Binary Quadratic Forms in Difference Sets

Alex Rice

Abstract We show that if $h(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ satisfies $\Delta(h) = b^2 - 4ac \neq 0$, then any subset of $\{1, 2, \ldots, N\}$ lacking nonzero differences in the image of h has size at most a constant depending on h times $N \exp(-c\sqrt{\log N})$, where $c = c(h) > 0$. We achieve this goal by adapting an L^2 density increment strategy previously used to establish analogous results for sums of one or more single-variable polynomials. Our exposition is thorough and self-contained, in order to serve as an accessible gateway for readers who are unfamiliar with previous implementations of these techniques.

MSC 2010 11B30

1 Introduction

Established independently by Sárközy and Furstenberg during the 1970s, settling a question of Lovász, it is a well-studied fact that any set of integers of positive upper density necessarily contains two distinct elements that differ by a perfect square. Equivalently, if $A \subseteq \mathbb{N}$ contains no such pair, then

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

Here we use $[1, N]$ to denote $\{1, 2, \ldots, N\}$ and $|X|$ to denote the size of a finite set X. Furstenberg [2] achieved this result qualitatively via ergodic theory, specifically his correspondence principle, but obtained no information on the rate at which the density must decay, while Sárközy [20] employed a Fourier analytic density increment strategy to show that if $A \subseteq [1, N]$ has no square differences, then

A. Rice (✉)
Department of Mathematics, Millsaps College, Jackson, MS 39210, USA
e-mail: riceaj@millsaps.edu

M. B. Nathanson (ed.), *Combinatorial and Additive Number Theory III*,
Springer Proceedings in Mathematics & Statistics 297,
https://doi.org/10.1007/978-3-030-31106-3_14

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

Throughout the paper we use log to denote the natural logarithm, and we use "$\ll$" to denote "less than a constant times", with subscripts indicating on what parameters, if any, the implied constant depends. Sárközy's argument was driven by the Hardy–Littlewood circle method, and was inspired by Roth's [14] proof that sets of positive upper density contain three-term arithmetic progressions.

Using a more intricate Fourier analytic argument, Pintz, Steiger, and Szemerédi [13] improved (1) to

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

with $c = 1/12$. While more elementary Fourier analytic proofs [3, 10] and a Fourier-free density increment proof [4] have also been discovered, it is versions of these two Fourier analytic attacks that have yielded the best quantitative information. In the ensuing decades, these two methods have been refined and applied to other sets of prohibited differences, such as more general polynomial images [1, 5, 9, 22], shifted primes [8, 19, 21], polynomial curves in higher-dimensional integer lattices [11], and images of the primes under polynomials [7, 17].

With regard to sums of one or more single-variable polynomials, the author [15] pushed these two methods to their breaking points. In the case of one single-variable polynomial, if $h \in \mathbb{Z}[x]$ has degree $k \geq 2$ and $h(\mathbb{N})$ contains a multiple of q for every $q \in \mathbb{N}$, known as an *intersective polynomial*, then any set $A \subseteq [1, N]$ with no nonzero differences in the image of h satisfies (2) for any $c < (\log((k^2+k)/2))^{-1}$, with the implied constant depending on h and c. The intersective condition is necessary to force any density decay, as otherwise one can take $A = q\mathbb{N}$ if $h(\mathbb{N})$ misses $q\mathbb{Z}$, and in that sense this is a maximal extension of the elaborate techniques developed in [1, 13].

Further, if we allow the additional degree of freedom of a second polynomial, then the more straightforward density increment approach yields density bounds that are even better than (2), as described below.

Theorem 1 ([15]) *Suppose $g, h \in \mathbb{Z}[x]$ are nonzero 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

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

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

As a notable example, Theorem 1 gives an upper bound of $\exp(-c\sqrt{\log N})$ for the density of subsets of $[1, N]$ lacking differences that are the sum of two squares. There is also a brief discussion of sums of three or more single-variable polynomials at the

end of [15], but the improvements in density bounds are modest as $\exp(-c\sqrt{\log N})$ arises as a natural limit of the method, a fact that we discuss in Sect. 2.3.

While the generality of Theorem 1 is pleasing, prohibited differences of the form $g(m) + h(n)$ can be thought of as the diagonal special case of differences of the form $h(m, n)$ where $h \in \mathbb{Z}[x, y]$. Of course, if $h(x, y) = \tilde{h}(g(x, y))$ for some $g \in \mathbb{Z}[x, y]$ and $\tilde{h} \in \mathbb{Z}[x]$ with $\deg(\tilde{h}) \geq 2$, then the image of h is contained in the image of $\tilde{h}$, in which case we could not hope to improve on the original setting of one single-variable polynomial. However, in other cases, we expect that the freedom of two variables should allow for improved density bounds. It is with this expectation in mind that we gently wade into the arena of potentially non-diagonal two-variable polynomials by exploring the following natural generalization of the aforementioned special case $m^2 + n^2$.

Definition 1 $h \in \mathbb{Z}[x, y]$ is called a *binary quadratic form* if

$$h(x, y) = ax^2 + bxy + cy^2$$

for some $a, b, c \in \mathbb{Z}$. Further, we define the *discriminant* of h by

$$\Delta(h) = b^2 - 4ac,$$

noting that $h(x, y) = d(rx + sy)^2$ for some $d, r, s \in \mathbb{Z}$ if and only if $\Delta(h) = 0$.

Our main result is the following, which says that under the necessary restriction that a binary quadratic form does not collapse into a dilated perfect square, we achieve the same density bounds previously established in the diagonal case, which are likely the best possible for our chosen method.

Theorem 2 *Suppose $h \in \mathbb{Z}[x, y]$ is a binary quadratic form with $\Delta(h) \neq 0$. If $A \subseteq [1, N]$ with*

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

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

$$|A| \ll_h Ne^{-c\sqrt{\log N}},$$

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

We note that the image of every nonzero binary quadratic form contains a dilation of the squares, and hence our result is only material because the established density bound is better than (2). Our goal for the remainder of the paper is twofold: to establish Theorem 2, which we hope will serve as a starting point for the application of these methods to more general polynomials in several variables, and to provide thorough and self-contained exposition of all of the components of this iteration scheme for those unfamiliar with its previous applications, such as the original case of the squares.

2 Main Iteration Lemma: Deducing Theorem 2

The principle behind a density increment strategy is that a set which lacks the desired arithmetic structure should spawn a new, significantly denser subset of a slightly smaller interval with an inherited lack of arithmetic structure. Iterating this procedure enough times for the density to reach 1 provides an upper bound on the density of the original set.

For this section, we fix a binary quadratic form $h \in \mathbb{Z}[x, y]$ with $\Delta(h) \neq 0$, and we let

$$I(h) = \{h(m, n) : m, n \in \mathbb{N}\} \setminus \{0\}.$$

Our iteration scheme is encapsulated by the following lemma, from which we quickly deduce Theorem 2.

Lemma 1 *Suppose* $A \subseteq [1, N]$ *with* $|A| = \delta N$ *and* $\delta \geq N^{-1/20}$. *If* $(A - A) \cap I(h) = \emptyset$, *then there exists* $A' \subseteq [1, N']$ *with* $|A'| = \delta' N'$ *and a constant* $c = c(h) > 0$ *with*

$$N' \gg_h \delta^4 N, \quad \delta' \geq (1 + c)\delta, \quad \text{and} \quad (A' - A') \cap I(h) = \emptyset.$$

2.1 Proof of Theorem 2

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$ and $(A - A) \cap I(h) = \emptyset$. Setting $A_0 = A$, $N_0 = N$, and $\delta_0 = \delta$, Lemma 1 yields, for each m, a set $A_m \subseteq [1, N_m]$ with $|A_m| = \delta_m N_m$ and $(A_m - A_m) \cap I(h) = \emptyset$ satisfying

$$N_m \geq c\delta^4 N_{m-1} \geq (c\delta^4)^m N \tag{3}$$

and

$$\delta_m \geq (1 + c)\delta_{m-1} \geq (1 + c)^m \delta \tag{4}$$

as long as

$$\delta_m \geq N_m^{-1/20}. \tag{5}$$

By (4), we see that the density δ_m will surpass 1, and hence (5) must fail, for $m = C \log(\delta^{-1})$. In particular, by (3) we have

$$\delta \leq (c\delta^4)^{-C \log(\delta^{-1})} N^{-1/20},$$

which can be rearranged to

$$N \leq e^{C \log^2(\delta^{-1})}$$

and hence implies

$$\delta \ll_h e^{-c\sqrt{\log N}},$$

as required. □

2.2 Roadmap for the Remainder of the Paper

Our task is is now completely reduced to a proof of Lemma 1, the two major components of which are described below.

i. The condition $(A - A) \cap I(h) = \emptyset$ represents unexpected, nonuniform behavior, which we expect to be detectable in the Fourier analytic behavior of A. More specifically, we use orthogonality of characters and adaptations of standard exponential sum estimates to locate a single small denominator q such that the Fourier transform of the characteristic function of A, translated to have mean value zero, has substantial L^2 concentration near rationals with denominator q. The Fourier analytic infrastructure is introduced in Sect. 3.1, the proof of this component is carried out in Sect. 4.2, and the required exponential sum estimates are exposed in great detail in Sect. 5.
ii. The substantial L^2 concentration of the transform of the translated characteristic function of A near rationals with a particular denominator q indicates a correlation of A with a linear phase function. In particular, we show that this implies that A has significantly increased relative density on a long arithmetic progression P of step size q. Since this implication has nothing to do with h, or any other assumptions about A, we prove a general version preemptively in Sect. 3.2. Finally, by shifting and rescaling the intersection of A with a subprogression of P of step size q^2, we obtain our new, denser set A' with $(A' - A') \cap I(h) = \emptyset$. The complete deduction of Lemma 1 from these two components is carried out in Sect. 4.1.

2.3 A Discussion of Novelty and Bounds

As indicated in the introduction, the procedure outlined in Sect. 2.2, though refined over the years, goes back to Sárközy in the 1970s. The improvement in bounds in Theorems 1 and 2, as compared to the case of one single-variable polynomial, comes from the details of the numerology in Lemma 1, most notably the size of the density increment $\delta' \geq (1 + c)\delta$. This effectively optimal increase in density is facilitated by the quality of the exponential sum estimates mentioned in item (i) above.

More specifically, the size of the density increment can be traced to the level of decay achieved in normalized complete local exponential sums. In the original setting of square differences, for example, the relevant decay comes from the standard estimate

$$\left| \frac{1}{q} \sum_{r=0}^{q-1} e^{2\pi i r^2 a/q} \right| \ll q^{-1/2} \tag{6}$$

for $(a, q) = 1$, which ultimately leads to a density increment $\delta' \geq \delta + c\delta^2$. Substituting this increment size, and other minor necessary modifications, into the proof

in Sect. 2.1 leads to the upper bound

$$\delta \ll \frac{\log\log N}{\log N},$$

which is better than Sárközy's original result (1). The reader may refer to [12] or [16] for full expositions of this refinement in the cases of squares, shifted primes, and, in the latter case, intersective polynomials.

In the case of sums of two squares, covered in Theorem 1, the relevant decay comes from the analogous two-variable sum that then splits, allowing one to use the same estimate (6) to conclude

$$\left|\frac{1}{q^2}\sum_{r,s=0}^{q-1} e^{2\pi i(r^2+s^2)a/q}\right| = \left|\frac{1}{q}\sum_{r=0}^{q-1} e^{2\pi i r^2 a/q}\right|^2 \ll q^{-1}$$

for $(a, q) = 1$, which is good enough to get the optimal density increment. The novelty of Theorem 2 is rooted in the fact that when $\Delta(h) \neq 0$, we get the same level of decay, namely

$$\left|\frac{1}{q^2}\sum_{r,s=0}^{q-1} e^{2\pi i h(r,s)a/q}\right| \ll_h q^{-1}$$

for $(a, q) = 1$, even though the sum no longer necessarily splits.

In order to improve on the bound $\exp(-c\sqrt{\log N})$ using this approach, for any fixed set of prohibited differences, one of two components of the numerology of Lemma 1 must be improved: either the ratio N'/N must decay more slowly than any power of δ, or the ratio δ'/δ must tend to infinity, as $\delta \to 0$, neither of which appear feasible in any nontrivial context. However, the question of whether the known upper bounds are even remotely sharp remains completely open in all of the aforementioned cases. For a more detailed discussion of lower bounds, constructions, and conjectures, the reader may refer to Sect. 1.4 of [15].

3 Preliminaries

3.1 Fourier Analysis and the Circle Method on $\mathbb{Z}$

We embed our finite sets in $\mathbb{Z}$, on which we utilize the 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 parametrized by the interval $[0, 1]$ with 0 and 1 identified, by

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

In this finite support context, Plancherel's Identity

$$\sum_{n\in\mathbb{Z}} |F(n)|^2 = \int_0^1 |\widehat{F}(\alpha)|^2 d\alpha \tag{7}$$

is a direct consequence of the orthogonality relation

$$\int_0^1 e^{2\pi i n\alpha} d\alpha = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \in \mathbb{Z} \setminus \{0\}. \end{cases} \tag{8}$$

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

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

We analyze $\widehat{f_A}$, and other exponential sums, using the Hardy–Littlewood circle method, decomposing the frequency space into two components: the set of points on the circle that are close to rationals with small denominator, and the complement.

Definition 2 Given $N \in \mathbb{N}$ and $\eta > 0$, we define, for each $q \in \mathbb{N}$ and $a \in [1, q]$,

$$\mathbf{M}_{a/q} = \mathbf{M}_{a/q}(N, \eta) = \left\{ \alpha \in \mathbb{T} : |\alpha - \frac{a}{q}| < \frac{1}{\eta^2 N} \right\}, \quad \mathbf{M}_q = \bigcup_{(a,q)=1} \mathbf{M}_{a/q},$$

and

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

We then define $\mathfrak{M}$, the *major arcs* and $\mathfrak{m}$, the *minor arcs*, by

$$\mathfrak{M} = \bigcup_{q=1}^{\eta^{-1}} \mathbf{M}_q, \quad \mathfrak{m} = \mathbb{T} \setminus \mathfrak{M}.$$

We note that if $\eta^2 N > 2Q^2$, then

$$\mathbf{M}_{a/q} \cap \mathbf{M}_{b/r} = \emptyset \tag{9}$$

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

3.2 Density Increment Lemma

The following standard result shows that for $A \subseteq [1, N]$, L^2 concentration of $\widehat{f_A}$ near rationals with a particular denominator q implies increased relative density on a long arithmetic progression of step size q, as described in item (ii) in Sect. 2.2.

Lemma 2 *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$. If $q \in \mathbb{N}$, $\sigma, \eta > 0$, and*

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

then there exists an arithmetic progression

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

with $qL \gg \min\{\sigma, \eta^2\}N$ and $|A \cap P| \geq (1 + \sigma/32)\delta L$.

Proof Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, $\sigma, \eta > 0$. Suppose further that

$$\int_{\mathbf{M}'_q} |\widehat{f_A}(\alpha)|^2 d\alpha \geq \sigma\delta^2 N, \tag{10}$$

and let $P = \{q, 2q, \ldots, Lq\}$ with $L = \lfloor \min\{\sigma, \eta^2\}N/128q \rfloor$. We will show that some translate of P satisfies the conclusion of Lemma 2. We note that for $\alpha \in [0, 1]$,

$$|\widehat{1_P}(\alpha)| = \left| \sum_{\ell=1}^{L} e^{-2\pi i \ell q \alpha} \right| \geq L - \sum_{\ell=1}^{L} |1 - e^{-2\pi i \ell q \alpha}| \geq L - 2\pi L^2 \|q\alpha\|, \tag{11}$$

where $\|\cdot\|$ denotes the distance to the nearest integer. Further, if $\alpha \in \mathbf{M}'_q$, then

$$\|q\alpha\| \leq \frac{q}{\eta^2 N} \leq \frac{1}{4\pi L}. \tag{12}$$

Therefore, by (11) and (12) we have

$$|\widehat{1_P}(\alpha)| \geq L/2 \quad \text{for all} \quad \alpha \in \mathbf{M}'_q. \tag{13}$$

By (10), (13), and Plancherel's Identity (7) we see

$$\sigma\delta^2 N \leq \int_{\mathbf{M}'_q} |\widehat{f_A}(\alpha)|^2 d\alpha \leq \frac{4}{L^2} \int_0^1 |\widehat{f_A}(\alpha)|^2 |\widehat{1_P}(\alpha)|^2 d\alpha = \frac{4}{L^2} \sum_{n \in \mathbb{Z}} |f_A * \widetilde{1_P}(n)|^2, \tag{14}$$

where $\widetilde{1_P}(n) = 1_P(-n)$ and

$$f_A * \widetilde{1_P}(n) = \sum_{m\in\mathbb{Z}} f_A(m)1_P(m-n) = |A \cap (P+n)| - \delta|(P+n) \cap [1,N]|. \tag{15}$$

We now take advantage of the fact that f_A, and consequently $f_A * \widetilde{1_P}$, has mean value zero. In other words,

$$\sum_{n\in\mathbb{Z}} f_A * \widetilde{1_P}(n) = 0. \tag{16}$$

As with any real valued function, we can write

$$|f_A * \widetilde{1_P}| = 2(f_A * \widetilde{1_P})_+ - f_A * \widetilde{1_P}, \tag{17}$$

where $(f_A * \widetilde{1_P})_+ = \max\{f_A * \widetilde{1_P}, 0\}$.

For the purposes of proving Lemma 2, we can assume that $f_A * \widetilde{1_P}(n) \le 2\delta L$ for all $n \in \mathbb{Z}$, as otherwise the progression $P + n$ would more than satisfy the conclusion. Combined with the trivial upper bound $f_A * \widetilde{1_P}(n) \ge -\delta L$, we can assume

$$|f_A * \widetilde{1_P}(n)| \le 2\delta L \quad \text{for all} \quad n \in \mathbb{Z}. \tag{18}$$

By (14), (16)–(18), we have

$$\sum_{n\in\mathbb{Z}} (f_A * \widetilde{1_P})_+(n) = \frac{1}{2}\sum_{n\in\mathbb{Z}} |f_A * \widetilde{1_P}| \ge \frac{1}{4\delta L}\sum_{n\in\mathbb{Z}} |f_A * \widetilde{1_P}|^2 \ge \frac{\sigma\delta NL}{16}. \tag{19}$$

By (15), we see that $f_A * \widetilde{1_P}(n) = 0$ if $n \notin [-qL, N]$. Letting $E = \{n \in \mathbb{Z} : P + n \subseteq [1, N]\}$ and $F = [-qL, N] \setminus E$, we see that $|F| \le 2qL$. Therefore, by (18), (19), and the bound $128qL \le \sigma N$, we have

$$\sum_{n\in E} (f_A * \widetilde{1_P})_+(n) \ge \frac{\sigma\delta NL}{16} - 2\delta L|F| \ge \frac{\sigma\delta NL}{16} - 4q\delta L^2 > \frac{\sigma\delta NL}{32}. \tag{20}$$

Recalling that $|E| \le N$ and $f_A * \widetilde{1_P}(n) = |A \cap (P + n)| - \delta L$ for all $n \in E$, we have that there exists $n \in \mathbb{Z}$ with

$$|A \cap (P + n)| \ge (1 + \sigma/32)\delta L,$$

as required.

4 L^2 Concentration

For this section, we once again fix a binary a quadratic form $h \in \mathbb{Z}[x, y]$ with $\Delta(h) \neq 0$, and let

$$I(h) = \{h(m, n) : m, n \in \mathbb{N}\} \setminus \{0\}.$$

The following result makes precise the implication outlined in item (i) in Sect. 2.2, in which the condition $(A - A) \cap I(h) = \emptyset$ forces substantial L^2 concentration of $\widehat{f_A}$ near rationals with a single small denominator. Combining this with Lemma 2, we then quickly deduce Lemma 1.

Lemma 3 *Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, and let $\eta = c_0\delta$ for a sufficiently small constant $c_0 = c_0(h) > 0$. If $(A - A) \cap I(h) = \emptyset$, $\delta \geq N^{-1/20}$, and $|A \cap (N/9, 8N/9)| \geq 3\delta N/4$, then there exists $q \leq \eta^{-1}$ such that*

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

4.1 Proof of Lemma 1

Suppose $A \subseteq [1, N]$, $|A| = \delta N$, $\delta \geq N^{-1/20}$, and $(A - A) \cap I(h) = \emptyset$.

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 3 and 2 apply, so in either case, letting $\eta = c_0\delta$, there exists $q \leq \eta^{-1}$ and an arithmetic progression

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

with $qL \gg_h \delta^2 N$ and $|A \cap P| \geq (1 + c)\delta L$. Partitioning P into subprogressions of step size q^2, the pigeonhole principle yields a progression

$$P' = \{y + \ell q^2 : 1 \leq \ell \leq N'\} \subseteq P$$

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

$$A' = \{\ell \in [1, N'] : y + \ell q^2 \in A\},$$

which clearly satisfies $|A'| \geq (1 + c)\delta N'$ and $N' \gg_h \delta^2 N/q^2 \gg_h \delta^4 N$. Moreover, since $q^2 h(m, n) = h(qm, qn)$, A' inherits the lack of $h(m, n)$ differences from A. □

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

4.2 Proof of Lemma 3

Suppose $A \subseteq [1, N]$ with $|A| = \delta N$, and let $\eta = c_0\delta$. We let $J = |b_1| + |b_2| + |b_3|$, $M = \sqrt{N/9J}$, $Z = \{(m, n) \in [1, M]^2 : h(m, n) = 0\}$, and $\Lambda = [1, M]^2 \setminus Z$.

We note that

$$|Z| \ll_h M. \tag{21}$$

If $(A - A) \cap I(h) = \emptyset$, then since $h(\Lambda) \subseteq [-N/9, N/9]$, we see that

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

Therefore, if $|A \cap (N/9, 8N/9)| \ge 3\delta N/4$, we have

$$\sum_{\substack{n\in\mathbb{Z}\\1\le m\le M}} f_A(n) f_A(x + h(m, n)) \le -\delta^2 N|\Lambda|/2. \tag{22}$$

One can check using orthogonality (8) and Plancherel's Identity (7) that

$$\begin{aligned}&\sum_{\substack{x\in\mathbb{Z}\\(m,n)\in\Lambda}} f_A(x) f_A(x + h(m, n))\\ &= \sum_{\substack{x,y\in\mathbb{Z}\\(m,n)\in\Lambda}} f_A(x) f_A(y) \int_0^1 e^{2\pi i(x-y+h(m,n))\alpha} d\alpha\\ &= \int_0^1 \left(\sum_{x\in\mathbb{Z}} f_A(x)e^{2\pi ix\alpha}\right)\left(\sum_{y\in\mathbb{Z}} f_A(y)e^{-2\pi iy\alpha}\right)\left(\sum_{(m,n)\in\Lambda} e^{2\pi ih(m,n)\alpha}\right) d\alpha\\ &= \int_0^1 |\widehat{f_A}(\alpha)|^2 S_M(\alpha) d\alpha + O(\delta N|Z|),\end{aligned}$$

where

$$S_x(\alpha) = \sum_{1 \le m,n \le x} e^{2\pi i h(m,n)\alpha}.$$

Combined with (21), (22), and the triangle inequality, this yields

$$\int_0^1 |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| d\alpha \ge \delta^2 N M^2/4. \tag{23}$$

By adapting traditional exponential sum estimates to this two-variable setting, and at one point carefully exploiting that $\Delta(h) \neq 0$, we have that if $\delta \ge N^{-1/20}$, then

$$|S_M(\alpha)| \ll_h M^2/q \quad \text{for } \alpha \in \mathbf{M}_q,\ q \le \eta^{-1}, \tag{24}$$

and

$$|S_M(\alpha)| \le C\eta M^2 \le \delta M^2/8 \quad \text{for } \alpha \in \mathfrak{m}, \tag{25}$$

provided we choose $c_0 \le 1/8C$. We prove and discuss these estimates in detail in Sect. 5.

By (25) and Plancherel's Identity (7), we have

$$\int_{\mathfrak{m}} |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| d\alpha \le \delta^2 N M^2/8,$$

which by (23) yields

$$\int_{\mathfrak{M}} |\widehat{f_A}(\alpha)|^2 |S_M(\alpha)| d\alpha \ge \delta^2 N M^2/8. \tag{26}$$

By (24) and (26) we have

$$\delta^2 N M^2 \ll_h \sum_{q=1}^{\eta^{-1}} \frac{M^2}{q} \int_{\mathbf{M}_q} |\widehat{f_A}(\alpha)|^2 d\alpha. \tag{27}$$

We then make use of the following proposition, a more general version of which can be found in Proposition 5.6 of [15], which exploits the more inclusive definition of $\mathbf{M}'_q$ as compared with $\mathbf{M}_q$.

Proposition 1 *If $\eta^2 N > 2Q^2$, then*

$$\max_{q \le Q} \int_{\mathbf{M}'_q} |\widehat{f_A}(\alpha)|^2 d\alpha \ge \frac{1}{2} \sum_{q=1}^{Q} q^{-1} \int_{\mathbf{M}_q} |\widehat{f_A}(\alpha)|^2 d\alpha.$$

Proof By (9) we have

$$\begin{aligned} Q \max_{q \le Q} \int_{\mathbf{M}'_q} |\widehat{f_A}(\alpha)|^2 d\alpha &\ge \sum_{q=1}^{Q} \int_{\mathbf{M}'_q} |\widehat{f_A}(\alpha)|^2 d\alpha \\ &= \sum_{q=1}^{Q} \sum_{r|q} \int_{\mathbf{M}_r} |\widehat{f_A}(\alpha)|^2 d\alpha \\ &= \sum_{r=1}^{Q} \lfloor Q/r \rfloor \int_{\mathbf{M}_r} |\widehat{f_A}(\alpha)|^2 d\alpha \\ &\ge \frac{Q}{2} \sum_{r=1}^{Q} r^{-1} \int_{\mathbf{M}_r} |\widehat{f_A}(\alpha)|^2 d\alpha, \end{aligned}$$

and the proposition follows.

Lemma 3 then follows immediately from (27) and Proposition 1. □

5 Exponential Sum Estimates

In this section, we carefully adapt traditional exponential sum estimates in order to establish the crucial upper bounds (24) and (25). For the entirety of the section, we fix a nonzero binary quadratic form

$$h(x, y) = b_1 x^2 + b_2 xy + b_3 y^2 \in \mathbb{Z}[x, y].$$

Unlike in previous sections, we do not make the perpetual assumption that $\Delta(h) = b_2^2 - 4b_1 b_3 \neq 0$, but rather enforce this condition only when necessary.

5.1 Major Arc Estimates

We begin our pursuit of (24) by establishing an asymptotic formula for the relevant exponential sum near rationals with small denominator. To achieve this goal, we make multiple appeals to the following standard formula, which is simply integration by parts applied to an appropriate Riemann–Stieltjes integral.

Lemma 4 (Abel's Partial Summation Formula) *If $\phi : \mathbb{R} \to \mathbb{C}$ is continuously differentiable, $f : \mathbb{N} \to \mathbb{C}$, $F(x) = \sum_{1 \le n \le x} f(n)$, and $M > 0$, then*

$$\sum_{1 \le n \le M} f(n)\phi(n) = F(M)\phi(M) - \int_0^M F(x)\phi'(x)dx.$$

We now proceed with the asymptotic formula, obtained by applying Lemma 4 one variable at a time.

Lemma 5 *If $a, q \in \mathbb{N}$, $\alpha = a/q + \beta$, and $M > 0$, then*

$$\begin{aligned} S_M(\alpha) &= \sum_{1 \le m,n \le M} e^{2\pi i h(m,n)\alpha} \\ &= q^{-2} G(a,q) \int_0^M \int_0^M e^{2\pi i h(x,y)\beta} dx dy + O(qM(1 + JM^2\beta)), \end{aligned}$$

where $J = |b_1| + |b_2| + |b_3|$ and

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

Proof For each fixed $1 \le m \le M$ and $y > 0$, we see that

$$\begin{aligned} S_y^m(a/q) &= \sum_{1 \le n \le y} e^{2\pi i h(m,n)a/q} \\ &= \sum_{s=0}^{q-1} e^{2\pi i h(m,s)a/q} \, |\{1 \le n \le y \ : \ n \equiv s \bmod q\}| \\ &= \frac{y}{q} G_m(a,q) + O(q), \end{aligned}$$

where

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

Then, letting $h_y = \frac{\partial h}{\partial y}$ and combining the above with Lemma 4 and integration by parts, we have

$$\begin{aligned} S_M^m(\alpha) &= \sum_{1 \le n \le M} e^{2\pi i h(m,n)a/q} e^{2\pi i h(m,n)\beta} \\ &= S_M^m(a/q) e^{2\pi i h(m,M)\beta} - \int_0^M S_y^m(a/q)(2\pi i h_y(m,y)\beta) e^{2\pi i h(m,y)\beta} dy \\ &= q^{-1} G_m(a,q) \left(M e^{2\pi i h(m,M)\beta} - \int_0^M y 2\pi i h_y(m,y)\beta e^{2\pi i h(m,y)\beta} dy \right) \\ &\quad + O(q(1 + JM^2\beta)) \\ &= q^{-1} G_m(a,q) \int_0^M e^{2\pi i h(m,y)\beta} dy + O(q(1 + JM^2\beta)). \end{aligned}$$

Similarly, summing in m we have

$$\begin{aligned}\tilde{S}_x(a/q) &= \sum_{1\le m\le x} G_m(a,q)\\ &= \sum_{r=0}^{q-1} G_r(a,q)\,|\{1\le m\le x\ :\ m\equiv r \bmod q\}|\\ &= \frac{x}{q}G(a,q)+O(q),\end{aligned}$$

and, letting $h_x = \frac{\partial h}{\partial x}$, we apply the same sequence of steps to see that $S_M(\alpha)$ equals

$$\begin{aligned}&q^{-1}\sum_{1\le m\le M} G_m(a,q)\int_0^M e^{2\pi i h(m,y)\beta}dy + O(qM(1+JM^2\beta))\\ =&q^{-1}\Big(\tilde{S}_M(a/q)\int_0^M e^{2\pi i h(M,y)\beta}dy\\ &-\int_0^M\int_0^M \tilde{S}_x(a/q)(2\pi i h_x(x,y)\beta)e^{2\pi i h(x,y)\beta}dxdy\Big)+O(qM(1+JM^2\beta))\\ =&q^{-2}G(a,q)\Big(M\int_0^M e^{2\pi i h(M,y)\beta}dy\\ &-\int_0^M\int_0^M x(2\pi i h_x(x,y)\beta)e^{2\pi i h(x,y)\beta}dxdy\Big)+O(qM(1+JM^2\beta))\\ =&q^{-2}G(a,q)\int_0^M\int_0^M e^{2\pi i h(x,y)\beta}dxdy+O(qM(1+JM^2\beta)),\end{aligned}$$

and the formula is established.

The crucial denominator q in (24) comes from the following result, previously discussed in Sect. 2.3, which is the one and only juncture at which we require $\Delta(h)\neq 0$. This key ingredient, as well as the standard proof we recreate for Lemma 8, rely on a technique known as *Weyl differencing*, in which we take the modulus squared of the exponential sum in order to reduce the quadratic dependence in each variable to a linear dependence.

Lemma 6 *If $\Delta(h)\neq 0$ and $a,q\in\mathbb{N}$ with $(a,q)=1$, then*

$$\left|\sum_{r,s=0}^{q-1} e^{2\pi i h(r,s)a/q}\right| \ll_h q.$$

Proof Fixing $a,q\in\mathbb{N}$ with $(a,q)=1$, exploiting that $|z|^2=z\overline{z}$ for any $z\in\mathbb{C}$, and changing variables $r'=r+t$, $s'=s+u$, we see that

$$
\begin{aligned}
&\left|\sum_{r,s=0}^{q-1} e^{2\pi i h(r,s)a/q}\right|^2 \\
&= \sum_{r,r',s,s'=0}^{q-1} e^{2\pi i(h(r',s')-h(r,s))a/q} \\
&= \sum_{r,s,t,u=0}^{q-1} e^{2\pi i(h(r+t,s+u)-h(r,s))a/q} \\
&= \sum_{r,s,t,u=0}^{q-1} e^{2\pi i(2b_1rt+b_1t^2+b_2ru+b_2st+b_2tu+2b_3su+b_3u^2)a/q} \\
&= \sum_{t,u=0}^{q-1} e^{2\pi i h(t,u)a/q} \left(\sum_{r=0}^{q-1} e^{2\pi i(2b_1t+b_2u)ra/q}\right)\left(\sum_{s=0}^{q-1} e^{2\pi i(b_2t+2b_3u)sa/q}\right) \\
&= \sum_{t,u=0}^{q-1} e^{2\pi i h(t,u)a/q} \begin{cases} q^2 & \text{if } 2b_1t+b_2u \equiv b_2t+2b_3u \equiv 0 \bmod q \\ 0 & \text{else} \end{cases},
\end{aligned}
$$

where the last equality follows from the orthogonality relation

$$
\sum_{r=0}^{q-1} e^{2\pi i rb/q} = \begin{cases} q & \text{if } q \mid b \\ 0 & \text{else} \end{cases}.
$$

Looking at the two congruence conditions above, multiplying the first expression by b_2, and multiplying the second expression by $2b_1$, we get the system

$$
2b_1b_2t + b_2^2u \equiv 2b_1b_2t + 4b_1b_3u \equiv 0 \bmod q.
$$

By subtracting the two resulting expressions we see that q must divide $\Delta(h)u$. Letting $d = \gcd(q, \Delta(h))$, we have that u must be one of the d multiples of q/d, which each yield at most $\gcd(q, 2b_1b_2)$ choices for t. In particular, if $\Delta(h) \neq 0$, then the number of simultaneous solutions is $O_h(1)$, and the lemma follows.

5.2 *Proof of (24)*

Returning to the setting of the proof of Lemma 3, if $\alpha \in \mathbf{M}_q$ with

$$
q \leq \eta^{-1} \ll_h \delta^{-1} \leq N^{1/20} \ll M^{1/10},
$$

then $\alpha = a/q + \beta$ with

$$|\beta| < \frac{1}{\eta^2 N} \ll_h N^{-9/10} \ll M^{-9/5}$$

for some a with $(a, q) = 1$. In this case, Lemma 5 tells us that

$$S_M(\alpha) = q^{-2} G(a, q) \int_0^M \int_0^M e^{2\pi i h(x,y)\beta} dx dy + O_h(M^{1.3}).$$

Applying Lemma 6 and trivially bounding the double integral by M^2, we have

$$|S_M(\alpha)| \ll_h M^2/q,$$

as claimed in (24). □

5.3 *Minor Arc Estimates*

We begin our pursuit of (25) with the following standard oscillatory integral estimate, which will allow us to exhibit (25) in the case that α is fairly close to a rational with small denominator, but not so close as to lie in the major arcs.

Lemma 7 (Van der Corput's Lemma for Quadratic Polynomials) *If $g(x) = x^2 + bx + c \in \mathbb{R}[x]$ and $I \subseteq \mathbb{R}$ is an interval, then*

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

Proof Fix $g(x) = x^2 + bx + c \in \mathbb{R}[x]$ and an interval $I \subseteq \mathbb{R}$, and let $E = (I + b/2) \cap \{x : |x| \geq |\beta|^{-1/2}\}$, where $I + b/2$ denotes the translation of the interval I by $b/2$. We know that the measure of $(I + b/2) \setminus E$ is at most $2|\beta|^{-1/2}$, so we complete the square and change variables to see that

$$\begin{aligned}
\left| \int_I e^{2\pi i g(x)\beta} dx \right| &= \left| \int_I e^{2\pi i((x+b/2)^2 - b^2/4 + c)\beta} dx \right| \\
&= \left| \int_I e^{2\pi i (x+b/2)^2 \beta} dx \right| \\
&= \left| \int_{I+b/2} e^{2\pi i y^2 \beta} dy \right| \\
&\ll |\beta|^{-1/2} + \left| \int_E e^{2\pi i y^2 \beta} dy \right|.
\end{aligned}$$

Writing

$$e^{2\pi i y^2 \beta} = \frac{1}{4\pi i y \beta} \frac{d}{dx}(e^{2\pi i y^2 \beta}),$$

we have by integration by parts that

$$\int_E e^{2\pi i y^2\beta}dy = \left[\frac{e^{2\pi i y^2\beta}}{4\pi i y\beta}\right] + \int_E \frac{e^{2\pi i y^2\beta}}{4\pi i y^2\beta}dy,$$

where the expression in brackets is appropriately evaluated at endpoints of E. By construction, $|y| \geq |\beta|^{-1/2}$ at each endpoint of E, and hence

$$\left|\int_E e^{2\pi i y^2\beta}dy\right| \ll |\beta|^{-1/2} + |\beta|^{-1}\int_{|y|\geq|\beta|^{-1/2}} \frac{1}{y^2}dy \ll |\beta|^{-1/2},$$

which establishes the desired estimate.

With regard to estimating the double integral in the conclusion of Lemma 5, since we assumed h was not identically zero, we can relabel or make a linear change of variables to reduce to the case where $b_1 \neq 0$. Then, by applying Lemma 7 to the integral in x for every fixed y, we immediately get the following estimate.

Corollary 1 *If $M > 0$, then*

$$\left|\int_0^M \int_0^M e^{2\pi i h(x,y)\beta}dxdy\right| \ll_h M|\beta|^{-1/2}. \tag{28}$$

For our final ingredient, we turn to the following traditional estimate, which we utilize to establish (25) when α is close to a denominator that is neither too small nor too large.

Lemma 8 (Weyl's Inequality for Quadratic Polynomials) *Suppose $g(x) = bx^2 + cx + d \in \mathbb{R}[x]$, $b \in \mathbb{N}$, $a, q \in \mathbb{N}$, $t \geq 1$, and $x > 0$. If $(a, q) = 1$ and $|\alpha - a/q| \leq tq^{-2}$, then*

$$\left|\sum_{1\leq n\leq x} e^{2\pi i g(n)\alpha}\right| \ll \left(bx\log q + tx + btx^2/q + q\log q\right)^{1/2}.$$

Proof Letting S denote the exponential sum we wish to estimate, we see that

$$|S|^2 = \sum_{1\leq n,n'\leq x} e^{2\pi i(h(n')-h(n))\alpha} = x + 2\Re\left(\sum_{1\leq n<n'\leq x} e^{2\pi i(h(n')-h(n))\alpha}\right), \tag{29}$$

where the x accounts for terms where $n = n'$, and $\Re$ denotes the real part. With a change of variables $n' = n + h$, we have

$$\begin{aligned}\sum_{1\le n<n'\le x} e^{2\pi i(h(n')-h(n))\alpha} &= \sum_{1\le n\le x-1}\sum_{1\le h\le x-n} e^{2\pi i(h(n+h)-h(n))\alpha}\\ &= \sum_{1\le n\le x-1}\sum_{1\le h\le x-n} e^{2\pi(2bnh+h^2+ch)\alpha}\\ &= \sum_{1\le h\le x-1} e^{2\pi i(h^2+ch)\alpha}\sum_{1\le n\le x-h} e^{2\pi i(2bhn)\alpha}.\end{aligned}$$

Applying the geometric series formula to the inner sum, and the triangle inequality, gives us

$$\left|\sum_{1\le n<n'\le x} e^{2\pi i(h(n')-h(n))\alpha}\right| \ll \sum_{1\le h\le 2bx} \min\left\{x, \|h\alpha\|^{-1}\right\}, \tag{30}$$

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

Fixing $q\in\mathbb{N}$ and breaking the sum in h into intervals of length q, we have

$$\sum_{1\le h\le 2bx} \min\left\{x, \|h\alpha\|^{-1}\right\} \le \sum_{1\le j\le 2bx/q}\sum_{s=0}^{q-1} \min\left\{x, \|(qj+s)\alpha\|^{-1}\right\}. \tag{31}$$

If $a\in\mathbb{N}$ with $|\alpha-a/q|\le tq^{-2}$, we can write $\alpha = a/q + O(t/q^2)$, and hence

$$(qj+s)\alpha = qj\alpha + \frac{sa}{q} + O(t/q).$$

Further, if we let k be the nearest integer to $q^2 j\alpha$, then $qj\alpha = k/q + O(t/q)$ and hence

$$(qj+s)\alpha = \frac{sa+k}{q} + O(t/q).$$

Combined with (31), this yields

$$\sum_{1\le h\le 2bx} \min\left\{x, \|h\alpha\|^{-1}\right\} \le \sum_{1\le j\le 2bx/q}\sum_{s=0}^{q-1} \min\left\{x, \|\frac{sa+k}{q} + O(t/q)\|^{-1}\right\}. \tag{32}$$

If $(a,q)=1$, then as s runs over all congruence classes modulo q, so does sa. In particular, the $O(t/q)$ error term dominates for at most $O(t)$ terms, and we have

$$\begin{aligned}\sum_{1\le j\le 2bx/q}\sum_{s=0}^{q-1} \min\left\{x, \|\frac{sa+k}{q} + O(t/q)\|^{-1}\right\} &\ll \sum_{1\le j\le 2bx/q}\left(tx + \sum_{s=1}^{q/2}\frac{q}{s}\right)\\ &\ll (2bx/q+1)(tx + q\log q),\end{aligned}$$

which combines with (29), (30), and (32) to yield the desired estimate.

In the same way we deduce Corollary 1 from Lemma 7, we reduce to the case of $b_1 \neq 0$ and apply Lemma 8 to the sum in m for every fixed n to immediately get the following estimate.

Corollary 2 *Suppose* $a, q \in \mathbb{N}$, $\alpha \in [0,1]$, *and* $x > 0$. *If* $(a,q) = 1$ *and* $|\alpha - a/q| \leq q^{-2}$, *then*

$$\left| \sum_{1 \leq m,n \leq x} e^{2\pi i h(m,n)\alpha} \right| \ll_h x \left(x \log q + x^2/q + q \log q \right)^{1/2}. \tag{33}$$

Remark. We note that under the assumption $\Delta(h) \neq 0$, the estimates (28) and (33) can be improved to $|\beta|^{-1}$ and

$$\left(x^4/q^2 + (x^3/q + x^2 + qx) \log q \right)^{1/2},$$

respectively. For the former, since it is in a continuous setting, one can simply use that if $b^2 - 4ac \neq 0$, then

$$ax^2 + bxy + cy^2 = u^2 + v^2$$

after an invertible linear change of variables, and then apply Lemma 7 separately in u and v. The latter estimate can be established by mimicking the two-variable Weyl differencing process, and exploitation of nonzero discriminant, exhibited in the proof of Lemma 6. However, for the purposes of proving Theorem 2, we only require this sort of "optimal cancellation" on the major arcs, so for the sake of brevity, and for the sake of exposing the components used in previous applications of this method, we leave the details of these improvements as exercises for the reader.

5.4 Proof of (25)

Returning to the setting of the proof of Lemma 3, we consider $\alpha \in \mathfrak{m}$. By the pigeonhole principle, there exists $1 \leq q \leq M^{7/4}$ and $(a,q) = 1$ such that

$$|\alpha - a/q| \leq \frac{1}{qM^{7/4}} \leq \frac{1}{q^2}.$$

Writing $\alpha = a/q + \beta$, if $q \leq M^{1/4}$, then we have from Lemma 5 that

$$S_M(\alpha) = q^{-2} G(a,q) \int_0^M \int_0^M e^{2\pi i h(x,y)\beta} dxdy + O_h(M^{3/2}). \tag{34}$$

If $q \leq \eta^{-1}$, then it must be the case that $|\beta| > (\eta^2 N)^{-1}$, since otherwise we would have $\alpha \in \mathfrak{M}$. In this case, recalling that $N \ll_h M^2$ and $\eta \gg_h \delta \geq N^{-1/20} \gg_h M^{-1/10}$, it follows from (34), Corollary 1, and trivially bounding $G(a, q)$ by q^2 that

$$|S_M(\alpha)| \ll M|\beta|^{-1/2} + O_h(M^{3/2}) \ll_h \eta M^2.$$

If $\eta^{-1} \leq q \leq M^{1/4}$, then by (34), Lemma 6, and trivially bounding the double integral by M^2, we have

$$S_M(\alpha) \ll_h M^2/q + O_h(M^{3/2}) \ll_h \eta M^2.$$

Finally, if $M^{1/4} \leq q \leq M^{7/4}$, then by Corollary 2 we have

$$|S_M(\alpha)| \ll_h M(M \log q + M^2/q + q \log q)^{1/2} \ll M^{15/8} \ll_h \eta M^2,$$

and (25) is established in all cases. □

Acknowledgements The author would like to thank Neil Lyall who co-authored the expository note [12], in the context of squares and shifted primes, that served as a template for this paper.

References

1. A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference sets without κ-th powers*, Acta. Math. Hungar. 65 (2) (1994), 165–187
2. H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), 204–256
3. B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour. 114 (2002) no. 2, 215–238
4. 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/
5. M. Hamel, N. Lyall, A. Rice, *Improved bounds on Sárközy's theorem for quadratic polynomials*, Int. Math. Res. Not. no. 8 (2013), 1761–1782
6. T. Kamae, M. Mendès France, *van der Corput's difference theorem*, Israel J. Math. 31, no. 3–4, (1978), pp. 335–342
7. H.- Z. Li, H. Pan, *Difference sets and polynomials of prime variables*, Acta. Arith. 138, no. 1 (2009), 25–52
8. J. Lucier, *Difference sets and shifted primes*, Acta. Math. Hungar. 120 (2008), 79–102
9. J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. 123 (2006), 57–95
10. N. Lyall, *A new proof of Sárközy's theorem*, Proc. Amer. Math. Soc. 141 (2013), 2253–2264
11. N. Lyall, À. Magyar, *Polynomial configurations in difference sets*, J. Number Theory 129 (2009), 439–450
12. N. Lyall, A. Rice, *Two theorems of Sárközy*, http://alexricemath.com/wp-content/uploads/2013/06/DoubleSarkozy.pdf
13. 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
14. K. F. Roth, *On certain sets of integers*, J. London Math. Soc. 28 (1953), pp. 104–109
15. A. Rice, *A maximal extension of the best-known bounds for the Sárközy-Furstenberg Theorem*, Acta Arith. 187 (2019), 1–41

16. 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
17. A. Rice, *Sárközy's theorem for $\mathcal{P}$ -intersective polynomials*, Acta Arith. 157 (2013), no. 1, 69–89
18. I. Ruzsa, *Difference sets without squares*, Period. Math. Hungar. 15 (1984), 205–209
19. I. Ruzsa, T. Sanders, *Difference sets and the primes*, Acta. Arith. 131, no. 3 (2008), 281–301
20. A. Sárközy, *On difference sets of sequences of integers I*, Acta. Math. Hungar. 31(1–2) (1978), 125–149
21. A. Sárközy, *On difference sets of sequences of integers III*, Acta. Math. Hungar. 31(3–4) (1978), 355–386
22. S. Slijepcević, *A polynomial Sárközy-Furstenberg theorem with upper bounds*, Acta Math. Hungar. 98 (2003), 275–280