \bigcap_{\mathcal{C}: z_j \in \mathcal{C}} \bigcup_{z_\ell \in \mathcal{C}} [B_{r_{\mathcal{C}, \delta}}(z_\ell) \cap A] \quad (14)$$

where the intersection is taken over all clusters $\mathcal{C} \subset \{z_1, \dots, z_m\}$ containing z_j . Here

$$r_{\mathcal{C}, \delta} := \left[2^{d-S(\mathcal{C})} \frac{\delta}{|a_d \prod_{z_k \notin \mathcal{C}} (z_j - z_k)^{m_k}|} \right]^{1/S(\mathcal{C})}$$

where $S(\mathcal{C}) = \sum_{j: z_j \in \mathcal{C}} m_j$ and the absolute value $|\cdot|$ in $r_{\mathcal{C}, \delta}$ and B_r is any extension of the original absolute value to K . When the absolute value $|\cdot|$ is non-archimedean, the factor $2^{d-S(\mathcal{C})}$ can be replaced by 1 in $r_{\mathcal{C}, \delta}$.

Proof Set $A_j := \{x \in A : |x - z_j| = \min_k (|x - z_k|)\}$ and note that

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{j=1}^m \{x \in A_j : |P(x)| \leq \delta\}.$$

³this sublevel set inclusion has been sharpened in [8] to give an equality of sets

Now fix j , $1 \leq j \leq m$, and observe that when $x \in A_j$,

$$|P(x)| \geq 2^{S(\mathcal{C})-d} |a_d \prod_{z_k \notin \mathcal{C}} (z_j - z_k)^{m_k}| \cdot \left| \prod_{z_k \in \mathcal{C}} (x - z_k)^{m_k} \right|$$

for any cluster \mathcal{C} containing z_j since $|z_j - z_k| \leq |z_j - x| + |x - z_k| \leq 2|x - z_k|$ when $x \in A_j$ (the factor of $2^{S(\mathcal{C})-d}$ can be replaced by 1 when the absolute value $|\cdot|$ is non-archimedean). Therefore for $x \in A_j$, if also $|P(x)| \leq \delta$, then $|\prod_{z_k \in \mathcal{C}} (x - z_k)^{m_k}| \leq r_{\mathcal{C}, \delta}^{S(\mathcal{C})}$ for any cluster \mathcal{C} containing z_j and this gives

$$\{x \in A_j : |P(x)| \leq \delta\} \subset \bigcap_{\mathcal{C}: z_j \in \mathcal{C}} \bigcup_{z_\ell \in \mathcal{C}} [B_{r_{\mathcal{C}, \delta}}(z_\ell) \cap A],$$

completing the proof of the proposition. \blacksquare

Before proceeding with the proof of Corollary 2.3, we pause to note that Proposition 4.1 gives a proof of Theorem 1.2. We apply Proposition 4.1 to P with $A = \mathfrak{o}$, $\delta = \|\mathfrak{p}\|^{-\alpha}$ for some integer $\alpha \geq 1$ and absolute value $|x| := \|\mathfrak{p}\|^{-\text{ord}_{\mathfrak{p}}(x)}$, noting that if some $B_r(z) \cap \mathfrak{o}$ appearing in (14) is nonempty, then there is an element $y \in \mathfrak{o}$ so that $B_r(z) \cap \mathfrak{o} = \{x \in \mathfrak{o} : |x - y| \leq r\}$. Therefore if s satisfies $\|\mathfrak{p}\|^{-s} \leq r < \|\mathfrak{p}\|^{-s+1}$ for some $s < \alpha$, then the number of disjoint ‘balls’ $\{x \in \mathfrak{o} : |x - x_0| \leq \|\mathfrak{p}\|^{-\alpha}\}$ which lie inside a fixed $B_r(z) \cap \mathfrak{o}$ is $\|\mathfrak{p}\|^{\alpha-s} \leq \|\mathfrak{p}\|^{\alpha} r$. The set inclusion (14) therefore leads to the bound

$$\#\{x \in \mathfrak{o}/\mathfrak{p}^\alpha : P(x) \equiv 0 \pmod{\mathfrak{p}^\alpha}\} \leq \sum_{j=1}^m \inf_{\mathcal{C}: z_j \in \mathcal{C}} \|\mathfrak{p}\|^{\alpha - \frac{(\alpha - \delta_{\mathfrak{p}}(P; \mathcal{C}, z_j))}{S(\mathcal{C})}} \#\mathcal{C}.$$

More details can be found in [8].

In order to establish Corollary 2.3 it is convenient to prove a slight generalisation, relaxing the normalisation of the polynomial in the following way. We will prove that for any $d \geq 1$ and $\sigma > 0$, there is a positive constant $A_{d, \sigma}$ so that if $P(x) = a_d x^d + \dots + a_0 \in A[X]$ with each $|a_j| \leq 1$ but $|a_{d-k}| \geq \sigma$ for some $k \leq d/2$, then

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{z \in \mathcal{R}_P} [B_{A_{d, \sigma} \delta^{1/d} \min(1, \delta^{1/d})}(z) \cap A] \quad (15)$$

holds. The proof of (15) is carried out by induction on k . When $k = 0$ (and so $|a_d| \geq \sigma$), we consider only the cluster $\mathcal{C} = \{z_1, z_2, \dots, z_m\}$ corresponding to *all* the roots in (14) and so Proposition 4.1 implies that

$$\{x \in A : |P(x)| \leq \delta\} \subset \bigcup_{j=1}^d [B_{[\delta/|a_d|]^{1/d}}(z_j) \cap A] \subset \bigcup_{j=1}^d [B_{[\delta/\sigma]^{1/d}}(z_j) \cap A],$$

establishing a stronger version of (15) in this case, the minimum $\min(1, \delta^{1/d})$ being replaced by 1. Now let us assume that (15) has been established for all $k' < k$. To carry out the induction step, we need the following, more refined result: for each $k \geq 0$ and every $\sigma > 0$, there are small positive constants $\sigma_0, \dots, \sigma_{k-1}$, depending only on σ, d ($\geq 2k$) and the absolute value $|\cdot|$ so that for any polynomial $Q(x) = b_d x^d + \dots + b_1 x + b_0$ with $\sigma \leq |b_{d-k}| \leq 1$, $|b_{d-j}| \leq \sigma_j$, $0 \leq j \leq k-1$ and

$$|b_{d-j}| \leq 1, j \geq k+1,$$

$$\{x \in A : |Q(x)| \leq \delta\} \subset \bigcup_{z \in \mathcal{R}_Q} [B_{A\delta^{1/(d-k)}}(z) \cap A] \quad (16)$$

holds for all $\delta > 0$, where A depends only on σ, σ_j 's and d .

The case $k = 0$ coincides with the strengthened version of (15) mentioned above. We will **not** proceed by induction to establish (16) for general k , instead we will do this directly for every k .

However before proceeding to the proof of (16), let us see how this implies (15) and hence Corollary 2.3. Recall that the case $k = 0$ has already been established and we proceed to the induction step, assuming the desired conclusion holds for all values $k' < k$. Let $\sigma > 0$ be given and fix a polynomial $P(x) = \sum_{j=0}^d a_j x^j$ satisfying the relaxed normalisation conditions $|a_j| \leq 1, j \geq 0$ and $|a_{d-k}| \geq \sigma$. For this k and $\sigma > 0$, the refined result (16) produces small positive constants $\sigma_0, \dots, \sigma_{k-1}$ so that (16) holds for any polynomial $Q(x) = \sum_{j=0}^d b_j x^j$ satisfying the relaxed normalisation conditions, together with the added conditions $|b_{d-j}| \leq \sigma_j, 0 \leq j \leq k-1$. Back to our polynomial P , if there is some coefficient $a_{d-j}, 0 \leq j \leq k-1$ satisfying $|a_{d-j}| \geq \sigma_j$, then we can apply the induction hypothesis with $k' = d-j < k$ to conclude that (15) holds. On the other hand, if all the coefficients $a_{d-j}, 0 \leq j \leq k-1$ satisfy $|a_{d-j}| \leq \sigma_j$, then (16) holds and this implies (15) holds as well since $k \leq d/2$. This completes the induction step.

We now turn to establish (16). Fix a polynomial $Q(x) = b_d x^d + \dots + b_0$ of degree d with $\sigma \leq |b_{d-k}| \leq 1$ for some $k \leq d/2$ and $|b_j| \leq 1$ for all j . Our goal is to see how small we need the sizes $|b_{d-j}|, 0 \leq j \leq k-1$ to be in order to conclude that (16) holds for this Q . First of all, Proposition 4.1 applied to Q gives

$$\{x \in A : |Q(x)| \leq \delta\} \subset \bigcup_{j=1}^m \bigcap_{C: z_j \in C} \bigcup_{z_\ell \in C} [B_{r_{C,\delta}}(z_\ell) \cap A] \quad (17)$$

where z_1, z_2, \dots, z_{m-1} and z_m are the distinct roots of Q with multiplicities m_1, m_2, \dots respectively and

$$r_{C,\delta} := \left[2^{d-S(C)} \frac{\delta}{|a_d \prod_{z_k \notin C} (z_j - z_k)^{m_k}|} \right]^{1/S(C)}.$$

Let $\{w_1, w_2, \dots, w_d\}$ be an enumeration of the roots $\{z_j\}$, listed with multiplicity. We now make a connection between root clusters defined in the introduction and clusters defined as subsets $L \subset \{1, \dots, d\}$ used in Section 2 to define the quantities Δ_k . For each $1 \leq j \leq m$, choose an index $n \in \{1, \dots, d\}$ so that $w_n = z_j$; it is an easy calculus exercise to verify that

$$\inf_{C: z_j \in C} \left[\frac{\delta}{|a_d \prod_{z_k \notin C} (z_j - z_k)^{m_k}|} \right]^{1/S(C)} = \inf_{L: n \in L} \left[\frac{\delta}{|a_d \prod_{\ell \notin L} (w_n - w_\ell)|} \right]^{1/|L|} \quad (18)$$

where the second infimum is taken over all subsets $L \subset \{1, \dots, d\}$ containing n .

According to (6) (the reformulation of Theorem 2.1 in terms of polynomials), we have that for every $n \geq 1$, there is a subset $L \subset \{1, 2, \dots, d\}$ of size $|L| = d - k$

containing n so that

$$|a_d \prod_{k \notin L} (w_n - w_k)| \geq c_{k,d}$$

holds whenever coefficients $|b_{d-j}|, 0 \leq j \leq k-1$ are small enough. This, together with (18), shows that (17) implies the desired set inclusion (16). This completes the proof of Corollary 2.3.

We now turn to the proof of Corollary 2.2. This follows in exactly the same way as the proof of Corollary 2.3 except we use the analogue of Proposition 4.1 for oscillatory integrals which can be found in [4] (the analogue of which for exponential and character sums holds but will appear elsewhere). We leave the details to the reader.

REFERENCES

- [1] L.K. Hua, *On an exponential sum*, J. Chinese Math. Soc. 20 (1940), 301-312..
- [2] M. W. Kowalski, *A comparative study of oscillatory integral, and sub-level set, operator norm estimates*, PhD thesis, University of Edinburgh, 2010.
- [3] J.H. Loxton and R.A. Smith, *On Hua's estimate for exponential sums*, J. London Math. Soc. **26** (1982), 15-20.
- [4] D.H. Phong and E.M. Stein, *Oscillatory integrals with polynomial phases*, Inventiones Math. **110** (1992), 39-62.
- [5] D.H. Phong, E.M. Stein and J.A. Sturm, *On the growth and stability of real analytic functions*, Amer. J. Math **121** (1999), 519-554.
- [6] E.M. Stein, *Harmonic Analysis*, Princeton University Press, 1990.
- [7] J. Wright, *From oscillatory integrals and sublevel sets to polynomial congruences and character sums*, to appear in J. Geom. Anal.
- [8] ———, *On polynomial congruences*, preprint.

35 MELBURY COURT, 240-280 KENSINGTON HIGH STREET, LONDON, W8 6NH, ENGLAND, UK

E-mail address: e2thepi@hotmail.com

MAXWELL INSTITUTE OF MATHEMATICAL SCIENCES AND THE SCHOOL OF MATHEMATICS, UNIVERSITY OF EDINBURGH, JCMB, KING'S BUILDINGS, MAYFIELD ROAD, EDINBURGH EH9 3JZ, SCOTLAND

E-mail address: J.R.Wright@ed.ac.uk