A MAXIMAL EXTENSION OF THE BEST-KNOWN BOUNDS FOR THE FURSTENBERG-SÁRKÖZY THEOREM

ALEX RICE

Abstract. We show that if $h \in \mathbb{Z}[x]$ is a polynomial of degree $k \geq 2$ such that $h(\mathbb{N})$ contains a multiple of q for every $q \in \mathbb{N}$, known as an *intersective polynomial*, then any subset of $\{1, 2, \ldots, N\}$ with no nonzero differences of the form $h(n)$ for $n \in \mathbb{N}$ has density at most a constant depending on h times $(\log N)^{-c \log \log \log \log N}$, where $c = (2 \log k)^{-1}$. Bounds of this type were previously known only for monomials and intersective quadratics, and this is currently the best-known bound for the original Furstenberg-Sárközy Theorem, i.e. $h(n) = n^2$. The intersective condition is necessary to force any density decay for polynomial difference-free sets, and in that sense our result is the maximal extension of this particular quantitative estimate. Further, we show that if $g, h \in \mathbb{Z}[x]$ are intersective, then any set lacking nonzero differences of the form $g(m) + h(n)$ for $m, n \in \mathbb{N}$ has density at most $\exp(-c(\log N)^{\mu})$, where $c = c(g, h) > 0$, $\mu = \mu(\deg(g), \deg(h)) > 0$, and $\mu(2, 2) = 1/2$. We also include a brief discussion of sums of three or more polynomials in the final section.

1. Introduction

1.1. **Background.** Lovász posed the following question: If $A \subseteq \mathbb{N}$ contains no pair of distinct elements that differ by a perfect square, must it be the case that

$$\lim_{N \to \infty} \frac{|A \cap [1, N]|}{N} = 0 \ ?$$

Here and throughout we use $[1, N]$ to denote $\{1, 2, \ldots, N\}$, and we use $|X|$ to denote the size of a finite set X. Furstenberg [4] answered this question in the affirmative via ergodic theory, specifically his correspondence principle, but obtained no quantitative information on the rate at which the density must decay. Independently, Sárközy [22] showed via Fourier analysis, specifically a density increment argument driven by the Hardy-Littlewood circle method, that if $A \subseteq [1, N]$ contains no nonzero square differences, then

$$\frac{|A|}{N} \ll \left(\frac{(\log \log N)^2}{\log N} \right)^{1/3}. \tag{1}$$

We use "$\ll$" to denote "less than a constant times", with subscripts indicating on what parameters, if any, the implied constant depends.

1.2. **Improvements and extensions.** Using a more intricate Fourier analytic argument, Pintz, Steiger, and Szemerédi [17] improved (1) to

$$\frac{|A|}{N} \ll (\log N)^{-c \log \log \log \log N}, \tag{2}$$

with $c = 1/12$.

A natural generalization of Lovász's question is to extend from perfect squares to the image of more general polynomials. Balog, Pelikan, Pintz, and Szemerédi [1] extended (2) to sets with no k-th power differences for a fixed $k \in \mathbb{N}$, with $c = 1/4$ and the implied constant depending on k.

More generally, to hope for such a result for a given nonzero polynomial $h \in \mathbb{Z}[x]$, it is clearly necessary that $h(\mathbb{N})$ contains a multiple of q for every $q \in \mathbb{N}$, as otherwise there is a set $q\mathbb{N}$ with positive density and no differences in the image of h. It follows from a theorem of Kamae and Mendès France [9] that this condition is also sufficient, in a qualitative sense, and in this case we say that h is an *intersective polynomial*.

2000 *Mathematics Subject Classification.* 11B30.

Equivalently, a nonzero polynomial is intersective if it has a p-adic integer root for every prime p. Examples of intersective polynomials include any nonzero polynomial with an integer root or two rational roots with coprime denominators. However, there are also intersective polynomials with no rational roots, such as $(x^3-19)(x^2+x+1)$.

It is a theorem of Lucier [14], with minor improvements exhibited by Lyall and Magyar [16] and the author [18], that if $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree $k \geq 2$ and $A \subseteq [1, N]$ has no nonzero differences in the image of h, then

$$\frac{|A|}{N} \ll_h \left(\frac{\log \log N}{\log N}\right)^{1/(k-1)}.$$

Further, Hamel, Lyall, and the author [7] extended (2) to all intersective polynomials of degree two, for any $c < 1/\log(3)$ and the implied constant depending on c and the polynomial.

Apart from the original results of Furstenberg and Sárközy, we have primarily alluded to the best-known results in each case, all established through versions of two Fourier analytic attacks. For an extensive literature of intermediate and related results, as well as alternative proofs, the reader may refer to (in chronological order) [23], [5], [25], [13], [21], [16], [12], [15], [19], and [6].

1.3. **Main results.** Here we adapt the Fourier analytic double iteration strategy first developed in [17] and extend (2) to the full collection of intersective polynomials.

Theorem 1.1. *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree $k \geq 2$ and $A \subseteq [1, N]$. If*

$$a - a' \neq h(n)$$

for all distinct pairs $a, a' \in A$ and all $n \in \mathbb{N}$, then

$$\frac{|A|}{N} \ll_h (\log N)^{-c \log \log \log \log N},$$

where $c = (2 \log k)^{-1}$.

By more closely mimicking the details of [1], one may be able to take the constant c in Theorem 1.1 to be an absolute constant, but for our exposition this choice of c is essentially optimal.

Further, we apply exponential sum estimates established in the proof of Theorem 1.1 in a more straightforward L^2 density increment, exhibiting stronger density bounds on sets free of nonzero differences that are the sum of two polynomial images.

Theorem 1.2. *Suppose $g, h \in \mathbb{Z}[x]$ are intersective polynomials and $A \subseteq [1, N]$. If*

$$a - a' \neq g(m) + h(n)$$

for all distinct pairs $a, a' \in A$ and all $m, n \in \mathbb{N}$, then

$$\frac{|A|}{N} \ll_{g,h} e^{-c(\log N)^{\mu}},$$

where $c = c(g, h) > 0$, $\mu = \mu(\deg(g), \deg(h)) > 0$, and $\mu(2, 2) = 1/2$.

Remark on generality of Theorem 1.2. We note that the necessary intersective condition makes perfect sense in a multivariable setting, and analogous results should hold for every intersective integral polynomial in several variables, not just diagonal forms. Further, there do exist intersective binary diagonal forms not covered in this theorem. For example, if p is a prime congruent to 1 modulo 90090 that is not the sum of two integer cubes (of which there are plenty), then, since p is a sum of two cubes modulo q for every $q \in \mathbb{N}$, $x^3 + y^3 - p$ is an intersective polynomial in two variables that cannot be expressed as the sum of two single-variable intersective polynomials.

1.4. **Lower bounds and conjectures.** For $k, N \in \mathbb{N}$, by fixing a prime $N^{1/k}/2 \leq p \leq N^{1/k}$ and letting

$$A = \{xp : 1 \leq x \leq p^{k-1}\},$$

we see that $A \subseteq [1, N]$ has no nonzero k-th power differences. More generally, for any polynomial $h \in \mathbb{Z}[x]$ of degree k, the greedy algorithm produces a set $A \subseteq [1, N]$ satisfying $|A| \gg_h N^{1-1/k}$ with no nonzero differences in the image of h.

Ruzsa [20] showed that if $q \in \mathbb{N}$ is squarefree and $B \subseteq \mathbb{Z}/q\mathbb{Z}$ has no nonzero differences that are k-th powers modulo q, then there exists $A \subseteq [1, N]$ with no nonzero k-th power differences satisfying $|A| \gg N^c$, where $c = (k - 1 + \log |B|/\log q)/k$, which is larger than the trivial construction with which we began this section. For $k = 2$, Lewko [11] utilized an extensive computer search and found an example with $q = 205$ and $|B| = 12$, yielding $c \approx 0.7334$, which is currently the best-known lower bound for the original square-difference question.

As Ruzsa remarks, if $k = 2$, then $\log |B|/\log q$ cannot exceed $1/2$ if q is prime, and he conjectured this to be the case for all squarefree q. This indicates that $N^{3/4}$ is a limitation of Ruzsa's construction for square difference-free sets. Further, an easy Fourier analytic argument yields that if p is prime and $A \subseteq (\mathbb{Z}/p\mathbb{Z})^2 = G$ has no nonzero differences of the form (t, t^2), a set of forbidden differences similar in density and structure to the squares in $[1, N]$, then $|A| \ll p^{3/2} = |G|^{3/4}$.

These observations could potentially be viewed as evidence toward $N^{3/4}$ as roughly the true threshold for avoiding square differences, but these heuristics are rather tenuous. In particular, the same Fourier analytic argument applied to $G = (\mathbb{Z}/p\mathbb{Z})^k$ gives an upper bound of about $|G|^{1-\frac{1}{2k}}$ for sets without differences of the form $(t, t^2, \dots, t^k)$, while Ruzsa's construction can beat this exponent for certain values of k. All of these questions are still massively open, and many believe that the thresholds actually grow faster than $N^{1-\epsilon}$ for any $\epsilon > 0$.

2. Preliminaries

In this section we make some preliminary definitions and observations required to execute the Fourier analytic double iteration strategy utilized to prove Theorem 1.1, as well as the more straightforward density increment utilized to prove Theorem 1.2. We also provide context and motivation in Section 2.4 for our most notable new ingredient, which is defined and discussed rigorously in Section 2.5.

2.1. **Fourier analysis and the circle method on $\mathbb{Z}/N\mathbb{Z}$.** We identify subsets of the interval $[1, N]$ with subsets of the finite group $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$, on which we utilize a normalized discrete Fourier transform. Specifically, for a function $F : \mathbb{Z}_N \to \mathbb{C}$, we define $\widehat{F} : \mathbb{Z}_N \to \mathbb{C}$ by

$$\widehat{F}(t) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} F(x) e^{-2\pi i x t/N}.$$

We analyze the Fourier analytic behavior of A using the Hardy-Littlewood circle method, decomposing the nonzero frequencies into two pieces: the points $t \in \mathbb{Z}_N$ such that t/N is close to a rational with small denominator, and the complement.

Definition 2.1. Given $N \in \mathbb{N}$ and $K, Q > 0$, we define, for each $q \in \mathbb{N}$ and $a \in [1, q]$,

$$\mathbf{M}_{a,q}(K) = \left\{ t \in \mathbb{Z}_N : \left| \frac{t}{N} - \frac{a}{q} \right| < \frac{K}{N} \right\} \quad \text{and} \quad \mathbf{M}_q(K) = \bigcup_{(a,q)=1} \mathbf{M}_{a,q}(K) \setminus \{0\}.$$

We then define $\mathfrak{M}(K, Q)$, the *major arcs*, by

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

and $\mathfrak{m}(K, Q)$, the *minor arcs*, by $\mathfrak{m}(K, Q) = \mathbb{Z}_N \setminus (\mathfrak{M}(K, Q) \cup \{0\})$. It is important to note that as long as $2KQ^2 < N$, we have that $\mathbf{M}_{a,q} \cap \mathbf{M}_{b,r} = \emptyset$ whenever $a/q \neq b/r$, $q, r \leq Q$.

We note that the sets defined above certainly depend on N, despite its absence from the notation. In practice, N should always be replaced with the size of the appropriate ambient group, often denoted in the intermediate stages of our iterations by L.

2.2. **Auxiliary polynomials.** Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial. For each prime p, we fix a p-adic integer z_p with $h(z_p)=0$. The objects defined below certainly depend on h, as well as on the choice of p-adic integer roots, though any choice works equally well for our purposes, and we suppress all of this dependence in the coming notation.

By reducing modulo prime powers and applying the Chinese Remainder Theorem, the choices of z_p determine, for each natural number d, a unique integer $r_d \in (-d,0]$, which consequently satisfies $d \mid h(r_d)$. We define the function λ on $\mathbb{N}$ by letting $\lambda(p)=p^m$ for each prime p, where m is the multiplicity of z_p as a root of h, and then extending it to be completely multiplicative. For each $d \in \mathbb{N}$, we define the *auxiliary polynomial*, h_d, by

$$h_d(x) = h(r_d+dx)/\lambda(d).$$

If $p^j \mid d$ for p prime and $j \in \mathbb{N}$, then since $r_d \equiv z_p \bmod p^j$, we see by factoring h over the p-adic integers that all the coefficients of $h(r_d+dx)$ are divisible by p^{jm}, hence each auxiliary polynomial has integer coefficients.

It is important to note that the leading coefficients of the auxiliary polynomials grow at least as quickly, up to a constant depending only on h, as the other coefficients. In particular, if $\deg(h)=k$ and b_d is the leading coefficient of h_d, then for any $x>0$ we have that if $b_d>0$, then

$$\Big|\{n \in \mathbb{N} : 0 < h_d(n) < x\} \ \triangle\ [1,(x/b_d)^{1/k}]\Big| \ll_h 1, \tag{3}$$

where $\triangle$ denotes the symmetric difference.

2.3. **Inheritance proposition.** We define these auxiliary polynomials to keep track of an inherited lack of prescribed differences at each step of a density increment iteration. To this end, for nonzero $h \in \mathbb{Z}[x]$, we define $I(h)$ to be the positive elements of $h(\mathbb{N})$ if $h \in \mathbb{Z}[x]$ has positive leading coefficient and the negative elements of $h(\mathbb{N})$ if $h \in \mathbb{Z}[x]$ has negative leading coefficient.

Further, if $h^{(1)},\dots,h^{(\ell)} \in \mathbb{Z}[x]$ is a collection of intersective polynomials, then we define $\lambda_1,\dots,\lambda_\ell$ as in Section 2.2 in terms of $h^{(1)},\dots,h^{(\ell)}$, respectively. Then, we define $\Lambda = \lambda_1 \circ \cdots \circ \lambda_\ell$ and

$$\tilde{\lambda}_i = \lambda_1 \circ \cdots \lambda_{i-1} \circ \lambda_{i+1} \circ \cdots \lambda_\ell$$

for $1 \le i \le \ell$. The following proposition makes the aforementioned inheritance precise, at a level of generality that is unnecessary for Theorem 1.1, but useful for later results. As is standard, we use

$$A \pm B = \{a \pm b : a \in A, b \in B\}$$

to denote the sum and difference sets, respectively.

Proposition 2.2. *Suppose $h^{(1)},\dots,h^{(\ell)} \in \mathbb{Z}[x]$ is a collection of intersective polynomials, $d_1,\dots,d_\ell \in \mathbb{N}$, and $A \subseteq \mathbb{N}$. If $x \in \mathbb{Z}$, $q \in \mathbb{N}$,*

$$(A-A) \cap \Big(I(h^{(1)}_{d_1}) + \cdots + I(h^{(\ell)}_{d_\ell})\Big) \subseteq \{0\},$$

and $A' \subseteq \{a \in \mathbb{N} : x + \Lambda(q)a \in A\}$, then

$$(A'-A') \cap \Big(I(h^{(1)}_{\tilde{\lambda}_1(q)d_1}) + \cdots + I(h^{(\ell)}_{\tilde{\lambda}_\ell(q)d_\ell})\Big) \subseteq \{0\}.$$

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

$$0 \neq a - a' = \sum_{i=1}^{\ell} h^{(i)}_{\tilde{\lambda}_i(q)d_i}(n_i) = \sum_{i=1}^{\ell} \frac{h^{(i)}\Big(r^{(i)}_{\tilde{\lambda}_i(q)d_i} + \tilde{\lambda}_i(q)d_in_i\Big)}{\lambda_i\Big(\tilde{\lambda}_i(q)d_i\Big)} = \sum_{i=1}^{\ell} \frac{h^{(i)}\Big(r^{(i)}_{\tilde{\lambda}_i(q)d_i} + \tilde{\lambda}_i(q)d_in_i\Big)}{\Lambda(q)\lambda_i(d_i)}$$

for some $n_1,\dots,n_\ell \in \mathbb{N}$, $a,a' \in A'$, with all polynomial terms having the same sign as the corresponding leading coefficient.

By construction we know that $r^{(i)}_{\tilde{\lambda}_i(q)d_i} \equiv r^{(i)}_{d_i} \bmod d_i$, so there exists $s_i \in \mathbb{Z}$ such that $r^{(i)}_{\tilde{\lambda}_i(q)d_i} = r^{(i)}_{d_i} + d_i s_i$, and therefore

$$0 \neq \sum_{i=1}^{\ell} h^{(i)}_{d_i}(s_i + \tilde{\lambda}_i(q)n_i) = \sum_{i=1}^{\ell} \frac{h^{(i)}(r^{(i)}_{d_i} + d_i(s_i + \tilde{\lambda}_i(q)n_i))}{\lambda_i(d_i)} = \Lambda(q)(a - a').$$

Because $A' \subseteq \{a \in \mathbb{N} : x + \Lambda(q)a \in A\}$, we know that $\Lambda(q)(a - a') \in A - A$, hence

$$(A - A) \cap \Big(I(h^{(1)}_{d_1}) + \cdots + I(h^{(\ell)}_{d_\ell}) \Big) \not\subseteq \{0\},$$

and the contrapositive is established. □

2.4. **Sieve motivation.** In this context, the guiding principle of the Hardy-Littlewood circle method is that if $h \in \mathbb{Z}[x]$, then the *Weyl sum*

$$\sum_{n=1}^{M} e^{2\pi i h(n)\alpha} \tag{4}$$

is much smaller than the trivial bound M, unless α is well-approximated by a rational number with small denominator.

On a coarse scale, this principle is captured by combining the pigeonhole principle with Weyl's Inequality (see Lemma 4.4), but for a more refined treatment, we must address the following question: If α IS close to a rational with a small denominator, for example smaller than a tiny power of M, can we beat the trivial bound at all?

This question turns out to be quite straightforward, as under these conditions (4) has a convenient asymptotic formula, and the gain from the trivial bound resides in a local version of the sum. Specifically, if α is close to a/q with q small, then, up to a small error, the magnitude of (4) is at most M times

$$q^{-1} \sum_{s=0}^{q-1} e^{2\pi i h(s)a/q}. \tag{5}$$

In general, the best decay we can hope for from (5) is $q^{-1/k}$, where $k = \deg(h)$ (see [2] for example). Unfortunately, it is completely vital to the double iteration method developed in [17] to establish (2) that one has decay at or near $q^{-1/2}$ (what we refer to as *square root cancellation*) for small denominators q. Of course, this is not an obstacle if $k = 2$, a fact exploited in [7] to establish (2) for all intersective quadratics.

In [1], Balog, Pintz, Steiger, and Szemerédi observed that by sieving the initial set of inputs, letting W equal a product of small primes and considering only inputs coprime to W, the gain from the trivial bound for α near a/q with small q is given roughly by

$$\phi(q)^{-1} \sum_{\substack{s=0 \\ (s,q)=1}}^{q-1} e^{2\pi i h(s)a/q}. \tag{6}$$

In the case of $h(n) = n^k$, one then exploits that, for all but the primes dividing k, units modulo p^j for $j \geq 2$ are k-th power residues if and only if they reduce to k-th power residues modulo p. This allows one to reduce to the case of squarefree q, where there is always square root cancellation.

However, a generic intersective polynomial need not have the root-lifting properties necessary to establish square root cancellation in (6), and so sieving away small prime factors is not a winning strategy for maximally extending (2). Alternatively, given an intersective polynomial $h \in \mathbb{Z}[x]$, we define a non-traditional sieve dependent on h, essentially defined by removing the zeros of the derivative h' modulo small primes, in order to mimic the aforementioned lifting observation using Hensel's Lemma.

2.5. **Sieve definitions and observations.** For an intersective polynomial $h \in \mathbb{Z}[x]$ and each prime p and $d \in \mathbb{N}$, we define $\gamma_d(p)$ to be the smallest power such that the derivative h_d' is not identically zero modulo $p^{\gamma_d(p)}$, and we let $j_d(p)$ denote the number of roots of h_d' modulo $p^{\gamma_d(p)}$. Finally, for $d \in \mathbb{N}$ and $Y > 0$ we define

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

In the absence of a subscript d in the usage of $\gamma(p), j(p)$, and $W(Y)$, we assume $d = 1$. It follows from a standard Brun sieve calculation that for $X > 0$ we have

$$|[1, X] \cap W_d(Y)| = X \prod_{p \leq Y} \left(1 - \frac{j_d(p)}{p^{\gamma_d(p)}}\right) + O\left(Xe^{-c\frac{\log X}{\log Y}}\right), \tag{7}$$

where $c > 0$ depends only on $\deg(h)$ and the collection of moduli for which h_d' is identically zero. The following observations assure that this collection of moduli remains under control.

Proposition 2.3. *If $g(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathbb{Z}[x]$ is identically zero modulo $q \in \mathbb{N}$, then*

$$q \mid k! \gcd(a_0, \ldots, a_k).$$

Proof. We first note that g is identically zero modulo q if and only if the polynomial g/q is integer-valued. In this case, since the binomial coefficients

$$\binom{x}{j} = \frac{x(x-1)\ldots(x-j+1)}{j!}$$

form a $\mathbb{Z}$-basis for integer-valued polynomials, we can write

$$g(x) = \sum_{j=0}^{k} qb_j \binom{x}{j}$$

for $b_0, \ldots, b_k \in \mathbb{Z}$. In particular, by clearing denominators we see that the coefficients of $k!g$ are all divisible by q, and the proposition follows. □

For $h(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathbb{Z}[x]$, we define the *content* of h by

$$\text{cont}(h) = \gcd(a_1, \ldots, a_k),$$

noting that any common factor of the coefficients of h' divides $k\text{cont}(h)$. The last hurdle in controlling the set of "bad moduli" in our sieve, as well as a major issue in our future exponential sum estimates, is the possibility that the coefficients of the auxiliary polynomials h_d gain larger and larger common factors as d grows, but the following lemma due to Lucier asserts that this is not case.

Lemma 2.4 (Lemma 28, [14]). *If $h \in \mathbb{Z}[x]$ is intersective with $\deg(h) = k$, then for every $d \in \mathbb{N}$,*

$$\text{cont}(h_d) \leq |\Delta(h)|^{(k-1)/2}\text{cont}(h),$$

where $\Delta(h) = a^{2k-2} \prod_{i \neq i'} (\alpha_i - \alpha_{i'})^{e_i e_{i'}}$ if h factors over the complex numbers as

$$h(x) = a(x - \alpha_1)^{e_1} \ldots (x - \alpha_r)^{e_r}$$

with all the α_i's distinct.

Not only have we established control over the error term in (7), but also if $h \in \mathbb{Z}[x]$ and $\deg(h) = k$, then Proposition 2.3, Lemma 2.4, and the fact that h_d' has at most $k - 1$ roots modulo every prime at which it is not identically zero, give

$$\prod_{p \leq Y} \left(1 - \frac{j_d(p)}{p^{\gamma_d(p)}}\right) \gg_h \prod_{k \leq p \leq Y} \left(1 - \frac{k-1}{p}\right) \gg (\log Y)^{1-k} \tag{8}$$

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

3. The Double Iteration Method: Proof of Theorem 1.1

In this section we execute an adapted version of the double iteration method originally developed in [17] and prove Theorem 1.1. We begin with an outline.

3.1. Overview of the argument.

We initially observe that if $h \in \mathbb{Z}[x]$ is an intersective polynomial, which by symmetry of difference sets we can assume has positive leading coefficient, and

$$(A - A) \cap I(h) = \emptyset$$

for a set $A \subseteq [1, N]$, then we can apply the circle method to show that this unexpected behavior implies substantial L^2 mass of $\widehat{A}$ over nonzero frequencies near rationals with small denominator.

At this point, the traditional method, which we employ in Section 5 to prove Theorem 1.2, is to use the pigeonhole principle to conclude that there is one single denominator q such that $\widehat{A}$ has L^2 concentration around rationals with denominator q. From this information, one can conclude that A has increased density on a long arithmetic progression with step size an appropriate multiple of q, leading to a new denser set with an inherited lack of polynomial differences and continued iteration.

Pintz, Steiger, and Szemerédi [17] observed that pigeonholing to obtain a single denominator q is a potentially wasteful step. We follow their approach, observing the following dichotomy:

> **Case 1.** There is a single denominator q such that $\widehat{A}$ has extremely high L^2 concentration, greater than yielded by the pigeonhole principle, around rationals with denominator q. This leads to a very large density increment on a long arithmetic progression.
>
> **Case 2.** The L^2 mass of $\widehat{A}$ on the major arcs is spread over many denominators. In this case, an iteration procedure using the "combinatorics of rational numbers" can be employed to build a large collection of frequencies at which $\widehat{A}$ is large, then Plancherel's identity is applied to bound the density of A.

Philosophically, Case 1 provides more structural information about the original set A than Case 2 does. The downside is that the density increment procedure yields a new set and potentially a new polynomial, while the iteration in Case 2 leaves these objects fixed.

With these cases in mind, we can now outline the argument, separated into two distinct phases.

> **Phase 1** (The Outer Iteration): Given a set A and an intersective polynomial $h \in \mathbb{Z}[x]$ with $(A - A) \cap I(h) = \emptyset$, we ask if the set falls into Case 1 or Case 2 described above. If it falls into Case 2, then we proceed to Phase 2.
>
> If the set A falls into Case 1, then the density increment procedure yields a small $q \in \mathbb{N}$ and a new subset A_1 of a slightly smaller interval with significantly greater density, and
>
> $$(A_1 - A_1) \cap I(h_q) = \emptyset.$$
>
> We can then iterate this process as long as the resulting interval is not too small, and the dichotomy holds as long as the coefficients of the auxiliary polynomial are not too large. We show that if the resulting sets remain in Case 1, and the process iterates until the interval shrinks down or the coefficients grow to the limit, then the density of the original set A must have satisfied a bound stronger than the one purported in Theorem 1.1.
>
> Contrapositively, we assume that the original density does not satisfy this stricter bound, and we conclude that one of the sets yielded by the density increment procedure must lie in a large interval, have no differences in $I(h_d)$ for reasonably small d, and fall into Case 2. We call that set $B \subseteq [1, L]$.

We now have a set $B \subseteq [1, L]$ with $(B - B) \cap I(h_d) = \emptyset$ which falls into Case 2, so we can adapt the strategy of [17], [1], and [7]. It is in this phase that we use the sieve outlined in Section 2.5, as the method breaks down without square root cancellation on the major arcs.

Phase 2 (The Inner Iteration): We prove that given a frequency $s \in \mathbb{Z}_L$ with s/L close to a rational a/q such that $\widehat{B}(s)$ is large, there are lots of nonzero frequencies $t \in \mathbb{Z}_L$ with t/L close to rationals b/r such that $\widehat{B}(s+t)$ is almost as large. This intuitively indicates that a set P of frequencies associated with large Fourier coefficients can be blown up to a much larger set P' of frequencies associated with nearly as large Fourier coefficients.

The only obstruction to this intuition is the possibility that there are many pairs $(a/q, b/r)$ and $(a'/q', b'/r')$ with

$$\frac{a}{q} + \frac{b}{r} = \frac{a'}{q'} + \frac{b'}{r'}.$$

Observations made in [17] and [1] on the combinatorics of rational numbers demonstrate that this potentially harmful phenomenon can not occur terribly often.

Starting with the trivially large Fourier coefficient at 0, this process is applied as long as certain parameters are not too large, and the number of iterations is ultimately limited by the growth of the divisor function. Once the iteration is exhausted, we use the resulting set of large Fourier coefficients and Plancherel's Identity to get the upper bound on the density of B, which is by construction larger than the density of the original set A, claimed in Theorem 1.1.

3.2. **Reduction to two key lemmas.** For the remainder of Section 3, we fix an intersective polynomial $h \in \mathbb{Z}[x]$ with positive leading coefficient and $\deg(h) = k \geq 2$, and we let

$$\rho = 2^{-10k}.$$

We let

$$m = 2k^2 - 1,$$

and we fix $\epsilon > 0$ such that

$$(1 - 17\epsilon)/\log(m/2) > [2\log(k)]^{-1}.$$

We note that any dependence of implied constants on m or ϵ is actually just dependence on k.

We also fix a natural number N, which we preemptively assume is sufficiently large with respect to h, and hence also k, m, and ϵ, and we let

$$\mathcal{Q} = (\log N)^{\epsilon \log\log\log N}.$$

We deduce Theorem 1.1 from two key lemmas, corresponding to the two phases outlined in the overview in Section 3.1, the first of which yields a set with substantial Fourier L^2 mass distributed over rationals with many small denominators.

Lemma 3.1. *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $(A - A) \cap I(h) = \emptyset$. If*

$$\delta \geq e^{-(\log N)^{\epsilon/4}}, \tag{9}$$

then there exists $B \subseteq [1, L]$ and $d \leq N^{\rho/2}$ satisfying $L \geq N^{1-\rho}$, $|B|/L = \sigma \geq \delta$, and

$$(B - B) \cap I(h_d) = \emptyset.$$

Further, B satisfies $|B \cap [1, L/2]| \geq \sigma L/3$ and

$$\max_{q \leq \mathcal{Q}} \sum_{t \in \mathbf{M}_q(\mathcal{Q})} |\widehat{B}(t)|^2 \leq \sigma^2 (\log N)^{-1+\epsilon}. \tag{10}$$

The second lemma corresponds to the iteration scheme in which a set of large Fourier coefficients from distinct major arcs is blown up in such a way that the relative growth of the size of the set is much greater than the relative loss of pointwise mass.

Lemma 3.2. *Suppose $B \subseteq [1, L]$ and $d \in \mathbb{N}$ are as in the conclusion of Lemma 3.1, let $B_1 = B \cap [1, L/2]$, and suppose $\sigma \geq \mathcal{Q}^{-1/m}$. Given $U, V, K \in \mathbb{N}$ with $\max\{U, V, K\} \leq \mathcal{Q}^{1/m}$ and a set*

$$P \subseteq \left\{ t \in \bigcup_{q=1}^{V} \mathbf{M}_q(K) \cup \{0\} : |\widehat{B_1}(t)| \geq \frac{\sigma}{U} \right\}$$

satisfying

$$|P \cap \mathbf{M}_{a,q}(K)| \leq 1 \quad \text{whenever} \quad q \leq V, \tag{11}$$

there exist $U', V', K' \in \mathbb{N}$ with $\max\{U', V', K'\} \ll_h (\max\{U, V, K\})^{m/2} \sigma^{-(m+4)/2}$ and a set

$$P' \subseteq \left\{ t \in \bigcup_{q=1}^{V'} \mathbf{M}_q(K') \cup \{0\} : |\widehat{B_1}(t)| \geq \frac{\sigma}{U'} \right\} \tag{12}$$

satisfying

$$|P' \cap \mathbf{M}_{a,q}(K')| \leq 1 \quad \text{whenever} \quad q \leq V' \tag{13}$$

and

$$\frac{|P'|}{(U')^2} \geq \frac{|P|}{U^2} (\log N)^{1-16\epsilon}. \tag{14}$$

3.3. **Proof of Theorem 1.1.** In order to establish Theorem 1.1, we can assume that

$$\delta \geq (\log N)^{-\log\log\log\log N}.$$

Therefore, Lemma 3.1 produces a set B of density $\sigma \geq \delta$ with the stipulated properties, and we set $P_0 = \{0\}$, $U_0 = 3$, and $V_0 = K_0 = 1$. Then, Lemma 3.2 yields, for each n, a set P_n with parameters U_n, V_n, K_n such that

$$\max\{U_n, V_n, K_n\} \leq (\log N)^{(m/2)^{n+3} \log\log\log\log N}$$

and

$$\frac{1}{\sigma} \geq \frac{1}{\sigma^2} \sum_{t \in P_n} |\widehat{B_1}(t)|^2 \geq \frac{|P_n|}{U_n^2} \gg (\log N)^{n(1-16\epsilon)},$$

where the left-hand inequality comes from Plancherel's Identity, as long as $\max\{U_n, V_n, K_n\} \leq \mathcal{Q}^{1/m}$. This holds with $n = (1-\epsilon)(\log\log\log\log N)/\log(m/2)$, as $(m/2)^{n+3} \leq (\log\log\log N)^{1-\epsilon/2}$. Since we chose $\epsilon > 0$ such that $(1-17\epsilon)/\log(m/2) > [2\log(k)]^{-1}$, the theorem follows. □

3.4. **The Outer Iteration.** We begin the first phase with the following standard L^2 density increment lemma, a version of which can be found in Lemma 20 of [14].

Lemma 3.3. *Suppose $B \subseteq [1, L]$ with $|B| = \sigma L$. If $0 < \theta \leq 1$, $q \in \mathbb{N}$, $K > 0$, and*

$$\sum_{t \in \mathbf{M}'_q(K)} |\widehat{B}(t)|^2 \geq \theta\sigma^2,$$

then there exists an arithmetic progression

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

with $qL' \gg \min\{\theta, K^{-1}\}L$ and $|B \cap P| \geq \sigma(1 + \theta/32)L'$.

Noting that the progression P in the conclusion of Lemma 3.3 can be partitioned into subprogressions of step size $\lambda(q)$, Lemma 3.3 and Proposition 2.2 immediately combine to yield the following iteration lemma, corresponding to Case 1 discussed in the overview, from which we deduce Lemma 3.1.

Lemma 3.4. *Suppose $B \subseteq [1, L]$ with $|B| = \sigma L$ and $(B - B) \cap I(h_d) = \emptyset$. If*

$$\sum_{t \in \mathbf{M}_q(\mathcal{Q})} |\widehat{B}(t)|^2 \geq \sigma^2 (\log N)^{-1+\epsilon}, \tag{15}$$

for some $q \leq \mathcal{Q}$, then there exists $B' \subseteq [1, L']$ satisfying $L' \gg L/\mathcal{Q}^{k+1}$,

$$(B' - B') \cap I(h_{qd}) = \emptyset,$$

and

$$|B'|/L' \geq \sigma(1 + (\log N)^{-1+\epsilon}/32).$$

Proof of Lemma 3.1. Setting $A_0{=}A$, $N_0 = N$, $\delta_0 = \delta$, and $d_0 = 1$, we iteratively apply Lemma 3.4. This yields, for each j, a set $A_j \subseteq [1, N_j]$ with $|A_j| = \delta_j N_j$ and

$$(A_j - A_j) \cap I(h_{d_j}) = \emptyset,$$

satisfying

$$N_j \geq N/(C\mathcal{Q})^{(k+1)j}, \quad \delta_j \geq \delta_{j-1}(1 + (\log N)^{-1+\epsilon}/32), \quad d_j \leq \mathcal{Q}^j, \tag{16}$$

where C is an absolute constant, as long as either

$$\max_{q \leq \mathcal{Q}} \sum_{t \in \mathbf{M}_q(\mathcal{Q})} |\widehat{A_j}(t)|^2 \geq \delta_j^2 (\log N)^{-1+\epsilon} \tag{17}$$

or

$$|A_j \cap [1, N_j/2]| < \delta_j N_j/3,$$

as the latter condition implies A_j has density at least $3\delta_j/2$ on the interval $(N_j/2, N_j]$.

We see that by (9) and (16), the density δ_j will exceed 1 after

$$64 \log(\delta^{-1})(\log N)^{1-\epsilon} \leq (\log N)^{1-\epsilon/2}$$

steps, hence (17) fails and $|A_j \cap [1, N_j/2]| \geq \delta_j N_j/3$ for some

$$j \leq (\log N)^{1-\epsilon/2}. \tag{18}$$

However, we see that (9), (16), and (18) imply

$$N_j \geq N/(C\mathcal{Q})^{(k+1)(\log N)^{1-\epsilon/2}} \geq N e^{-(\log N)^{1-\epsilon/4}} \geq N^{1-\rho},$$

so we set $B = A_j$, $L = N_j$, $\sigma = \delta_j$, and $d = d_j$, and we see further that

$$d \leq \mathcal{Q}^{(\log N)^{1-\epsilon/2}} \leq e^{(\log N)^{1-\epsilon/4}} \leq N^{\rho/2},$$

as required. □

Our task for Section 3 is now completely reduced to a proof of Lemma 3.2.

3.5. **The Inner Iteration: Proof of Lemma 3.2.** Let $B \subseteq [1, L]$ and $d \in \mathbb{N}$ be as in the conclusion of Lemma 3.1, let $B_1 = B \cap [1, L/2]$, and suppose $\sigma = |B|/L \geq \mathcal{Q}^{-1/m}$. Further, let $M = \lfloor (L/3b_d)^{1/k} \rfloor$, where b_d is the leading coefficient of h_d. Letting

$$H = \{n \in \mathbb{N} : 0 < h_d(n) < L/3\}$$

we note that by (3) we have

$$|H \bigtriangleup [1, M]| \ll_h 1. \tag{19}$$

Suppose we have a set P with parameters U, V, K as specified in the hypotheses of Lemma 3.2. We fix an element $s \in P$, we let $\eta = c_0 \sigma / U$ for a sufficiently small constant $c_0 = c_0(h) > 0$, and we let $Y = \eta^{-(k+\epsilon)}$.

Since $(B - B) \cap I(h_d) = \emptyset$, we see that there are no solutions to

$$a - b \equiv h_d(n) \mod L, \quad a \in B, \ b \in B_1, \ n \in H.$$

Combined with (19) and the orthogonality relation

$$\frac{1}{L}\sum_{t\in\mathbb{Z}_L} e^{2\pi i x t/L} = \begin{cases} 1 & \text{if } x=0 \\ 0 & \text{if } x\in\mathbb{Z}_L\setminus\{0\} \end{cases},$$

this implies

$$\sum_{t\in\mathbb{Z}_L} \widehat{B}(t)\overline{\widehat{B_1}(s+t)}S(t) = \frac{1}{wL^2}\sum_{\substack{x\in\mathbb{Z}_L \\ n\in[1,M]\cap W_d(Y)}} h_d'(n)B(x+h_d(n))B_1(x)e^{2\pi i x s/L} = O_h((wM)^{-1}),$$

where

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

and

$$S(t)=\frac{1}{wL}\sum_{\substack{n=1 \\ n\in W_d(Y)}}^{M} h_d'(n)e^{2\pi i h_d(n)t/L},$$

which immediately yields

$$\sum_{t\in\mathbb{Z}_L\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| \ge \left|\sum_{t\in\mathbb{Z}_L\setminus\{0\}} \widehat{B}(t)\overline{\widehat{B_1}(s+t)}S(t)\right| = \widehat{B}(0)\left|\widehat{B_1}(s)\right|S(0) - O_h\left((wM)^{-1}\right).$$

Therefore, since $\widehat{B}(0)=\sigma$, $|\widehat{B_1}(s)|\ge\sigma/U$, $S(0)\ge 1/4$, and $\sigma^{-1},U\le\mathcal{Q}$, we have that

$$\sum_{t\in\mathbb{Z}_L\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| \ge \frac{\sigma^2}{5U}, \tag{20}$$

where we also use (8) to absorb the error term.

Using a variety of exponential sum estimates, both old and new, we find that

$$|S(t)|\le\frac{\sigma}{10U} \quad \text{for all } t\in\mathfrak{m}\left(\eta^{-1},\eta^{-(2+\epsilon)}\right), \tag{21}$$

provided we choose c_0 sufficiently small, and

$$|S(t)| \ll_h C^{\omega(q)}q^{-1/2}\min\left\{1,(L\,|t/L-a/q|)^{-1}\right\} \tag{22}$$

if $t\in\mathbf{M}_{a/q}(\eta^{-1})$, $(a,q)=1$, and $q\le\eta^{-(2+\epsilon)}$, where $\omega(q)$ is the number of distinct prime factors of q.

Remark. As discussed in Section 2.4, the exponent of $-1/2$ in (22), which we obtain thanks to our careful sieving of inputs and the application of Hensel's Lemma, is crucial to the remainder of the argument. The inability to establish this square root cancellation for general polynomials had previously been the fundamental obstacle in extending this method. We discuss these estimates in detail in Section 4.

We have by (21), Cauchy-Schwarz, and Plancherel's Identity that

$$\sum_{t\in\mathfrak{m}\left(\eta^{-1},\eta^{-(2+\epsilon)}\right)} |\widehat{B}(t)||\widehat{B_1}(t)||S(t)| \le \frac{\sigma^2}{10U},$$

which together with (20) yields

$$\sum_{t\in\mathfrak{M}\left(\eta^{-1},\eta^{-(2+\epsilon)}\right)} |\widehat{B}(t)||\widehat{B_1}(t)||S(t)| \ge \frac{\sigma^2}{10U}. \tag{23}$$

We now wish to assert that we can ignore those frequencies in the major arcs at which the transform of B or B_1 is particularly small. In order to make this precise, we first need to invoke a weighted version of known estimates on the higher moments of Weyl sums.

Specifically, it follows from Theorem 1.1 of [26] that

$$\sum_{t\in\mathbb{Z}_L} |S(t)|^m \leq C, \tag{24}$$

where $C = C(m)$. Choosing a constant $0 < c_1 < (40C^{1/m})^{-m/2}$, where C comes from (24), we define

$$\mathcal{X} = \left\{ t \in \mathfrak{M}\left(\eta^{-1}, \eta^{-(2+\epsilon)}\right) : \min\left\{ |\widehat{B}(t)|, |\widehat{B_1}(s+t)| \right\} \leq c_1 \sigma^{(m+1)/2} U^{-m/2} \right\} \tag{25}$$

and

$$\mathcal{Y} = \mathfrak{M}\left(\eta^{-1}, \eta^{-(2+\epsilon)}\right) \setminus \mathcal{X}.$$

Using Hölder's Inequality to exploit the higher moment estimate on S, followed by Plancherel's Identity, we see that

$$\begin{aligned}
\sum_{t\in\mathcal{X}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| &\leq \left(\sum_{t\in\mathcal{X}} |\widehat{B}(t)|^{\frac{m}{m-1}} |\widehat{B_1}(s+t)|^{\frac{m}{m-1}} \right)^{\frac{m-1}{m}} \left(\sum_{t\in\mathbb{Z}_L} |S(t)|^m \right)^{\frac{1}{m}} \\
&\leq \frac{c_1^{2/m} \sigma^{\frac{m+1}{m}}}{U} \left(\sum_{t\in\mathbb{Z}_L} \max\left\{ |\widehat{B}(t)|^2, |\widehat{B_1}(s+t)|^2 \right\} \right)^{\frac{m-1}{m}} \cdot C^{1/m} \\
&\leq \frac{\sigma^{\frac{m+1}{m}}}{40U} \left(\sum_{t\in\mathbb{Z}_L} |\widehat{B}(t)|^2 + |\widehat{B_1}(s+t)|^2 \right)^{\frac{m-1}{m}} \\
&\leq \frac{\sigma^2}{20U},
\end{aligned}$$

and hence by (23) we have

$$\sum_{t\in\mathcal{Y}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| \geq \frac{\sigma^2}{20U}. \tag{26}$$

For $i, j, \ell \in \mathbb{N}$, we define

$$\mathcal{R}_{i,j,\ell} = \left\{ a/q : (a,q) = 1,\ 2^{i-1} \leq q \leq 2^i,\ \frac{\sigma}{2^j} \leq \max |\widehat{B}(t)| \leq \frac{\sigma}{2^{j-1}},\ \frac{\sigma}{2^\ell} \leq \max |\widehat{B_1}(s+t)| \leq \frac{\sigma}{2^{\ell-1}} \right\},$$

where the maximums are taken over nonzero frequencies $t \in \mathbf{M}_{a/q}(\eta^{-1})$. We see that we have

$$\sum_{a/q\in\mathcal{R}_{i,j,\ell}} \sum_{t\in\mathbf{M}_{a/q}(\eta^{-1})\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| \ll |\mathcal{R}_{i,j,\ell}| \frac{\sigma^2}{2^j 2^k} \max_{a/q\in\mathcal{R}_{i,j,\ell}} \sum_{t\in\mathbf{M}_{a/q}(\eta^{-1})} |S(t)|. \tag{27}$$

It follows from (22), the bound $U, \sigma^{-1} \leq \mathcal{Q}^{1/m}$, and the standard estimate $\omega(q) \ll \log q/\log\log q$, that if $(a,q) = 1$ and $q \leq \eta^{-(2+\epsilon)}$, then

$$\begin{aligned}
\sum_{t\in\mathbf{M}_{a/q}(\eta^{-1})} |S(t)| &\ll_h C^{\omega(q)} q^{-1/2} \log(\mathcal{Q}) \\
&\ll_h q^{-1/2} (\log N)^\epsilon.
\end{aligned}$$

Therefore, by (27) we have

$$\sum_{a/q\in\mathcal{R}_{i,j,\ell}} \sum_{t\in\mathbf{M}_{a/q}(\eta^{-1})\setminus\{0\}} |\widehat{B}(t)||\widehat{B_1}(s+t)||S(t)| \ll_h |\mathcal{R}_{i,j,\ell}| \frac{\sigma^2}{2^j 2^\ell} 2^{-i/2} (\log N)^\epsilon. \tag{28}$$

By our definitions, the sets $\mathcal{R}_{i,j,\ell}$ exhaust $\mathcal{Y}$ by taking $1 \leq 2^i \leq \eta^{-(2+\epsilon)}$ and $1 \leq 2^j, 2^\ell \leq U^{m/2}/c_1\sigma^{(m-1)/2}$, a total search space of size $\ll (\log \mathcal{Q})^3$. Therefore, by (26) and (28) there exist i, j, ℓ in the above range such that

$$\frac{\sigma^2}{U(\log \mathcal{Q})^3} \ll_h |\mathcal{R}_{i,j,\ell}| \frac{\sigma^2}{2^j 2^\ell} 2^{-i/2} (\log N)^\epsilon.$$

In other words, we can set $V_s = 2^i$, $W_s = 2^j$, and $U_s = 2^\ell$ and take an appropriate nonzero frequency from each of the pairwise disjoint major arcs specified by $\mathcal{R}_{i,j,\ell}$ to form a set

$$P_s \subseteq \left\{ t \in \bigcup_{q=V_s/2}^{V_s} \mathbf{M}_q(\eta^{-1}) : \ |\widehat{B_1}(s+t)| \geq \frac{\sigma}{U_s} \right\}$$

which satisfies

$$|P_s| \gg_h \frac{U_s W_s V_s^{1/2}}{U(\log N)^{2\epsilon}}, \quad |P_s \cap \mathbf{M}_{a,q}(\eta^{-1})| \leq 1 \ \text{ whenever } \ q \leq V_s, \tag{29}$$

and

$$\max_{t \in \mathbf{M}_{a/q}(\eta^{-1}) \setminus \{0\}} |\widehat{B}(t)| \geq \frac{\sigma}{W_s} \text{ whenever } q \leq V_s \text{ and } \mathbf{M}_{a/q}(\eta^{-1}) \cap P_s \neq \emptyset, \tag{30}$$

noting by disjointness that $a/q \in \mathcal{R}_{i,j,\ell}$ whenever $q \leq V_s$ and $\mathbf{M}_{a/q}(\eta^{-1}) \cap P_s \neq \emptyset$.

We now observe that by pigeonholing there is a subset $\tilde{P} \subseteq P$ with $|\tilde{P}| \gg |P|/(\log \mathcal{Q})^3$, and hence

$$|\tilde{P}| \gg |P|/(\log N)^\epsilon, \tag{31}$$

for which the triple U_s, W_s, V_s is the same. We call those common parameters $\tilde{U}, \tilde{W}$ and $\tilde{V}$, respectively, and we can now foreshadow by asserting that the claimed parameters in the conclusion of Lemma 3.2 will be $U' = \tilde{U}$, $V' = \tilde{V}V$, and $K' = K + \eta^{-1}$, which do satisfy the purported bound.

We let

$$\mathcal{R} = \left\{ \frac{a}{q} + \frac{b}{r} : s \in \mathbf{M}_{a/q}(K) \text{ for some } s \in \tilde{P} \text{ and } t \in \mathbf{M}_{b/r}(\eta^{-1}) \text{ for some } t \in P_s \right\}.$$

By taking one frequency $s + t$ associated to each element in $\mathcal{R}$, we form our set P', which immediately satisfies conditions (12) and (13) from the conclusion of Lemma 3.2. However, the crucial condition (14) on $|P'|$, which by construction is equal to $|\mathcal{R}|$, remains to be shown. To this end, we invoke the work on the combinatorics of rational numbers found in [17] and [1].

Lemma 3.5 (Lemma CR of [1])**.**

$$|\mathcal{R}| \geq \frac{|\tilde{P}|(\min_{s \in \tilde{P}} |P_s|)^2}{\tilde{V} E \tau^8 (1 + \log V)},$$

where

$$E = \max_{r \leq \tilde{V}} \left| \left\{ b : \ (b,r) = 1, \ \mathbf{M}_{b/r}(\eta^{-1}) \cap \bigcup_{s \in \tilde{P}} P_s \neq \emptyset \right\} \right|,$$

$\tau(q)$ is the divisor function and $\tau = \max_{q \leq V\tilde{V}} \tau(q)$.

It is a well-known fact of the divisor function that $\tau(n) \leq n^{1/\log\log n}$ for large n, and since $\eta^{-1}, V\tilde{V} \leq \mathcal{Q}$, we have that $\tau \leq (\log N)^\epsilon$. We also have from (10) that

$$\sigma^2 (\log N)^{-1+\epsilon} \geq \max_{r \leq \mathcal{Q}} \sum_{t \in \mathbf{M}_r(\mathcal{Q})} |\widehat{B}(t)|^2 \geq \max_{r \leq \tilde{V}} \sum_{t \in \mathbf{M}_r(\eta^{-1})} |\widehat{B}(t)|^2 \geq \frac{\sigma^2}{\tilde{W}^2} E,$$

where the last inequality follows from (30), and hence $E \leq \tilde{W}^2 (\log N)^{-1+\epsilon}$.

Combining the estimates on τ and E with (29), (31), and Lemma 3.5, we have

$$|P'| \gg_h \frac{|P|}{(\log N)^\epsilon} \frac{\tilde{U}^2 \tilde{W}^2 \tilde{V}}{U^2 (\log N)^{4\epsilon}} \frac{(\log N)^{1-\epsilon}}{\tilde{V} \tilde{W}^2 (\log N)^{9\epsilon}} = \tilde{U}^2 \frac{|P|}{U^2} (\log N)^{1-15\epsilon}.$$

Recalling that we set $U' = \tilde{U}$, we see that for sufficiently large N we have

$$\frac{|P'|}{(U')^2} \geq \frac{|P|}{U^2} (\log N)^{1-16\epsilon},$$

as claimed. ☐

4. Exponential Sum Estimates

In this section, we either invoke or prove all exponential sum estimates necessary to establish the crucial major and minor arc upper bounds in Section 3.5, namely (21), and (22). Throughout this section, given a polynomial $g \in \mathbb{Z}[x]$, we let $\gamma(p)$, $j(p)$, and $W(Y)$ be defined in terms of g as in Section 2.5. Further, for each $q \in \mathbb{N}$, we define

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

The first lemma provides asymptotic formulae for the relevant sifted Weyl sums near rationals with small denominator.

Lemma 4.1. *Suppose $k \in \mathbb{N}$, $g(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}[x]$, and let $J = |a_0| + |a_1| + \cdots + |a_k|$. If $X \geq 0$, $Y \geq 2$, $a, q \in \mathbb{N}$, and $\alpha = a/q + \beta$, then*

$$\sum_{\substack{n=1 \\ n \in W(Y)}}^{X} g'(n) e^{2\pi i g(n)\alpha} = \frac{1}{q} \prod_{\substack{p \leq Y \\ p^{\gamma(p)} \nmid q}} \left(1 - \frac{j(p)}{p^{\gamma(p)}}\right) \sum_{\substack{s=0 \\ s \in W^q(Y)}}^{q-1} e^{2\pi i g(s) \frac{a}{q}} \int_0^X g'(x) e^{2\pi i g(x)\beta} dx$$

$$+ O\left(kJX^k e^{-c\frac{\log\left(\frac{X}{q}\right)}{\log Y}} (1 + JX^k|\beta|)\right),$$

where $c = c(k, \text{cont(g)}) > 0$.

Proof. We begin by noting that for any $a, q \in \mathbb{N}$ and $x \geq 0$,

$$\sum_{\substack{n=1 \\ n \in W(Y)}}^{x} g'(n) e^{2\pi i g(n)a/q} = \sum_{s=0}^{q-1} e^{2\pi i g(s)a/q} \sum_{\substack{n=1 \\ n \in W(Y) \\ n \equiv s \bmod q}}^{x} g'(n)$$

$$= \frac{g(x)}{q} \prod_{\substack{p \leq Y \\ p^{\gamma(p)} \nmid q}} \left(1 - \frac{j(p)}{p^{\gamma(p)}}\right) \sum_{\substack{s=0 \\ s \in W^q(Y)}}^{q-1} e^{2\pi i g(s)a/q} + O\left(kJx^k e^{-c\frac{\log(x/q)}{\log Y}}\right),$$

since for $s \in W^q(Y)$ we have by the same calculation as (7) and partial summation that

$$\sum_{\substack{n=1 \\ n \in W(Y) \\ n \equiv s \bmod q}}^{x} g'(n) = \frac{g(x)}{q} \prod_{\substack{p \leq Y \\ p^{\gamma(p)} \nmid q}} \left(1 - \frac{j(p)}{p^{\gamma(p)}}\right) + O\left(\frac{kJx^k}{q} e^{-c\frac{\log(x/q)}{\log Y}}\right),$$

whereas for $s \notin W^q(Y)$ the sum is zero.

Then, by partial summation we have that if $\alpha = a/q + \beta$, then

$$\sum_{\substack{n=1 \\ n\in W(Y)}}^{X} g'(n)e^{2\pi i g(n)\alpha} = \frac{1}{q} \prod_{\substack{p\leq Y \\ p^{\gamma(p)}\nmid q}} \left(1 - \frac{j(p)}{p^{\gamma(p)}}\right) \sum_{\substack{s=0 \\ s\in W^q(Y)}}^{q-1} e^{2\pi i g(s)a/q}$$

$$\cdot \left(g(X)e^{2\pi i g(X)\beta} - \int_0^X g(x)(2\pi i\beta g'(x))e^{2\pi i g(x)\beta}dx\right)$$

$$+ O\left(kJX^k e^{-c\frac{\log\left(\frac{X}{q}\right)}{\log Y}}(1 + JX^k|\beta|)\right).$$

Finally, noting that

$$g(X)e^{2\pi i g(X)\beta} - \int_0^X g(x)(2\pi i\beta g'(x))e^{2\pi i g(x)\beta}dx = \int_0^X g'(x)e^{2\pi i g(x)\beta}dx,$$

the lemma follows. □

To establish the required square root cancellation for the restricted exponential sums that arise in the conclusion of Lemma 4.1, we use the following standard fact about lifting roots of polynomials, the details of which motivate the sieve outlined in Section 2.5. Here we focus only on the existence of the lifts, ignoring the extent of uniqueness or "closeness", and this statement follows, for example, from Proposition 2 in Chapter II, Section 2 of [10].

Lemma 4.2 (Hensel's Lemma)**.** *Suppose $g \in \mathbb{Z}[x]$, p is prime, and $n, \gamma, j \in \mathbb{N}$ with $j \geq 2\gamma - 1$. If*

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

and $g'(n) \not\equiv 0 \bmod p^{\gamma}$, then there exists $m \in \mathbb{N}$ with $g(m) \equiv 0 \bmod p^j$.

Armed with Lemma 4.2, we exhibit the restricted exponential sum estimate that was previously the missing ingredient to proving Theorem 1.1.

Lemma 4.3. *If $g \in \mathbb{Z}[x]$ with $\deg(g) = k \geq 2$, $a, q \in \mathbb{N}$ with $(a, q) = 1$, and $Y > 0$, then*

$$\left|\sum_{\substack{s=0 \\ s\in W^q(Y)}}^{q-1} e^{2\pi i g(s)a/q}\right| \ll_k \gcd(\text{cont}(g), q)^{3/2} C^{\omega(q)} \begin{cases} q^{1/2} & \text{if } q \leq Y \\ q^{1-1/k} & \text{for all } q \end{cases}.$$

Proof. Factor $q = q_1 \cdots q_4$, where $q_1, \ldots, q_4$ are pairwise coprime, q_1 houses the prime power factors p^j of q satisfying $p \leq Y$, $\gamma(p) > 1$, and $j < 2\gamma(p)$, q_2 is a product of distinct primes $p \leq Y$ satisfying $\gamma(p) = 1$, q_3 is the product of p^j satisfying $p \leq Y$, $j \geq 2\gamma(p)$, and all prime factors of q_4 are greater than Y.

By the Chinese Remainder Theorem, we have

$$\sum_{\substack{s=0 \\ s\in W^q(Y)}}^{q-1} e^{2\pi i g(s)a/q} = \prod_{i=1}^{4} \sum_{\substack{s=0 \\ s\in W^{q_i}(Y)}}^{q_i-1} e^{2\pi i g(s)a_i/q_i},$$

where $a_1, \ldots, a_4$ are the unique residues satisfying

$$\frac{a}{q} \equiv \frac{a_1}{q_1} + \cdots + \frac{a_4}{q_4} \bmod 1.$$

Since $p^{2\gamma(p)-1} \leq p^{3(\gamma(p)-1)}$ if $\gamma(p) > 1$, we have by Proposition 2.3 and Lemma 2.4 that

$$q_1 \ll_k \gcd(\text{cont}(g), q_1)^3.$$

Further decomposing q_2 into a product of primes, using the fact that g' has at most $k-1$ roots modulo each of these primes, and applying the standard Weil bound (see for example Theorem 3.1 of [8]), we have

$$\left|\sum_{\substack{s=0\\ s\in W^p(Y)}}^{p-1} e^{2\pi i g(s)b/p}\right| \ll_k p^{1/2}$$

provided $p\nmid b\text{cont}(g)$, and hence

$$\left|\sum_{\substack{s=0\\ s\in W^{q_2}(Y)}}^{q_2-1} e^{2\pi i g(s)a_2/q_2}\right| \leq C^{\omega(q_2)}\gcd(\text{cont}(g),q_2)^{1/2}q_2^{1/2},$$

where $C=C(k)$.

Now suppose that p is prime, $j\geq 2\gamma(p)$, and $\ell=2\gamma(p)-1$. If $0\leq s\leq p^j-1$ and s_1 is the reduced residue class of s modulo p^ℓ, then $g(s)\equiv p^\ell s_2+g(s_1) \bmod p^j$ for some $0\leq s_2\leq p^{j-\ell}-1$. Conversely, if $0\leq s_1\leq p^\ell-1$ with $g'(s_1)\not\equiv 0 \bmod p^{\gamma(p)}$, then for every $0\leq s_2\leq p^{j-\ell}-1$, Lemma 4.2 applied to the polynomial $g(x)-p^\ell s_2+g(s_1)$ yields $0\leq s\leq p^j-1$ with $g(s)\equiv p^\ell s_2+g(s_1) \bmod p^j$. In other words, the map F on $\mathbb{Z}/p^{j-\ell}\mathbb{Z}$ defined by $g(p^\ell s_2+s_1)\equiv p^\ell F(s_2)+g(s_1) \bmod p^j$ is a bijection. In particular, if $p\nmid b$, then

$$\begin{aligned}\sum_{\substack{s=0\\ s\in W^{p^j}(Y)}}^{p^j-1} e^{2\pi i g(s)b/p^j} &= \sum_{\substack{s_1=0\\ g'(s_1)\not\equiv 0 \bmod p^{\gamma(p)}}}^{p^\ell-1}\sum_{s_2=0}^{p^{j-\ell}-1} e^{2\pi i g(p^\ell s_2+s_1)b/p^j}\\ &= \sum_{\substack{s_1=0\\ g'(s_1)\not\equiv 0 \bmod p^{\gamma(p)}}}^{p^\ell-1}\sum_{s_2=0}^{p^{j-\ell}-1} e^{2\pi i\left(p^\ell s_2+g(s_1)\right)b/p^j}\\ &= 0,\end{aligned}$$

where the last equality is the fact that the sum in s_2 runs over the full collection of $p^{j-\ell}$-th roots of unity. In particular, we have that

$$\sum_{\substack{s=0\\ s\in W^{q_3}(Y)}}^{q_3-1} e^{2\pi i g(s)a_3/q_3} = \begin{cases}1 & \text{if } q_3=1\\ 0 & \text{else}\end{cases}.$$

Finally, noting that $W^{q_4}(Y)=\mathbb{N}$, we utilize the standard complete sum estimate (see [2] for example)

$$\left|\sum_{s=0}^{q_4-1} e^{2\pi i g(s)a_4/q_4}\right| \ll_k \gcd(\text{cont}(g),q_4)^{1/k}q_4^{1-1/k},$$

and the lemma follows. □

We now invoke a variation of the most traditional minor arc estimate, Weyl's Inequality.

Lemma 4.4 (Lemma 3 in [3]). *Suppose $k\in\mathbb{N}$, $g(x)=a_0+a_1x+\cdots+a_kx^k$ with $a_1\dots,a_k\in\mathbb{R}$ 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*

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

Finally, we carefully adapt Lemma 4.4 to our particular sieve to get the desired estimates far from rationals with small denominator.

Lemma 4.5. *Suppose* $k \in \mathbb{N}$, $g(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{Z}[x]$ *with* $a_k > 0$. *Suppose further that* $X, Y, Z \geq 2$ *and* $a, q \in \mathbb{N}$ *with* $(a,q) = 1$. *If* $|\alpha - a/q| < q^{-2}$, *then*

$$\left| \sum_{\substack{n=1 \\ n \in W(Y)}}^{X} e^{2\pi i g(n)\alpha} \right| \ll_k \operatorname{cont}(g)^5 (\log Y)^{ek} X \left(e^{-\frac{\log Z}{\log Y}} + \left(a_k \log^{k^2}(a_k q X) \left(q^{-1} + \frac{Z}{X} + \frac{qZ^k}{a_k X^k} \right) \right)^{2^{-k}} \right).$$

Proof. Let r be the number of primes that are at most Y, and let P be the set of products $p_1^{\gamma(p_1)} \cdots p_s^{\gamma(p_s)}$ with $p_1 < \cdots < p_s \leq Y$. By inclusion-exclusion and Proposition 2.3,

$$\left| \sum_{\substack{n=1 \\ n \in W(Y)}}^{X} e^{2\pi i g(n)\alpha} \right| = \left| \sum_{s=0}^{r} (-1)^s \sum_{p_1 < \cdots < p_s \leq Y} \sum_{\substack{n=1 \\ g'(n) \equiv 0 \bmod p_1^{\gamma(p_1)} \cdots p_s^{\gamma(p_s)}}}^{X} e^{2\pi i g(n)\alpha} \right|$$

$$\ll_k \operatorname{cont}(g)^2 \sum_{D \in P} k^{\omega(D)} \max_{0 \leq b \leq D} \left| \sum_{n=0}^{X/D} e^{2\pi i g(Dn+b)\alpha} \right|,$$

where we use that if $\gamma(p) = 1$, then g' has fewer than k roots modulo p, and the $\operatorname{cont}(g)^2$ term accounts for the primes p for which $\gamma(p) > 1$.

Further, we see from Lemma 4.4 that

$$\sum_{\substack{D \in P \\ D \leq Z}} k^{\omega(D)} \max_{0 \leq b \leq D} \left| \sum_{n=0}^{X/D} e^{2\pi i g(Dn+b)\alpha} \right| \ll_k \sum_{\substack{D \in P \\ D \leq Z}} k^{\omega(D)} \frac{X}{D} \left(a_k \log^{k^2}(a_k q X) \left(q^{-1} + \frac{D}{X} + \frac{qD^k}{a_k X^k} \right) \right)^{2^{-k}}$$

$$\ll_k X \left(a_k \log^{k^2}(a_k q X) \left(q^{-1} + \frac{Z}{X} + \frac{qZ^k}{a_k X^k} \right) \right)^{2^{-k}} \sum_{D \in P} \frac{k^{\omega(D)}}{D}$$

$$\ll_k X (\log Y)^k \left(a_k \log^{k^2}(a_k q X) \left(q^{-1} + \frac{Z}{X} + \frac{qZ^k}{a_k X^k} \right) \right)^{2^{-k}},$$

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

$$\sum_{D \in P} \frac{C^{\omega(D)}}{D} = \prod_{p \leq Y} \left(1 + \frac{C}{p^{\gamma(p)}} \right) \leq \prod_{p \leq Y} \left(1 + \frac{C}{p} \right) \ll (\log Y)^C. \tag{32}$$

If $D \in P$ with $D > Z$, then, since $D \ll_k \operatorname{cont}(g)^2 Y^{\omega(D)}$ and $Y \geq 2$, we know that

$$\operatorname{cont}(g)^3 e^{\omega(D) - \frac{\log Z}{\log Y}} \gg_k 1. \tag{33}$$

Finally, by trivially bounding the inner sum and applying (33) and (32), we have

$$\sum_{\substack{D\in P\\ D>Z}} k^{\omega(D)} \max_{0\le b\le D}\left|\sum_{n=0}^{X/D} e^{2\pi i g(Dn+b)\alpha}\right| \ll \sum_{\substack{D\in P\\ D>Z}} k^{\omega(D)}\frac{X}{D}$$

$$\ll_k \mathrm{cont}(g)^3 e^{-\frac{\log Z}{\log Y}} X \sum_{D\in P}\frac{(ek)^{\omega(D)}}{D}$$

$$\ll \mathrm{cont}(g)^3 e^{-\frac{\log Z}{\log Y}} (\log Y)^{ek} X,$$

and the estimate follows. □

4.1. **Proof of (21) and (22).** We return to the setting of the proof of Lemma 3.2 in Section 3.5, recalling all assumptions, notation, and fixed parameters. Further, we let

$$Z = e^{(\log\log N)^3},$$

noting that

$$e^{\frac{\log Z}{\log Y}} > \mathcal{Q}^2. \tag{34}$$

Fixing $t \in \mathbb{Z}_L$, the pigeonhole principle guarantees the existence of $1 \le q \le L/Z^{2k}$ and $(a,q) = 1$ with

$$\left|\frac{t}{L} - \frac{a}{q}\right| < \frac{Z^{2k}}{qL}.$$

Letting $\beta = t/L - a/q$, we have by Lemma 4.1 and (8) that

$$S(t) = \frac{w_q}{qL} \sum_{\substack{s=0\\ s\in W^q(Y)}}^{q-1} e^{2\pi i h_d(s)a/q} \int_0^M h_d'(x) e^{2\pi i h_d(x)\beta}dx + O_h\left(e^{-c\frac{\log\left(\frac{M}{q}\right)}{\log Y}} Z^{3k}\right), \tag{35}$$

where

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

We note that $w_q \ll_h 2^{\omega(q)}$ by Proposition 2.3 and Lemma 2.4.

Combining (35) and Lemma 4.3 with the fact that

$$\left|\int_0^M h_d'(x)e^{2\pi i h_d(x)\beta}dx\right| = \left|\int_0^{h_d(M)} e^{2\pi i y\beta}dy\right| \ll \min\{L, |\beta|^{-1}\} \tag{36}$$

yields (22) if

$$q \le \eta^{-(2+\epsilon)} \quad \text{and} \quad |\beta| < (\eta L)^{-1},$$

as well as (21) if

$$q \le \eta^{-(2+\epsilon)} \text{ and } |\beta| \ge (\eta L)^{-1} \quad \text{or} \quad \eta^{-(2+\epsilon)} < q \le L^{2k\rho}.$$

Finally, recalling that the leading coefficient b_d of h_d satisfies $b_d \ll_h d^k \le L^{k\rho}$, we have by Lemma 4.5, Lemma 2.4, (34), and partial summation that if $L^{2k\rho} \le q \le L/Z^{2k}$, then

$$|S(t)| \ll_h \mathcal{Q}^{-1},$$

and in particular (21) holds. □

5. Single Iteration Method: Proof of Theorem 1.2

In this section, we further exploit the estimates established in Section 4 and apply a more traditional L^2 density increment, essentially an improved, streamlined version of Sárközy's [22] original method, in order to prove Theorem 1.2. The core of this method has been utilized in [14], [16], [21], and [19], among others.

We also provide a brief discussion on sums of three or more polynomials in Section 5.6. We begin with another preliminary discussion of the circle method, this time with a continuous frequency domain.

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

For this argument, rather than identify an interval of integers with a cyclic group, 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 $|A| = \delta N$, rather than singling out the zero frequency, we examine the Fourier analytic behavior of A by considering the *balanced function*, f_A, defined by

$$f_A = 1_A - \delta 1_{[1,N]}.$$

We then define the major and minor arcs on $\mathbb{T}$, analogous to our definitions from Section 2.1.

Definition 5.1. Given $\gamma > 0$ and $Q \geq 1$, we define, for each $q \in \mathbb{N}$ and $a \in [1, q]$,

$$\mathbf{M}_{a/q}(\gamma) = \left\{\alpha \in \mathbb{T} : \left|\alpha - \frac{a}{q}\right| < \gamma\right\},$$

$$\mathbf{M}_q(\gamma) = \bigcup_{(a,q)=1} \mathbf{M}_{a/q}(\gamma),$$

and

$$\mathbf{M}'_q(\gamma) = \bigcup_{r|q} \mathbf{M}_r(\gamma) = \bigcup_{a=1}^{q} \mathbf{M}_{a/q}(\gamma).$$

We then define $\mathfrak{M}(\gamma, Q)$, the *major arcs*, by

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

and $\mathfrak{m}(\gamma, Q)$, 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

$$\mathbf{M}_{a/q}(\gamma) \cap \mathbf{M}_{b/r}(\gamma) = \emptyset \qquad (37)$$

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

5.2. Main iteration lemma and proof of Theorem 1.2.

For the remainder of Section 5 we fix intersective polynomials $g, h \in \mathbb{Z}[x]$, and we let $k = \deg(g)$, $\ell = \deg(h)$, $D = \left(k^{-1} + \ell^{-1}\right)^{-1}$, and $\rho = 2^{-10k\ell}$. Finally, for $N \in \mathbb{N}$ we let

$$\mathcal{Q} = \mathcal{Q}(N) = e^{\rho\sqrt{\log N}}.$$

We deduce Theorem 1.2 from the following iteration lemma, which states that a set deficient in the desired pattern spawns a new, significantly denser subset of a slightly smaller interval with an inherited deficiency in the pattern associated to appropriate auxiliary polynomials.

Lemma 5.2. *Suppose* $A \subseteq [1, N]$ *with* $|A| = \delta N$*. If* $(A - A) \cap (I(g_{d_1}) + I(h_{d_2})) \subseteq \{0\}$ *and* $d_1, d_2, \delta^{-1} \leq \mathcal{Q}$*, then there exist* $q \ll_h \delta^{-2}$ *and* $A' \subseteq [1, N']$ *with* $N' \gg_h \delta^{2D(k\ell+1)} N$*,*

$$\frac{|A'|}{N'} \geq (1 + c \log^{-C}(\delta^{-1}))\delta,$$

and

$$(A' - A') \cap \left(I(g_{\lambda_2(q)d_1}) + I(h_{\lambda_1(q)d_2})\right) \subseteq \{0\},$$

for some $c = c(g, h) > 0$ *and* $C = C(k, \ell)$*.*

Proof of Theorem 1.2. 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 can depend only on g and h. We use C' and c' similarly, but these constants can depend only on k and ℓ.

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

$$(A - A) \cap (I(g) + I(h)) \subseteq \{0\}.$$

Setting $A_0 = A$, $N_0 = N$, $d_1^{(0)}, d_2^{(0)} = 1$, and $\delta_0 = \delta$, Lemma 5.2 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and

$$(A_m - A_m) \cap \left(I\left(g_{d_1^{(m)}}\right) + I\left(h_{d_2^{(m)}}\right)\right) \subseteq \{0\}.$$

Further, we have that

$$N_m \geq c\delta^{2D(k\ell+1)} N_{m-1} \geq (c\delta)^{2D(k\ell+1)m} N, \tag{38}$$

$$\delta_m \geq (1 + c \log^{-C'}(\delta_{m-1}^{-1}))\delta_{m-1}, \tag{39}$$

and

$$d_i^{(m)} \leq (c\delta)^{-2k\ell} d_i^{(m-1)} \leq (c\delta)^{-2k\ell m}, \tag{40}$$

as long as

$$d_i^{(m)}, \delta_m^{-1} \leq e^{\rho\sqrt{\log N_m}}. \tag{41}$$

However, we see that the density δ_m will exceed 1, and hence (41) must fail for $m = C \log^{C'}(\delta^{-1})$, which by (38) and (40) yields $(c\delta)^{-C \log^{C'}(\delta^{-1})} \geq e^{\sqrt{\log N}}$, and hence

$$\delta \ll_h e^{-(\log N)^{c'}}.$$

This establishes Theorem 1.2 outside of the claim that we can take $c' = 1/2$ if $\deg(g) = \deg(h) = 2$, which we discuss in Section 5.6. □

5.3. **Deducing Lemma 5.2 from L^2 Fourier concentration.** The philosophy behind the proof of Lemma 5.2 is that a deficiency in polynomial differences in a set A represents nonrandom behavior, which should be detected 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 use that information to find a long arithmetic progression on which A has increased density.

Lemma 5.3. *Suppose* $A \subseteq [1, N]$ *with* $|A| = \delta N$*,* $\eta = c_0\delta$ *for a sufficiently small constant* $c_0 = c_0(g, h) > 0$*, and* $\gamma = \eta^{-2D}/N$*. If* $(A - A) \cap (I(g_{d_1}) + I(h_{d_2})) \subseteq \{0\}$*,* $d_1, d_2, \delta^{-1} \leq \mathcal{Q}$*, and* $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$*, then there exists* $q \leq \eta^{-2}$ *such that*

$$\int_{\mathbf{M}'_q(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \gg_h \delta^2 \log^{-C}(\delta^{-1}) N$$

for some $C = C(k, \ell)$*.*

Lemma 5.2 follows from Lemma 5.3 and the following standard L^2 density increment lemma, the continuous analog of Lemma 3.3.

Lemma 5.4 (Lemma 2.3 in [18], see also [14], [21]). *Suppose $A \subseteq [1,N]$ with $|A| = \delta N$. If $0 < \theta \leq 1$, $q \in \mathbb{N}$, $\gamma > 0$, and*

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

then there exists an arithmetic progression

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

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

Proof of Lemma 5.2. Suppose $A \subseteq [1,N]$, $|A| = \delta N$, $(A-A)\cap(I(g_{d_1}) + I(h_{d_2})) \subseteq \{0\}$, and $d_1, d_2, \delta^{-1} \leq \mathcal{Q}$. 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 5.3 and 5.4 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \leq \eta^{-2}$ and an arithmetic progression

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

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

$$|A \cap P|/L \geq (1 + c\log^{-C}(\delta^{-1}))\delta.$$

Partitioning P into subprogressions of step size $\Lambda(q) = \lambda_1(\lambda_2(q))$, the pigeonhole principle yields a progression

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

with $N' \geq qL/2\Lambda(q)$ and $|A \cap P'|/N' \geq |A \cap P|/L$. 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 $N' \gg_h \delta^{2D} N/\Lambda(q) \gg_h \delta^{2D(k\ell+1)} N$. Moreover, by Proposition 2.2, $(A - A) \cap (I(g_{d_1}) + I(h_{d_2})) \subseteq \{0\}$ implies $(A' - A') \cap \big(I(g_{\lambda_2(q)d_1}) + I(h_{\lambda_1(q)d_2})\big) \subseteq \{0\}$. □

Our task for this section is now completely reduced to a proof of Lemma 5.3.

5.4. **Preliminary notation for proof of Lemma 5.3.** Before delving into the proof of Lemma 5.3, we take the opportunity to define some relevant sets and quantities, depending on our intersective polynomials $g, h \in \mathbb{Z}[x]$, scaling parameters d_1, d_2, a parameter $Y > 0$, and the size of the ambient interval N. In all the notation defined below, we suppress all of the aforementioned dependence, as the relevant objects will be fixed in context.

We define $W^{(1)}_{d_1}$, $\gamma^{(1)}_{d_1}$, and $j^{(1)}_{d_1}$ in terms of g as in Section 2.5. We then define H_1 to be the collection of natural number inputs $m \in W^{(1)}_{d_1}(Y)$ such that $g_{d_1}(m)$ is strictly between 0 and $\pm N/18$, where the sign is the sign of the leading coefficient of g. We let $M_1 = \left(\frac{N}{18|b|}\right)^{1/k}$, where b is the leading coefficient of g_{d_1}, and we let

$$w_1 = \prod_{p \leq Y} \left(1 - \frac{j^{(1)}_{d_1}(p)}{p^{\gamma^{(1)}_{d_1}(p)}}\right).$$

We then analogously define $W^{(2)}_{d_2}$, $\gamma^{(2)}_{d_2}$, $j^{(2)}_{d_2}$, H_2, M_2, and w_2 in terms of h and d_2, we let

$$Z = \{(m,n) \in H_1 \times H_2 : g_{d_1}(m) + h_{d_2}(n) = 0\},$$

and we let $H = (H_1 \times H_2) \setminus Z$. Letting $M = w_1 w_2 M_1 M_2$, it follows from (3), (7), and (8) that

$$\left| H_1 \triangle \left([1, M_1] \cap W^{(1)}_{d_1}(Y)\right)\right| \ll_g 1, \tag{42}$$

with the analogous statement for H_2, and

$$|H| \geq M/2, \tag{43}$$

provided, for example, that $Y < e^{\sqrt{\log N}}$.

5.5. **Proof of Lemma 5.3.** Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, $(A - A) \cap (I(g_{d_1}) + I(h_{d_2})) \subseteq \{0\}$, and $d_1, d_2, \delta^{-1} \leq \mathcal{Q}$. Further, let $\eta = c_0\delta$ for an appropriately small $c_0 = c_0(g, h) > 0$, let $Q = \eta^{-2}$, and let $Y = \eta^{-2D}$. Since $g_{d_1}(H_1) + h_{d_2}(H_2) \subseteq [-N/9, N/9]$, we have

$$\begin{aligned}\sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} f_A(x)f_A(x + g_{d_1}(m) + h_{d_2}(n)) = &\sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} 1_A(x)1_A(x + g_{d_1}(m) + h_{d_2}(n)) \\ &- \delta \sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} 1_A(x)1_{[1,N]}(x + g_{d_1}(m) + h_{d_2}(n)) \\ &- \delta \sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} 1_{[1,N]}(x + g_{d_1}(m) + h_{d_2}(n))1_A(x) \\ &+ \delta^2 \sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} 1_{[1,N]}(x)1_{[1,N]}(x + g_{d_1}(m) + h_{d_2}(n)) \\ &\leq \Big(\delta^2 N - 2\delta|A \cap (N/9, 8N/9)|\Big)|H|.\end{aligned}$$

Therefore, if $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then by (43) we have

$$\sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} f_A(x)f_A(x + g_{d_1}(m) + h_{d_2}(n)) \leq -\delta^2 NM/4. \tag{44}$$

We see from (42) and the orthogonality relation

$$\int_0^1 e^{2\pi i n\alpha} d\alpha = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \in \mathbb{Z} \setminus \{0\} \end{cases}$$

that

$$\sum_{\substack{x\in\mathbb{Z}\\(m,n)\in H}} f_A(x)f_A(x + g_{d_1}(m) + h_{d_2}(n)) = \int_0^1 |\widehat{f_A}(\alpha)|^2 S(\alpha)d\alpha + O_{g,h}(N(w_1M_1 + w_2M_2)), \tag{45}$$

where

$$S_1(\alpha) = \sum_{\substack{m=1\\W_{d_1}^{(1)}(Y)}}^{M_1} e^{2\pi i g_{d_1}(m)\alpha}, \quad S_2(\alpha) = \sum_{\substack{n=1\\W_{d_2}^{(2)}(Y)}}^{M_2} e^{2\pi i h_{d_2}(n)\alpha}, \quad \text{and} \quad S(\alpha) = S_1(\alpha)S_2(\alpha).$$

Combining (44) and (45), we have

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S(\alpha)| d\alpha \geq \delta^2 NM/8. \tag{46}$$

Letting $\gamma = \eta^{-2D}/N$, the estimates in Section 4 yield that if $d_1, d_2, \delta^{-1} \leq \mathcal{Q}$, then for $\alpha \in \mathbf{M}_q(\gamma)$, $q \leq Q$, we have

$$|S(\alpha)| \ll_{g,h} C^{\omega(q)} M/q, \tag{47}$$

where $C = C(k, \ell)$. Further, for $\alpha \in \mathfrak{m}(\gamma, Q)$ we have

$$|S(\alpha)| \leq \delta M/16, \tag{48}$$

provided c_0 is chosen sufficiently small. The verification of (47) and (48) is completely analogous to, though strictly easier than, the establishment of (21) and (22) in Section 4.1.

From (48) and Plancherel's Identity, we have

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

which together with (46) yields

$$\int_{\mathfrak{M}(\gamma,Q)} |\widehat{f_A}(\alpha)|^2 |S(\alpha)| d\alpha \geq \delta^2 NM/16. \tag{49}$$

From (47) and (49) , we have

$$\sum_{q=1}^{Q} \frac{C^{\omega(q)}}{q} \int_{\mathbf{M}_q(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \gg_{g,h} \delta^2 N. \tag{50}$$

The function $b(q) = C^{\omega(q)}$ satisfies $b(qr) \geq b(r)$, and we make use of the following proposition.

Proposition 5.5. *For any $\gamma, Q > 0$ satisfying $2\gamma Q^2 < 1$ and any function $b : \mathbb{N} \to [0, \infty)$ satisfying $b(qr) \geq b(r)$ for all $q, r \in \mathbb{N}$, we have*

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

Proof. By (37) we have

$$\begin{aligned}
\Big(\sum_{q=1}^{Q} b(q)\Big) \max_{q \leq Q} \int_{\mathbf{M}'_q(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha &\geq \sum_{q=1}^{Q} b(q) \int_{\mathbf{M}'_q(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \\
&= \sum_{q=1}^{Q} b(q) \sum_{r|q} \int_{\mathbf{M}_r(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \\
&= \sum_{r=1}^{Q} \int_{\mathbf{M}_r(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha \sum_{q=1}^{Q/r} b(qr) \\
&\geq \frac{Q}{2} \sum_{r=1}^{Q} \frac{b(r)}{r} \int_{\mathbf{M}_r(\gamma)} |\widehat{f_A}(\alpha)|^2 d\alpha,
\end{aligned}$$

where the last inequality comes from replacing $b(qr)$ with $b(r)$, and the proposition follows. ☐

Invoking the known estimate

$$\sum_{q=1}^{Q} C^{\omega(q)} \ll_C Q \log^C Q$$

for any $C > 0$ (see [24]), the lemma follows from (50) and Proposition 5.5. ☐

5.6. **Discussion of the case** $\deg(g) = \deg(h) = 2$ **and sums of** $\ell \geq 3$ **polynomials.** In the case that $\deg(g) = \deg(h) = 2$, the desired square root cancellation is already present in the complete exponential sums, and hence no sieving of inputs is required. This allows us to take $\mathcal{Q} = \mathcal{Q}(N) = N^\rho$ instead of $\mathcal{Q} = e^{\rho\sqrt{\log N}}$. Further, the $C^{\omega(q)}$ term is absent from the estimate (47), which allows us to replace $\log^{-C}(\delta^{-1})$ with a small constant c in the conclusions of Lemmas 5.2 and 5.3. Appropriately adjusting the proof in Section 5.2 yields

$$\delta \ll_{g,h} e^{-c\sqrt{\log N}},$$

as claimed.

The $C^{\omega(q)}$ term can also be removed from (47) if we consider sums of three or more intersective polynomials, and we can avoid sieving provided the reciprocals of the degrees of these polynomials add to at least 1. These observations yield the following result, with which we conclude our discussion.

Theorem 5.6. *Suppose $\ell \geq 3$, $h_1, \dots, h_\ell \in \mathbb{Z}[x]$ are intersective polynomials, and $A \subseteq [1, N]$. If*

$$a - a' \neq \sum_{i=1}^{\ell} h_i(n_i)$$

for all distinct pairs $a - a'$ and all $n_1, \dots, n_\ell \in \mathbb{N}$, then

$$\frac{|A|}{N} \ll_{h_1,\dots,h_\ell} e^{-c(\log N)^\mu},$$

where

$$\mu = \begin{cases} 1/2 & \text{if } \sum_{i=1}^{\ell} \deg(h_i)^{-1} \geq 1 \\ 1/4 & \text{else} \end{cases}.$$

Acknowledgements: The author would like to thank Steve Gonek and Paul Pollack for their helpful comments and references, as well as Neil Lyall for his perpetual support.

References

[1] A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference sets without κ-th powers*, Acta. Math. Hungar. 65 (2) (1994), 165-187.
[2] J.R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719.
[3] E. Croot, N. Lyall, A. Rice, *Polynomials and primes in generalized arithmetic progressions*, Int. Math. Res. Not., no. 15 (2015), 6021-6043.
[4] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), 204-256.
[5] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour. 114 (2002) no.2, 215-238.
[6] 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/.
[7] M. Hamel, N. Lyall, A. Rice, *Improved bounds on Sárközy's theorem for quadratic polynomials*, Int. Math. Res. Not. no. 8 (2013), 1761-1782
[8] E. Kowalski, *Exponential sums over finite fields I: elementary methods*, http://www.math.ethz.ch/ kowalski/exp-sums.pdf
[9] T. Kamae, M. Mendès France, *van der Corput's difference theorem*, Israel J. Math. 31, no. 3-4, (1978), pp. 335-342.
[10] S. Lang, *Algebraic number theory*, third edition, Springer-Verlag, 1994.
[11] M. Lewko, *An improved lower bound related to the Sárközy-Furstenberg Theorem*, Electron. J. Combin. 22 (2015), No. 32, 1-6.
[12] H.-Z. Li, H. Pan, *Difference sets and polynomials of prime variables*, Acta. Arith. 138, no. 1 (2009), 25-52.
[13] J. Lucier, *Difference sets and shifted primes*, Acta. Math. Hungar. 120 (2008), 79-102.
[14] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. 123 (2006), 57-95.
[15] N. Lyall, *A new proof of Sárközy's theorem*, Proc. Amer. Math. Soc. 141 (2013), 2253-2264.
[16] N. Lyall, À. Magyar, *Polynomial configurations in difference sets*, J. Number Theory 129 (2009), 439-450.
[17] 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.
[18] 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.
[19] A. Rice, *Sárközy's theorem for $\mathcal{P}$-intersective polynomials*, Acta Arith. 157 (2013), no. 1, 69-89.
[20] I. Ruzsa, *Difference sets without squares*, Period. Math. Hungar. 15 (1984), 205-209.
[21] I. Ruzsa, T. Sanders, *Difference sets and the primes*, Acta. Arith. 131, no. 3 (2008), 281-301.
[22] A. Sárközy, *On difference sets of sequences of integers I*, Acta. Math. Hungar. 31(1-2) (1978), 125-149.
[23] A. Sárközy, *On difference sets of sequences of integers III*, Acta. Math. Hungar. 31(3-4) (1978), 355-386.
[24] A. Selberg, *A note on a paper of J. G. Sathe*, J. Indian Math. Soc. 18 (1954), 83-87.
[25] S. Slijepčević, *A polynomial Sárközy-Furstenberg theorem with upper bounds*, Acta Math. Hungar. 98 (2003), 275-280.
[26] T.D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, Duke Math. J. 162 (2013), 673-730.

Department of Mathematics, Millsaps College, Jackson, MS 39202

E-mail address: riceaj@millsaps.edu