POLYNOMIALS AND PRIMES IN GENERALIZED ARITHMETIC PROGRESSIONS (REVISED VERSION)

ERNIE CROOT NEIL LYALL ALEX RICE

Abstract. We provide upper bounds on the density of a symmetric generalized arithmetic progression lacking nonzero elements of the form $h(n)$ with $n \in \mathbb{N}$ or $h(p)$ with p prime for appropriate $h \in \mathbb{Z}[x]$. The prime variant can be interpreted as a multi-dimensional, polynomial extension of Linnik's Theorem. This version is a revision of the published version. Most notably, the properness hypotheses have been removed from Theorems 2 and 3, and the numerology in Theorem 2 has been improved.

1. Introduction

Given $N \in \mathbb{N}$, it is rather trivial to determine, up to a multiplicative constant, how large an arithmetic progression of the form $A = \{xd : 1 \le x \le L\} \subseteq [1, N] := \{1, \dots, N\}$ can be before it is guaranteed to contain a nonzero perfect square. Specifically, $d^2 \in A$ if $L \ge d$, so if A contains no squares, then $L^2 < Ld \le N$, and therefore $L < \sqrt{N}$. To observe the sharpness of this bound, fix any prime $p \in [\sqrt{N}/2, \sqrt{N}]$ and let $A = \{xp : 1 \le x \le p-1\}$. However, with an additional degree of freedom, say if

$$A = \{x_1 d_1 + x_2 d_2 : \ |x_1| \le L_1, \ |x_2| \le L_2\} \subseteq [-N, N],$$

the analogous question becomes far less trivial. We begin the exploration of such questions with a standard definition.

Definition 1. A *generalized arithmetic progression (GAP)* of dimension k (in $\mathbb{Z}$) is a set of the form

$$A = \{a + x_1 d_1 + \cdots + x_k d_k \ : \ 1 \le x_i \le L_i\},$$

where a, $x_i \in \mathbb{Z}$ and d_i, $L_i \in \mathbb{N}$. A is called *symmetric* if it takes the form

$$A = \{x_1 d_1 + \cdots + x_k d_k \ : \ |x_i| \le L_i\}.$$

In Section 3.1, before delving into our more general main results, we give a pleasingly brief, essentially self-contained proof of the following upper bound in the two-dimensional case, with an additional simplifying assumption to suppress any obscuring technical details.

Theorem 1. *Suppose $A = \{x_1 d_1 + x_2 d_2 : |x_1| \le L_1, \ |x_2| \le L_2\} \subseteq [-N, N]$ is proper, which is to say*

$$|A| = (2L_1 + 1)(2L_2 + 1).$$

If $L_2 d_2 \ge L_1 d_1$, d_2 is prime, and A contains no nonzero squares, then

$$|A| \ll N^{5/6} (\log N)^{1/3}.$$

Notational Remark. We shall frequently employ the $\ll$ symbol to mean "less than a constant times", utilizing subscripts to indicate what the implied constant depends on. In the absence of a subscript, the implied constant is absolute.

Comparing Theorem 1 to the trivial and sharp bound of $\sqrt{N}$ in the one-dimensional case, it is natural to ask if one can construct a family of examples of two-dimensional GAPs $A \subset [-N, N]$ with no nonzero squares and $|A|$ significantly greater than $\sqrt{N}$. This sort of lower bound, in this and more general contexts, has thus far proven elusive, and any such examples would be rather interesting.

2000 *Mathematics Subject Classification.* 11B30.

1.1. **Main Results.**

1.1.1. *Intersective polynomials.* One can generalize the inquiries mentioned thus far in the following way: given a polynomial $h \in \mathbb{Z}[x]$, how large can a symmetric GAP of dimension k be before it is guaranteed to contain a nonzero element in the image of h? The following definition encapsulates the largest possible class of polynomials for which a meaningful result of this type is possible.

Definition 2. A polynomial $h \in \mathbb{Z}[x]$ is *intersective* if for every $q \in \mathbb{N}$, there exists $r \in \mathbb{Z}$ such that $q \mid h(r)$.

Intersective polynomials include all polynomials with an integer root, but also include certain polynomials without rational roots such as $(x^3-19)(x^2+x+1)$. In this context it is clear that the intersective condition is necessary, as if $h \in \mathbb{Z}[x]$ has no root modulo q, a symmetric GAP $A = \{x_1d_1 + \cdots + x_kd_k \ : \ |x_i| \leq L_i\}$ completely misses the image of h whenever $q \mid d_i$ for all $1 \leq i \leq k$. Our first main result is the following.

Theorem 2. *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree ℓ and $A \subseteq [-N, N]$ is a symmetric GAP of dimension k. If $A \cap h(\mathbb{Z}) \subseteq \{0\}$, then*

$$|A| \ll_h N^{1-\left(\ell(2^{\ell+2}+1)^{k-1}\right)^{-1}} (6k)^{2k} \log N.$$

The bound in Theorem 2 is meaningful for a somewhat small range of dimensions (up to about $k = \log\log N$), but it gives the expected power saving in low dimensions. We include the intersective hypothesis in Theorem 2 because those are the only polynomials that are compatible with *all* GAPs, but given a fixed GAP, the polynomial only needs to have roots at certain moduli, as indicated by the result's more precise formulation in Section 3.

1.1.2. *$\mathcal{P}$-intersective polynomials.* If we further modify this discussion by restricting the inputs for our polynomials to the primes, which we denote by $\mathcal{P}$, we need to further restrict the class of admissible polynomials, leading to the following definition.

Definition 3. A polynomial $h \in \mathbb{Z}[x]$ is *$\mathcal{P}$-intersective* if for every $q \in \mathbb{N}$, there exists $r \in \mathbb{Z}$ such that $q \mid h(r)$ and $(r, q) = 1$.

$\mathcal{P}$-intersective polynomials include all polynomials with a root at 1 or -1, but again include polynomials without rational roots, in fact the previous example $(x^3-19)(x^2+x+1)$ still qualifies. The necessity of this condition in this context is again clear, and our second main result is the following.

Theorem 3. *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective polynomial of degree ℓ and $A \subseteq [-N, N]$ is a symmetric GAP of dimension $k \leq c(\log\log N)/\ell$ for a sufficiently small absolute constant $c > 0$. If $A \cap h(\mathcal{P}) \subseteq \{0\}$, then*

$$|A| \ll_h N^{1-c^k 5^{-\ell k}}.$$

Remark relating Theorem 3 to Linnik's theorem. As with Theorem 2, we give a sharper version of this result in Section 4 in which we fix a GAP and only insist that the polynomial has coprime roots at certain moduli, a result that can be interpreted as a multi-dimensional, polynomial extension of Linnik's theorem. Specifically, after some rearrangement of the traditional statement, Linnik's theorem says that if $|a| \leq d$ with $(a, d) = 1$ and $p - a \notin \{xd : |x| \leq L\}$ for all $p \in \mathcal{P}$, then $L \ll (Ld)^{1-\epsilon}$ for some $\epsilon > 0$ (it is proven that $\epsilon \geq 1/5$ [25] and conjectured that $\epsilon = 1/2$). Our refinement of Theorem 3, the proof of which prominently utilizes a quantitative version of Linnik's theorem, says that if $h \in \mathbb{Z}[x]$ with $\deg(h) = \ell$ has a coprime root modulo d_i for $1 \leq i \leq k$, $A = \{x_1d_1 + \cdots + x_kd_k : |x_i| \leq L_i\}$ and $A \cap h(\mathcal{P}) \subseteq \{0\}$, then

$$\prod_{i=1}^{k} L_i \ll_h \Big(\sum_{i=1}^{k} L_i d_i\Big)^{1-\epsilon}$$

for some $\epsilon = \epsilon(k, \ell) > 0$. In the traditional case of $h(p) = p - a$, close inspection of the argument reveals that the implied constant can be taken independent of a, as required for a true generalization of Linnik's theorem, provided for example that $|a| \leq \min\{d_i\}_{i=1}^{k}$.

1.2. **Motivation from Difference Sets.** In a series of papers in the late 1970s, Sárközy ([19], [20]) showed that a set of natural numbers of positive upper density necessarily contains two distinct elements which differ by a perfect square, as well as two elements which differ by one less than a prime number, verifying conjectures of Lovász and Erdős, respectively. An extensive literature has been developed on extensions and quantitative improvements of these results, for which the reader may refer to [14], [1], [22], [10], [12], [7], [4], [11], [9], [17], [8] and [16]. For a survey of many of these developments, the reader may refer to Chapter 1 of [15]. The following theorems summarize the best known bounds analogous to Theorems 2 and 3 for the difference set $A - A = \{a - a' \ : \ a, a' \in A\} \subseteq \mathbb{Z}$.

Theorem A ([1], [4], [10], [15]). *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree $\ell \geq 2$. If $A \subseteq [1, N]$ and $(A - A) \cap h(\mathbb{N}) \subseteq \{0\}$, then*

$$\frac{|A|}{N} \ll_{h,\mu} \begin{cases} (\log N)^{-\mu \log\log\log\log N} & \text{if } \ell = 2 \text{ or } h(x) = x^\ell \\ \left(\frac{\log\log N}{\log N}\right)^{1/(\ell-1)} & \text{else} \end{cases}$$

for any $\mu < 1/\log 3$.

Theorem B ([17], [16]). *Suppose $h \in \mathbb{Z}[x]$ is a $\mathcal{P}$-intersective polynomial of degree $\ell \geq 2$. If $A \subseteq [1, N]$ and $(A - A) \cap h(\mathcal{P}) \subseteq \{0\}$, then*

$$\frac{|A|}{N} \ll_{h,\mu} \begin{cases} e^{-c(\log N)^{1/4}} & \text{if } \ell = 1 \\ (\log N)^{-\mu} & \text{if } \ell \geq 2 \end{cases} \tag{1}$$

for any $\mu < 1/(2\ell - 2)$, where $c > 0$ is an absolute constant.

The original theorems of Sárközy, and the improvements and extensions thereof, are examples of the more general philosophy that sets which are in a sense "randomly distributed" and avoid certain local biases (such as shifted primes or the image of an intersective polynomial) should always intersect predictably with structured, centrally symmetric sets (such as a difference set). Perhaps the simplest and most explicit example of a highly structured, centrally symmetric set is a low-dimensional symmetric GAP, so the known results for difference sets foreshadow the possibility that similar results for GAPs may be available with more elementary methods and better bounds. In a sense, these questions for GAPs can be interpreted as a "fantasy model" for the analogous questions for less understood objects like difference sets.

1.3. **Diophantine Approximation and Expected Bounds.** We conclude this introductory section with an attempt to contextualize our results as being in some sense parallel to far more well-studied questions in Diophantine approximation, and we attempt to provide some intuition and motivation for what sort of bounds we expect to hold in place of those in Theorems 2 and 3. We speak rather informally, in particular the referenced results are somewhat roughly approximated, and we make light of the distinction between an interval of integers $[-N, N]$ and a finite cyclic group $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$.

We continue the theme of the previous section by considering another related example of a highly structured, centrally symmetric set. Given a natural number N, a set of frequencies $\Gamma = \{\xi_1, \dots, \xi_k\} \subseteq \mathbb{Z}_N$, and $\epsilon > 0$, the Bohr set $B = B(\Gamma, \epsilon) \subseteq \mathbb{Z}_N$ is defined by

$$B = \{x \in \mathbb{Z}_N \ : \ \|x\xi_j/N\| < \epsilon \text{ for } 1 \leq j \leq k\},$$

where $\|\cdot\|$ denotes the distance to the nearest integer. We refer to k as the *rank* of B. If we pose the analogous questions for Bohr sets that we have been considering for symmetric GAPs, then we wade into questions of Diophantine approximation. An example of such an analog is the following result of Green and Tao, a refinement of an argument due to Schmidt [21].

Theorem C (Proposition A.2 in [3]). *Given $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ and $N \in \mathbb{N}$, there exists an integer $1 \leq n \leq N$ such that*

$$\|n^2\alpha_j\| \ll kN^{-c/k^2} \quad \text{for all} \quad 1 \leq j \leq k.$$

The second and third authors further adapted this argument to include all intersective polynomials.

Theorem D (Theorem 1 in [13]). *Given $\alpha_1, \dots, \alpha_k \in \mathbb{R}$, an intersective polynomial $h \in \mathbb{Z}[x]$ of degree ℓ, and $N \in \mathbb{N}$, there exists an integer $1 \le n \le N$ with $h(n) \neq 0$ and*

$$\|h(n)\alpha_j\| \ll_h kN^{-c^\ell/k^2} \text{ for all } 1 \le j \le k,$$

where $c > 0$ is an absolute constant.

In particular, Theorem D says that a Bohr set $B \subseteq \mathbb{Z}_N$ of rank k contains a nonzero element in the image of h provided the radius is at least a large constant times kN^{-c^ℓ/k^2}. Probabilistically, we expect a Bohr set $B \subseteq \mathbb{Z}_N$ of rank k and radius ϵ to have size about $\epsilon^k N$, suggesting that if $B \cap h(\mathbb{N}) \subseteq \{0\}$ and k is much smaller than $\sqrt{\log N}$, then

$$|B| \ll_h N^{1-c^\ell/k}. \tag{2}$$

It is conjectured that the k^2 in the exponent in Theorem B can be replaced with $k^{1+o(1)}$, suggesting bounds even stronger than (2).

Bohr sets and symmetric GAPs can be thought of as similar, intimately related objects. Like a symmetric GAP, a Bohr set is a centrally symmetric set with a great deal of structure mimicking that of a subgroup. It is a standard fact (see [23] for example) that a Bohr set $B \subseteq \mathbb{Z}_N$ of rank k and radius ϵ contains a symmetric GAP $A \subseteq \mathbb{Z}_N$ (defined analogously to a GAP in $\mathbb{Z}$) of dimension k with $|A| \ge (\epsilon/k)^k N$. Conversely, if $A \subseteq \mathbb{Z}_N$ is a symmetric GAP of dimension k with $|A| = \delta N$, then work of Sanders [18] and Croot, Laba, and Sisask [2] shows that A contains a Bohr set of rank roughly $\log(1/\delta) + k^4$ and radius roughly 2^{-k}. The latter conclusion combines with Theorem D to yield

$$h \in \mathbb{Z}[x] \text{ intersective }, \ A \cap h(\mathbb{Z}) \subseteq \{0\} \Longrightarrow |A| \ll N \exp\big(c(k^4 - \sqrt{\log N/k})\big). \tag{3}$$

Compared to Theorem 2, this result is nontrivial for a much larger range of dimensions, up to about $k = (\log N)^{1/9}$, but requires much heavier machinery and provides unsatisfying bounds in low dimensions. In contrast, our proofs of Theorems 2 and 3 rely only on very basic Fourier analytic methods and standard number theory and circle method facts.

Due to the aforementioned intimate connections between symmetric GAPs and Bohr sets, we believe that the analysis of polynomial configurations in Bohr sets via Diophantine approximation provides meaningful insight into the analogous questions for GAPs. The structure of a Bohr set is richer than that of a GAP, so for now we tread lightly with our conjectures, but these heuristics for bounds like (2) (or beyond) suggest that the doubly exponential dependence on the dimension k in Theorems 2 and 3 is far from the truth. We return to the consideration of improved bounds in Section 5.

Funding

The first author was partially supported by National Science Foundation Grant DMS-1001111. The second author was partially supported by Simons Foundation Collaboration Grant for Mathematicians 245792.

Acknowledgements

The authors would like to thank Paul Pollack for helpful comments, as well as the referees for their helpful corrections and recommendations.

2. Preliminaries

2.1. **Fourier Analysis on $\mathbb{Z}/d\mathbb{Z}$.** For $d \in \mathbb{N}$ and a complex-valued function f on $\mathbb{Z}_d := \mathbb{Z}/d\mathbb{Z}$, we utilize the unnormalized, discrete Fourier transform $\widehat{f} : \mathbb{Z}_d \to \mathbb{C}$, defined by

$$\widehat{f}(t) = \sum_{x \in \mathbb{Z}_d} f(x) e^{-2\pi i x t/d}.$$

In this discrete setting, the Fourier inversion formula

$$f(x) = \frac{1}{d}\sum_{t\in\mathbb{Z}_d} \widehat{f}(t)e^{2\pi ixt/d} \tag{4}$$

is a simple consequence of the orthogonality relation

$$\frac{1}{d}\sum_{t\in\mathbb{Z}_d} e^{2\pi ixt/d} = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \in \mathbb{Z}_d \setminus \{0\} \end{cases}. \tag{5}$$

For two functions $f, g : \mathbb{Z}_d \to \mathbb{C}$, we define the convolution $f * g : \mathbb{Z}_d \to \mathbb{C}$ by

$$f * g(x) = \sum_{y\in\mathbb{Z}_d} f(y)g(x-y),$$

and the property

$$\widehat{f * g}(t) = \widehat{f}(t)\widehat{g}(t) \tag{6}$$

also follows quickly from (5).

2.2. **Exponential Sum Estimates.** The key to the argument, as is often the case, is to take advantage of cancellation in exponential sums over the image of a polynomial away from rationals with small denominator. First, we include a proof of the standard estimate in the special case of quadratic polynomials, with a view toward a self-contained proof of Theorem 1.

Lemma 1. *If $t, a_1, a_2 \in \mathbb{Z}$ and $n, d \in \mathbb{N}$, then*

$$\Big|\sum_{m=1}^{n} e^{2\pi i(a_1m+a_2m^2)t/d}\Big| \le \Big(2n^2/d' + 7(n+d')\log d'\Big)^{1/2},$$

where $d' = d/(2a_2t, d)$.

Proof. Using a change of variables ($m = s + h$), we see

$$\Big|\sum_{m=1}^{n} e^{2\pi i(a_1m+a_2m^2)t/d}\Big|^2 = \sum_{m,s=1}^{n} e^{2\pi i\Big((a_1m+a_2m^2)-(a_1s+a_2s^2)\Big)t/d} = \sum_{s=1}^{n}\sum_{h=1-s}^{n-s} e^{2\pi i\Big(a_2(2sh+h^2)+a_1h\Big)t/d}$$

$$= n + \sum_{h=1}^{n-1}\sum_{s=1}^{n-h} e^{2\pi i\Big(a_2(2sh+h^2)+a_1h\Big)t/d} + \sum_{h=1-n}^{-1}\sum_{s=1-h}^{n} e^{2\pi i\Big(a_2(2sh+h^2)+a_1h\Big)t/d}$$

$$\le n + 2\sum_{h=1}^{n-1}\Big|\sum_{s=1}^{n-h} e^{2\pi ish(2a_2t)/d}\Big|.$$

Writing $2a_2t/d = t'/d'$ with $(t', d') = 1$, letting $\|\cdot\|$ denote distance to the nearest integer, and applying the geometric series formula, we have

$$\sum_{h=1}^{n-1}\Big|\sum_{s=1}^{n-h} e^{2\pi isht'/d'}\Big| \le \sum_{h=1}^{n-1}\min\{n, (2\|ht'/d'\|)^{-1}\} \le \Big(\frac{n}{d'}+1\Big)\Big(n + \sum_{h=1}^{d'-1}\frac{d'}{h}\Big) \le n^2/d' + 3(n+d')\log d',$$

provided $d' > 1$ (the lemma is trivial if $d' = 1$), and the result follows. □

For more general polynomials, we first invoke the following standard bound obtained from Weyl differencing.

Lemma 2 (Proposition 8.2 in [6])**.** *If $h(x) = \alpha x^\ell + \cdots \in \mathbb{R}[x]$, then*

$$\Big|\sum_{m=1}^{n} e^{2\pi ih(m)}\Big| \ll n\Big(n^{-\ell}\sum_{-n<m_1,\dots,m_{\ell-1}<n}\min\{n, \|\alpha\ell!m_1\dots m_{\ell-1}\|^{-1}\}\Big)^{2^{1-\ell}}.$$

From Lemma 2, we deduce the following refined version of Weyl's Inequality by exploiting the second moment, as opposed to the maximum value, of an appropriate divisor function.

Lemma 3. *Suppose $h(x) = a_0 + a_1 x + \cdots + a_\ell x^\ell$ with $a_i \in \mathbb{R}$ and $a_\ell \in \mathbb{N}$. If $(t,d) = 1$ and $|\alpha - t/d| < d^{-2}$, then*

$$\Big|\sum_{m=1}^{n} e^{2\pi i h(m)\alpha}\Big| \ll_\ell n\Big(a_\ell \log^{\ell^2}(a_\ell dn)(1/d + 1/n + d/a_\ell n^\ell)\Big)^{2^{-\ell}}.$$

Proof. We begin by recalling that if $d_j(m) = \Big|\{(a_1,\dots,a_j) : a_i \in \mathbb{N},\ a_1\cdots a_j = m\}\Big|$, then we know from standard estimates (see [6] for example) that

$$\sum_{m=1}^{M} d_j(m)^2 \ll_j M\log^{j^2-1}(M). \tag{7}$$

Applying Lemma 2, Cauchy-Schwarz, and (7), we have

$$\begin{aligned}
\Big|\sum_{m=1}^{n} e^{2\pi i h(m)\alpha}\Big| &\ll n\Big(n^{-\ell}\sum_{-n<m_1,\dots,m_{\ell-1}<n} \min\{n, \|\alpha \ell! a_\ell m_1\dots m_{\ell-1}\|^{-1}\}\Big)^{2^{1-\ell}} \\
&\ll_\ell n^{1-\ell 2^{1-\ell}}\Big(n^{\ell-1} + \sum_{1\le m\le n^{\ell-1}} d_{\ell-1}(m)\min\{n, \|\alpha\ell! a_\ell m\|^{-1}\}\Big)^{2^{1-\ell}} \\
&\le n^{1-\ell 2^{1-\ell}}\Big(n^{\ell-1} + \big(\sum_{1\le m\le n^{\ell-1}} d_{\ell-1}(m)^2\big)^{1/2}\big(\sum_{1\le m\le n^{\ell-1}} \min\{n, \|\alpha\ell! a_\ell m\|^{-1}\}^2\big)^{1/2}\Big)^{2^{1-\ell}} \\
&\ll_\ell n^{1-\ell 2^{1-\ell}}\Big(n^{\ell-1} + n^{\ell/2}\log^{\frac{\ell^2-1}{2}}(n)\big(\sum_{1\le m\le n^{\ell-1}} \min\{n, \|\alpha\ell! a_\ell m\|^{-1}\}\big)^{1/2}\Big)^{2^{1-\ell}}.
\end{aligned}$$

By Lemma 2.2 in [24], we know that if $|\alpha - t/d| < d^{-2}$ with $(t,d) = 1$, then

$$\sum_{1\le m\le n^{\ell-1}} \min\{n, \|\alpha\ell! a_\ell m\|^{-1}\} \ll a_\ell n^\ell \log(a_\ell dn)\Big(1/d + 1/n + d/a_\ell n^\ell\Big),$$

and the result follows. □

For the primes we invoke the following analog of Weyl's inequality, a nominal generalization of Theorem 4.1 in [8], extracted in a slightly more precise way as compared to Lemma 12 in [16].

Lemma 4. *Suppose $h(x) = a_0 + a_1 x + \cdots + a_\ell x^\ell \in \mathbb{Z}[x]$ with $a_\ell > 0$, and let $L = 64\ell^2 4^\ell$. If $U \ge \log n$, $a_\ell \ge C\Big(|a_{\ell-1}| + \cdots + |a_0|\Big)$, and $q, |r|, a_\ell \le U^\ell$, then*

$$\sum_{\substack{m=1\\ qm+r\in\mathcal{P}}}^{n} \log(qm+r)e^{2\pi i h(m)\alpha} \ll_C \frac{n}{U} + U^L n^{1-4^{-\ell}}$$

provided

$$|\alpha - t/d| < d^{-2} \quad \text{for some} \quad U^L \le d \le h(n)/U^L \quad \text{and} \quad (t,d) = 1.$$

Because Lemma 4 does not give any information for very small denominators, we require the following high-moment estimate, which follows in particular from a solution to the Waring-Goldbach problem (see [5] for example).

Lemma 5. *If $h \in \mathbb{Z}[x]$ with $\deg(h) = \ell$ and $s > 2^\ell$, then*

$$\sum_{t \in \mathbb{Z}_d} \Big| \sum_{\substack{m=1 \\ qm+a \in \mathcal{P}}}^{n} \log(qm+a) e^{2\pi i h(m) t/d} \Big|^s \ll_h d n^{s-\ell} + n^s.$$

2.3. **Primes in Arithmetic Progressions.** In order to obtain the bound purported in Theorem 3, we need a quantitative strengthening of Linnik's theorem, which says that if $(a,q) = 1$, then there are plenty of primes less than a parameter x which are congruent to a modulo q, even if q is as large as a small power of x. This exceeds, at the expense of a sharp asymptotic formula, the allowed modulus size for usual prime number theorems for arithmetic progressions.

Lemma 6 (Quantitative Linnik's theorem, Corollary 18.8 in [6])**.** *If $(a,q) = 1$ and $q \le cx^c$ for a sufficiently small constant $c > 0$, then*

$$\psi(x,a,q) := \sum_{\substack{p \in \mathcal{P} \cap [1,x] \\ p \equiv a \bmod q}} \log p \gg \frac{x}{\phi(q)\sqrt{q}},$$

where ϕ is the Euler totient function.

The requisite tools are now in place for us to proceed with proving Theorems 1, 2, and 3.

3. Intersective Polynomials

3.1. **The Model Case.** In this section, we prove the simplest nontrivial extension of the initial trivial observation made in the introduction, which exposes the fundamental ideas of our general argument.

Proof of Theorem 1. Suppose $A = \{x_1 d_1 + x_2 d_2 : |x_1| \le L_1,\ |x_2| \le L_2\} \subseteq [-N, N]$ is proper, $L_2 d_2 \ge L_1 d_1$, and $d_2 \in \mathcal{P}$. Let $n = (L_2 d_2/4)^{1/2}$. Suppose further that A contains no nonzero squares, which crucially means that no sufficiently small square is congruent to any sufficiently small multiple of d_1 modulo d_2.

Let $A_1 = \{x d_1 : |x| \le L_1/4\} \subseteq \mathbb{Z}_{d_2}$. We note that, by properness and the fact that $L_1 d_1 \le L_2 d_2$, all of these multiples of d_1 reduce to distinct residues modulo d_2, and in particular $|A_1| \gg L_1$. We define f as a function on $\mathbb{Z}_{d_2}$ by

$$f(x) = |A_1|^{-1} 1_{A_1} * 1_{A_1}(x).$$

Clearly f is a nonnegative function supported on $\{x d_1 : |x| \le L_1/2\} \subseteq \mathbb{Z}_{d_2}$ and $f(x) \le f(0) = 1$. The symmetry of A_1 makes $\widehat{1_{A_1}}$ a real-valued function, and by (6) we know that $\widehat{f}(t) = |A_1|^{-1} \widehat{1_{A_1}}(t)^2$, therefore

$$0 \le \widehat{f}(t) \le \widehat{f}(0) = |A_1|.$$

We note that if $f(m^2) > 0$ for some $1 \le m \le n$, then there exists x with $|x| \le L_1/2$ and $x d_1 \equiv m^2 \mod d_2$. In other words, $x d_1 - m^2 = \ell d_2$ and

$$|\ell| \le (L_1 d_1/2 + m^2)/d_2 \le (L_2 d_2/2 + L_2 d_2/2)/d_2 = L_2,$$

hence $m^2 = x d_1 - \ell d_2 \in A$. Therefore, since we assumed A contained no nonzero squares, it follows from the orthogonality relation (5) that

$$d_2 \sum_{1 \le m \le n} f(m^2) = \sum_{t \in \mathbb{Z}_{d_2}} \widehat{f}(t) W(t) = 0,$$

where

$$W(t) = \sum_{m=1}^{n} e^{2\pi i m^2 t/d_2}.$$

Combined with the positivity of $\widehat{f}$, this yields

$$\sum_{t \ne 0} \widehat{f}(t) |W(t)| \ge \widehat{f}(0) W(0) \gg L_1 (L_2 d_2)^{1/2}. \tag{8}$$

Since $d_2 \in \mathcal{P}$ and $n \le d_2$, as otherwise $d_2^2 \in A$, we have from Lemma 1 that

$$|W(t)| \ll (d_2 \log d_2)^{1/2} \text{ for all } t \neq 0,$$

which by the Fourier inversion formula (4) and the fact that $f(0) = 1$ gives

$$\sum_{t \neq 0} \widehat{f}(t)|W(t)| \ll (d_2 \log d_2)^{1/2} \sum_{t \in \mathbb{Z}_{d_2}} \widehat{f}(t) = (d_2 \log d_2)^{1/2} d_2 f(0) \le d_2 (d_2 \log N)^{1/2}. \tag{9}$$

Combining (8) and (9), we have

$$L_1 (L_2 d_2)^{1/2} \ll d_2 (d_2 \log N)^{1/2},$$

which can be manipulated to yield

$$|A| \ll L_1 L_2 \ll \frac{L_2 d_2}{L_2^{1/2}} (\log N)^{1/2} \le \frac{N}{L_2^{1/2}} (\log N)^{1/2}.$$

Further, we know from our discussion of the one dimensional case that $L_1 \ll N^{1/2}$, and hence

$$|A| \ll \min\{N^{1/2} L_2, \frac{N}{L_2^{1/2}} (\log N)^{1/2}\}.$$

The quantity on the right hand side is maximized when $L_2 = (N \log N)^{1/3}$, and the theorem follows. □

3.2. **The General Case.** In this section we prove Theorem 2 in a more flexible form, and we begin by making part of this flexibility precise with a definition.

Definition 4. For $M > 0$, we say that a GAP A is *M-proper* if each element of A is represented in at most M ways. In the case of a symmetric progression $A = \{x_1 d_1 + \cdots + x_k d_k : |x_i| \le L_i\}$, this means

$$\left| \left\{ (x_1, \ldots, x_k) \in \mathbb{Z}^k : |x_i| \le L_i,\ x_1 d_1 + \cdots + x_k d_k = x \right\} \right| \le M \text{ for all } x \in \mathbb{Z}.$$

We now deduce Theorem 2 from the following.

Theorem 4. *Suppose $A = \{x_1 d_1 + \cdots + x_k d_k :\ |x_i| \le L_i\} \subseteq [-N, N]$ is an M-proper, symmetric GAP with $L_1 \le \cdots \le L_k$, and suppose $h \in \mathbb{Z}[x]$ is a polynomial of degree ℓ which has a root modulo $\gcd(d_i, \ldots, d_k)$ for all $1 \le i \le k$. If $A \cap h(\mathbb{Z}) \subseteq \{0\}$, then*

$$\prod_{i=1}^{k} L_i \ll_h N^{1 - \left(\ell(2^{\ell+2}+1)^{k-1}\right)^{-1}} (4k)^k M \log N.$$

Proof that Theorem 4 implies Theorem 2. Suppose $A = \{x_1 d_1 + \cdots + x_k d_k :\ |x_i| \le L_i\} \subseteq [-N, N]$ and let

$$M = \max_{x \in \mathbb{Z}} \left| \left\{ (x_1, \ldots, x_k) \in \mathbb{Z}^k : |x_i| \le L_i,\ x_1 d_1 + \cdots + x_k d_k = x \right\} \right|$$

Fixing an $x \in \mathbb{Z}$ at which this maximum is attained, we find by taking differences of the M representations of x that there are at least M representations

$$\begin{aligned} y_1^{(1)} + \cdots + y_k^{(1)} &= 0 \\ y_1^{(2)} + \cdots + y_k^{(2)} &= 0 \\ &\cdots \\ y_1^{(m)} + \cdots + y_k^{(m)} &= 0 \end{aligned}$$

with $|y_i| \le 2L_i$. In particular, there are at least M representations of every element of A inside the larger GAP $\{x_1 d_1 + \cdots + x_k d_k : |x_i| \le 3L_i\}$, and hence

$$M|A| \le \prod_{i=1}^{k} (6L_i + 1).$$

Theorem 2 then follows immediately from Theorem 4 □

We deduce Theorem 4 from the following lemma, which states that, provided there are no obvious local obstructions, a GAP contains a nonzero element in the image of a given polynomial as long as it is sufficiently "wide" in each direction. Theorem 4 then follows from an iteration that is responsible for the doubly exponential dependence on the dimension k in the final result.

Lemma 7. *Suppose $A = \{x_1d_1 + \cdots + x_kd_k : |x_i| \le L_i\} \subseteq [-N, N]$ is an M-proper, symmetric GAP with $L_1 \cdots L_k = \delta N$, and suppose $h \in \mathbb{Z}[x]$ is a polynomial of degree ℓ which has a root modulo $(d_1, \dots, d_k)$. If*

$$\min\{L_i\}_{i=1}^k \ge C\Big(M(4k)^k\delta^{-1}\log N\Big)^{2^{\ell+2}} \tag{10}$$

for a sufficiently large constant C depending only on h, then A contains a nonzero element of $h(\mathbb{Z})$.

3.2.1. *Proof of Theorem 4.* Fix an M-proper GAP

$$A_0 = \{x_1d_1 + \cdots + x_kd_k : |x_i| \le L_i\} \subseteq [-N, N]$$

with $L_1 \cdots L_k = \delta_0 N$, ordered such that $L_1 \le \cdots \le L_k$, and fix a polynomial $h \in \mathbb{Z}[x]$ of degree ℓ such that h has a root modulo $(d_i, \dots, d_k)$ for all $1 \le i \le k$ and $A \cap h(\mathbb{Z}) \subseteq \{0\}$. By Lemma 7, we know

$$L_1 \le C\Big(M(4k)^k\delta_0^{-1}\log N\Big)^{2^{\ell+2}},$$

and removing the first dimension yields

$$A_1 = \{x_2d_2 + \cdots + x_kd_k : |x_i| \le L_i\}$$

with $L_2 \cdots L_k = \delta_1 N$ and

$$\delta_1 = \delta_0/L_1 \ge C\Big(M(4k)^k\delta_0^{-1}\log N\Big)^{-(2^{\ell+2}+1)}.$$

Iterating this process yields GAPs

$$A_j = \{x_{j+1}d_{j+1} + \cdots + x_kd_k : |x_i| \le L_i\}$$

with $L_{j+1} \cdots L_k = \delta_j N$ and

$$\delta_j \ge \Big(CM(4k)^k\delta_0^{-1}\log N\Big)^{-(2^{\ell+2}+1)^j}$$

for $1 \le j \le k-1$. Further, if $r \in [0, d_k)$ is a root of h modulo d_k, then one of

$$\{h(r), h(r+d_k), \dots, h(r+(\ell+1)d_k)\},$$

call it $h(n)$, is nonzero, and hence $h(n) \notin A_k$. Therefore, since $d_k \mid h(n)$, it must be the case that

$$L_kd_k \le |h(n)| \ll_h d_k^\ell,$$

and hence

$$(\delta_{k-1}N)^{1+1/(\ell-1)} = L_k^{1+1/(\ell-1)} \ll_h L_kd_k \le N.$$

This implies that $\delta_{k-1} \ll_h N^{-1/\ell}$, hence

$$\Big(CM(4k)^k\delta_0^{-1}\log N\Big)^{(2^{\ell+2}+1)^{k-1}} \ge N^{1/\ell},$$

and the theorem follows. □

3.2.2. *Proof of Lemma 7.* Fix an M-proper GAP

$$A = \{x_1 D_1 + \cdots + x_k D_k : \ |x_i| \le L_i\} \subseteq [-N, N],$$

let $\delta = L_1 \cdots L_k / N$, let $q = (D_1, \ldots, D_k)$, and fix a polynomial $h \in \mathbb{Z}[x]$ of degree ℓ with a root modulo q, which by symmetry we can assume has positive leading coefficient. To show that A contains a nonzero element in the image of h, it suffices to show that

$$A' = \{x_1 d_1 + \cdots + x_k d_k : \ |x_i| \le L_i\}$$

contains an nonzero element in the image of $h_q(x) = h(r + qx)/q \in \mathbb{Z}[x]$, where $r \in [0, d)$ is a root of h modulo q and $d_i = D_i/q$. Let

$$S = \{m \in \mathbb{N} : 0 < h_q(m) < L_k d_k/2\}$$

and $n = \Big(\frac{L_k d_k}{2q^{\ell-1}b}\Big)^{1/\ell}$, where b is the leading coefficient of h, noting that

$$\Big|S \triangle [1, n]\Big| \ll_h 1. \tag{11}$$

For $1 \le i \le k-1$, assume without loss of generality that $L_i d_i \le L_k d_k$, let

$$A_i = \{x d_i : |x| \le L_i/4k\} \subseteq \mathbb{Z},$$

and define g_i, f_i as functions on $\mathbb{Z}_{d_k}$ by

$$g_i(x) = \sum_{|y| \le L_i/4k} 1_{y d_i}(x) \quad \text{and} \quad f_i(x) = |A_i|^{-1} g_i * g_i(x).$$

As in the model case, f_i is supported on $\{x d_i : |x| \le L_i/2k\} \subseteq \mathbb{Z}_{d_k}$ and

$$0 \le \widehat{f_i}(t) \le \widehat{f_i}(0) = |A_i|.$$

Letting $M_i = \max(f_i)$, we see that $\prod_{i=1}^{k-1} M_i \le M$ by M-properness, and $f_1 * \cdots * f_{k-1}(0)$ is bounded above by

$$\Big|\Big\{(x_1 d_1, \ldots, x_{k-1} d_{k-1}) \in \mathbb{Z}_{d_k}^{k-1} \ : \ |x_i| \le L_i/2k, \ x_1 d_1 + \cdots + x_k d_k \equiv 0 \mod d_k\Big\}\Big| \prod_{i=1}^{k-1} M_i \le M^2. \tag{12}$$

Further, if $f_1 * \cdots * f_{k-1}(h_q(m)) > 0$ for some $m \in S$, then $h_q(m) \in A'$, so we need only show

$$d_k \sum_{m \in S} f_1 * \cdots * f_{k-1}(h_q(m)) = \sum_{t \in \mathbb{Z}_{d_k}} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) W(t) > 0,$$

where the equality follows from (5) and

$$W(t) = \sum_{m \in S} e^{2\pi i h_q(m) t/d_k},$$

for which it suffices to show

$$\sum_{t \ne 0} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) |W(t)| < \widehat{f_1}(0) \cdots \widehat{f_{k-1}}(0) W(0) = (n + O_h(1)) \prod_{i=1}^{k-1} |A_i|, \tag{13}$$

where the estimate on $W(0)$ follows from (11). Noting that the leading coefficient of h_q is at most q^ℓ times the leading coefficient of h, and that $q \le \delta^{-1}$ by definition, we have from Lemma 3 and (11) that if $(t, d_k) = D$, then

$$|W(t)| \ll_h n\Big(\delta^{-\ell} \log^{\ell^2} N(D/d_k + 1/n + 1/DL_k)\Big)^{2^{-\ell}}. \tag{14}$$

We also have by (12) and the Fourier inversion formula that

$$\sum_{t \in \mathbb{Z}_{d_k}} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) = d_k f_1 * \cdots * f_{k-1}(0) \le M^2 d_k. \tag{15}$$

Further, we know that

$$d_k \le N/L_k = \Big(\prod_{i=1}^{k} L_i\Big)/\delta L_k \le \Big(\prod_{i=1}^{k-1} |A_i|\Big)(4k)^k/\delta. \tag{16}$$

By (14), (15), and (16), we see that for any $X > 0$

$$\sum_{(t,d_k)\le d_k/X} \widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t)|W(t)| \ll_h n\Big(\prod_{i=1}^{k-1}|A_i|\Big)\Big(\delta^{-\ell}\log^{\ell^2} N(1/X+1/n+1/L_k)\Big)^{2^{-\ell}} M^2(4k)^k/\delta \tag{17}$$

We see that if $(t,d_k) = D > d_k/X$, and $d_k/(t,d_k) \nmid d_j$, then

$$\widehat{f_j}(t) = |A_j|^{-1}\Big|\sum_{|x|\le L_j/4k} e^{2\pi i x d_j t/d_k}\Big|^2 \le |A_j|^{-1}\|d_j t/d_k\|^{-2} \le X^2/|A_j|,$$

where $\|\cdot\|$ denotes the distance to the nearest integer. Therefore,

$$\sum_{(t,d_k)=D} \widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t) \le X^2|A_j|^{-1}\sum_{D|t}\prod_{i\ne j}\widehat{f_i}(t) \le X^3\Big(\prod_{i=1}^{k-1}|A_i|\Big)/|A_j|^2. \tag{18}$$

There are trivially at most X divisors of d_k satisfying $D > d_k/X$, and since $(d_1,\dots,d_k) = 1$, (18) implies

$$\sum_{(t,d_k)>d_k/X} \widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t)|W(t)| \ll_h n\Big(\prod_{i=1}^{k-1}|A_i|\Big)X^4/\min\{|A_i|\}^2. \tag{19}$$

Setting $X = CM^{2^{\ell+1}}(4k)^{2^\ell k}(\log N)^{\ell^2}\delta^{-(2^\ell+\ell)}$ for a sufficiently large constant C depending on h, we see that if A satisfies (10), then

$$\min\{|A_i|\}_{i=1}^{k-1} \ge \min\{L_i\}_{i=1}^{k-1}/2k \ge C'X^2$$

for a sufficiently large constant C', provided the constant in (10) is sufficiently large with respect to the constant defining X. Combining (17) and (19), we see that the left-hand side of (13) is dominated by a small constant times the right-hand side of (13), and the lemma follows. □

4. $\mathcal{P}$-intersective Polynomials

Analogous to Section 3, we deduce Theorem 3 from the following result.

Theorem 5. *Suppose $A = \{x_1d_1+\cdots+x_kd_k : |x_i| \le L_i\} \subseteq [-N,N]$ is an M-proper, symmetric GAP with $L_1 \le L_2 \le \cdots \le L_k$, and suppose $h \in \mathbb{Z}[x]$ is a polynomial of degree ℓ which has a root modulo $(d_i,\dots,d_k)$ that is coprime to $(d_i,\dots,d_k)$ for all $1 \le i \le k$. If $A \cap h(\mathcal{P}) \subseteq \{0\}$, then*

$$\prod_{i=1}^{k} L_i \ll N^{1-c\ell^{-1}(200\ell^2 4^\ell)^{1-k}}(4k)^k M\log N$$

for an absolute constant $c > 0$, where the implied constant depends only on h.

Virtually identical to the deduction of Theorem 4 from Lemma 7, Theorem 5 follows from Linnik's theorem and the following lemma.

Lemma 8. *Suppose $A = \{x_1d_1+\cdots+x_kd_k : |x_i| \le L_i\} \subseteq [-N,N]$ is an M-proper, symmetric GAP with $L_1\cdots L_k = \delta N$, and suppose $h \in \mathbb{Z}[x]$ is a polynomial of degree ℓ with a root modulo $(d_1,\dots,d_k)$ that is coprime to $(d_1,\dots,d_k)$. If $\delta \ge CN^{-c/\ell}$ and*

$$\min\{L_i\}_{i=1}^{k} \ge \Big(CM(4k)^k\delta^{-1}\log N\Big)^{200\ell^2 4^\ell - 1} \tag{20}$$

for sufficiently large and small constants C and c, respectively, then $0 \ne h(p) \in A$ for some $p \in \mathcal{P}$.

Proof. Fix an M-proper GAP

$$A = \{x_1 D_1 + \cdots + x_k D_k : \ |x_i| \le L_i\} \subseteq [-N, N],$$

let $q = (D_1, \ldots, D_k)$, and fix a polynomial $h \in \mathbb{Z}[x]$ of degree ℓ with a root $r \in [0, q)$ modulo q such that $(r, q) = 1$, which by symmetry we can assume has positive leading coefficient. To show that A contains a nonzero element of the form $h(p)$ with $p \in \mathcal{P}$, it suffices to show that

$$A' = \{x_1 d_1 + \cdots + x_k d_k : \ |x_i| \le L_i\}$$

contains a nonzero element of the form $h_q(m) = h(qm + r)/q$ with $qm + r \in \mathcal{P}$, where $d_i = D_i/q$. Let

$$\Lambda = \{m \in \mathbb{N} : qm + r \in \mathcal{P}, \ 0 < h_q(m) < L_k d_k/2\}$$

and let $n = \Big(\dfrac{L_k d_k}{2q^{\ell-1}b}\Big)^{1/\ell}$, where b is the leading coefficient of h.

For $1 \le i \le k-1$, assume without loss of generality that $L_i d_i \le L_k d_k$, let

$$A_i = \{x d_i : |x| \le L_i/4k\} \subseteq \mathbb{Z},$$

and define g_i, f_i as functions on $\mathbb{Z}_{d_k}$ by

$$g_i(x) = \sum_{|y| \le L_i/4k} 1_{y d_i}(x) \quad \text{and} \quad f_i(x) = |A_i|^{-1} g_i * g_i(x).$$

As in the proof of Lemma 7, f_i is supported on $\{x d_i : |x| \le L_i/2k\} \subseteq \mathbb{Z}_{d_k}$,

$$f_1 * \cdots * f_{k-1}(0) \le M^2 \tag{21}$$

by M-properness, and

$$0 \le \widehat{f_i}(t) \le \widehat{f_i}(0) = |A_i|.$$

Further, if $f_1 * \cdots * f_{k-1}(h_q(m)) > 0$ for some $m \in \Lambda$, then $0 \ne h(p) \in A$ for some $p \in \mathcal{P}$, so we need only show

$$d_k \sum_{m \in \Lambda} \log(qm + r) f_1 * \cdots * f_{k-1}(h_q(m)) = \sum_{t \in \mathbb{Z}_{d_k}} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) V(t) > 0,$$

where the equality follows from (5) and

$$V(t) = \sum_{m \in \Lambda} \log(qm + r) \ e^{-2\pi i h_q(m) t/d_k},$$

for which if suffices to show

$$\sum_{t \ne 0} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) |V(t)| < \widehat{f_1}(0) \cdots \widehat{f_{k-1}}(0) V(0) = (\psi(qn + r, r, q) + O_h(\log N)) \prod_{i=1}^{k-1} |A_i|. \tag{22}$$

where the estimate on $V(0)$ follows from (11), and we recall that

$$\psi(x, a, q) := \sum_{\substack{p \in \mathcal{P} \cap [1, x] \\ p \equiv a \bmod q}} \log p.$$

We now apply Lemma 4 with $U = C\delta^{-1}(4k)^k \log N$ for a sufficiently large constant C depending on h, noting that if A satisfies (20) then $d_k > h_q(n)/U^L$, where $L = 64\ell^2 4^\ell$. Therefore, by (15) and (16), if $(t, d_k) < d_k/U^L$ then

$$\sum_{(t, d_k) \le d_k/U^L} \widehat{f_1}(t) \cdots \widehat{f_{k-1}}(t) |V(t)| \ll_h (n/U + U^L n^{1 - 4^{-\ell}}) \prod_{i=1}^{k-1} |A_i| (4k)^k/\delta. \tag{23}$$

Again we see that if $(t,d_k) > d_k/U^L$ and $d_k/(t,d_k) \nmid d_j$, then $\widehat{f_j}(t) \le U^{2L}/|A_j|$. Applying Lemma 5, (15), and Hölder's Inequality with $s = 2^\ell + 1$, we have

$$\sum_{(t,d_k)\ge d_k/U^L} \widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t)|V(t)| \ll_h \Big(\sum_{t\in\mathbb{Z}_{d_k}} |V(t)|^s\Big)^{1/s}\Big(\sum_{(t,d_k)\ge d_k/U^L} (\widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t))^{1+1/(s-1)}\Big)^{(s-1)/s}$$
$$\ll_h nU^{2L/s}(\min\{|A_i|\}_{i=1}^{k-1})^{-2/s}\Big(\prod_{i=1}^{k-1}|A_i|\Big)^{1/s}(M^2d_k)^{(s-1)/s},$$

which combined with (16) yields

$$\sum_{(t,d_k)\ge d_k/U^L} \widehat{f_1}(t)\cdots\widehat{f_{k-1}}(t)|V(t)| \ll_h nM^2U^{2L/s}(\min\{|A_i|\}_{i=1}^{k-1})^{-2/s}\prod_{i=1}^{k-1}|A_i|(4k)^k/\delta. \tag{24}$$

If $\delta \ge CN^{-c/\ell}$ for appropriately large and small constants, respectively, then in particular $n > N^{1/2\ell}$, and since $q \le \delta^{-1}$ we know from Lemma 6 that

$$\psi(qn+r,r,q) \gg \frac{qn}{\phi(q)\sqrt{q}} \ge \delta^{1/2}n. \tag{25}$$

We see that if A satisfies (20), then in particular $\min\{|A_i|\}_{i=1}^{k-1} \ge U^{2L}(M(4k)^k/\delta)^s$. In this case, we see from (23), (24), and (25) that the left-hand side of (22) is bounded by a small constant times the right-hand side of (22), and the lemma follows. □

5. Some Remarks on Special Cases and Expected Bounds

Here we note that the "wideness" conditions stipulated in Lemmas 7 and 8 are stronger, simplified formulations of what are actually used in the respective proofs. Specifically, in the proof of Lemma 7, we exhibited the following.

Lemma 9. *Suppose $A = \{x_1D_1 + \cdots + x_kD_k : |x_i| \le L_i\} \subseteq [-N,N]$ is an M-proper, symmetric GAP with $L_1\cdots L_k = \delta N$ and $L_kD_k \ge L_iD_i$ for $1 \le i \le k$, suppose $h \in \mathbb{Z}[x]$ is a polynomial of degree ℓ which has a root modulo $q = (D_1,\dots,D_k)$, and let $d_i = D_i/q$. If $L_k \ge C\Big(M(4k)^k\delta^{-1}\log N\Big)^{2^{\ell+2}}$ and for every $D \ge d_k\Big(CM^{2^{\ell+1}}(4k)^{2^\ell k}(\log N)^{\ell^2}\delta^{-(2^\ell+\ell)}\Big)^{-1}$ with $D \mid d_k$, there exists $1 \le i \le k-1$ with $D \nmid d_i$ and*

$$L_i \ge C\Big(M(4k)^k\delta^{-1}\log N\Big)^{2^{\ell+2}} \tag{26}$$

for a sufficiently large constant C depending only on h, then A contains a nonzero element of $h(\mathbb{Z})$.

One can also extract a sharper version of Lemma 8, and these more careful formulations allow one to deduce much improved bounds in special cases in which the iteration procedure used to prove Theorems 4 and 5 is not necessary. In particular, if the GAP is equally "wide" in each dimension, i.e.

$$A = \{x_1d_1 + \cdots + x_kd_k \ : \ |x_i| \le L\} \subseteq [-N,N],$$

then one obtains bounds of the form

$$|A| \ll_h N^{1-c^\ell/k}, \tag{27}$$

which hold for dimensions up to about $k = \sqrt{\log N}$. Of course, if the elements of the GAP are extremely concentrated in one dimension, then one immediately has excellent bounds by reducing to the one-dimensional case. The difficulty lies in intermediate cases such as

$$A = \{x_1d_1 + \cdots + x_kd_k \ : \ |x_i| \le L_i\}, \quad |A| = \delta N, \quad L_i \approx \delta^{-2^i},$$

but we believe this to be a shortcoming of the proof rather than a genuine obstruction, and it is likely that, in both the unrestricted and prime input settings, bounds of the form (27) hold in full generality.

References

[1] A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference Sets Without k-th Powers*, Acta. Math. Hungar. 65 (2) (1994), pp. 165-187.

[2] E. Croot, I. Łaba, O. Sisask, *Arithmetic progressions in sumsets and L^p almost periodicity*, Combinatorics, Probability, and Computing 22 (2013), 351-365.

[3] B. Green, T. Tao, *New bounds for Szemerédi's theorem II. A new bound for $r_4(N)$,* Analytic number theory, 180-204, Cambridge Univ. Press, 2009.

[4] M. Hamel, N. Lyall, A. Rice, *Improved bounds on Sárközy's theorem for quadratic polynomials*, Int. Math. Res. Not. no. 8 (2013), 1761-1782

[5] L. K. Hua, *Additive theory of prime numbers* , American Mathematical Society, Providence, RI 1965.

[6] H. Iwaniec, E. Kowalski, *Analytic number theory*, AMS Colloquium Publications Volume 53, American Mathematical Society, Providence, Rhode Island, 2004.

[7] T. H. Lê, *Intersective polynomials and the primes*, J. Number Theory 130 no. 8 (2010), pp. 1705-1717.

[8] H.-Z. Li, H. Pan, *Difference sets and polynomials of prime variables*, Acta. Arith. 138, no. 1 (2009), 25-52.

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

[10] J. Lucier, *Intersective Sets Given by a Polynomial*, Acta Arith. 123 (2006), pp. 57-95.

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

[12] N. Lyall, À. Magyar, *Polynomial configurations in difference sets*, J. Number Theory 129 (2009), pp. 439-450.

[13] N. Lyall, A. Rice, *A quantitative result on diophantine approximation for intersective polynomials*, preprint available at `arxiv.org/abs/1404.5161`

[14] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. 37 (1988), pp. 219-231.

[15] A. Rice, *Improvements and extensions of two theorems of Sárközy*, Ph.D. thesis, University of Georgia, 2012, available at `alexricemath.com/wp-content/uploads/2013/06/AlexThesis.pdf`

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

[17] I. Ruzsa, T. Sanders, *Difference sets and the primes*, Acta. Arith. 131, no. 3 (2008), 281-201.

[18] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE 5 (2012), no. 3, 627-655.

[19] A. Sárközy, *On difference sets of sequences of integers I*, Acta. Math. Hungar. 31(1-2) (1978), pp. 125-149.

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

[21] W. M. Schmidt, *Small fractional parts of polynomials*, CBMS Regional Conference Series in Math., **32**, Amer. Math. Soc., 1977.

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

[23] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics 105, Cambridge University Press, paperback, 2010.

[24] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, second edition, 1997.

[25] T. Xylouris, *The zeros of Dirichlet L-functions and the least prime in an arithmetic progression*, Ph. D. thesis, Universitt Bonn, Mathematisches Institut, 2011.

School of Mathematics, Georgia Institute of Technology, Atlanta GA 30332, USA

E-mail address: `ecroot@math.gatech.edu`

Department of Mathematics, The University of Georgia, Athens, GA 30602, USA

E-mail address: `lyall@math.uga.edu`

Department of Mathematics, University of Rochester, Rochester, NY 14612, USA

E-mail address: `alex.rice@rochester.edu`