DISCRETE ANALYSIS, 2021:11, 46 pp.
www.discreteanalysisjournal.com

Multivariate Polynomial Values in Difference Sets

John R. Doyle* Alex Rice

Received 14 September 2020; Published 8 September 2021

Abstract: For $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ of degree $k \geq 2$, we show that every subset $A \subseteq \{1,2,\dots,N\}$ lacking nonzero differences in $h(\mathbb{Z}^\ell)$ satisfies $|A| \ll_h Ne^{-c(\log N)^\mu}$, where $c = c(h) > 0$, $\mu = [(k-1)^2+1]^{-1}$ if $\ell = 2$, and $\mu = 1/2$ if $\ell \geq 3$, provided $h(\mathbb{Z}^\ell)$ contains a multiple of every natural number and h satisfies certain nonsingularity conditions. We also explore these conditions in detail, drawing on a variety of tools from algebraic geometry.

1 Introduction

Originating with conjectures of Erdős and Lovász, an extensive literature has developed over the past several decades concerning the existence of particular differences within dense sets of integers. For sets $A,B \subseteq \mathbb{Z}$, we define the sum and difference sets, respectively, as usual by $A \pm B = \{a \pm b : a \in A, b \in B\}$, and we also define the following threshold.

Definition 1.1. For $X \subseteq \mathbb{Z}$ and $N \in \mathbb{N}$, we define $D(X,N) = \max\{|A| : A \subseteq [1,N],\ (A-A) \cap X \subseteq \{0\}\}$.

We use $[1,N]$ to denote $\{1,2,\dots,N\}$ and $|A|$ to denote the size of a finite set A. To clarify, $D(X,N)$ is the threshold such that any subset of $\{1,2,\dots,N\}$ with more than $D(X,N)$ elements necessarily contains two distinct elements that differ by an element of X. As an introductory offering prior to extensive discussions of history, motivation, notation, and terminology, a very special case of our results in this paper is the following:

*Partially supported by NSF grant DMS-2001486.

DOI: 10.19086/da.27995

Theorem 1.2. *Suppose $h \in \mathbb{Z}[x,y]$ is a homogeneous polynomial of degree $k \geq 2$. If $\Delta(h) \neq 0$, then*

$$D(h(\mathbb{Z}^2),N) \ll_h Ne^{-c(\log N)^{\mu}}, \tag{1}$$

where $c = c(h) > 0$ and $\mu = [(k-1)^2+1]^{-1}$.

Here Δ denotes the usual homogeneous discriminant, and we use $\ll$ to denote "less than a constant times", with subscripts indicating on what parameters, if any, the implied constant depends. We take the same convention with subscripts on Big O notation. Theorem 1.2 follows from Corollary 2.6 and our main result, Theorem 2.4, of which we discuss various improvements and important special cases throughout Section 2.

1.1 Background

Lovász asked whether a set of positive upper density must contain two distinct elements that differ by a perfect square, or equivalently whether $D(S,N) = o(N)$, where $S = \{n^2 : n \in \mathbb{N}\}$. Similarly, Erdős conjectured that $D(\mathcal{P}-1,N) = o(N)$, where $\mathcal{P}-1 = \{p-1 : p \text{ prime}\}$. Furstenberg [10] verified the former using ergodic methods, specifically his correspondence principle, in the same paper in which he provided the second known proof of Szemerédi's Theorem on arithmetic progressions. Independently and concurrently, Sárközy ([35], [36]) verified both conjectures with a Fourier analytic density increment argument driven by the Hardy-Littlewood circle method. Further, Sárközy's results included quantitative information, showing $D(S,N) \ll_\varepsilon N(\log N)^{-1/3+\varepsilon}$ and $D(\mathcal{P}-1,N) \ll_\varepsilon N(\log\log N)^{-2+\varepsilon}$ for every $\varepsilon > 0$.

These results have been incrementally improved and generalized in multiple ways, both through tightening of the quantitative bounds and expansion of the possibilities for the set X of prohibited differences. Regarding the former, Pintz, Steiger and Szemerédi [26] utilized a more elaborate Fourier analytic strategy to show

$$D(S,N) \ll N(\log N)^{-c\log\log\log\log N} \tag{2}$$

for a constant $c > 0$.

Dramatically improving Sárközy's original bound, Ruzsa and Sanders [32] showed

$$D(\mathcal{P}-1,N) \ll Ne^{-c(\log N)^{\mu}} \tag{3}$$

with $\mu = 1/4$, recently improved to $\mu = 1/3$ by Wang [39]. Regarding alternative choices for the set of prohibited differences, one must first consider obvious local obstructions. For example, we consider $\mathcal{P}-1$, rather than $\mathcal{P}$, because $\mathcal{P} \cap 4\mathbb{Z} = \emptyset$ implies $D(\mathcal{P},N) \geq \lceil N/4 \rceil$ by taking A to be a congruence class modulo 4. Analogously, if $h \in \mathbb{Z}[x]$ and $h(\mathbb{Z})$ contains no multiples of $q \in \mathbb{N}$, then $D(h(\mathbb{Z}),N) \geq \lceil N/q \rceil$. Therefore, for even a qualitative $o(N)$ result, it is clearly necessary that $h(\mathbb{Z})$ contains a nonzero multiple of every $q \in \mathbb{N}$, in which case we say that h is an *intersective polynomial*. Examples of intersective polynomials include any nonzero polynomial with an integer root or a collection of rational roots with coprime denominators. However, there are also intersective polynomials with no rational roots, such as $(x^3-19)(x^2+x+1)$.

Balog, Pelikán, Pintz, and Szemerédi [1] extended (2) with S replaced by $\{n^k : n \in \mathbb{N}\}$ for any fixed $k \in \mathbb{N}$. For a general univariate intersective polynomial, Kamae and Mendes-France [18] established the qualitative $o(N)$ result, the first quantitative bounds were due to Lucier [23], and the second author [28] fully extended (2). In a recent preprint, Bloom and Maynard [3] both simplified and improved the ideas of [26], using a more traditional density increment to establish

$$D(S,N) \ll N(\log N)^{-c\log\log\log N} \tag{4}$$

for a constant $c > 0$, which is currently the best-known bound for the original square difference question. Further, the methods of [3] are completely compatible with those of [28], so in fact (4) should hold for the full class of intersective polynomials. For other intermediate and related results, as well as alternative proofs, the reader may refer to (in chronological order) [11], [37], [24], [22], [21], [25], [14], [30], and [12].

Also in [28], the second author showed that if $g,h \in \mathbb{Z}[x]$ are intersective polynomials, then

$$D(g(\mathbb{Z})+h(\mathbb{Z}),N) \ll_{g,h} Ne^{-c(\log N)^{\mu}}, \tag{5}$$

where $c = c(g,h) > 0$ and $\mu = \mu(\deg(g),\deg(h)) > 0$. Further, the second author [31] considered the simplest nontrivial case of a non-diagonal multivariate polynomial, showing that for a binary quadratic form $h(x,y) = ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ with $b^2-4ac \neq 0$, we have

$$D(h(\mathbb{Z}^2),N) \ll_h Ne^{-c\sqrt{\log N}}. \tag{6}$$

1.2 Motivation

As outlined in Section 2.4 of [28], the quoted upper bounds in the previous section, all of which result from adaptations of the two aforementioned Fourier analytic arguments developed in [35] and [26], respectively, are partially determined by the degree of decay in local exponential averages similar to

$$q^{-1}\sum_{s=0}^{q-1} e^{2\pi i h(s)a/q}. \tag{7}$$

The best general upper bound for (7) is of the order $q^{-1/k}$ where $k = \deg(h)$, but the elaborate double iteration method developed in [26], and the simplified improvement developed in [3], which lead to upper bounds like (2) and (4), require decay at or near $q^{-1/2}$, which we refer to as *square-root cancellation*. Inspired by [1], the second author [28] eliminated this discrepancy for $k > 2$ in the general case by employing a polynomial-specific sieve to the set of considered inputs that, roughly speaking, reduced the issue to estimating (7) at prime moduli, for which the desired square-root cancellation is a well-known result of Weil. This sieve technique can be thought of as a bridge from the integer setting to the best available exponential sum estimates over finite fields.

Ruzsa and Sanders [32], and later Wang [39], were able to adapt the more traditional density increment method to establish (3), which is a stronger type of upper bound as compared with (2) or (4), based on

two key factors: the high degree of decay in the relevant exponential averages, which are modifications of

$$\phi(q)^{-1} \sum_{\substack{s=0 \\ (s,q)=1}}^{q-1} e^{2\pi i s/q} = \frac{\mu(q)}{\phi(q)},$$

and the careful analysis of the distribution of primes in arithmetic progressions, including the consideration of exceptional zeros of Dirichlet L-functions. In the polynomial setting, the distribution of inputs in arithmetic progressions is not as delicate of an issue, though it does rear its head when employing a sieve, but this level of local decay is out of reach with a single variable. Specifically, bounds like (1) from the density increment require decay at or near q^{-1} (more specifically, q^{-1} times a function of average value at most polylogarithmic in q, and the exponent μ depends on the power of the logarithm), which we refer to as *q-cancellation*.

While the image of a multivariate intersective polynomial does not necessarily contain the image of a univariate intersective polynomial, it is the case that, by only exploiting cancellation in one variable, the methods of [28] and [3] can be adapted to show that (4) holds for such an image, so upper bounds in the multivariate setting are only novel if they are stronger than (4). The observation made in [28] to establish (5) was a rather simple one: if we consider differences of the form $g(m)+h(n)$, then the relevant exponential sum factors into a product, our sieve gives square-root cancellation in each variable, and these combine to give q-cancellation. However, this observation does not fully generalize to the case of a single polynomial in several variables with nonzero cross-terms. In particular, simple examples like $h(x,y) = (x+y)^2$ make it clear that one cannot always exploit cancellation in each variable, so some sort of nonsingularity assumption is required.

In the setting of binary quadratic forms, the natural assumption is nonzero discriminant, and since sieving is not required to get square-root cancellation from each variable in degree 2, the adaptation of the usual density increment is relatively straightforward, as done in [31] to establish (6). Section 2 of [31] provides a helpful description of the density increment method in a simpler, sieve-free context.

For higher degrees, the sieve technique can indeed be adapted to the multivariate setting, which leads us toward the best available estimates on exponential sums for multivariate polynomials over finite fields, due to Deligne [8] in his proof of the Weil conjectures, and their associated nonsingularity assumptions. Recall that $\mathbb{A}^n$ and $\mathbb{P}^n$ denote n-dimensional affine and projective space, respectively.

Definition 1.3. Suppose F is a field, $\ell \in \mathbb{N}$, and $g \in F[x_1,\dots,x_\ell]$ is a homogeneous polynomial. We say that g is *smooth* if the vanishing of g defines a smooth hypersurface in $\mathbb{P}^{\ell-1}$ (as opposed to $\mathbb{A}^\ell$). In other words, g is smooth if the system $g(\boldsymbol{x}) = \frac{\partial g}{\partial x_1}(\boldsymbol{x}) = \cdots = \frac{\partial g}{\partial x_\ell}(\boldsymbol{x}) = 0$ has no solution besides $x_1 = \cdots = x_\ell = 0$ in $\overline{F}^\ell$, where the bar indicates the algebraic closure. For a general polynomial $h \in F[x_1,\dots,x_\ell]$ with $h = \sum_{i=0}^k h^i$, where h^i is homogeneous of degree i and $h^k \neq 0$, we say that h is *Deligne* if the characteristic of F does not divide k and h^k is smooth.

Remark on notation. For the remainder of the paper, we take the notational convention that, for a polynomial h, h^i denotes the degree-i homogeneous part of h, as opposed to h raised to the i-th power.

Theorem 1.4 (Theorem 8.4, [8]). *Suppose $\ell \in \mathbb{N}$ and $p \in \mathcal{P}$. If $h \in \mathbb{F}_p[x_1,\dots,x_\ell]$ is Deligne, then*

$$\left| \sum_{\boldsymbol{x} \in \mathbb{F}_p^\ell} e^{2\pi i h(\boldsymbol{x})/p} \right| \leq (\deg(h)-1)^\ell p^{\ell/2}.$$

This estimate provides a guide, but additional consideration is required to develop sufficient conditions on a multivariate polynomial for an application of Theorem 1.4 that is compatible enough with the density increment procedure to establish an upper bound like (1). We explore these details in Section 2.

1.3 Lower bounds and a special case

In all the nontrivial cases we have explored, there is a large gap in the best-known upper and lower bounds for $D(X,N)$. For an intersective polynomial $h \in \mathbb{Z}[x]$, all known lower bounds with $X = h(\mathbb{Z})$ are of order N^c for some $c < 1$. The greedy algorithm gives $c = 1 - 1/\deg(h)$, and higher values of c are known for monomials (see [33] and [20]) and certain other polynomials divisible by x^2 (due to Younis [41], and explored from an algebraic number theory perspective by Wessel [40]). For $X = \mathcal{P} - 1$, the gap is even larger, and the best-known lower bound is of the form $N^{o(1)}$ (see [34]). Younis [41] established lower bounds for certain homogeneous multivariate polynomials, including $D(S+S,N) \gg \sqrt{N}$, where S is the set of squares. All of these results are descended from methods of Ruzsa that transfer examples from the modular setting to the integer setting. In the absence of stronger lower bounds, the greedy algorithm gives $D(X,N) \geq (N-1)/(|X \cap [-N,N]|+1)$ for any set $X \subseteq \mathbb{Z}$ (see [25]).

As an aside, one very special case where stronger upper bounds on $D(X,N)$ are available, and where the upper and lower bounds can be relatively close, is the case when X is itself, or at least contains, a difference set. Specifically, if $Y \subseteq \{1,\dots,N\}$ and $X = Y - Y$, then for a set $A \subseteq \{1,\dots,N\}$ satisfying $(A-A) \cap X \subseteq \{0\}$, we have $a+y \neq a'+y'$ for all $a,a' \in A$ and $y,y' \in Y$ with $(a,y) \neq (a',y')$. In particular, the map $(a,y) \mapsto a+y$ into $\{1,\dots,2N\}$ is an injection, so $|A||Y| \leq 2N$, and hence $D(X,N) \leq 2N/|Y|$, while the greedy algorithm gives $D(X,N) \gg N/|X| \geq N/|Y|^2$. For an example relating to our discussion of multivariate polynomials, if X is the set of differences of k-th powers for a fixed $k \in \mathbb{N}$, then we have $D(X,N) \ll N^{1-1/k}$, but this observation does not immediately generalize beyond the case where $X \supseteq Y - Y$.

2 Main definitions and results

The density increment procedure takes as input a set $A \subseteq \{1,2,\dots,N\}$ lacking nonzero differences in the image of a polynomial h, and produces a new, denser subset of a slightly smaller interval lacking nonzero differences in the image of a potentially modified polynomial. The following definition keeps track of the changes in the polynomial over the course of the iteration.

Definition 2.1. Fix $\ell \in \mathbb{N}$. As in the univariate setting, we say that $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is *intersective* if $h(\mathbb{Z}^\ell)$ contains a nonzero multiple of every $q \in \mathbb{N}$. Equivalently, h is intersective if it is not identically zero and has a root in $\mathbb{Z}_p^\ell$ for every prime p, where $\mathbb{Z}_p$ denotes the p-adic integers.

Suppose $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is an intersective polynomial and fix, for each prime p, $\boldsymbol{z}_p \in \mathbb{Z}_p^\ell$ with $h(\boldsymbol{z}_p) = 0$. All objects defined below certainly depend on this choice of p-adic integer roots, but we suppress that dependence in the subsequent notation.

By reducing modulo prime powers and applying the Chinese Remainder Theorem, the choice of roots determines, for each $d \in \mathbb{N}$, a unique $\boldsymbol{r}_d \in (-d,0]^\ell$ with $\boldsymbol{r}_d \equiv \boldsymbol{z}_p \bmod p^j$ for all prime powers $p^j \mid d$.

We define a completely multiplicative function λ (depending on h and $\{\boldsymbol{z}_p\}$) on $\mathbb{N}$ by letting $\lambda(p) = p^{m_p}$ for each prime p, where m_p is the multiplicity of $\boldsymbol{z}_p$ as a root of h, that is,

$$m_p = \min\left\{ i_1 + \cdots + i_\ell : \frac{\partial^{i_1+\cdots+i_\ell} h}{\partial x_1^{i_1} \cdots \partial x_\ell^{i_\ell}}(\boldsymbol{z}_p) \neq 0 \right\}.$$

Roughly speaking, $\lambda(d)$ is the largest guaranteed factor of $h(\boldsymbol{n})$ for $\boldsymbol{n} \equiv \boldsymbol{r}_d \pmod d$.

Definition 2.2. With notation as described above, for each $d \in \mathbb{N}$ we define the *auxiliary polynomial* $h_d \in \mathbb{Z}[x_1,\dots,x_\ell]$ by

$$h_d(\boldsymbol{x}) = h(\boldsymbol{r}_d + d\boldsymbol{x})/\lambda(d).$$

Combining the hypotheses of Theorem 1.4 with the technical details of the density increment iteration, the following definition captures a sufficient condition for the success of the method.

Definition 2.3. When considering polynomials with integer coefficients, we use the terms *smooth* and *Deligne* as previously defined by embedding the coefficients in the field of rational numbers. In particular, $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ of degree $k \geq 1$ is Deligne if the system $h^k(\boldsymbol{x}) = \frac{\partial h^k}{\partial x_1}(\boldsymbol{x}) = \cdots = \frac{\partial h^k}{\partial x_\ell}(\boldsymbol{x}) = 0$ has no solution besides $x_1 = \cdots = x_\ell = 0$ in $\overline{\mathbb{Q}}^\ell$. In this case, there exists a finite set of primes $X = X(h)$ such that the reduction of h modulo p is Deligne for all $p \notin X$: Indeed, one can take $X(h)$ to be the set of primes dividing the Macaulay resultant $\operatorname{Res}\left(h^k, \frac{\partial h^k}{\partial x_1}, \cdots, \frac{\partial h^k}{\partial x_\ell}\right)$, which is nonzero precisely when h is Deligne. (See also Prop. A.9.1.6 of [16].)

Further, we say that h is *strongly Deligne* if there exists a finite set of primes $X = X(h)$ and a choice $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ of p-adic integer roots of h such that the reduction of h_d modulo p is Deligne for all $p \notin X$ and all $d \in \mathbb{N}$. We note that strongly Deligne polynomials are necessarily both Deligne and intersective.

To highlight some of the subtlety of this definition, we first note that $h_d^k = \frac{d^k}{\lambda(d)} h^k$, so for a prime $p \nmid d$, we have that if h is Deligne modulo p, then h_d is Deligne modulo p. However, complications arise when $p \mid d$, because h_d^i has a factor of $d^i/\lambda(d)$, and hence vanishes modulo p for all $i > m_p$. For an example of a polynomial that is Deligne and intersective but not strongly Deligne, see "the ugly" in Section 2.4.

For $k,\ell \geq 2$, we let $\mu(k,\ell) = \begin{cases} [(k-1)^2+1]^{-1} & \text{if } \ell = 2 \\ 1/2 & \text{if } \ell \geq 3 \end{cases}$. The central result of this paper is the following:

Theorem 2.4. *If $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is a strongly Deligne polynomial of degree $k \geq 2$, then*

$$D(h(\mathbb{Z}^\ell), N) \ll_h N e^{-c(\log N)^{\mu(k,\ell)}}, \tag{8}$$

where $c = c(h) > 0$.

Remark. In Theorem 2.4, the full image $h(\mathbb{Z}^\ell)$ is considered for ease of exposition, and to make the conclusion invariant under input translation. However, by inspection of the proof, the same upper bound can be seen to hold for $D(h([1,N^\varepsilon]^\ell),N)$ for any $\varepsilon > 0$, with c and the implied constant depending on ε. Also, in several of our results and definitions, we exclude the case $k = 1$ only out of convenience due to its triviality in this context. Specifically, if $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(h) = 1$, then $D(h(\mathbb{Z}^\ell),N) \ll_h 1$ if $0 \in h(\mathbb{Z}^\ell)$ and $D(h(\mathbb{Z}^\ell),N) \gg_h N$ otherwise.

After setting the stage with preliminary definitions and observations in Section 3, we prove Theorem 2.4 in Section 4, and then establish the needed exponential sum estimates, which we state separately as Theorem 3.9, in Section 7. More imminently, in Sections 2.1 and 2.2, we describe sufficient conditions under which $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is strongly Deligne, and hence (8) holds. Then, in Section 2.3, we explain that in many cases we may still get a bound similar to (8) even when the strongly Deligne condition is significantly relaxed.

2.1 The integer root case

The simplest sufficient condition for the intersectivity of a nonzero polynomial is the existence of an integer root. In this case, all p-adic integer roots can be taken to equal said integer root, which simplifies the auxiliary polynomial definition, giving rise to a pleasantly tangible sufficient condition for the strongly Deligne property, as captured with the following proposition.

Proposition 2.5. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $h(\mathbf{0}) = 0$. If the highest and lowest degree homogeneous parts of h are smooth, then h is strongly Deligne.*

Proof. Suppose h satisfies the hypotheses, let $k = \deg(h)$, let j denote the lowest degree of the nonzero terms of h, and let X denote the finite set of primes p such that $p \mid jk$ or either h^k or h^j is not smooth modulo p. Making the natural choice of p-adic integer roots $\boldsymbol{z}_p = \mathbf{0}$ for all p, we then have $h_d(\boldsymbol{x}) = h(d\boldsymbol{x})/d^j$, hence $h_d^i(\boldsymbol{x}) = d^{i-j}h^i(\boldsymbol{x})$. Fix $p \notin X$. If $p \nmid d$, then the highest degree part of h_d modulo p is a nonzero multiple of h^k, which is smooth modulo p, hence h_d is Deligne modulo p. If $p \mid d$, then the only nonvanishing homogeneous part of h_d is precisely h^j, which is smooth modulo p, hence h_d is Deligne modulo p. □

Remark. We note that $h(\mathbb{Z}^\ell)$, hence the threshold $D(h(\mathbb{Z}^\ell),N)$, as well as the Deligne and strongly Deligne properties, are all invariant under translations of the form $h(\boldsymbol{x}+\boldsymbol{n})$ for a fixed $\boldsymbol{n} \in \mathbb{Z}^\ell$. In particular, Proposition 2.5 applies provided there exists $\boldsymbol{n} \in \mathbb{Z}^\ell$ such that $h(\boldsymbol{n}) = 0$ and the highest and lowest degree parts of $h(\boldsymbol{x}+\boldsymbol{n})$ are smooth. More generally, all of our results that hold for a polynomial h also hold for the full translation equivalence class of h.

For homogeneous bivariate polynomials, smoothness of the corresponding (0-dimensional) variety is equivalent to non-vanishing of the discriminant. Therefore, for $\ell = 2$, we have the following, which in particular combines with Theorem 2.4 to yield Theorem 1.2 as a special case.

Corollary 2.6. *Suppose $h \in \mathbb{Z}[x,y]$ with $h(0,0) = 0$. If the highest and lowest degree homogeneous parts of h have nonzero homogeneous discriminant, then h is strongly Deligne.*

2.2 The Deligne case

Taking the next step in complexity, here we consider the case of a polynomial that is Deligne and intersective, but may not have an integer root. Recalling that if $p \mid d$, then h_d^i vanishes modulo p for all $i > m_p$, we make the following definition with the hopes of exploiting the fact that a nonzero homogeneous linear polynomial is guaranteed to be smooth.

Definition 2.7. For $\ell \in \mathbb{N}$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ we say that h is *smoothly intersective* if there exists a choice $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ of p-adic integer roots of h such that $m_p = 1$ for all but finitely many p. In other words, the variety defined by $h = 0$ has at least one point over $\mathbb{Z}_p$ for all p, and at least one nonsingular point over $\mathbb{Z}_p$ for all but finitely many p.

For low-hanging examples of polynomials that are intersective but not smoothly intersective, one could consider the square of any intersective polynomial, but such polynomials do not pass even our coarsest of nonsingularity filters. For an example of a polynomial that is intersective but not smoothly intersective in a more subtle and problematic way, see our discussion of "the ugly" in Section 2.4. Combining the motivation for the smoothly intersective definition with the fact that the highest degree part of a Deligne polynomial is assumed to be smooth, the following proposition provides a sufficient condition for the strongly Deligne property, and includes two notable special cases.

Proposition 2.8. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is Deligne and intersective with $\deg(h) = k \geq 2$. If there exists a choice $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ of p-adic integer roots of h satisfying $m_p \in \{1,k\}$ for all but finitely many p, then h is strongly Deligne. In particular, if $k = 2$ or h is smoothly intersective, then h is strongly Deligne.*

Using estimates on the number of nonsingular points on irreducible varieties over finite fields, we obtain the following convenient criterion for smooth intersectivity.

Proposition 2.9. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is Deligne and intersective, and let $h = g_1 \cdots g_n$ be an irreducible factorization of h in $\mathbb{Z}[x_1,\dots,x_\ell]$. If g_i is geometrically irreducible for some $1 \leq i \leq n$, then h is smoothly intersective, hence strongly Deligne.*

Remark. The conclusion of Proposition 2.9 remains true under weaker assumptions on the factorization of h. We give this cleaner statement here, but prove the more general statement in Corollary 5.4.

For $\ell \geq 3$, the Deligne condition actually implies geometric irreducibility, yielding the following:

Corollary 2.10. *Suppose $\ell \geq 3$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$. If h is Deligne and intersective, then h is smoothly intersective, hence strongly Deligne.*

Proof. By Proposition 2.9, it suffices to show that if h is a Deligne polynomial in $\ell \geq 3$ variables, then h is geometrically irreducible. Suppose to the contrary that $h = g_1 g_2$ with $g_1, g_2 \in \overline{\mathbb{Q}}[x_1,\dots,x_\ell]$ nonconstant of degrees d and $k-d$, respectively. In particular, we have $h^k = g_1^d g_2^{k-d}$. Each of $\{g_1^d = 0\}$ and $\{g_2^{k-d} = 0\}$ has codimension 1 in $\mathbb{P}^{\ell-1}$ (since they are hypersurfaces) and dimension at least 1 (since we assumed $\ell \geq 3$). In particular, $\{g_1^d = 0\}$ and $\{g_2^{k-d} = 0\}$ have nontrivial intersection, and any intersection point must be a singular point of the union $\{h^k = 0\}$, contradicting the fact that h is Deligne. □

In Section 5, we collect some crucial tools from algebraic geometry, which are followed by the proofs of both Proposition 2.8 and the aforementioned generalization of Proposition 2.9.

2.3 The singular case

While the Deligne condition is required to apply Theorem 1.4 to get the desired cancellation in our exponential sums, brief consideration reveals that the condition is not strictly necessary for a bound like (8) to hold, provided the failure of the Deligne condition is in balance with the freedom of extra variables. For a particularly simple example, consider $h(x,y,z) = (x+z)^4 + (x+z)y^3 + y^4$. This is a homogeneous degree-4 polynomial, and the variety $\widehat{V} \subseteq \mathbb{P}^2$ defined by its vanishing has a unique singular point, namely $(1:0:-1)$. In particular, h is not Deligne. However, by fixing $z = 0$, we can define $g(x,y) = h(x,y,0) = x^4 + xy^3 + y^4$, which is a bivariate homogeneous polynomial of nonzero discriminant. In particular, g is strongly Deligne, so Theorem 2.4 applies, and moreover $g(\mathbb{Z}^2) = h(\mathbb{Z}^3)$, so (8) holds for h as well, applied as if $\ell = 2$ as opposed to $\ell = 3$.

This example hints at a less black-and-white consideration of the singularity of a projective variety. For $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(h) = k \geq 1$, h is Deligne precisely when the variety $\widehat{V} \subseteq \mathbb{P}^{\ell-1}$ defined by $h^k = 0$ is nonsingular. The example above indicates that we should really only need to avoid this variety being "too singular", which leads to the following definition.

Definition 2.11. For $\ell \in \mathbb{N}$ and a nonconstant homogeneous polynomial $g \in \mathbb{Z}[x_1,\dots,x_\ell]$, let $\widehat{V} \subseteq \mathbb{P}^{\ell-1}$ be the variety defined by $g = 0$, and let $\widehat{V}^{\mathrm{s}}$ be the singular locus of $\widehat{V}$. We define the *rank* of g to be the codimension of $\widehat{V}^{\mathrm{s}}$ in $\mathbb{P}^{\ell-1}$, with the convention that the empty set has dimension -1, hence the codimension of the empty set in $\mathbb{P}^{\ell-1}$ is ℓ. This is a notion of rank developed by Birch in [2] and utilized, for example, in [6].

For $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(h) = k \geq 1$, the rank of h^k should, roughly speaking, encode the number of variables r such that $g(\mathbb{Z}^r) \subseteq h(\mathbb{Z}^\ell)$ for some Deligne polynomial $g \in \mathbb{Z}[x_1,\dots,x_r]$. In particular, h is Deligne if and only if the rank of h^k is ℓ. In Section 6, using careful dimension-lowering arguments, we successfully expand the class of polynomials for which a result analogous to Theorem 2.4 holds, generalizing our efforts from Sections 2.1 and 2.2 as follows.

Theorem 2.12. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $h(\mathbf{0}) = 0$ and $\deg(h) = k \geq 2$. Let r be the minimum rank of the highest and lowest degree homogeneous parts of h. If $r \geq 2$, then*

$$D(h(\mathbb{Z}^\ell), N) \ll_h N e^{-c(\log N)^{\mu(k,r)}}, \tag{9}$$

where $c = c(h) > 0$.

Theorem 2.13. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ is intersective of degree $k \geq 2$. Let r be the rank of h^k. If $r \geq 3$, OR if $r = 2$ and there exists a choice $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ of p-adic integer roots of h satisfying $m_p \in \{1,k\}$ for all but finitely many p, then (9) holds.*

Remark. To shed light on the hypotheses of Theorems 2.12 and 2.13, we note that, for $\ell \geq 2$ and a nonconstant homogeneous polynomial $g \in \mathbb{Z}[x_1,\dots,x_\ell]$ of rank r, we have $r \geq 2$ if and only if g is squarefree—in other words, if and only if $g = 0$ defines a reduced variety.

2.4 Summary of results

For this section, we suppose $k, \ell \geq 2$ and $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $\deg(h) = k$, and we let r denote the rank of h^k. We assume h is intersective, as otherwise $D(h(\mathbb{Z}^\ell), N) \gg_h N$. The following bullet points summarize the reach and limitations of our results.

- **The good:** In addition to previously known results on sums of univariate intersective polynomials (Theorems 1.2 and 5.7 of [28]), we now have that (9) holds provided h, or in the case of (iii) any translation of h, meets any of the following criteria:

  (i) $r \geq 3$ (including Deligne with $\ell \geq 3$)

  (ii) $r = k = 2$ (including Deligne with $\ell = k = 2$)

  (iii) $r = 2$ (including Deligne with $\ell = 2$), $h(\mathbf{0}) = 0$, and the lowest degree homogeneous part of h has rank at least 2. This includes as a special case bivariate homogeneous polynomials with nonzero discriminant, which is Theorem 1.2 from the introduction.

  (iv) $r = 2$ (including Deligne with $\ell = 2$) and h is smoothly intersective, the latter of which in particular holds if any irreducible (over $\mathbb{Z}$) factor of h is geometrically irreducible. Parts of this item can be made slightly more general, as seen in the hypotheses of Proposition 2.9 and Corollary 5.4.

  An interesting example of (iv) that does not fit into any other category is $h(x,y) = x^3 + y^3 - q$, where q is a prime congruent to 1 modulo 90090 that is not expressable as the sum of two integer cubes, of which there are plenty. This polynomial has no rational root, and it cannot be decomposed into a sum of two univariate intersective polynomials, but it is Deligne and it has simple roots in $\mathbb{Z}_p^2$ for all primes p. This example was discussed in a remark following Theorem 1.2 in [28] to illustrate a limitation of that result.

- **The bad:** The methods utilized here fail to improve on univariate results in the case that $r = 1$, or equivalently the case that h^k has a repeated factor. It should be noted that we can only definitively say that it is impossible to reach beyond the cutting edge of the univariate setting if $h = f \circ g$ for some $g \in \mathbb{Z}[x_1, \dots, x_\ell]$ and $f \in \mathbb{Z}[x]$ with $\deg(f) \geq 2$, because in this case $h(\mathbb{Z}^\ell) \subseteq f(\mathbb{Z})$. This was hinted at in the introduction with the example $h(x,y) = (x+y)^2$. In this situation, h^k is a proper power of the highest-degree part of g, so we definitely have $r = 1$. While it is certainly possible to have $r = 1$ without h being given as a composition of this sort, our current methods cannot distinguish between the two.

- **The ugly:** A more subtle remaining hurdle is the case where $r = 2$ (including Deligne with $\ell = 2$), $k \geq 3$, and h does not meet either of the criteria described in items (iii) or (iv). Focusing on the $\ell = 2$ Deligne case, such a polynomial must satisfy $\Delta(h^k) \neq 0$, must be intersective and hence have roots in $\mathbb{Z}_p^2$ for all primes p, but by Proposition 2.8, for infinitely many p, all roots in $\mathbb{Z}_p^2$ must satisfy $2 \leq m_p \leq k-1$. In particular, by Proposition 2.9, at least one coefficient in every geometrically irreducible factor of h must fail to be an integer. Finally, by Corollary 2.6, if h satisfies $h(0,0) = 0$, then the lowest degree part of h must have discriminant 0.

One example is

$$h(x,y) = x^4 - 2y^4 + 2x^2(x+y) + (x+y)^2 = \left(x^2 - \sqrt{2}y^2 + (x+y)\right)\left(x^2 + \sqrt{2}y^2 + (x+y)\right).$$

For any prime p such that 2 is not a square in $\mathbb{Q}_p$, the only $\mathbb{Q}_p$ roots of h are $(0,0)$ and $(-1,0)$. With these choices for $\boldsymbol{z}_p$, the highest degree nonvanishing part of h_p modulo p is either $(x+y)^2$ or $(x-y)^2$, respectively. In both cases $\Delta(h_p^2) = 0$, and hence h_p is not Deligne at this infinite collection of primes. In other words, h is not strongly Deligne, and we cannot claim that (9) holds.

- **The future:** The issue in the previous bullet point may represent an avoidable artifact of the method, in which case the upper bound (9) could be shown to hold for all intersective polynomials satisfying $r \geq 2$. Regarding improved bounds, as noted in Section 2.3 of [31], and as implicitly referenced in [32] when noting that the exponent μ in (3) could be increased to $1/2$ conditioned on the Generalized Riemann Hypothesis, an upper bound of order $Ne^{-c\sqrt{\log N}}$ appears to be the limit of a Fourier analytic L^2 density increment. More specifically, if $(\delta, N) \mapsto (\delta', N')$ represents the change in density and interval size at each step of the iteration, then any further improvement would require either N'/N to decay more slowly than any power of δ, or δ'/δ to tend to infinity, as $\delta \to 0$, both of which appear incompatible with the method. To be clear, this is not at all to say that much stronger upper bounds do not hold, even in the univariate polynomial setting. As discussed in Section 1.3, this question is rather murky. However, to achieve such a goal would likely require a fundamentally different proof strategy.

3 Preliminaries

In this section we make some preliminary definitions and observations required to execute the sieve-powered L^2 density increment strategy utilized to prove Theorem 2.4.

3.1 Fourier analysis and the circle method on $\mathbb{Z}$

We embed our finite sets in $\mathbb{Z}$, on which we utilize an unnormalized discrete Fourier transform. Specifically, for a function $F : \mathbb{Z} \to \mathbb{C}$ with finite support, we define $\widehat{F} : \mathbb{T} \to \mathbb{C}$, where $\mathbb{T}$ denotes the circle parameterized by the interval $[0,1]$ with 0 and 1 identified, by

$$\widehat{F}(\alpha) = \sum_{x \in \mathbb{Z}} F(x) e^{-2\pi i x \alpha}.$$

Given $N \in \mathbb{N}$ and a set $A \subseteq [1,N]$ with $|A| = \delta N$, we examine the Fourier analytic behavior of A by considering the *balanced function*, f_A, defined by $f_A = 1_A - \delta 1_{[1,N]}$.

As is standard, we decompose the frequency space into two pieces: the points of $\mathbb{T}$ that are close to rational numbers with small denominator, and the complement.

Definition 3.1. Given $\gamma > 0$ and $Q \geq 1$, we define, for each $a, q \in \mathbb{N}$ with $0 \leq a \leq q-1$,

$$\mathbf{M}_{a/q}(\gamma) = \left\{\alpha \in \mathbb{T} : \left|\alpha - \frac{a}{q}\right| < \gamma\right\}, \ \mathbf{M}_q(\gamma) = \bigcup_{(a,q)=1} \mathbf{M}_{a/q}(\gamma), \text{ and } \mathbf{M}'_q(\gamma) = \bigcup_{r|q} \mathbf{M}_r(\gamma) = \bigcup_{a=0}^{q-1} \mathbf{M}_{a/q}(\gamma).$$

We then define the *major arcs* by

$$\mathfrak{M}(\gamma, Q) = \bigcup_{q=1}^{Q} \mathbf{M}_q(\gamma),$$

and the *minor arcs* by $\mathfrak{m}(\gamma, Q) = \mathbb{T} \setminus \mathfrak{M}(\gamma, Q)$. We note that if $2\gamma Q^2 < 1$, then

$$\mathbf{M}_{a/q}(\gamma) \cap \mathbf{M}_{b/r}(\gamma) = \emptyset \tag{10}$$

whenever $a/q \neq b/r$ and $q, r \leq Q$.

3.2 Inheritance proposition

As previously noted, we defined auxiliary polynomials to keep track of an inherited lack of prescribed differences at each step of a density increment iteration. The following proposition makes this inheritance precise.

Proposition 3.2. *Suppose $\ell \in \mathbb{N}$, $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ is intersective, $d, q \in \mathbb{N}$, and $A \subseteq \mathbb{N}$.*
If $(A-A) \cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$ and $A' \subseteq \{a : x + \lambda(q)a \in A\}$ for some $x \in \mathbb{Z}$, then $(A'-A') \cap h_{qd}(\mathbb{Z}^\ell) \subseteq \{0\}$.

Proof. Suppose that $A \subseteq \mathbb{N}$, $A' \subseteq \{a : x + \lambda(q)a \in A\}$, and

$$a - a' = h_{qd}(\boldsymbol{n}) = h(\boldsymbol{r}_{qd} + qd\boldsymbol{n})/\lambda(qd) \neq 0$$

for some $\boldsymbol{n} \in \mathbb{Z}^\ell$, $a, a' \in A'$. By construction we have that $\boldsymbol{r}_{qd} \equiv \boldsymbol{r}_d \bmod d$, so there exists $\boldsymbol{s} \in \mathbb{Z}^\ell$ such that $\boldsymbol{r}_{qd} = \boldsymbol{r}_d + d\boldsymbol{s}$. Further, λ is completely multiplicative, and therefore

$$0 \neq h_d(\boldsymbol{s} + q\boldsymbol{n}) = h(\boldsymbol{r}_d + d(\boldsymbol{s} + q\boldsymbol{n}))/\lambda(d) = \lambda(q)h_{qd}(\boldsymbol{n}) = \lambda(q)a - \lambda(q)a' \in A - A.$$

Since $a - a' \neq 0$, we have $(A-A) \cap h_d(\mathbb{Z}^\ell) \not\subseteq \{0\}$, and the contrapositive is established. □

3.3 Sieve definitions and observations

As in [28], we apply a polynomial-specific sieve to our set of considered inputs in order to, roughly speaking, reduce our analysis of local exponential averages to the case of prime moduli, which in the multivariate setting allows for the application of Theorem 1.4. To this end, for $\ell \in \mathbb{N}$, an intersective polynomial $h \in \mathbb{Z}[x_1, \dots, x_\ell]$, and each prime p and $d \in \mathbb{N}$, we define $\gamma_d(p)$ to be the smallest power such

that ∇h_d modulo $p^{\gamma_d(p)}$ does not vanish identically *as a function on* $(\mathbb{Z}/p^{\gamma_d(p)}\mathbb{Z})^\ell$, and we let $j_d(p)$ denote the number of solutions to $\nabla h_d = \mathbf{0}$ in $(\mathbb{Z}/p^{\gamma_d(p)}\mathbb{Z})^\ell$. Then, for $d \in \mathbb{N}$ and $Y > 0$ we define

$$W_d(Y) = \left\{ \boldsymbol{n} \in \mathbb{N}^\ell : \nabla h_d(\boldsymbol{n}) \not\equiv \mathbf{0} \bmod p^{\gamma_d(p)} \text{ for all } p \le Y \right\}.$$

In the absence of a subscript d in the usage of $\gamma(p), j(p)$, and $W(Y)$, we assume $d = 1$, in which case the definitions make sense even for non-intersective polynomials. Further, for any $g \in \mathbb{Z}[x_1,\dots,x_\ell]$ and $q \in \mathbb{N}$, we define

$$W^q(Y) = \left\{ \boldsymbol{n} \in \mathbb{N}^\ell : \nabla g(\boldsymbol{n}) \not\equiv \mathbf{0} \bmod p^{\gamma(p)} \text{ for all } p \le Y,\ p^{\gamma(p)} \mid q \right\}.$$

Unlike in the univariate case, the size of $W(Y)$ here can be estimated with a straightforward application of the inclusion-exclusion principle, as opposed to a Brun sieve truncation thereof (see Proposition 2.4 in [28]). To achieve this goal, however, we must first look forward and invoke an estimate established in Section 7.1. For the following two statements, we assume $\ell \ge 2$ and $g \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(g) = k \ge 1$.

Lemma 3.3. *If p is prime and g is Deligne modulo p, then $j(p) \ll_{k,\ell} 1$.*

Proposition 3.4. *For any $x_1,\dots,x_\ell, Y > 0$ we have*

$$|B \cap W(Y)| = x_1 x_2 \cdots x_\ell \prod_{p \le Y} \left(1 - \frac{j(p)}{p^{\gamma(p)\ell}}\right) + E, \tag{11}$$

where $B = [1,x_1] \times \cdots \times [1,x_\ell]$,

$$E = \begin{cases} O(X^{\ell-1}\log^C(Y)) & \text{if } \ell = 2 \\ O(X^{\ell-1}) & \text{if } \ell \ge 3 \end{cases},$$

$X = \max\{x_1,\dots,x_\ell\}$, $C = C(k,\ell)$, and the implied constants depend only on k, ℓ, the moduli at which ∇g identically vanishes, and the primes $p \le Y$ modulo which g is not Deligne.

Proof. Fix $x_1,\dots,x_\ell, Y > 0$ and let $X = \max\{x_1,\dots,x_\ell\}$. For primes $p_1 < p_2 < \cdots < p_s$, we let

$$\mathcal{A}_{p_1\cdots p_s} = \mathcal{A}_{p_1\cdots p_s}(x_1,\dots,x_\ell) = \left| \left\{ \boldsymbol{n} \in B : \nabla g(\boldsymbol{n}) \equiv \mathbf{0} \bmod p_i^{\gamma(p_i)} \text{ for all } 1 \le i \le s \right\} \right|.$$

Fixing $Y > 0$ and letting r denote the number of primes that are at most Y, we have by the Chinese Remainder Theorem and the inclusion-exclusion principle that

$$|B \cap W(Y)| = \sum_{s=0}^{r} (-1)^s \sum_{p_1 < \cdots < p_s \le Y} \mathcal{A}_{p_1\cdots p_s}. \tag{12}$$

Further,

$$\mathcal{A}_p = \frac{j(p)}{p^{\gamma(p)\ell}} x_1 \cdots x_\ell + R_p, \tag{13}$$

where $|R_p| \ll_\ell j(p)(X/p^{\gamma(p)})^{\ell-1}$. We trivially have $j(p) \le p^{\gamma(p)\ell}$, while if g is Deligne modulo p, then $\gamma(p) = 1$ and, by Lemma 3.3, $j(p) \le C = C(k,\ell)$. In particular, we can apply the Chinese Remainder Theorem again and extend (13) to

$$\mathcal{A}_{p_1\cdots p_s} = x_1\cdots x_\ell \prod_{i=1}^{s} \frac{j(p_i)}{p_i^{\gamma(p_i)\ell}} + R_{p_1\cdots p_s}, \tag{14}$$

where $|R_{p_1\cdots p_s}| \le KC^s(X/p_1\cdots p_s)^{\ell-1}$, where K depends only on the moduli at which ∇g identically vanishes and the primes $p \le Y$ modulo which g is not Deligne. Now, by (12) and (14) we have

$$\begin{aligned}
|B \cap W(Y)| &= \sum_{s=0}^{r} (-1)^s \sum_{p_1<\cdots<p_s\le Y} \mathcal{A}_{p_1\cdots p_s} \\
&= \sum_{s=0}^{r} (-1)^s \sum_{p_1<\cdots<p_s\le Y} \left(x_1\cdots x_\ell \prod_{i=1}^{s} \frac{j(p_i)}{p_i^{\gamma(p_i)\ell}} + R_{p_1\cdots p_s} \right) \\
&= x_1x_2\cdots x_\ell \prod_{p\le Y} \left(1 - \frac{j(p)}{p^{\gamma(p)\ell}}\right) + E,
\end{aligned}$$

where

$$|E| \le KX^{\ell-1} \sum_{s=0}^{r} \sum_{p_1<\cdots<p_s\le Y} \frac{C^s}{(p_1\cdots p_s)^{\ell-1}} = KX^{\ell-1} \prod_{p\le Y} \left(1 + \frac{C}{p^{\ell-1}}\right),$$

and the estimate follows. □

3.4 Control over gradient vanishing: Part I

A potential hazard of the density increment method is the possibility that, as d grows, ∇h_d could identically vanish at a larger and larger collection of moduli. This section is dedicated to establishing that, for strongly Deligne polynomials, this does not occur. We begin by noting that the collection of moduli at which a polynomial identically vanishes is firmly controlled in terms of its degree and the gcd of its coefficients. Throughout this section we assume $k, \ell \in \mathbb{N}$.

Definition 3.5. We define a *multi-index* to be an ℓ-tuple $\boldsymbol{i} = (i_1, \dots, i_\ell)$ of nonnegative integers. We let $|\boldsymbol{i}| = i_1 + \cdots + i_\ell$, we let $\boldsymbol{i}! = i_1! \cdots i_\ell!$, and for $\boldsymbol{x} = (x_1, \dots, x_\ell)$, we let $\boldsymbol{x}^{\boldsymbol{i}} = x_1^{i_1} \cdots x_\ell^{i_\ell}$. Finally, for a polynomial $g(\boldsymbol{x})$, we let $\partial^{\boldsymbol{i}} g = \frac{\partial^{|\boldsymbol{i}|} g}{\partial x_1^{i_1} \cdots \partial x_\ell^{i_\ell}}$.

Proposition 3.6. *If $g(\boldsymbol{x}) = \sum_{|\boldsymbol{i}|\le k} a_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{Z}[x_1, \dots, x_\ell]$ is identically zero modulo $q \in \mathbb{N}$, then*

$$q \mid k! \gcd(\{a_{\boldsymbol{i}}\}).$$

Proof. We first note that g is identically zero as a function on $\mathbb{Z}/q\mathbb{Z}$ if and only if the polynomial g/q is integer-valued. In this case, since products of binomial coefficients

$$\binom{\boldsymbol{x}}{\boldsymbol{i}} = \binom{x_1}{i_1} \cdots \binom{x_\ell}{i_\ell} = \frac{x(x-1)\dots(x-i_1+1)}{i_1!} \cdots \frac{x(x-1)\dots(x-i_\ell+1)}{i_\ell!}$$

form a $\mathbb{Z}$-basis for integer-valued polynomials in $\mathbb{Q}[x_1,\dots,x_\ell]$, we can write $g(x)=\sum_{|\boldsymbol{i}|\le k} q b_{\boldsymbol{i}}\binom{\boldsymbol{x}}{\boldsymbol{i}}$ for $b_{\boldsymbol{i}}\in\mathbb{Z}$. In particular, by clearing denominators we see that the coefficients of $k!g$ are all divisible by q, and the proposition follows. □

Further, we note that the gcd of the coefficients of each partial derivative of a polynomial $h\in\mathbb{Z}[x_1,\dots,x_\ell]$ divides $k!$ times the gcd of the nonconstant coefficients of h. With this in mind, the following definition and proposition complete the task at hand.

Definition 3.7. For $h(\boldsymbol{x})=\sum_{|\boldsymbol{i}|\le k} a_{\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}\in\mathbb{Z}[x_1,\dots,x_\ell]$, we define

$$\operatorname{cont}(h)=\gcd(\{a_{\boldsymbol{i}} : |\boldsymbol{i}|>0\}).$$

We note that our use of $\operatorname{cont}(h)$ does not precisely align with the standard notion of the *content* of a polynomial, as we exclude the constant coefficient.

Proposition 3.8. *If $h\in\mathbb{Z}[x_1,\dots,x_\ell]$ is a strongly Deligne polynomial of degree k, then*

$$\operatorname{cont}(h_d)\ll_h 1.$$

Proof. Suppose $d\in\mathbb{N}$ and $h\in\mathbb{Z}[x_1,\dots,x_\ell]$ is a strongly Deligne polynomial of degree k. Let $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ and X denote the choice of p-adic integer roots and the finite set of primes, respectively, guaranteed by the strongly Deligne condition. In particular, h_d is Deligne modulo p for all $p\notin X$. Because constant polynomials are not Deligne, $\operatorname{cont}(h_d)$ can only be divisible by primes in X.

Recalling that $h_d(\boldsymbol{x})=h(\boldsymbol{r}_d+d\boldsymbol{x})/\lambda(d)$, we make the trivial note that for any multi-index $\boldsymbol{i}$ with $|\boldsymbol{i}|=k$, the $\boldsymbol{x}^{\boldsymbol{i}}$ coefficient of h_d is precisely $d^k/\lambda(d)$ times the corresponding coefficient $a_{\boldsymbol{i}}$ of h. In particular,

$$\operatorname{cont}(h_d)\mid \frac{d^k}{\lambda(d)}a_{\boldsymbol{i}} \text{ whenever } |\boldsymbol{i}|=k. \tag{15}$$

Now fix $p\in X$. By definition of the multiplicity m_p, there exists a multi-index $\boldsymbol{i}$ with $|\boldsymbol{i}|=m_p$ and $\partial^{\boldsymbol{i}}h(\boldsymbol{z}_p)\neq 0$, so in particular $\partial^{\boldsymbol{i}}h(\boldsymbol{z}_p)$ has some finite p-adic valuation $v_1(p)$.

If $p^{v_1(p)+1}\nmid d$, then by (15), we have that $p^{kv_1(p)+v_2(p)+1}\nmid\operatorname{cont}(h_d)$, where $v_2(p)$ is the minimum p-adic valuation amongst the degree-k coefficients of h. Now suppose that $p^{v_1(p)+1}\mid d$.

Let $b_{\boldsymbol{i}}$ denote the $\boldsymbol{x}^{\boldsymbol{i}}$ coefficient of h_d. By Taylor's formula, we have that

$$b_{\boldsymbol{i}}=\frac{d^{m_p}}{\lambda(d)}\frac{\partial^{\boldsymbol{i}}h(\boldsymbol{r}_d)}{\boldsymbol{i}!}.$$

By definition of λ we have $p\nmid(d^{m_p}/\lambda(d))$, and since $\boldsymbol{r}_d\equiv\boldsymbol{z}_p \bmod p^{v_1(p)+1}$ and $p^{v_1(p)+1}\nmid\partial^{\boldsymbol{i}}h(\boldsymbol{z}_p)$, we have that $p^{v_1(p)+1}\nmid b_{\boldsymbol{i}}$. In either case, we have that $p^{kv_1(p)+v_2(p)+1}\nmid\operatorname{cont}(h_d)$, and hence

$$\operatorname{cont}(h_d)\le\prod_{p\in X}p^{kv_1(p)+v_2(p)+1}\ll_h 1,$$

as required. □

For strongly Deligne $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(h) = k$, we have now established control over not only the error term in the size of $W_d(Y)$, but also the main term, since Lemma 3.3, Proposition 3.6, and Proposition 3.8 give

$$\prod_{p\le Y}\left(1-\frac{j_d(p)}{p^{\gamma_d(p)\ell}}\right) \gg_h \prod_{C=C(h)\le p\le Y}\left(1-\frac{C}{p^\ell}\right) \gg_h 1 \tag{16}$$

for all $d \in \mathbb{N}$ and $Y \ge 2$.

3.5 Summary of new exponential sum estimates

In Section 7, we combine new and old techniques to establish the sieved multivariate exponential sum estimates necessary to prove Theorem 2.4. These estimates are obtained through a sequence of lemmas presented in the context of the larger proof, so we separately present a summary here in case the estimates are of independent interest to the reader.

For the following theorem, a multivariate generalization of Theorem 2.7 in [28], we utilize all the sieve-related notation and definitions from Section 3.3. Further, we use τ and ω to denote the divisor and distinct prime divisor counting functions, respectively, as well as ϕ to denote the Euler totient function.

Theorem 3.9. *For $k,\ell \ge 2$, $g(\boldsymbol{x}) = \sum_{|\boldsymbol{i}|\le k} a_{\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{Z}[x_1,\dots,x_\ell]$, $J = \sum_{|\boldsymbol{i}|\le k}|a_{\boldsymbol{i}}|$, and $a,q \in \mathbb{N}$, the following estimates hold:*

(i) **Major arc estimate:** *If $X,Y > 0$ and $\alpha = a/q+\beta$, then*

$$\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)} e^{2\pi i g(\boldsymbol{n})\alpha} = q^{-\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)} e^{2\pi i g(\boldsymbol{s})a/q}\int_{[0,X]^\ell} e^{2\pi i g(\boldsymbol{x})\beta}\,d\boldsymbol{x}$$

$$+ O_{k,\ell}\left(qE(1+JX^k|\beta|)^\ell\right),$$

where E is as in Proposition 3.4.

(ii) **Local cancellation:** *If $(a,q) = 1$ and $Y > 0$, then*

$$\left|\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)} e^{2\pi i g(\boldsymbol{s})a/q}\right| \le C_1\begin{cases}(k-1)^{\ell\omega(q)}\Phi(q,\ell)q^{\ell/2} & \text{if } q\le Y\\ C_2^{\omega(q)}\tau(q)^\ell q^{\ell-1/k} & \text{for all } q\end{cases},$$

where $C_2 = C_2(k)$, $\Phi(q,2) = (q/\phi(q))^{C_2}$, $\Phi(q,\ell) \ll_{k,\ell} 1$ for $\ell \ge 3$, and C_1 depends only on the moduli at which ∇g identically vanishes and the primes $p \le Y$ dividing q modulo which g is not Deligne.

(iii) **Minor arc estimate:** *If $X,Y,Z \ge 2$, $YZ \le X$, $(a,q) = 1$, and $|\alpha - a/q| < q^{-2}$, then*

$$\left|\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)} e^{2\pi i g(\boldsymbol{n})\alpha}\right| \ll_{k,\ell} \mathrm{cont}(g)^6(\log Y)^{ek}X^\ell\left(e^{-\frac{\log Z}{\log Y}} + \left(J\log^{k^2}(JqX)\left(q^{-1}+\frac{Z}{X}+\frac{qZ^k}{X^k}\right)\right)^{2^{-k}}\right).$$

4 Proof of Theorem 2.4

In this section, we exploit the estimates enumerated in Theorem 3.9 and apply a Fourier analytic L^2 density increment, essentially an improved, streamlined version of Sárközy's [35] original method, in order to prove Theorem 2.4. The core of this method has been utilized in [23], [22], [32], and [30], among others. Most specifically, this section very closely follows Section 5 of [28].

4.1 Main iteration lemma and proof of Theorem 2.4

For the remainder of Section 4 we fix $k,\ell \geq 2$, a strongly Deligne polynomial $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(h) = k$, and positive constants $C_0 = C_0(h)$ and $c_0 = c_0(h)$ that are appropriately large and small, respectively. For $N \in \mathbb{N}$ we let

$$\Omega = \Omega(N,h) = e^{c_0\sqrt{\log N}}.$$

For a density $\delta \in (0,1]$, we define $\theta(k,\ell,\delta)$ by $\theta(k,\ell,\delta) = 1$ if $\ell \geq 3$ and $\theta(k,2,\delta) = \log^{-k(k-2)}((c_0\delta)^{-1})$.

We deduce Theorem 2.4 from the following iteration lemma, which makes precise the aforementioned passage from a set lacking nonzero differences in the image of a polynomial to a new, denser subset of a slightly smaller interval lacking nonzero differences in the image of an appropriate auxiliary polynomial.

Lemma 4.1. *Suppose $A \subseteq [1,N]$ with $|A| = \delta N$. If $(A-A)\cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$, $C_0, \delta^{-1} \leq \Omega$, and $d \leq N^{c_0}$, then there exists $q \ll_h \delta^{-2}$ and $A' \subseteq [1,N']$ such that $N' \gg_h \delta^{4k}N$,*

$$|A'| \geq (1 + c\theta(k,\ell,\delta))\delta N',$$

where $c = c(h) > 0$, and

$$(A'-A')\cap h_{qd}(\mathbb{Z}^\ell) \subseteq \{0\}.$$

Proof of Theorem 2.4. Throughout this proof, we let C and c denote sufficiently large or small positive constants, respectively, which we allow to change from line to line, but which depend only on h.

Suppose $A \subseteq [1,N]$ with $|A| = \delta N$ and

$$(A-A)\cap h(\mathbb{Z}^\ell) \subseteq \{0\}.$$

Setting $A_0 = A$, $N_0 = N$, $d_0 = 1$, and $\delta_0 = \delta$, Lemma 4.1 yields, for each m, a set $A_m \subseteq [1,N_m]$ with $|A_m| = \delta_m N_m$ and $(A_m - A_m)\cap h_{d_m}(\mathbb{Z}^\ell) \subseteq \{0\}$. Further, we have that

$$N_m \geq c\delta^{4k}N_{m-1} \geq (c\delta)^{4km}N, \tag{17}$$

$$\delta_m \geq (1 + c\theta(k,\ell,\delta))\delta_{m-1}, \tag{18}$$

and

$$d_m \leq (c\delta)^{-2}d_{m-1} \leq (c\delta)^{-2m}, \tag{19}$$

as long as

$$C, \delta_m^{-1} \le e^{c\sqrt{\log N_m}}, \quad d \le N_m^c. \tag{20}$$

By (18), the density δ_m will exceed 1, and hence (20) must fail, for $m = M = M(h,\delta)$, where

$$M(h,\delta) = \begin{cases} C\log(C\delta^{-1}) & \text{if } \ell \ge 3 \\ C\log^{(k-1)^2}(C\delta^{-1}) & \text{if } \ell = 2 \end{cases}.$$

However, by (17), (18), and (19), (20) holds for $m = M$ if

$$(c\delta)^{4kM} = e^{C\log^{\mu(k,\ell)^{-1}}(C\delta^{-1})} \le N^c. \tag{21}$$

Therefore, (21) must fail, or in other words $\delta \ll_h e^{-c(\log N)^{\mu(k,\ell)}}$, as claimed. □

4.2 L^2 Fourier concentration and proof of Lemma 4.1

The philosophy behind the proof of Lemma 4.1 is that the condition $(A-A)\cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$ represents highly nonrandom behavior, which should be detectable in the Fourier analytic behavior of A. Specifically, we locate one small denominator q such that $\widehat{f_A}$ has L^2 concentration around rationals with denominator q, then invoke a standard lemma stating that L^2 concentration of $\widehat{f_A}$ implies the existence a long arithmetic progression on which A has increased density.

Lemma 4.2. *Suppose $A \subseteq [1,N]$ with $|A| = \delta N$, $\eta = c_0\delta$, and $\gamma = \eta^{-2k}/N$. If $(A-A)\cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$, $C_0, \delta^{-1} \le \Omega$, $d \le N^{c_0}$, and $|A \cap (N/9, 8N/9)| \ge 3\delta N/4$, then there exists $q \le \eta^{-2}$ such that*

$$\int_{\mathbf{M}_q'(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \gg_h \theta(k,\ell,\delta)\delta^2 N.$$

Lemma 4.1 follows from Lemma 4.2 and the following standard L^2 density increment lemma.

Lemma 4.3 (Lemma 2.3 in [29], see also [23], [32])**.** *Suppose $A \subseteq [1,N]$ with $|A| = \delta N$. If $0 < \theta \le 1$, $q \in \mathbb{N}$, $\gamma > 0$, and*

$$\int_{\mathbf{M}_q'(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \ge \theta\delta^2 N,$$

then there exists an arithmetic progression

$$P = \{x + \ell q : 1 \le \ell \le L\}$$

with $qL \gg \min\{\theta N, \gamma^{-1}\}$ and $|A \cap P| \ge (1+\theta/32)\delta L$.

Proof of Lemma 4.1. Suppose $A \subseteq [1,N]$, $|A| = \delta N$, $(A-A)\cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$, $C_0, \delta^{-1} \le \Omega$, and $d \le N^{c_0}$. If $|A \cap (N/9, 8N/9)| < 3\delta N/4$, then $\max\{|A\cap[1,N/9]|, |A\cap[8N/9,N]|\} > \delta N/8$. In other words, A has density at least $9\delta/8$ on one of these intervals.

Otherwise, Lemmas 4.2 and 4.3 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \le \eta^{-2}$ and an arithmetic progression

$$P = \{x + \ell q : 1 \le \ell \le L\}$$

with $qL \gg_h \delta^{2k}N$ and

$$|A \cap P| \ge (1 + c\theta(k,\ell,\delta))\delta L.$$

Partitioning P into subprogressions of step size $\lambda(q)$, the pigeonhole principle yields a progression

$$P' = \{y + a\lambda(q) : 1 \le a \le N'\} \subseteq P$$

with $N' \ge qL/2\lambda(q)$ and $|A \cap P'|/N' \ge |A \cap P|/L$. This allows us to define a set $A' \subseteq [1,N']$ by

$$A' = \{a \in [1,N'] : y + a\lambda(q) \in A\},$$

which satisfies $|A'| = |A \cap P'|$ and $N' \gg_h \delta^{2k}N/\lambda(q) \gg_h \delta^{4k}N$. Moreover, $(A-A) \cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$ implies $(A'-A') \cap h_{qd}(\mathbb{Z}^\ell) \subseteq \{0\}$ by Proposition 3.2. □

Our task for this section is now completely reduced to a proof of Lemma 4.2.

4.3 Preliminary notation for proof of Lemma 4.2

Before delving into the proof of Lemma 4.2, we take the opportunity to define some relevant sets and quantities, depending on our strongly Deligne polynomial $h \in \mathbb{Z}[x_1,\dots,x_\ell]$, scaling parameter d, a parameter $Y > 0$, and the size N of the ambient interval. In all the notation defined below, we suppress all of the aforementioned dependence, as the relevant objects will be fixed in context.

We define W_d, γ_d, and j_d in terms of h as in Section 3.3. We then let $M = \left(\frac{N}{9J}\right)^{1/k}$, where J is the sum of the absolute value of all the coefficients of h_d, and hence $h_d([1,M]^\ell) \subseteq [-N/9,N/9]$. We let

$$w = \prod_{p \le Y} \left(1 - \frac{j_d(p)}{p^{\gamma_d(p)\ell}}\right),$$

and we let $T = wM^\ell$.

We let $Z = \{\boldsymbol{n} \in \mathbb{Z}^\ell : h_d(\boldsymbol{n}) = 0\}$, and we let $H = \big([1,M]^\ell \cap W_d(Y)\big) \setminus Z$. We note that the hypothesis $\mathcal{Q} \ge C_0$ allows us to assume at any point that $\mathcal{Q}$, and hence also N, are sufficiently large with respect to h, which we take as a perpetual assumption moving forward. Under this assumption, it follows from (11), (16), and the estimate

$$|Z \cap [1,M]^\ell| \ll_h M^{\ell-1} \tag{22}$$

that

$$|H| \ge T/2. \tag{23}$$

4.4 Proof of Lemma 4.2

Suppose $A \subseteq [1,N]$ with $|A| = \delta N$, $(A-A) \cap h_d(\mathbb{Z}^\ell) \subseteq \{0\}$, $C_0, \delta^{-1} \leq Q$, and $d \leq N^{c_0}$. Further, let $\eta = c_0\delta$, let $Q = \eta^{-2}$, and let $Y = \eta^{-2k}$. Since $h_d(H) \subseteq [-N/9, N/9] \setminus \{0\}$, we have

$$\begin{aligned}\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} f_A(x)f_A(x+h_d(\boldsymbol{n})) &= \sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} 1_A(x)1_A(x+h_d(\boldsymbol{n})) - \delta\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} 1_A(x)1_{[1,N]}(x+h_d(\boldsymbol{n}))\\ &\quad - \delta\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} 1_A(x+h_d(\boldsymbol{n}))1_{[1,N]}(x) + \delta^2\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} 1_{[1,N]}(x)1_{[1,N]}(x+h_d(\boldsymbol{n}))\\ &\leq \Big(\delta^2 N - 2\delta|A\cap(N/9,8N/9)|\Big)|H|.\end{aligned}$$

Therefore, if $|A\cap(N/9,8N/9)| \geq 3\delta N/4$, then by (23) we have

$$\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} f_A(x)f_A(x+h_d(\boldsymbol{n})) \leq -\delta^2 NT/4. \tag{24}$$

We see from (22) and orthogonality of characters that

$$\sum_{\substack{x\in\mathbb{Z}\\ \boldsymbol{n}\in H}} f_A(x)f_A(x+h_d(\boldsymbol{n})) = \int_0^1 |\widehat{f_A}(\alpha)|^2 S(\alpha)\,d\alpha + O_h(NM^{\ell-1}), \tag{25}$$

where

$$S(\alpha) = \sum_{\boldsymbol{n}\in[1,M]^\ell\cap W_d(Y)} e^{2\pi i h_d(\boldsymbol{n})\alpha}.$$

Combining (24) and (25), we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S(\alpha)|\,d\alpha \geq \delta^2 NT/8. \tag{26}$$

Letting $\gamma = \eta^{-2k}/N$, Theorem 3.9 yields that for $\alpha \in \mathbf{M}_q(\gamma)$, $q \leq Q$, we have

$$|S(\alpha)| \ll_h (k-1)^{\ell\omega(q)}\Phi(q,\ell)q^{-\ell/2}T, \tag{27}$$

where $\Phi(q,2) = (q/\phi(q))^C$ for $C = C(k)$ and $\Phi(q,\ell) \ll_{k,\ell} 1$ for $\ell \geq 3$. Further, for $\alpha \in \mathfrak{m}(\gamma,Q)$ we have

$$|S(\alpha)| \leq \delta T/16. \tag{28}$$

The proof of the estimates in Theorem 3.9 and the subsequent deduction of (27) and (28) can be found in Section 7. From (28) and Plancherel's Identity, we have

$$\int_{\mathfrak{m}(\gamma,Q)} |\widehat{f_A}(\alpha)|^2 |S(\alpha)|\,d\alpha \leq \delta^2 NT/16,$$

which together with (26) yields

$$\int_{\mathfrak{M}(\gamma,Q)} |\widehat{f_A}(\alpha)|^2 |S(\alpha)|\,d\alpha \geq \delta^2 NT/16. \tag{29}$$

From (27) and (29) , we have

$$\sum_{q=1}^{Q}(k-1)^{\ell\omega(q)}\Phi(q)q^{-\ell/2}\int_{\mathbf{M}_q(\gamma)}|\widehat{f_A}(\alpha)|^2d\alpha \gg_h \delta^2 N. \tag{30}$$

For $\ell=2$, the function $b(q)=(k-1)^{2\omega(q)}(q/\phi(q))^C$ satisfies $b(qr)\geq b(r)$, and we make use of the following proposition, which is based on a trick that originated in [32].

Proposition 4.4 (Proposition 5.6, [28]). *For any $\gamma, Q>0$ satisfying $2\gamma Q^2<1$, and for any function $b:\mathbb{N}\to[0,\infty)$ satisfying $b(qr)\geq b(r)$ for all $q,r\in\mathbb{N}$, we have*

$$\max_{q\leq Q}\int_{\mathbf{M}'_q(\gamma)}|\widehat{f_A}(\alpha)|^2d\alpha \geq Q\Big(2\sum_{q=1}^{Q}b(q)\Big)^{-1}\sum_{r=1}^{Q}\frac{b(r)}{r}\int_{\mathbf{M}_r(\gamma)}|\widehat{f_A}(\alpha)|^2d\alpha.$$

Because b is a multiplicative function, $b(p^v)=(k-1)^2(1+1/(p-1))^C\ll_k 1$ for all prime powers p^v, and

$$\sum_{q=1}^{Q}\frac{b(q)}{q}\leq\prod_{p\leq Q}\left(1+\frac{b(p)}{p}+\frac{b(p)}{p^2}+\cdots\right)=\prod_{p\leq Q}\left(1+\frac{(k-1)^2}{p}+O_k(1/p^2)\right)\ll_k \log^{(k-1)^2}Q,$$

it follows from Theorem 01 of [13] that

$$\sum_{q=1}^{Q}b(q)\ll_k Q\log^{(k-1)^2-1}Q,$$

and the lemma for $\ell=2$ follows from (30) and Proposition 4.4. For $\ell\geq 3$, since $(k-1)^{\ell\omega(q)}\ll_{k,\ell,\varepsilon}q^{\varepsilon}$ for any $\varepsilon>0$, the sum $\sum_{q=1}^{\infty}(k-1)^{\ell\omega(q)}q^{-\ell/2}$ is convergent, and hence (30) immediately yields

$$\max_{q\leq Q}\int_{\mathbf{M}_q(\gamma)}|\widehat{f_A}(\alpha)|^2d\alpha \gg_h \delta^2 N.$$

Since $\mathbf{M}_q(\gamma)\subseteq\mathbf{M}'_q(\gamma)$, this establishes the lemma for $\ell\geq 3$. □

5 Criteria for strongly Deligne polynomials

In this section, we prove Proposition 2.8 and a stronger version of Proposition 2.9. We begin, though, by collecting a few facts from algebraic geometry that will be useful in subsequent sections. Throughout this section, for a variety V, we let V^{s} denote the singular locus of V, and we let $V^{\mathrm{ns}}=V\setminus V^{\mathrm{s}}$.

5.1 Results from algebraic geometry

We first state a classical version of Bézout's Theorem; see [9, Example 8.4.6].

Lemma 5.1 (Bézout's Theorem)**.** *Let $V_1, \dots, V_k$ be subvarieties of $\mathbb{P}^\ell$. Then $\deg \bigcap_{i=1}^k V_i \le \prod_{i=1}^k \deg V_i$. In particular, if the intersection is finite, then $\left|\bigcap_{i=1}^k V_i\right| \le \prod_{i=1}^k \deg V_i$.*

We now record estimates due to Lang and Weil [19] on the number of points on varieties over finite fields. The following is a well known consequence of Theorem 1 of [19] (see, for example, Theorem 5.1 of [27]), but we give the short proof for completeness.

Lemma 5.2. *Let k, ℓ, m, and r be positive integers, and let q be a prime power. Let V be a (reduced) closed subvariety of $\mathbb{P}^\ell$, defined over $\mathbb{F}_q$ (the field with q elements), of degree k and dimension r. Let $m \ge 1$ be the number of geometrically irreducible components of V which are defined over $\mathbb{F}_q$. Then*

$$|V(\mathbb{F}_q)|,\ |V^{\mathrm{ns}}(\mathbb{F}_q)| = mq^r + O_{k,\ell,r}(q^{r-1/2}). \tag{31}$$

Moreover, the same is true if we replace V with a closed subvariety $W \subseteq \mathbb{A}^\ell$.

Proof. The proof is by induction on r, noting that the case $r = 0$ is elementary, and amounts to considering the following observations.

1. If $P \in Z(\mathbb{F}_q)$ for a component $Z \subset V$ not defined over $\mathbb{F}_q$, then $P = P^\sigma \in Z^\sigma \ne Z$ for nontrivial $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, hence $P \in Z \cap Z^\sigma$, which has dimension strictly less than r. Thus, the number of points on components not defined over $\mathbb{F}_q$ is absorbed into the error term.

2. Each component of V defined over $\mathbb{F}_q$ has $q^r + O_{k,\ell,r}(q^{r-1/2})$ by Theorem 1 of [19]. Summing the number of points on each component is an overcount, but the surplus is due to points on pairwise intersections of components, which again is absorbed into the error term. (Note that $m \le k$, so even after multiplying the error by m, the implied constant still depends only on k, ℓ, and r.) Thus $|V(\mathbb{F}_q)|$ has the claimed magnitude.

3. We have $V^{\mathrm{ns}} := V \setminus V^{\mathrm{s}}$; since V^{s} has dimension at most $r-1$ and degree controlled by k, r, and ℓ (by Bézout's Theorem), the size of $V^{\mathrm{s}}(\mathbb{F}_q)$ is included in the error term. Thus, $|V^{\mathrm{ns}}(\mathbb{F}_q)|$ also has the desired magnitude.

4. Finally, if we let V be the projective closure of W, then $W = V \setminus (V \cap H)$, where H is the hyperplane at infinity. Since $V \cap H$ has lower dimension and degree k, we are once again removing a set whose cardinality is subsumed by the error term, so $W(\mathbb{F}_q)$ (and, similarly, $W^{\mathrm{ns}}(\mathbb{F}_q)$) has the appropriate cardinality. □

5.2 A key equivalence

The following equivalence observation yields a strengthening of Proposition 2.9 as a corollary, and is also instrumental in subsequent proofs.

Lemma 5.3. *Let V be a variety (reduced, but not necessarily irreducible) of dimension $d \geq 1$ defined over $\mathbb{Z}$. For a sufficiently large (with respect to V) prime p, the following are equivalent:*

(a) $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$.

(b) $V^{\mathrm{ns}}(\mathbb{Z}_p) \neq \emptyset$.

(c) At least one of the geometric components of V is defined over $\mathbb{Z}_p$.

Proof.

((a) $\implies$ (b)) Suppose $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$, and let $Q \in V^{\mathrm{ns}}(\mathbb{F}_p)$. By Hensel's lemma, there exists $P \in V(\mathbb{Z}_p)$ such that $\widetilde{P} = Q$. Since $\widetilde{P}$ is nonsingular, so must be P.

((b) $\implies$ (c)) Let $P \in V^{\mathrm{ns}}(\mathbb{Z}_p)$, and let Z be a geometric component of V containing P. As in part 1 of the proof of Lemma 5.2, if Z were not defined over $\mathbb{F}_q$, then P would lie in the intersection of two components, hence would be a singular point on V, contradicting our assumption on P.

((c) $\implies$ (a)) Let $Z_1, \dots, Z_m$ be the irreducible components of V. By Lemma 5.2, for each $1 \leq i \leq m$ there exists a bound B_i such that for all $p \geq B_i$ with Z_i defined over $\mathbb{Z}_p$, $Z_i^{\mathrm{ns}}(\mathbb{F}_p)$ contains a point that does not lie on Z_j for any $j \neq i$. Letting $B = \max\{B_1, \dots, B_m\}$, we have that for $p \geq B$, the existence of Z_i defined over $\mathbb{Z}_p$ implies the existence of $Q \in Z_i^{\mathrm{ns}}(\mathbb{F}_p) \setminus \bigcup_{j \neq i} Z_j(\mathbb{F}_p)$. Since Q is nonsingular on Z_i and is not a point of intersection with any other component Z_j, we have $Q \in V^{\mathrm{ns}}(\mathbb{F}_p)$. □

As previously noted, if $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ is Deligne, then $h = 0$ defines a reduced variety. Further, a nonsingular point over $\mathbb{Z}_p$ on this variety corresponds precisely to a root $\boldsymbol{z}_p \in \mathbb{Z}_p^\ell$ of h satisfying $m_p = 1$, hence Lemma 5.3 establishes the following sufficient condition for smooth intersectivity. Here we let $\overline{\mathbb{Z}}$ denote the ring of algebraic integers.

Corollary 5.4. *Suppose $\ell \geq 2$ and $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ is Deligne and intersective, and let $h = g_1 \cdots g_n$ be an irreducible factorization of h in $\overline{\mathbb{Z}}[x_1, \dots, x_\ell]$. If, for all but finitely many $p \in \mathcal{P}$, g_i has coefficients in $\mathbb{Z}_p$ for some $1 \leq i \leq n$, then h is smoothly intersective, hence strongly Deligne.*

Note that Proposition 2.9 is an immediate consequence of Corollary 5.4, since the hypotheses of the proposition imply that one of the factors over $\overline{\mathbb{Z}}$ is defined over $\mathbb{Z}$, hence over $\mathbb{Z}_p$ for all p. We now complete this section by using Lemma 5.3 to prove Proposition 2.8.

Proof of Proposition 2.8. Let $\ell \geq 2$, and suppose $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ is Deligne and intersective with $\deg(h) = k \geq 2$. Let $\{\boldsymbol{z}_p\}_{p \in \mathcal{P}}$ be a choice of p-adic integer roots of h satisfying $m_p \in \{1, k\}$ for all but finitely many p. Let X denote the finite set of primes such that

- $m_p \notin \{1, k\}$, or
- $p \mid k$, or
- h^k is not smooth modulo p, or
- the equivalence in Lemma 5.3 fails.

We note that the first item is assumed to be finite, the second item is clearly finite, the fourth item is proven to be finite in Lemma 5.3, and the third item is finite because h is Deligne (see Definition 2.3).

Fix $d \in \mathbb{N}$ and $p \notin X$. If $p \nmid d$ or $m_p = k$, then $p \nmid \frac{d^k}{\lambda(d)}$, so $h_d^k = \frac{d^k}{\lambda(d)} h^k$ is a nonzero scalar multiple of h^k, hence remains smooth modulo p. Therefore, h_d is Deligne modulo p.

The remaining case is $p \mid d$ and $m_p = 1$. In this case, since h_d^i has a factor of $\frac{d^i}{\lambda(d)}$, the definition of λ assures that the polynomial h_d^i identically vanishes modulo p for all $i > 1$. Since nonzero homogeneous linear polynomials are automatically smooth, we need only argue that

$$h_d^1(\boldsymbol{x}) = \frac{d}{\lambda(d)} \sum_{i=1}^{\ell} \frac{\partial h}{\partial x_i}(\boldsymbol{r}_d) x^i$$

does not identically vanish modulo p. We know that $p \nmid \frac{d}{\lambda(d)}$ by definition of λ. Further, the fact that h is Deligne ensures that $h = 0$ defines a reduced variety, so by Lemma 5.3, we can choose $\boldsymbol{z}_p$ to reduce to a nonsingular point over $\mathbb{F}_p$. Since $\boldsymbol{r}_d \equiv \boldsymbol{z}_p \pmod{p}$, we have that $\frac{\partial h}{\partial x_i}(\boldsymbol{r}_d) \equiv \frac{\partial h}{\partial x_i}(\boldsymbol{z}_p) \not\equiv 0 \pmod{p}$ for some $1 \le i \le \ell$, as required. Therefore, h_d is Deligne modulo p for all $p \notin X$, hence h is strongly Deligne. □

6 Dimension lowering argument

In this section, we generalize the phenomenon exemplified at the beginning of Section 2.3, establishing Theorems 2.12 and 2.13 by reducing to the case covered in Theorem 2.4. In the integer root setting, this reduction is very direct, as Theorem 2.12 follows immediately from Theorem 2.4 and the following proposition.

Proposition 6.1. *Suppose $\ell \ge 2$ and $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $h(\mathbf{0}) = 0$. Let r be the minimum rank of the highest and lowest degree homogeneous parts of h. If $r \ge 2$, then there exists a strongly Deligne polynomial $g \in \mathbb{Z}[x_1, \dots, x_r]$ such that $g(\mathbb{Z}^r) \subseteq h(\mathbb{Z}^\ell)$.*

Before delving into the proof of this proposition, we state a version of Bertini's theorem that will allow us to eliminate the singularity in the top-degree parts of our polynomials, one dimension at a time. Throughout this section we let $(\mathbb{P}^n)^*$ denote the dual space of $\mathbb{P}^n$, that is, the space of hyperplanes in $\mathbb{P}^n$. Note that $(\mathbb{P}^n)^*$ is isomorphic to $\mathbb{P}^n$, with the hyperplane $\{a_0 x_0 + \cdots + a_n x_n = 0\} \in (\mathbb{P}^n)^*$ corresponding to the point $(a_0 : \cdots : a_n) \in \mathbb{P}^n$. A *linear system of hyperplanes in* $\mathbb{P}^n$ is a linear subspace of $(\mathbb{P}^n)^*$.

Theorem 6.2 (Bertini's Theorem)**.** *Let V be a (quasi-projective) subvariety of $\mathbb{P}^n$ with irreducible components $V_1,\dots,V_m$ of equal dimension $d \geq 1$, and let $\mathcal{L} \subseteq (\mathbb{P}^n)^*$ be a linear system. After a change of coordinates if necessary, we may assume that there exists $k \in \{0,\dots,n\}$ such that $\mathcal{L}$ is the space of all hyperplanes of the form $\{a_k x_k + \cdots + a_n x_n = 0\}$. Assume that the coordinates $x_k,\dots,x_n$ do not simultaneously vanish at any point on V (i.e., the linear system $\mathcal{L}$ has no base-points in V), so that*

$$\begin{aligned} \Phi_{\mathcal{L}} : V &\longrightarrow \mathbb{P}^{n-k} \\ (z_0 : \cdots : z_n) &\longmapsto (z_k : \cdots : z_n) \end{aligned}$$

defines a morphism. Then there exists a nonempty open subset $U \subseteq \mathcal{L}$ such that for all hyperplanes $H \in U$,

(a) $V^{\mathrm{ns}} \cap H$ is nonsingular, and

(b) $\dim(V^{\mathrm{s}} \cap H) < \dim V^{\mathrm{s}}$ (if $V^{\mathrm{s}} \neq \emptyset$).

Moreover, if $\dim \Phi_{\mathcal{L}}(V) \geq 2$, then U may be chosen so that for all $H \in U$ we have

(c) for all $1 \leq i \leq m$, the intersection $V_i \cap H$ is either empty or geometrically irreducible.

Remark. Theorem 6.2 is stated somewhat more generally than we need, so we specify the two situations for which we will actually need the result:

1. Let V be a closed hypersurface in $\mathbb{P}^n$ and let $\mathcal{L} = (\mathbb{P}^n)^*$. Then $\Phi_{\mathcal{L}}$ is just the inclusion map of V into $\mathbb{P}^n$, and the hypotheses of Theorem 6.2 are satisfied. Moreover, since each component V_i is a closed subvariety of $\mathbb{P}^n$ of positive dimension, each intersection $V_i \cap H$ is nonempty; thus, if $d = \dim V = \dim \Phi_{\mathcal{L}}(V) \geq 2$, then $V_i \cap H$ is irreducible for all $1 \leq i \leq m$ and all $H \in U$.
2. Identify $\mathbb{A}^n$ with the Zariski open subset $\{x_0 \neq 0\} \subset \mathbb{P}^n$. Let V be a closed hypersurface in $\mathbb{A}^n$ *not containing the origin* $\mathbf{0} = (0,\dots,0)$, and let $\mathcal{L}$ be the space of all hypersurfaces of the form $\{a_1 x_1 + \cdots + a_n x_n = 0\}$. Then the conditions of Theorem 6.2 are satisfied once again. A fiber of $\Phi_{\mathcal{L}}$ is precisely the intersection of V with a line in $\mathbb{A}^n$ passing through $\mathbf{0}$. Since V is closed in $\mathbb{A}^n$ and does not contain $\mathbf{0}$, V cannot contain a line through $\mathbf{0}$, hence each such intersection is finite. In particular, this means the map $\Phi_{\mathcal{L}}$ has finite fibers, so $\dim \Phi_{\mathcal{L}}(V) = \dim V = d$. Moreover, the failure of a hyperplane $H \in \mathcal{L}$ to intersect every V_i is a proper Zariski closed condition. Therefore, removing such hyperplanes from U if necessary, we again have that $V_i \cap H$ is nonempty for all $1 \leq i \leq n$ and $H \in U$, thus $V_i \cap H$ is irreducible for all $1 \leq i \leq n$ and $H \in U$ as long as $d \geq 2$.

Proof of Theorem 6.2. Consider the set $\mathcal{X}$ of hyperplanes $H \in \mathcal{L}$ satisfying the following conditions:

(a′) $V_i^{\mathrm{ns}} \cap H$ is nonsingular for all $1 \leq i \leq m$;

(b′) H does not contain any components of V_i^{s} nor $(V_i \cap V_j)$ for $1 \leq i, j \leq m$ with $i \neq j$; and

(c′) for all $1 \leq i \leq m$, the intersection $V_i \cap H$ is either empty or geometrically irreducible (if $d \geq 2$).

We begin by showing that if $H \in \mathcal{X}$, then H satisfies properties (a), (b), and (c). Indeed, condition (c′) is exactly condition (c), so we need only show that H also satisfies (a) and (b).

For (a), note that a point $P \in V$ is nonsingular if and only if P is a nonsingular point on V_i for some $1 \le i \le m$ and $P \notin V_j$ for all $j \ne i$. Thus V^{ns} is a *disjoint* union $V^{\mathrm{ns}} = \bigsqcup_{i=1}^m W_i$, where each W_i is a subset of V_i^{ns}. Then (a) follows from (a′) since $V^{\mathrm{ns}} \cap H = \bigsqcup_{i=1}^m (W_i \cap H)$ and each $W_i \cap H \subseteq V_i^{\mathrm{ns}} \cap H$ is nonsingular. Finally, (b′) implies that H intersects each component of V^{s} properly (assuming $V^{\mathrm{s}} \ne \emptyset$), so (b) follows.

It remains to show that $\mathcal{X}$ contains a Zariski open subset of $\mathcal{L}$. By the standard form of Bertini's Theorem (see Corollaire 6.11 of [17], or Corollary 10.9 and Remark 10.9.1 of [15]), since $\mathcal{L}$ has no base-points in V, the set of hyperplanes $H \in \mathcal{L}$ satisfying (a′) and (c′) contains a nonempty open subset of $\mathcal{L}$. Moreover, H containing any of a finite collection of nonempty subvarieties of $\mathbb{P}^n$ is a proper closed condition on H, so condition (b′) is a nonempty open condition; therefore, $\mathcal{X}$ contains a nonempty open subset of $\mathcal{L}$. □

Armed with Theorem 6.2, the proof of Proposition 6.1 is pleasingly straightforward.

Proof of Proposition 6.1. Suppose that $\ell \ge 2$ and $h \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $h(\mathbf{0}) = 0$. Let k and j denote the highest and lowest degrees, respectively, of the terms appearing in h, and let r denote the minimum rank of h^k and h^j. Let $\widehat{V}_k, \widehat{V}_j \subseteq \mathbb{P}^{\ell-1}$ denote the varieties defined by $h^k = 0$ and $h^j = 0$, respectively. By Theorem 6.2 (see also case 1 of the remark that follows) applied to the linear system $\mathcal{L} = (\mathbb{P}^{\ell-1})^*$ and the varieties $\widehat{V}_k$ and $\widehat{V}_j$, respectively, the set of hyperplanes H in $\mathbb{P}^{\ell-1}$ satisfying

- $H \cap \widehat{V}_k^{\mathrm{ns}}$ and $H \cap \widehat{V}_j^{\mathrm{ns}}$ are nonsingular, and
- $\dim(H \cap \widehat{V}_k^{\mathrm{s}}) < \dim \widehat{V}_k^{\mathrm{s}}$, if $V^{\mathrm{s}} \ne \emptyset$, and $\dim(H \cap \widehat{V}_j^{\mathrm{s}}) < \dim \widehat{V}_j^{\mathrm{s}}$, if $\widehat{V}_j^{\mathrm{s}} \ne \emptyset$,

contains a nonempty open subset $U \subseteq (\mathbb{P}^{\ell-1})^*$. Thus, we can choose $H \in U$ defined by the vanishing of $l(x_1, \dots, x_\ell) = a_1 x_1 + \cdots + a_{\ell-1} x_{\ell-1} - x_\ell$ with $a_1, \dots, a_{\ell-1} \in \mathbb{Z}$. Here, we're using the fact that the set of integer points is Zariski dense in the affine space $\mathbb{A}^{\ell-1} \subset \mathbb{P}^{\ell-1} \cong (\mathbb{P}^{\ell-1})^*$.

Let $\mu(x_1, \dots, x_{\ell-1}) := a_1 x_1 + \cdots + a_{n-1} x_{\ell-1}$, and set

$$g_1(x_1, \dots, x_{\ell-1}) := h(x_1, \dots, x_{\ell-1}, \mu(x_1, \dots, x_{\ell-1})).$$

Note that, by construction, $g_1(\mathbb{Z}^{\ell-1}) \subseteq h(\mathbb{Z}^\ell)$, $g_1(\mathbf{0}) = 0$, and the highest and lowest degrees of the nonzero terms of g_1 are still k and j, respectively.

Now, the subvariety $\widehat{W}_k$ (resp., $\widehat{W}_j$) of $\mathbb{P}^{\ell-2}$ defined by $g_1^k = 0$ (resp., $g_1^j = 0$) is isomorphic to $H \cap \widehat{V}_k$ (resp., $H \cap \widehat{V}_j$). In particular, the minimum rank of g_1^k and g_1^j can only drop below r if both singular loci were originally empty, which would imply $r = \ell$. Thus, repeating this process $(\ell - r)$ times yields a sequence of polynomials $(g_i(x_1, \dots, x_{\ell-i}))_{i=0}^{\ell-r}$, with $g_0 := h$, satisfying

- $g_i(\mathbb{Z}^{\ell-i}) \subseteq g_{i-1}(\mathbb{Z}^{\ell-i+1})$ for all $1 \le i \le \ell - r$,
- $g_i(\mathbf{0}) = 0$ for all $0 \le i \le \ell - r$,
- the highest and lowest degrees of the nonzero terms of each g_i are k and j, respectively, and
- the rank of each g_i^k (resp., g_i^j) is at least r.

Finally, let $g := g_{\ell-r} \in \mathbb{Z}[x_1,\dots,x_r]$, so the rank for each of g^k and g^j is r. In other words, g^k and g^j are smooth, and thus by Proposition 2.5, g is strongly Deligne. □

Remark. The conclusion of Proposition 6.1 technically holds for $r = 1$ as well, since nonconstant univariate polynomials are necessarily Deligne; however, this case is not useful for our purposes.

6.1 Proof of Theorem 2.13

We now proceed with the more elaborate of our two dimension-lowering arguments, in which we cannot exploit the existence of an integer root. Throughout this section, we fix $\ell \geq 2$ and a polynomial $h \in \mathbb{Z}[x_1,\dots,x_\ell]$ satisfying all hypotheses of Theorem 2.13, and we recall that $k = \deg(h)$ and r denotes the rank of h^k. Note that the hypotheses of Theorem 2.13 imply that $r \geq 2$. We assume without loss of generality that $h(\mathbf{0}) \neq 0$, which is permissible because $h(\mathbb{Z}^\ell)$ is invariant under input translation. We let $V \subseteq \mathbb{A}^\ell$ and $\widehat{V} \subseteq \mathbb{P}^{\ell-1}$ denote the varieties defined by $h = 0$ and $h^k = 0$, respectively. The following crucial lemma says that we can eliminate the singularity in the top-degree part of h, one dimension at a time, while maintaining the existence of nonsingular $\mathbb{F}_p$-points.

Lemma 6.3. *Suppose $\ell \geq 3$. Then there exists a homogeneous linear polynomial $l \in \mathbb{Z}[x_1,\dots,x_\ell]$, monic in x_ℓ, for which the following holds: Letting $\widehat{L}$ and L denote the hyperplanes in $\mathbb{P}^{\ell-1}$ and $\mathbb{A}^\ell$, respectively, defined by $l = 0$, we have*

(i) $\dim(\widehat{V} \cap \widehat{L})^{\mathrm{s}} < \dim \widehat{V}^{\mathrm{s}}$, *if* $\widehat{V}^{\mathrm{s}} \neq \emptyset$; *and*

(ii) For sufficiently large p, $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$ implies $(V \cap L)^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$.

Proof. Let $\widehat{\mathcal{L}}$ and $\mathcal{L}$ denote the linear systems of *hyperplanes in* $\mathbb{P}^{\ell-1}$ and *hyperplanes in* $\mathbb{A}^\ell$ *passing through* $\mathbf{0}$, respectively. We identify each of $\widehat{\mathcal{L}}$ and $\mathcal{L}$ with $\mathbb{P}^{\ell-1}$, with the point $\boldsymbol{a} = (a_1 : \cdots : a_\ell) \in \mathbb{P}^{\ell-1}$ corresponding to the hyperplanes $\{a_1x_1 + \cdots + a_\ell x_\ell = 0\}$ in $\mathbb{P}^{\ell-1}$ and $\mathbb{A}^\ell$, respectively.

The hypotheses of Theorem 6.2 are satisfied by $\widehat{V}$ and $\widehat{\mathcal{L}}$ (resp., V and $\mathcal{L}$), as explained in case 1 (resp., case 2) of the remark immediately following the theorem. Thus, there is a nonempty open set $U \subseteq \mathbb{P}^{\ell-1}$ such that for all $\boldsymbol{a} = (a_1 : \cdots : a_\ell) \in U$, the hyperplanes $\widehat{L}_{\boldsymbol{a}} \subset \mathbb{P}^{\ell-1}$ and $L_{\boldsymbol{a}} \subset \mathbb{A}^\ell$ defined by $l_{\boldsymbol{a}} := a_1x_1 + \cdots + a_\ell x_\ell = 0$ satisfy the conclusion of Theorem 6.2 (intersected with $\widehat{V} \subset \mathbb{P}^{\ell-1}$ and $V \subset \mathbb{A}^\ell$, respectively). Similar to the proof of Proposition 6.1, we may choose $\boldsymbol{a} \in U$ of the form $\boldsymbol{a} = (a_1 : \cdots : a_{\ell-1} : 1)$ with $a_1,\dots,a_{\ell-1} \in \mathbb{Z}$. Set $l := l_{\boldsymbol{a}}$ for such a choice of $\boldsymbol{a} \in U$, hence also $\widehat{L} = \widehat{L}_{\boldsymbol{a}}$ and $L = L_{\boldsymbol{a}}$. By construction, we immediately have that $l \in \mathbb{Z}[x_1,\dots,x_\ell]$, l is monic in x_ℓ, and property (i) holds, so it remains only to show that (ii) holds.

Let $V_1,\dots,V_m$ be the geometrically irreducible components of V. Since $\dim V = \ell - 1 \geq 2$, our choice of $\boldsymbol{a}$ guarantees that the geometrically irreducible components of $V \cap L$ are $V_i \cap L$ with $1 \leq i \leq m$. (We are again using Theorem 6.2 and case 2 of the remark that follows.) By Lemma 5.3, if p is sufficiently large, then $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$ implies that V_i is defined over $\mathbb{Z}_p$ for some $1 \leq i \leq m$. Since L is defined over $\mathbb{Z}$, hence over $\mathbb{Z}_p$, the intersection $V_i \cap L$ is also defined over $\mathbb{Z}_p$. Appealing to Lemma 5.3 once more implies that $(V \cap L)^{\mathrm{ns}}(\mathbb{F}_p)$ is nonempty. □

The hyperplane produced by Lemma 6.3 quickly yields a suitable polynomial with one fewer variable.

Corollary 6.4. *Suppose $\ell \geq 3$. Then there exists $g' \in \mathbb{Z}[x_1,\dots,x_{\ell-1}]$ with $\deg(g') = k$ such that*

(i) $g'(\mathbf{0}) \neq 0$;

(ii) $g'(\mathbb{Z}^{\ell-1}) \subseteq h(\mathbb{Z}^\ell)$;

(iii) $\dim(\widehat{W}')^{\mathrm{s}} < \dim \widehat{V}^{\mathrm{s}}$, *if* $\widehat{V}^{\mathrm{s}} \neq \emptyset$; *and*

(iv) for sufficiently large p, $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$ implies $(W')^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$;

where $\widehat{W}' \subset \mathbb{P}^{\ell-2}$ and $W' \subset \mathbb{A}^{\ell-1}$ are the varieties defined by $(g')^k = 0$ and $g' = 0$, respectively.

Proof. Let $L = L_{\boldsymbol{a}}$ be as in Lemma 6.3, and write $l = l_{\boldsymbol{a}} = a_1x_1 + \cdots + a_{\ell-1}x_{\ell-1} + x_\ell$. To ease notation, we also set $\mu = \mu_{\boldsymbol{a}} := -(a_1x_1 + \cdots + a_{\ell-1}x_{\ell-1})$. Now, define

$$g'(x_1,\dots,x_{\ell-1}) := h(x_1,\dots,x_{\ell-1},\mu(x_1,\dots,x_{\ell-1})).$$

Clearly $g'(\mathbb{Z}^{\ell-1}) \subseteq h(\mathbb{Z}^\ell)$ and, since μ is homogeneous, $g'(\mathbf{0}) = h(\mathbf{0}) \neq 0$. Finally, since $V \cap L \cong W'$ and $\widehat{V} \cap \widehat{L} \cong \widehat{W}'$, properties (iii) and (iv) follow immediately from Lemma 6.3. □

Recall our assumption that the rank satisfies $r \geq 2$. Repeated application of Corollary 6.4 yields the following:

Corollary 6.5. *There exists $g \in \mathbb{Z}[x_1,\dots,x_r]$ with $\deg(g) = k$ such that*

(i) $g(\mathbb{Z}^r) \subseteq h(\mathbb{Z}^\ell)$;

(ii) g is Deligne; and

(iii) for sufficiently large p, $V^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$ implies $W^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$;

where $W \subseteq \mathbb{A}^r$ is the variety defined by $g = 0$.

Proof. When $\ell \geq 3$, this follows immediately by applying Corollary 6.4 recursively $(\ell - r)$ times. The fact that $r \geq 2$ ensures that at each step we are applying Corollary 6.4 to a polynomial in at least 3 variables.

When $\ell = 2$, the statement is trivial, since $r = 2$ implies that h is already Deligne, so we can take $g = h$. □

Remark. Using the construction from the proof of Corollary 6.4, the polynomial g of Corollary 6.5 may be written in the form

$$g(x_1,\dots,x_r) = h(x_1,\dots,x_r,\mu_{r+1}(x_1,\dots,x_r),\dots,\mu_\ell(x_1,\dots,x_r)),$$

where each μ_j is a homogeneous linear polynomial. We will use this precise form in our proof of Theorem 2.13, which we are now ready to begin.

Proof of Theorem 2.13. Let $g \in \mathbb{Z}[x_1,\dots,x_r]$ be as in Corollary 6.5, and let $W \subseteq \mathbb{A}^r$ be the variety defined by $g=0$. Throughout this proof we use the notation $\tilde{\boldsymbol{x}} = (x_1,\dots,x_r)$ and $\boldsymbol{x} = (x_1,\dots,x_\ell)$.

As mentioned in the remark above, g may be given by $g(\tilde{\boldsymbol{x}}) = h(M\tilde{\boldsymbol{x}})$, where

$$M(x_1,\dots,x_r) = (x_1,\dots,x_r,\mu_{r+1}(x_1,\dots,x_r),\dots,\mu_\ell(x_1,\dots,x_r))$$

for linear forms $\mu_{r+1},\dots,\mu_\ell$. Note that g and the linear forms have been constructed once and for all from h, so any quantities depending on them implicitly depend only on h.

Let $X = X(h)$ be the set of primes p for which

- $p \mid k$;
- g^k is not smooth modulo p; or
- $W^{\mathrm{ns}}(\mathbb{F}_p) = \emptyset$ and $m_p \neq k$ for all $\boldsymbol{z}_p \in V(\mathbb{Z}_p)$.

The first item clearly defines a finite set, the second item defines a finite set because g is Deligne (see Definition 2.3). If $r \geq 3$, then the third item defines a finite set by Lemma 5.3 and the fact that Deligne polynomials in $r \geq 3$ variables are geometrically irreducible, as seen in the proof of Corollary 2.10. If $r = 2$, then item (iii) of Corollary 6.5, Lemma 5.3, and the hypotheses of Theorem 2.13 ensure that the third item defines a finite set. Thus, X is finite.

In order to construct auxiliary polynomials h_d for $d \in N$, we first choose $\mathbb{Z}_p$-roots of h as follows: If $p \in X$, then choose a point $\boldsymbol{z}_p \in V(\mathbb{Z}_p)$ arbitrarily; such points exist because h is intersective. For $p \notin X$ with $W^{\mathrm{ns}}(\mathbb{F}_p) \neq \emptyset$, choose $\tilde{\boldsymbol{z}}_p \in W(\mathbb{Z}_p)$ to be a Hensel lift of a nonsingular point on $W(\mathbb{F}_p)$, then set $\boldsymbol{z}_p = M\tilde{\boldsymbol{z}}_p \in V(\mathbb{Z}_p)$. Finally, for all remaining $p \notin X$, fix $\boldsymbol{z}_p \in V(\mathbb{Z}_p)$ with $m_p = k$.

For each prime p, by definition of multiplicity, we have a decomposition of the form

$$h(\boldsymbol{x}+\boldsymbol{z}_p) = \sum_{m_p \leq |\boldsymbol{i}| \leq k} b_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \tag{32}$$

for $b_{\boldsymbol{i}} \in \mathbb{Z}_p$. However, the substitution $\boldsymbol{x} = M\tilde{\boldsymbol{x}}$ could cause some homogeneous parts to identically vanish, so we define $\tilde{m}_p$ to be the multiplicity of $\boldsymbol{0}$ as a root of $h(M\tilde{\boldsymbol{x}}+\boldsymbol{z}_p)$, so in particular

$$h(M\tilde{\boldsymbol{x}}+\boldsymbol{z}_p) = \sum_{m_p \leq |\boldsymbol{i}| \leq k} b_{\boldsymbol{i}} (M\tilde{\boldsymbol{x}})^{\boldsymbol{i}} = \sum_{\tilde{m}_p \leq |\boldsymbol{i}| \leq k} a_{\boldsymbol{i}} \tilde{\boldsymbol{x}}^{\boldsymbol{i}}, \tag{33}$$

where $a_{\boldsymbol{i}} \neq 0$ for some $\boldsymbol{i}$ with $|\boldsymbol{i}| = \tilde{m}_p$. We quickly note that $\tilde{m}_p = m_p$ for all $p \notin X$. If $p \notin X$ with $m_p = k$, the degree-k part of $h(M\tilde{\boldsymbol{x}}+\boldsymbol{z}_p)$ is the same as the degree-k part of g. If $p \notin X$ and $\boldsymbol{z}_p = M\tilde{\boldsymbol{z}}_p$ as above, then $h(M\tilde{\boldsymbol{x}}+\boldsymbol{z}_p)$ is precisely $g(\tilde{\boldsymbol{x}}+\tilde{\boldsymbol{z}}_p)$, and in particular the linear part does not vanish modulo p.

To account for this possible increase in multiplicity for primes $p \in X$, we define a completely multiplicative function $\tilde{\lambda}(d)$ by setting $\lambda(p) = p^{\tilde{m}_p}$ for all primes p. We define $\{\boldsymbol{r}_d\}_{d\in\mathbb{N}}$ from $\{\boldsymbol{z}_p\}_{p\in\mathcal{P}}$ as usual from the Chinese remainder theorem, then define the slightly modified auxiliary polynomials $\{\tilde{h}_d\}_{d\in\mathbb{N}}$ by

$$\tilde{h}_d(\boldsymbol{x}) = h(\boldsymbol{r}_d + d\boldsymbol{x})/\tilde{\lambda}(d).$$

We note that $\tilde{h}_d$ can potentially have non-integer coefficients, with denominators divisible by primes in X. However, the analog of Proposition 3.2, and the deduction of Lemma 4.1 from Lemma 4.2 and Proposition 3.2, still hold because $d \mid \tilde{\lambda}(d)$ and $\tilde{\lambda}$ is completely multiplicative.

We now let $d' = \prod_{p|d} p^{(\tilde{m}_p - m_p + 1)\mathrm{ord}_p(d)} \leq d^k$, and we define

$$g_d(\tilde{\boldsymbol{x}}) = \tilde{h}_d(\boldsymbol{s}_d + M\tilde{\boldsymbol{x}}) = h(\boldsymbol{r}_{d'} + dM\tilde{\boldsymbol{x}})/\tilde{\lambda}(d),$$

where $\boldsymbol{s}_d$ satisfies $\boldsymbol{r}_{d'} = \boldsymbol{r}_d + d\boldsymbol{s}_d$. We will establish the following properties of g_d:

(i) $g_d(\mathbb{Z}^r) \subseteq \tilde{h}_d(\mathbb{Z}^\ell)$,

(ii) g_d has integer coefficients,

(iii) g_d is Deligne modulo p for all $p \notin X$,

(iv) The coefficients of g_d are of size $O_h(d^{k^2})$,

(v) $\mathrm{cont}(g_d) \ll_h 1$.

Unlike Proposition 6.1, these efforts cannot be applied "externally" to immediately yield Theorem 2.13 because the family $\{g_d\}_{d\in\mathbb{N}}$ is not necessarily the set of auxiliary polynomials of a single intersective polynomial. However, the enumerated properties of this family make it perfectly suited for us to apply our efforts "internally", using the estimates enumerated in Theorem 3.9, as follows:

(1) Replace all occurrences of h_d in the proof of Theorem 2.4 with $\tilde{h}_d$. The fact that $\tilde{h}_d$ potentially has non-integer coefficients is not a problem, as the analog of Proposition 3.2 still holds, and as explained in the next step.

(2) When proving Lemma 4.2 (the only piece of the proof of Theorem 2.4 that requires integer coefficients or a nonsingularity condition), use that $(A-A)\cap g_d(\mathbb{Z}^r) \subseteq (A-A)\cap \tilde{h}_d(\mathbb{Z}^\ell) \subseteq \{0\}$, then do the remainder of the proof with h_d replaced by g_d. For this purpose, properties (ii)-(v) above assure that g_d functions as if it were the auxiliary polynomial of a strongly Deligne polynomial in r variables. In particular, the conclusion of Lemma 4.2 holds with $\theta(k,\ell,\delta)$ replaced by $\theta(k,r,\delta)$.

(3) The remainder of the argument is identical, and Theorem 2.13 follows.

Our task is now reduced to verifying properties (i)-(v). Properties (i) and (iv) are immediate from the definition of g_d and $\tilde{h}_d$. We next simultaneously establish (ii) and the property

$$\mathrm{ord}_p(\mathrm{cont}(g_d)) \ll_{h,p} 1 \text{ for all } p \in \mathcal{P}. \tag{34}$$

When we later establish (iii), it immediately combines with (34) to yield (v), because $p \nmid \mathrm{cont}(g_d)$ if g_d is Deligne modulo p. We fix $p \in \mathcal{P}$ and set $j = \mathrm{ord}_p(d)$. By (32), we have

$$g_d(\tilde{\boldsymbol{x}}) = \tilde{h}_d(\boldsymbol{s}_d + M\tilde{\boldsymbol{x}}) = \frac{1}{\tilde{\lambda}(d)} h(\boldsymbol{r}_{d'} + dM\tilde{\boldsymbol{x}}) = \frac{1}{\tilde{\lambda}(d)} \sum_{m_p \leq |\boldsymbol{i}| \leq k} b_{\boldsymbol{i}}(dM\tilde{\boldsymbol{x}} + \boldsymbol{r}_{d'} - \boldsymbol{z}_p)^{\boldsymbol{i}}. \tag{35}$$

Since $p^j \mid d$ and $p^{(\tilde{m}_p - m_p + 1)j}$ divides all coordinates of $\boldsymbol{r}_{d'} - \boldsymbol{z}_p$, all terms in the summation apart from

$$\sum_{m_p \le |\boldsymbol{i}| \le \tilde{m}_p - 1} b_{\boldsymbol{i}} (dM\tilde{\boldsymbol{x}})^{\boldsymbol{i}} \tag{36}$$

have coefficients divisible by $p^{j\tilde{m}_p}$, and the polynomial (36) identically vanishes by definition of $\tilde{m}_p$. Since $\mathrm{ord}_p(\tilde{\lambda}(d)) = j\tilde{m}_p$, all coefficients of g_d have nonnegative p-adic valuation. Since $p \in \mathcal{P}$ was arbitrary, it follows that g_d has integer coefficients.

Further, we see in (35) that all degree-$\tilde{m}_p$ terms have a factor of p^j apart from those arising from

$$\frac{d^{\tilde{m}_p}}{\tilde{\lambda}(d)} \sum_{|\boldsymbol{i}| = \tilde{m}_p} b_{\boldsymbol{i}} (M\tilde{\boldsymbol{x}})^{\boldsymbol{i}} = \frac{d^{\tilde{m}_p}}{\tilde{\lambda}(d)} \sum_{|\boldsymbol{i}| = \tilde{m}_p} a_{\boldsymbol{i}} \tilde{\boldsymbol{x}}^{\boldsymbol{i}},$$

where $a_{\boldsymbol{i}} \neq 0$ for some $\boldsymbol{i}$ with $|\boldsymbol{i}| = \tilde{m}_p$.

Since $p \nmid (d^{\tilde{m}_p}/\tilde{\lambda}(d))$, we have that

$$\mathrm{ord}_p(\mathrm{cont}(g_d)) \le v := \min_{|\boldsymbol{i}| = \tilde{m}_p} \mathrm{ord}_p(a_{\boldsymbol{i}}),$$

provided $j > v$. Alternatively, if $j \le v$, then $\mathrm{ord}_p(\mathrm{cont}(g_d))$ is at most kv plus the minimum p-adic valuation of the degree-k coefficients of g, which establishes (34).

Our task is now reduced to verifying property (iii), for which we fix $p \notin X$, and proceed similarly to the proof of Proposition 2.8. Since g_d^k is precisely $\frac{d^k}{\tilde{\lambda}(d)} g^k$, we know that if $p \nmid d$ or $m_p = k$, then g_d^k modulo p is a nonzero multiple of g^k, hence remains smooth. Therefore, g_d is Deligne modulo p.

The remaining case is when $p \mid d$ and $\boldsymbol{z}_p = M\tilde{z}_p$, where $\tilde{z}_p \in W(\mathbb{Z}_p)$ is a Hensel lift of a nonsingular point of $W(\mathbb{F}_p)$, so in particular the linear part of $g(\tilde{\boldsymbol{x}} + \tilde{z}_p) = h(M\tilde{\boldsymbol{x}} + \boldsymbol{z}_p)$ does not identically vanish modulo p.

Using (32), letting $j = \mathrm{ord}_p(d)$, we note that $\mathrm{ord}_p(\tilde{\lambda}(d)) = j$ and p^j divides all coordinates of $\boldsymbol{r}_{d'} - \boldsymbol{z}_p$, and we have

$$g_d(\tilde{\boldsymbol{x}}) = \frac{1}{\tilde{\lambda}(d)} \sum_{1 \le |\boldsymbol{i}| \le k} b_{\boldsymbol{i}} (dM\tilde{\boldsymbol{x}} + \boldsymbol{r}_{d'} - \boldsymbol{z}_p)^{\boldsymbol{i}} = p^j f(\tilde{\boldsymbol{x}}) + \frac{d}{\tilde{\lambda}(d)} \sum_{|\boldsymbol{i}| = 1} b_{\boldsymbol{i}} (M\tilde{\boldsymbol{x}})^{\boldsymbol{i}} + C$$

for some $f \in \mathbb{Z}_p[x_1, \ldots, x_r]$ and constant C. In particular, modulo p, the highest-degree part of g_d is a nonzero multiple of the nonvanishing linear part of $g(\tilde{\boldsymbol{x}} + \tilde{\boldsymbol{z}}_p)$, hence g_d is Deligne modulo p. All five properties of g_d are now verified and the proof of Theorem 2.13 is complete. □

7 Exponential sum estimates

In this final section, we establish the exponential sum estimates claimed in Theorem 3.9, which we then use to deduce (27) and (28). This effort consists primarily of careful multivariate adaptations of the tools used to prove Theorem 2.7 in [28], but we begin with another foray into varieties over finite fields.

7.1 Control over gradient vanishing: Part II

Since we are sieving away inputs at which the gradient of our polynomial vanishes, but then appealing to Theorem 1.4, which is a complete exponential sum estimate, it is important for us to have an upper bound on the number of points our sieve might be throwing away. With this in mind, we make the following definition.

Definition 7.1. For a field F and $g \in F[x_1,\dots,x_\ell]$ we define the *gradient locus* of g to be the variety

$$\mathcal{G}_g = \{\boldsymbol{x} \in \mathbb{A}^\ell : \nabla g(\boldsymbol{x}) = \boldsymbol{0}\} \subseteq \mathbb{A}^\ell.$$

The following proposition establishes firm control over the gradient locus of a Deligne polynomial.

Proposition 7.2. *Suppose F is a field, $\ell \in \mathbb{N}$, and $g \in F[x_1,\dots,x_\ell]$ with $\deg(g) = k \geq 1$. If g is Deligne, then $\mathcal{G}_g = \emptyset$ or $\dim \mathcal{G}_g = 0$.*

Proof. First, assume g is not homogeneous. Let $G(x_0,x_1,\dots,x_\ell)$ be the homogenization of g. Thus, we have

$$g(x_1,\dots,x_\ell) = G(1,x_1,\dots,x_\ell) \quad \text{and} \quad g^k(x_1,\dots,x_\ell) = G(0,x_1,\dots,x_\ell).$$

The variety

$$\widehat{W} := \{G = 0\} \cap \{x_0 = 0\} \subset \mathbb{P}^\ell$$

is isomorphic to $\{g^k = 0\}$, hence is nonsingular since g is Deligne. Thus, the Jacobian matrix

$$\begin{pmatrix} \dfrac{\partial G}{\partial x_0} & \dfrac{\partial G}{\partial x_1} & \cdots & \dfrac{\partial G}{\partial x_\ell} \\ \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

has rank 2 at every point on $\widehat{W}$. In other words, the system

$$G = x_0 = \frac{\partial G}{\partial x_1} = \cdots = \frac{\partial G}{\partial x_\ell} = 0$$

has no solutions in $\mathbb{P}^\ell$. The equation $G = 0$ is actually superfluous here; by Euler's theorem on homogeneous functions, we have

$$kG(x_0,x_1,\dots,x_\ell) = x_0\frac{\partial G}{\partial x_0} + x_1\frac{\partial G}{\partial x_1} + \cdots + x_\ell\frac{\partial G}{\partial x_\ell},$$

so the vanishing of x_0 and the x_1- through x_ℓ-partials would guarantee the vanishing of G. Here we use the fact that the characteristic of F does not divide k, as included in the definition of the Deligne property. It follows that the system

$$x_0 = \frac{\partial G}{\partial x_1} = \cdots = \frac{\partial G}{\partial x_\ell} = 0$$

has no solutions in $\mathbb{P}^\ell$, so the subvariety of $\mathbb{P}^\ell$ defined by

$$\frac{\partial G}{\partial x_1} = \cdots = \frac{\partial G}{\partial x_\ell} = 0 \tag{37}$$

is contained in $\{\boldsymbol{x} \in \mathbb{P}^\ell \mid x_0 \neq 0\} \cong \mathbb{A}^\ell$ and has dimension 0. But, for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{A}^\ell$, we have

$$\frac{\partial g}{\partial x_i}(\boldsymbol{\alpha}) = \frac{\partial G}{\partial x_i}(1, \boldsymbol{\alpha})$$

for all $1 \leq i \leq \ell$. Thus, $\mathcal{G}_g$ is (isomorphic to) the zero-dimensional subvariety of $\mathbb{P}^\ell$ given by (37), concluding the proof in the case that g is not homogeneous.

Finally, suppose g is homogeneous. Again using Euler's theorem on homogeneous functions, we write

$$kg(x_1, \ldots, x_\ell) = x_1 \frac{\partial g}{\partial x_1} + \cdots + x_\ell \frac{\partial g}{\partial x_\ell}.$$

Thus, if all partials of g vanish at $\boldsymbol{x}$, then $g(\boldsymbol{x}) = 0$ as well. By hypothesis, $g = g^k$ is smooth, so there are no common zeroes of $g, \frac{\partial g}{\partial x_1}, \ldots, \frac{\partial g}{\partial x_\ell}$ in $\mathbb{P}^\ell$, so in $\mathbb{A}^\ell$ the only possible common zero is the origin. Therefore, $\mathcal{G}_g$ contains at most one point. □

Proposition 7.2 combines with Bézout's Theorem (Lemma 5.1) to yield the following estimate on the size of the gradient vanishing locus for a Deligne polynomial over a finite field, which yields Lemma 3.3 as a special case.

Corollary 7.3. *If $\ell \geq 1$ and $g \in \mathbb{F}_q[x_1, \ldots, x_\ell]$ is a Deligne polynomial of degree $k \geq 1$, then $|\mathcal{G}_g|$ is bounded by a constant depending only k and ℓ.*

7.2 Major arc estimates

In this section we establish item (i) of Theorem 3.9. Derivations of asymptotic formulas of this type typically rely on partial summation, so we begin with a multivariate version thereof, proven by induction from the usual formula.

Lemma 7.4 (Multivariable Partial Summation)**.** *Suppose $\ell \in \mathbb{N}$ and $a : \mathbb{N}^\ell \to \mathbb{C}$. Suppose further that $\psi : \mathbb{R}^\ell \to \mathbb{C}$ is C^ℓ. For any $X > 0$, we have*

$$\sum_{\boldsymbol{n} \in [1,X]^\ell} a(\boldsymbol{n})\psi(\boldsymbol{n}) = A(X, \ldots, X)\psi(X, \ldots, X) + \sum_{i=1}^{\ell} (-1)^i \sum_{1 \leq j_1 < \cdots < j_i \leq \ell} \int_{[0,X]^i} A(\star) \frac{\partial^i \psi}{\partial x_{j_1} \cdots \partial x_{j_i}}(\star)\, dx_{j_1} \cdots dx_{j_i},$$

where

$$A(x_1, \ldots, x_\ell) = \sum_{\boldsymbol{n} \in [1,x_1] \times \cdots \times [1,x_\ell]} a(\boldsymbol{n})$$

and $\star = (X, \ldots, x_{j_1}, \ldots, x_{j_i}, \ldots, X)$, with $x_{j_1}, \ldots, x_{j_i}$ plugged into coordinate positions $j_1, \ldots, j_i$ and all other coordinates evaluated at X.

Proof. We induct on ℓ. The base case $\ell = 1$ is the usual partial summation formula

$$\sum_{1\le n\le X} a(n)\psi(n) = A(X)\psi(X) - \int_0^X A(x)\psi'(x)\,dx.$$

Fix $\ell \ge 2$ and assume the formula holds for $\ell - 1$. Defining some notation before proceeding, let

$$\tilde{A}(x_1,\dots,x_{\ell-1},n_\ell) = \sum_{\boldsymbol{n}\in[1,x_1]\times\cdots\times[1,x_{\ell-1}]} a(\boldsymbol{n},n_\ell),$$

let

$$\tilde{I}(j_1,\dots,j_i,n_\ell) = \int_{[0,X]^i} \tilde{A}(\star,n_\ell)\frac{\partial^i\psi}{\partial x_{j_1}\cdots\partial x_{j_i}}(\star,n_\ell)\,dx_{j_1}\cdots dx_{j_i},$$

and let

$$I(j_1,\dots,j_i) = \int_{[0,X]^i} A(\star)\frac{\partial^i\psi}{\partial x_{j_1}\cdots\partial x_{j_i}}(\star)\,dx_{j_1}\cdots dx_{j_i},$$

where A and $\star$ are as defined in the statement of the lemma. By our inductive hypothesis, we have

$$\begin{aligned}\sum_{\boldsymbol{n}\in[1,X]^\ell} a(\boldsymbol{n})\psi(\boldsymbol{n}) &= \sum_{1\le n_\ell\le X}\sum_{\boldsymbol{n}\in[1,X]^{\ell-1}} a(\boldsymbol{n},n_\ell)\psi(\boldsymbol{n},n_\ell)\\ &= \sum_{1\le n_\ell\le X}\Big(\tilde{A}(X,\dots,X,n_\ell)\psi(X,\dots,X,n_\ell) + \sum_{i=1}^{\ell-1}(-1)^i\sum_{1\le j_1<\cdots<j_i\le\ell-1}\tilde{I}(j_1,\dots,j_i,n_\ell)\Big).\end{aligned}$$

We now apply the standard single-variable formula to the first term and each individual integral, yielding

$$\sum_{1\le n_\ell\le X}\tilde{A}(X,\dots,n_\ell)\psi(X,\dots,n_\ell) = A(X,\dots,X)\psi(X,\dots,X) - \int_0^X A(X,\dots,x_\ell)\frac{\partial\psi}{\partial x_\ell}(X,\dots,x_\ell)dx_\ell, \quad (38)$$

and

$$\begin{aligned}&\sum_{1\le n_\ell\le X}(-1)^i\tilde{I}(j_1,\dots,j_i,n_\ell)\\ &\quad= (-1)^i\int_{[0,X]^i}\left(A(\star,X)\frac{\partial^i\psi}{\partial x_{j_1}\cdots\partial x_{j_i}}(\star,X) - \int_0^X A(\star,x_\ell)\frac{\partial^{i+1}\psi}{\partial x_{j_1}\cdots\partial x_{j_i}\partial x_\ell}(\star,x_\ell)dx_\ell\right)dx_{j_1}\cdots dx_{j_i}\\ &\quad= (-1)^i I(j_1,\dots,j_i) + (-1)^{i+1}I(j_1,\dots,j_i,\ell).\end{aligned}$$

Summing this final expression over $1\le i\le\ell-1$ and over all choices of $1\le j_1<\cdots<j_i\le\ell-1$ accounts for all required terms with $1\le i\le\ell$ and $1\le j_1<\cdots<j_i\le\ell$, with the single exception of $i=1$ and $j_1=\ell$, which is precisely the integral present in (38), and the induction is complete. □

We use Lemma 7.4 and the same calculation as in Proposition 3.4 to establish our asymptotic formula for sieved multivariate exponential sums near rationals with small denominator.

Lemma 7.5. *Suppose $\ell,k\in\mathbb{N}$, $g(\boldsymbol{x})=\sum_{|\boldsymbol{i}|\le k}a_{\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}}\in\mathbb{Z}[x_1,\dots,x_\ell]$, and let $J=\sum_{|\boldsymbol{i}|\le k}|a_{\boldsymbol{i}}|$. If $X,Y>0$, $a,q\in\mathbb{N}$, and $\alpha=a/q+\beta$, then*

$$\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)}e^{2\pi ig(\boldsymbol{n})\alpha}=q^{-\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)}e^{2\pi ig(\boldsymbol{s})a/q}\int_{[0,X]^\ell}e^{2\pi ig(\boldsymbol{x})\beta}d\boldsymbol{x}$$

$$+O_{k,\ell}\left(qE(1+JX^k|\beta|)^\ell\right),$$

where E is as in Proposition 3.4.

Proof. We begin by noting that for any $a,q\in\mathbb{N}$ and $0\le x_1,\dots,x_\ell\le X$, letting

$$B=[1,x_1]\times\cdots\times[1,x_\ell],$$

we have

$$\begin{aligned}T(x_1,\dots,x_\ell)&:=\sum_{\boldsymbol{n}\in B\cap W(Y)}e^{2\pi ig(\boldsymbol{n})a/q}\\&=\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell}e^{2\pi ig(\boldsymbol{s})a/q}\left|\{\boldsymbol{n}\in B\cap W(Y):\boldsymbol{n}\equiv\boldsymbol{s}\pmod q\}\right|.\end{aligned}$$

For $s\in W^q(Y)$ we have by the same calculation as Proposition 3.4 that

$$|\{\boldsymbol{n}\in B\cap W(Y):\boldsymbol{n}\equiv\boldsymbol{s}\pmod q\}|=\frac{x_1\cdots x_\ell}{q^\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)+E/q^{\ell-1},$$

where E is as in Proposition 3.4, whereas for $s\notin W^q(Y)$ the set is empty.

Therefore,

$$T(x_1,\dots,x_\ell)=\frac{x_1\cdots x_\ell}{q^\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)}e^{2\pi ig(\boldsymbol{s})a/q}+O(qE).\tag{39}$$

Letting $\psi(\boldsymbol{n})=e^{2\pi ig(\boldsymbol{n})\beta}$, we now decompose our sum as

$$\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)}e^{2\pi ig(\boldsymbol{n})\alpha}=\sum_{\boldsymbol{n}\in[1,X]^\ell}\left(1_{W(Y)}(\boldsymbol{n})e^{2\pi ig(\boldsymbol{n})a/q}\right)\psi(\boldsymbol{n})$$

and apply Lemma 7.4, yielding

$$\begin{aligned}\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)}e^{2\pi ig(\boldsymbol{n})\alpha}&=T(X,\dots,X)\psi(X,\dots,X)\\&\quad+\sum_{m=1}^{\ell}(-1)^m\sum_{1\le j_1<\cdots<j_m\le\ell}\int_{[0,X]^m}T(\star)\frac{\partial^m\psi}{\partial x_{j_1}\cdots\partial x_{j_m}}(\star)\,dx_{j_1}\cdots dx_{j_m},\end{aligned}$$

where $\star$ is as in Lemma 7.4. Substituting (39) gives the main term

$$q^{-\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)}e^{2\pi i g(\boldsymbol{s})a/q}\Big(X^\ell\psi(X,\dots,X)$$
$$+\sum_{m=1}^{\ell}(-1)^m\sum_{1\le j_1<\dots<j_m\le\ell}X^{\ell-m}\int_{[0,X]^m}x_{j_1}\cdots x_{j_m}\frac{\partial^m\psi}{\partial x_{j_1}\cdots\partial x_{j_m}}(\star)\,dx_{j_1}\cdots dx_{j_m}\Big).$$

By iteratively applying integration by parts, this equals

$$q^{-\ell}\prod_{\substack{p\le Y\\ p^{\gamma(p)}\nmid q}}\left(1-\frac{j(p)}{p^{\gamma(p)\ell}}\right)\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell\cap W^q(Y)}e^{2\pi i g(\boldsymbol{s})a/q}\int_{[0,X]^\ell}\psi(\boldsymbol{x})d\boldsymbol{x},$$

as desired. It remains to bound the error term that results from our substitution of (39). This error term is the sum of a first term of order qE and $2^\ell-1$ terms of the form

$$qE\left(\int_{[0,X]^m}\frac{\partial^m\psi}{\partial x_{j_1}\cdots\partial x_{j_m}}(\star)\,dx_{j_1}\cdots dx_{j_m}\right).$$

Iteratively applying the product rule, we see that $\frac{\partial^m\psi}{\partial x_{j_1}\cdots\partial x_{j_m}}$ is the sum of less than $m!$ terms bounded in absolute value by $(2\pi k^m J|\beta|)^j X^{jk-m}$ for some $1\le j\le m$. In particular, each integral is bounded by

$$\ell!\max_{1\le j\le\ell}(2\pi k^\ell JX^k|\beta|)^j\le\ell!(1+2\pi k^\ell JX^k|\beta|)^\ell,$$

and the error bound follows. □

7.3 Local cancellation

In this section, we apply Theorem 1.4 to establish the necessary cancellation in our sieved local exponential sums, yielding item (ii) in Theorem 3.9. We begin by invoking a multivariate version of Hensel's Lemma that allows us to reduce to the case of prime moduli. This statement in particular follows from Theorem 1.1 of [5].

Lemma 7.6 (Multivariable Hensel's Lemma)**.** *Suppose $\ell\in\mathbb{N}$, $g\in\mathbb{Z}[x_1,\dots,x_\ell]$, p is prime, $\boldsymbol{n}\in\mathbb{Z}^\ell$, and $\gamma,\nu\in\mathbb{N}$ with $\nu\ge 2\gamma-1$. If*

$$g(\boldsymbol{n})\equiv 0 \bmod p^{2\gamma-1}$$

and $\nabla g(\boldsymbol{n})\not\equiv\boldsymbol{0}\bmod p^\gamma$, then there exists $\boldsymbol{m}\in\mathbb{Z}^\ell$ with $g(\boldsymbol{m})\equiv 0\bmod p^\nu$.

We now prove the following multivariate generalization of Lemma 4.3 in [28].

Lemma 7.7. *Suppose $\ell \in \mathbb{N}$, $g \in \mathbb{Z}[x_1,\dots,x_\ell]$ with $\deg(g) = k \geq 2$, and $Y > 0$. If $q \in \mathbb{N}$ has prime factorization $q = p_1^{v_1}\cdots p_r^{v_r}$ with $p_1 < \cdots < p_t \leq Y < p_{t+1} < \cdots < p_r$, and $(a,q) = 1$, then*

$$\left|\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell \cap W^q(Y)} e^{2\pi i g(\boldsymbol{s})a/q}\right| \leq C_1 \prod_{i=1}^{t}\Big((k-1)^\ell p_i^{\ell/2} + j(p_i)\Big)\prod_{i=t+1}^{r} C_2(v_i+1)^\ell p_i^{v_i(\ell-1/k)},$$

where $C_2 = C_2(k)$ and C_1 depends only on the moduli at which ∇g identically vanishes and the primes $p \leq Y$ dividing q modulo which g is not Deligne. Further, the sum is 0 if $v_i \geq 2\gamma(p_i)$ for some $1 \leq i \leq t$.

Proof. Factor $q = p_1^{v_1}\cdots p_r^{v_r}$ as in the lemma. By the Chinese Remainder Theorem, we have

$$\sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell \cap W^q(Y)} e^{2\pi i g(\boldsymbol{s})a/q} = \prod_{m=1}^{r}\sum_{\boldsymbol{s}\in\{0,\dots,p_m^{v_m}-1\}^\ell \cap W^{p_m^{v_m}}(Y)} e^{2\pi i g(\boldsymbol{s})a_m/p_m^{v_m}},$$

where $a_1,\dots,a_r$ are the unique residues satisfying $a/q \equiv a_1/p_1^{v_1} + \cdots + a_r/p_r^{v_r} \bmod 1$.

Suppose $p^v = p_m^{v_m}$ with $\gamma(p) > 1$ and $v < 2\gamma(p)$. By definition of γ, ∇g identically vanishes modulo $p^{\gamma(p)-1}$. Since $p^{2\gamma(p)-1} \leq p^{3(\gamma(p)-1)}$, we can bound p^v by the cube of a modulus at which ∇g identically vanishes, trivially bound the corresponding sum, and absorb it into the constant C_1 in the conclusion of the lemma.

Next suppose $p^v = p_m^{v_m}$ with $p \leq Y$ and $v = \gamma(p) = 1$. Recalling that $j(p)$ is the number of zeros of ∇g modulo p and applying Theorem 1.4, we have for $p \nmid b$ that

$$\left|\sum_{\boldsymbol{s}\in\{0,\dots,p-1\}^\ell \cap W^p(Y)} e^{2\pi i g(\boldsymbol{s})b/p}\right| \leq (k-1)^\ell p^{\ell/2} + j(p),$$

provided g is Deligne modulo p, and the remaining such primes are absorbed into C_1.

Now suppose that $p^v = p_m^{v_m}$ with $p \leq Y$ and $v \geq 2\gamma(p)$, and let $w = 2\gamma(p) - 1$. If $\boldsymbol{s} \in \{0,\dots,p^v-1\}^\ell$ and $\tilde{\boldsymbol{s}}$ is the reduced residue class of $\boldsymbol{s}$ modulo p^w, then we have that $g(\boldsymbol{s}) \equiv p^w t + g(\tilde{\boldsymbol{s}}) \pmod{p^v}$ for some $0 \leq t \leq p^{v-w}-1$. Conversely, if $\tilde{\boldsymbol{s}} \in \{0,\dots,p^w-1\}^\ell$ with $\nabla g(\tilde{\boldsymbol{s}}) \not\equiv \boldsymbol{0} \pmod{p^{\gamma(p)}}$, then for every $0 \leq t \leq p^{v-w}-1$, Lemma 7.6 applied to the polynomial $g(\boldsymbol{x}) - (p^w t + g(\tilde{\boldsymbol{s}}))$ yields $\boldsymbol{s} \in \{0,\dots,p^v-1\}^\ell$ with $g(\boldsymbol{s}) \equiv p^w t + g(\tilde{\boldsymbol{s}}) \pmod{p^v}$.

In other words, the map F on $\mathbb{Z}/p^{v-w}\mathbb{Z}$ defined by $g(p^w t + \tilde{\boldsymbol{s}}) \equiv p^w F(t) + g(\tilde{\boldsymbol{s}}) \pmod{p^v}$ is a bijection. In particular, if $p \nmid b$, then

$$\begin{aligned}
\sum_{\boldsymbol{s}\in\{0,\dots,p^v-1\}^\ell \cap W^{p^v}(Y)} e^{2\pi i g(\boldsymbol{s})b/p^v} &= \sum_{\substack{\tilde{\boldsymbol{s}}\in\{0,\dots,p^w-1\}^\ell \\ \nabla g(\tilde{\boldsymbol{s}})\not\equiv\boldsymbol{0} \pmod{p^{\gamma(p)}}}} \sum_{t=0}^{p^{v-w}-1} e^{2\pi i g(p^w t+\tilde{\boldsymbol{s}})b/p^v} \\
&= \sum_{\substack{\tilde{\boldsymbol{s}}\in\{0,\dots,p^w-1\}^\ell \\ \nabla g(\tilde{\boldsymbol{s}})\not\equiv\boldsymbol{0} \pmod{p^{\gamma(p)}}}} \sum_{t=0}^{p^{v-w}-1} e^{2\pi i (p^w t+g(\tilde{\boldsymbol{s}}))b/p^v} \\
&= 0,
\end{aligned}$$

where the last equality is the fact that the sum in t runs over the full collection of p^{v-w}-th roots of unity. Finally, suppose $p^v = p_m^{v_m}$ with $p > Y$. We note that $W^{p^v}(Y) = \mathbb{N}$ and we only exploit cancellation in a single variable. To this end, for each $\tilde{\boldsymbol{s}} = (s_2, \dots, s_\ell) \in \{0, \dots, p^v - 1\}^{\ell-1}$, we define $\tilde{g}$ by $\tilde{g}(x) = g(x, \tilde{\boldsymbol{s}})$. Utilizing the standard single-variable complete sum estimate (see [4] for example), we have for $b \nmid p$ that

$$\left| \sum_{\boldsymbol{s} \in \{0,\dots,p^v-1\}^\ell} e^{2\pi i g(\boldsymbol{s}) b/p^v} \right| \le \sum_{\tilde{\boldsymbol{s}} \in \{0,\dots,p^v-1\}^{\ell-1}} \left| \sum_{s=0}^{p^v-1} e^{2\pi i \tilde{g}(s) b/p^v} \right| \ll_k p^{v(1-1/k)} \sum_{\tilde{\boldsymbol{s}} \in \{0,\dots,p^v-1\}^{\ell-1}} \gcd(\mathrm{cont}(\tilde{g}), p^v)^{1/k}.$$

To analyze the remaining sum, we note that at the expense of the term $\gcd(\mathrm{cont}(g), p^v)^{1/k}$ in our final estimate, we can cancel factors of p from the coefficients of g and assume that $p \nmid \mathrm{cont}(g)$. In this case, suppose $a_{\boldsymbol{i}} = a_{i_1,\dots,i_\ell}$ with $0 < |\boldsymbol{i}| \le k$ is a coefficient of g, corresponding to $x_1^{i_1} \cdots x_\ell^{i_\ell}$, that is not divisible by p. Further, assume that $i_1 > 0$, as if $i_1 = 0$ then we could just relabel our coordinates. In this case, for each $0 \le w \le v$, $\gcd(\mathrm{cont}(\tilde{g}), p^v) = p^w$ only if $p^w \mid s_2^{i_2} \cdots s_\ell^{i_\ell}$, so in particular $p^{\lceil w/k \rceil} \mid s_2 \cdots s_\ell$, which occurs for fewer than $(w+1)^{\ell-1} p^{v(\ell-1)-w/k}$ choices of $\tilde{\boldsymbol{s}}$. In particular,

$$\begin{aligned} \sum_{\tilde{s} \in \{0,\dots,p^v-1\}^{\ell-1}} \gcd(\mathrm{cont}(\tilde{g}), p^v)^{1/k} &\le \gcd(\mathrm{cont}(g), p^v)^{1/k} \sum_{w=0}^{v} (w+1)^{\ell-1} p^{v(\ell-1)-w/k} p^{w/k} \\ &\le (v+1)^\ell \gcd(\mathrm{cont}(g), p^v)^{1/k} p^{v(\ell-1)}. \end{aligned}$$

The $\gcd(\mathrm{cont}(g), p^v)^{1/k}$ term can be absorbed into C_1, and the remaining bound on the exponential sum modulo p^v is a constant depending on k times $p^{v(1-1/k)}(v+1)^\ell p^{\ell(v-1)} = (v+1)^\ell p^{v(\ell-1/k)}$, as required. Having accounted for all prime divisors of q, the proof is complete. □

Lemma 7.7 combines with Lemma 3.3 as well as the estimates $\prod_{p \mid q} \left(1 + \frac{C}{p}\right) \le (q/\phi(q))^C$ and $\prod_{p \mid q} \left(1 + \frac{C}{p^{3/2}}\right) \ll_C 1$ to yield item (ii) of Theorem 3.9, restated below.

Corollary 7.8. *If $\ell \ge 2$, $g \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $\deg(g) = k \ge 2$, and $(a, q) = 1$, then*

$$\left| \sum_{\boldsymbol{s} \in \{0,\dots,q-1\}^\ell \cap W^q(Y)} e^{2\pi i g(\boldsymbol{s}) a/q} \right| \le C_1 \begin{cases} (k-1)^{\ell\omega(q)} \Phi(q,\ell) q^{\ell/2} & \text{if } q \le Y \\ C_2^{\omega(q)} \tau(q)^\ell q^{\ell-1/k} & \text{for all } q \end{cases},$$

where $C_2 = C_2(k)$, $\Phi(q,2) = (q/\phi(q))^{C_2}$, $\Phi(q,\ell) \ll_{k,\ell} 1$ for $\ell \ge 3$, and C_1 depends only on the moduli at which ∇g identically vanishes and the primes $p \le Y$ dividing q modulo which g is not Deligne.

7.4 Oscillatory integral estimate

In order to establish (28) in the case that α is close, but not too close, to a rational with very small denominator, we need to control the oscillatory integral in the asymptotic formula given by Lemma 7.5. To achieve this, we invoke the following standard estimate, given for example in Lemma 2.8 of [38].

Lemma 7.9 (Van der Corput's Lemma)**.** *If $X > 0$, $\beta \neq 0$, $k \in \mathbb{N}$, and $g \in \mathbb{Z}[x]$ with $\deg(g) = k$, then*

$$\left| \int_0^X e^{2\pi i g(x)\beta} dx \right| \ll |\beta|^{-1/k}.$$

Utilizing Lemma 7.9 to exploit cancellation in a single variable, then trivially bounding the integral in the remaining variables, we have the following bound for the integral in the conclusion of Lemma 7.5.

Corollary 7.10. *If $X > 0$, $\beta \neq 0$, $k, \ell \in \mathbb{N}$, and $g \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $\deg(g) = k$, then*

$$\left| \int_{[0,X]^\ell} e^{2\pi i g(\boldsymbol{x})\beta} d\boldsymbol{x} \right| \ll \min\{X^\ell, X^{\ell-1}|\beta|^{-1/k}\}.$$

7.5 Minor arc estimates

In an effort to establish item (iii) of Theorem 3.9, we begin by invoking a variation of the most traditional minor arc estimate, Weyl's Inequality.

Lemma 7.11 (Lemma 3, [7])**.** *Suppose $k \in \mathbb{N}$, $g(x) = a_0 + a_1 x + \cdots + a_k x^k$ with $a_0 \dots, a_k \in \mathbb{R}$ and $a_k \in \mathbb{N}$. If $X > 0$, $a, q \in \mathbb{N}$ with $(a,q) = 1$, and $|\alpha - a/q| < q^{-2}$, then*

$$\left| \sum_{n=1}^{X} e^{2\pi i g(n)\alpha} \right| \ll_k X \left(a_k \log^{k^2}(a_k q X) \left(q^{-1} + X^{-1} + \frac{q}{a_k X^k} \right) \right)^{2^{-k}}.$$

We now carefully adapt Lemma 7.11 to our particular sieve, and to the multivariate setting, though as in Corollary 7.10, we ultimately only exploit cancellation in a single variable.

Lemma 7.12. *Suppose $k, \ell \in \mathbb{N}$ and $g(\boldsymbol{x}) = \sum_{|\boldsymbol{i}| \leq k} a_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $\deg(g) = k$. Suppose further that $X, Y, Z \geq 2$, $YZ \leq X$, and $a, q \in \mathbb{N}$ with $(a,q) = 1$, and let $J = \sum_{|\boldsymbol{i}| \leq k} |a_{\boldsymbol{i}}|$. If $|\alpha - a/q| < q^{-2}$, then*

$$\left| \sum_{\boldsymbol{n} \in [1,X]^\ell \cap W(Y)} e^{2\pi i g(\boldsymbol{n})\alpha} \right| \ll_{k,\ell} \mathrm{cont}(g)^6 (\log Y)^{ek} X^\ell \left(e^{-\frac{\log Z}{\log Y}} + \left(J \log^{k^2}(JqX) \left(q^{-1} + \frac{Z}{X} + \frac{qZ^k}{X^k} \right) \right)^{2^{-k}} \right).$$

Proof. Suppose $k, \ell \in \mathbb{N}$ and $g(\boldsymbol{x}) = \sum_{|\boldsymbol{i}| \leq k} a_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{Z}[x_1, \dots, x_\ell]$ with $\deg(g) = k$. We begin by conducting an invertible (over $\mathbb{Z}$) change of variables to reduce to the case where the x_1^k coefficient $a_{(k,0,\dots,0)}$ is nonzero. To this end, consider the polynomial $\tilde{g} \in \mathbb{Z}[x_2, \dots, x_\ell]$ defined by $\tilde{g}(x_2, \dots, x_\ell) = g^k(1, x_2, \dots, x_\ell)$, where g^k denotes the top degree homogeneous part of g, noting that $\tilde{g}$ is not identically zero. Let $(c_2, \dots, c_\ell) \in \{0, 1, \dots, k\}^{\ell-1}$ be such that $\tilde{g}(c_2, \dots, c_\ell) \neq 0$.

As an aside, the existence of such a "small integer non-root" of a general nonzero multivariate polynomial $F \in \mathbb{Z}[x_1, \dots, x_j]$ can be shown via induction, which we sketch here. The base case $j = 1$ corresponds to nonzero univariate polynomials, which have at most k roots, hence at least one non-root in $\{0, 1, \dots, k\}$. Then, for higher degrees, fix one variable that appears at least once in F (without loss of generality,

assume x_1 appears at least once), let d be the degree of F as a polynomial in x_1 only, and let $\tilde{F}(x_2,\dots,x_j)$ be the polynomial of degree at most $k-d$ that forms the x_1^d coefficient. By the inductive hypothesis, we can choose $(m_2,\dots,m_j)\in\{0,\dots,k\}^{j-1}$ such that $\tilde{F}(m_2,\dots,m_j)\neq 0$. Then, $F(x_1,m_2,\dots,m_j)$ is a nonzero degree-d polyomial in x_1, which has a non-root in $\{0,\dots,k\}$, completing the induction.

Back to the proof at hand, we see that the change of variables $x_1=y_1$ and $x_j=y_j+c_jy_1$ for $2\le j\le \ell$ yields a y_1^k coefficient of $\tilde{g}(c_2,\dots,c_\ell)\neq 0$. Let M denote the $\ell\times\ell$ matrix satisfying $M\boldsymbol{x}=\boldsymbol{y}$ corresponding to the described change of variables, and let $f(y_1,\dots,y_\ell)=\sum_{|\boldsymbol{i}|\le k} b_{\boldsymbol{i}}\boldsymbol{y}^{\boldsymbol{i}}$ be the polynomial satisfying $f(\boldsymbol{y})=g(M^{-1}\boldsymbol{y})$. By taking the complex conjugate of the relevant exponential sum if necessary, we can assume that $b=b_{(k,0,\dots,0)}>0$. Further, the effect of the transformation on the size of this coefficient is well-controlled, in that $b\ll_{k,l} J$.

Let $T=M([1,X]^\ell)$, so

$$\sum_{\boldsymbol{n}\in[1,X]^\ell\cap W(Y)} e^{2\pi i g(\boldsymbol{n})\alpha}=\sum_{\boldsymbol{n}\in T\cap W(Y)} e^{2\pi i f(\boldsymbol{n})\alpha},$$

where $W(Y)$ is defined on each side in terms of the corresponding polynomial.

Let $\tilde{T}$ denote the projection of T onto the last $\ell-1$ coordinates, noting that $|\tilde{T}|\le(2kX)^{\ell-1}$ due to the details of our change of variables. For each fixed $\tilde{\boldsymbol{n}}=(n_2,\dots,n_\ell)\in\mathbb{N}^{\ell-1}$, we let $I=\{n\in\mathbb{N}:(n,\tilde{\boldsymbol{n}})\in T\}$, which is an interval of integers of length at most X, we let $\tilde{W}(Y)=\{n\in\mathbb{N}:(n,\tilde{\boldsymbol{n}})\in W(Y)\}$, and we let $\tilde{f}(x)=f(x,\tilde{\boldsymbol{n}})$. We see trivially that

$$\left|\sum_{\boldsymbol{n}\in T\cap W(Y)} e^{2\pi i f(\boldsymbol{n})\alpha}\right|\le(2kX)^{\ell-1}\max_{\tilde{\boldsymbol{n}}\in\tilde{T}}\left|\sum_{n\in I\cap\tilde{W}(Y)} e^{2\pi i\tilde{f}(n)\alpha}\right|. \tag{40}$$

We now proceed with $\tilde{\boldsymbol{n}}=(n_2,\dots,n_\ell)$ fixed, and we define L and m so that $I=[m,L+m]$, so in particular $L\le X$. All subsequent conclusions will be independent of $\tilde{\boldsymbol{n}}$. Let P be the set of products $p_1^{\gamma(p_1)}\cdots p_s^{\gamma(p_s)}$ for primes $p_1<\cdots<p_s\le Y$, let P_1 denote the set of elements of P that are at most Z, and let P_2 denote the set of elements of P that are greater than Z.

By inclusion-exclusion, we have

$$\left|\sum_{n\in I\cap\tilde{W}(Y)} e^{2\pi i\tilde{f}(n)\alpha}\right|=\left|\sum_{D\in P}(-1)^{\omega(D)}\sum_{\substack{n\in I\\ \nabla f(n,\tilde{\boldsymbol{n}})\equiv\boldsymbol{0}\ (\mathrm{mod}\ D)}} e^{2\pi i\tilde{f}(n)\alpha}\right|, \tag{41}$$

where $\omega(D)$ is the number of distinct prime factors of D. For $D\in P_1$, we use the fact that the set of n for which $\nabla f(n,\tilde{\boldsymbol{n}})\equiv\boldsymbol{0}\ (\mathrm{mod}\ D)$ is contained in the set of n for which $\tilde{f}'(n)\equiv 0\ (\mathrm{mod}\ D)$. Noting that $\tilde{f}'$ can have at most k roots modulo any prime at which it does not identically vanish, we have

$$\left|\sum_{D\in P_1}(-1)^{\omega(D)}\sum_{\substack{n\in I\\ \nabla f(n,\tilde{\boldsymbol{n}})\equiv\boldsymbol{0}\ (\mathrm{mod}\ D)}} e^{2\pi i\tilde{f}(n)\alpha}\right|\ll_k(\mathrm{cont}(g))^2\sum_{D\in P_1}k^{\omega(D)}\max_{0\le c\le D}\left|\sum_{n=0}^{L/D} e^{2\pi i\tilde{f}(Dn+m+c)\alpha}\right|,$$

where the $\mathrm{cont}(g)^2$ term accounts for the primes p for which $\gamma(p) > 1$ by Proposition 3.6. Further, we see from Lemma 7.11 and the estimate $1 \le b \ll_{k,l} J$ that

$$\begin{aligned}\sum_{D\in P_1} k^{\omega(D)} \max_{0\le c\le D}\left|\sum_{n=0}^{L/D} e^{2\pi i \tilde{f}(Dn+m+c)\alpha}\right| &\ll_{k,l} \sum_{D\in P_1} k^{\omega(D)}\frac{L}{D}\left(b\log^{k^2}(bqL)\left(q^{-1}+\frac{D}{L}+\frac{qD^k}{bL^k}\right)\right)^{2^{-k}}\\ &\ll_{k,l} X\left(J\log^{k^2}(JqX)\left(q^{-1}+\frac{Z}{X}+\frac{qZ^k}{X^k}\right)\right)^{2^{-k}}\sum_{D\in P_1}\frac{k^{\omega(D)}}{D}\\ &\ll_{k,l} X(\log Y)^k\left(J\log^{k^2}(JqX)\left(q^{-1}+\frac{Z}{X}+\frac{qZ^k}{X^k}\right)\right)^{2^{-k}},\end{aligned}$$

where the last inequality uses that if $C > 0$, then

$$\sum_{D\in P}\frac{C^{\omega(D)}}{D} = \prod_{p\le Y}\left(1+\frac{C}{p^{\gamma(p)}}\right) \le \prod_{p\le Y}\left(1+\frac{C}{p}\right) \ll (\log Y)^C. \tag{42}$$

This combines with (40) to close the book on the contributions to (41) from P_1. It remains to account for the contribution to (41) from P_2. Because P_2 has so many elements, it is crucial for us to exploit the cancellation provided by the term $(-1)^{\omega(D)}$.

To this end, for a fixed $n \in I$, let $P^n = \{D \in P : \nabla f(n,\tilde{\boldsymbol{n}}) \equiv \mathbf{0} \pmod D\}$, and let $P_2^n = P^n \cap P_2$. The only issue is the possibility that way more elements of P_n^2 have an even number of prime factors than odd, or vice versa, which we show below does not happen.

Let q be the largest prime power of the form $p^{\gamma(p)}$ with $p \le Y$, and let q_n be the largest such prime power lying in P^n, noting that $q_n \le q \ll_k \mathrm{cont}(g)Y$ by Proposition 3.6. Let A denote the set of elements of P^n that have an even number of prime factors, let B denote the set of elements of P^n that have odd number of prime factors, and let A' and B', respectively, denote the same for elements of P_2^n. The quantity we need control of is $||A'|-|B'||$.

Let A_1 be the elements of A that are greater than Z and not divisible by q_n, and let A_2 be the elements of A that are greater than q_nZ and divisible by q_n. Likewise define B_1 and B_2. The map $D \to q_nD$ defines an injection from A_1 to B_2, while the map $D \to D/q_n$ defines an injection from A_2 to B_1. Letting A_3 denote all the elements of A greater than q_nZ, we have

$$|A_3| \le |A_1|+|A_2| \le |B_1|+|B_2| \le |B'|.$$

Symmetrically, we have $|B_3| \le |A'|$. Finally, letting A_4 and B_4 denote the elements of A' and B' satisfying $Z < D \le q_nZ$, we have $|A'| = |A_3|+|A_4| \le |B'|+|A_4|$ and similarly $|B'| \le |A'|+|B_4|$, so the magnitude of $|A'|-|B'|$ is bounded above by $|A_4|+|B_4|$, which is the size of the set $\overline{P^n}$ of elements of P^n satisfying $Z < D \le q_nZ$.

We now see

$$\begin{aligned}\left|\sum_{D\in P_2}(-1)^{\omega(D)}\sum_{\substack{n\in I\\ \nabla f(n,\tilde{\boldsymbol{n}})\equiv\mathbf{0}\ (\mathrm{mod}\ D)}}e^{2\pi i\tilde{f}(n)\alpha}\right| &= \left|\sum_{n\in I}e^{2\pi i\tilde{f}(n)\alpha}\sum_{D\in P_2^n}(-1)^{\omega(D)}\right|\\ &\le \sum_{n\in I}|\overline{P^n}|\\ &= \sum_{\substack{D\in P\\ Z<D\le qZ}}|\{n\in I:\nabla f(n,\tilde{\boldsymbol{n}})\equiv\mathbf{0}\ (\mathrm{mod}\ D)\}|\\ &\ll_k (\mathrm{cont}(g))^2\sum_{\substack{D\in P\\ Z<D\le qZ}}k^{\omega(D)}\left(\frac{L}{D}+1\right)\\ &\ll (\mathrm{cont}(g))^3X\sum_{\substack{D\in P\\ D>Z}}\frac{k^{\omega(D)}}{D},\end{aligned}$$

provided $YZ\le X$. If $D\in P$ with $D>Z$, then, since $D\ll_k \mathrm{cont}(g)^2Y^{\omega(D)}$ and $Y\ge 2$, we know that

$$\mathrm{cont}(g)^3e^{\omega(D)-\frac{\log Z}{\log Y}}\gg_k 1. \tag{43}$$

Finally, (42) and (43) imply

$$\begin{aligned}\sum_{\substack{D\in P\\ D>Z}}\frac{k^{\omega(D)}}{D} &\ll_k \mathrm{cont}(g)^3e^{-\frac{\log Z}{\log Y}}\sum_{D\in P}\frac{(ek)^{\omega(D)}}{D}\\ &\ll \mathrm{cont}(g)^3e^{-\frac{\log Z}{\log Y}}(\log Y)^{ek},\end{aligned}$$

and the lemma follows. □

We now conclude our discussion by combining the tools developed in this section to establish (27) and (28), thus completing the proof of Theorem 2.4.

7.6 Proof of (27) and (28)

We return to the proof of Lemma 4.2 in Section 4.4, recalling all assumptions, notation, and fixed parameters. We let $Z=N^{c_0}$, and we let J denote the sum of the absolute value of the coefficients of h_d, noting that

$$J\ll_h d^k\le Z^k. \tag{44}$$

Fixing $\alpha\in\mathbb{T}$, the pigeonhole principle guarantees the existence of $1\le q\le M^k/Z^{3k}$ and $(a,q)=1$ such that

$$\left|\alpha-\frac{a}{q}\right|<\frac{Z^{3k}}{qM^k}.$$

Letting $\beta = \alpha - a/q$, we have by Lemma 7.5, as well as Lemma 3.3, Proposition 3.6, and Lemma 3.8, that

$$S(\alpha) = \frac{w}{w_q q^\ell} \sum_{\boldsymbol{s}\in\{0,\dots,q-1\}^\ell \cap W^q(Y)} e^{2\pi i g(\boldsymbol{s})a/q} \int_{[0,M]^\ell} e^{2\pi i g(\boldsymbol{x})\beta} d\boldsymbol{x} + O_h\left(qM^{\ell-1}\log^C(Y)Z^{4k\ell}\right), \tag{45}$$

where

$$w_q = \prod_{\substack{p\le Y \\ p^{\gamma(p)}|q}} \left(1 - \frac{j_d(p)}{p^{\gamma_d(p)\ell}}\right) \gg_h 1.$$

Combining (45) with Corollary 7.8, Lemma 3.8, and Corollary 7.10 yields (27) if

$$q \le Q \text{ and } |\beta| < \gamma,$$

as well as (28) if

$$q \le Q \text{ and } |\beta| \ge \gamma \quad \text{or} \quad Q \le q \le Z^{3k}.$$

For this latter conclusion, when applying Corollary 7.8 we use standard estimates that assure

$$C^{\omega(q)}\tau(q)^\ell \ll_{k,\ell,\varepsilon} q^\varepsilon$$

for all $\varepsilon > 0$. Finally, it follows from Lemma 7.12 and Proposition 3.8 that (28) holds whenever $Z^{3k} \le q \le M^k/Z^{3k}$. □

Acknowledgments

The authors would like to thank Neil Lyall, Ákos Magyar, Steve Gonek, and Paul Pollack for their helpful conversations and references. The authors would also like to thank the anonymous referee for their comments and suggestions. The second author would like to thank Gouquan Li for alerting him to an oversight in the proof of Lemma 4.5 in [28], which is rectified in the proof of Lemma 7.12 in this paper.

References

[1] A. BALOG, J. PELIKÁN, J. PINTZ, E. SZEMERÉDI, *Difference sets without κ-th powers*, Acta. Math. Hungar. 65 (2) (1994), 165-187. 3

[2] B. BIRCH, *Forms in many variables*, Proc. Royal Soc. London. Ser. A. 265.1321 (1962), 245-263. 9

[3] T. BLOOM, J. MAYNARD, *A new upper bound for sets with no square differences*, preprint (2020), `arxiv:2011.13266`. 3, 4

[4] J.R. CHEN, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719. 38

[5] K. CONRAD, *A multivariable Hensel's lemma*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf 36

[6] B. COOK, A. MAGYAR, *Diophantine equations in the primes*, Inven. Math. 198 (2014), 701-737. 9

[7] E. CROOT, N. LYALL, A. RICE, *Polynomials and primes in generalized arithmetic progressions*, Int. Math. Res. Not., no. 15 (2015), 6021-6043. 39

[8] P. DELIGNE, *La conjecture de Weil I*, Pub. Math. I.H.E.S. 43 (1974), 273-307. 4, 5

[9] W. FULTON, *Intersection theory*, Second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics **2**, Springer-Verlag, Berlin, 1998. 21

[10] H. FURSTENBERG, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), 204-256. 2

[11] B. GREEN, *On arithmetic structures in dense sets of integers*, Duke Math. Jour. 114 (2002) no.2, 215-238. 3

[12] B. GREEN, T. TAO, T. ZIEGLER, *A Fourier-free proof of the Furstenberg-Sárközy theorem*, https://terrytao.wordpress.com/2013/02/28/a-fourier-free-proof-of-the-furstenberg-sarkozy-theorem/. 3

[13] R. HALL, G. TENANBAUM, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, 1990. 21

[14] M. HAMEL, N. LYALL, A. RICE, *Improved bounds on Sárközy's theorem for quadratic polynomials*, Int. Math. Res. Not. no. 8 (2013), 1761-1782 3

[15] R. HARTSHORNE, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer-Verlag, New York-Heidelberg, 1977. 26

[16] M. HINDRY AND J. H. SILVERMAN, *Diophantine geometry: an introduction*, Grad. Texts in Math. **201**, Springer-Verlag, New York, 2000. 6

[17] J.-P. JOUANOLOU, *Théorèmes de Bertini et applications*, Progress in Mathematics **42**, Birkhäuser, Boston, 1983. 26

[18] T. KAMAE, M. MENDÈS FRANCE, *van der Corput's difference theorem*, Israel J. Math. 31, no. 3-4, (1978), pp. 335-342. 3

[19] S. LANG AND A. WEIL, *Number of points of varieties in finite fields*, Amer. J. Math. 76 (1954), 819-827. 22

[20] M. LEWKO, *An improved lower bound related to the Sárközy-Furstenberg Theorem*, Electron. J. Combin. 22 (2015), No. 32, 1-6. 5

[21] H.-Z. LI, H. PAN, *Difference sets and polynomials of prime variables*, Acta. Arith. 138, no. 1 (2009), 25-52. 3

[22] N. LYALL, À. MAGYAR, *Polynomial configurations in difference sets*, J. Number Theory 129 (2009), 439-450. 3, 17

[23] J. LUCIER, *Intersective sets given by a polynomial*, Acta Arith. 123 (2006), 57-95. 3, 17, 18

[24] J. LUCIER, *Difference sets and shifted primes*, Acta. Math. Hungar. 120 (2008), 79-102. 3

[25] N. LYALL, *A new proof of Sárközy's theorem*, Proc. Amer. Math. Soc. 141 (2013), 2253-2264. 3, 5

[26] J. PINTZ, W. L. STEIGER, E. SZEMERÉDI, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. 37 (1988), 219-231. 2, 3

[27] B. POONEN, K. SLAVOV, *The exceptional locus in the Bertini irreducibility theorem for a morphism*, preprint (2020), `arXiv:2001.08672v2`. 22

[28] A. RICE, *A maximal extension of the best-known bounds for the Furstenberg-Sárközy Theorem*, Acta Arith. 187 (2019), 1-41. 3, 4, 10, 12, 13, 16, 17, 21, 31, 36, 43

[29] A. RICE, *Improvements and extensions of two theorems of Sárközy*, Ph.D. thesis, University of Georgia, 2012. http://alexricemath.com/wp-content/uploads/2013/06/AlexThesis.pdf. 18

[30] A. RICE, *Sárközy's theorem for $\mathcal{P}$-intersective polynomials*, Acta Arith. 157 (2013), no. 1, 69-89. 3, 17

[31] A. RICE, *Binary quadratic forms in difference sets*, Combinatorial and Additive Number Theory III, Springer Proc. of Math. and Stat., vol. 297 (2020), 175-196. 3, 4, 11

[32] I. RUZSA, T. SANDERS, *Difference sets and the primes*, Acta. Arith. 131, no. 3 (2008), 281-301. 2, 3, 11, 17, 18, 21

[33] I. RUZSA, *Difference sets without squares*, Period. Math. Hungar. 15 (1984), 205-209. 5

[34] I. RUZSA, *On measures on intersectivity*, Acta Math. Hungar. 43(3-4) (1984), 335-340. 5

[35] A. SÁRKÖZY, *On difference sets of sequences of integers I*, Acta. Math. Hungar. 31(1-2) (1978), 125-149. 2, 3, 17

[36] A. SÁRKÖZY, *On difference sets of sequences of integers III*, Acta. Math. Hungar. 31(3-4) (1978), 355-386. 2

[37] S. SLIJEPČEVIĆ, *A polynomial Sárközy-Furstenberg theorem with upper bounds*, Acta Math. Hungar. 98 (2003), 275-280. 3

[38] R. C. VAUGHAN, *The Hardy-Littlewood method*, Cambridge University Press, Second Edition, 1997. 38

[39] R. WANG, *On a theorem of Sárközy for difference sets and shifted primes*, Journal of Number Theory, Volume 211 (2020), 220-234. 2, 3

[40] M. WESSEL, *An algebraic interpretation of the polynomial Szemerédi theorem*, Universiteit Utrecht Bachelor thesis (2020). 5

[41] K. YOUNIS, *Lower bounds in the polynomial Szemerédi theorem*, preprint (2019), arXiv:1908.06058. 5

AUTHORS

John R. Doyle
Department of Mathematics
Oklahoma State University
Stillwater, OK 74078, USA
john.r.doyle@okstate.edu
https://math.okstate.edu/people/jdoyle/

Alex Rice
Department of Mathematics
Millsaps College
Jackson, MS 39210, USA
riceaj@millsaps.edu
https://alexricemath.com/