A SIMPLE PROOF OF SÁRKÖZY'S THEOREM

NEIL LYALL

Abstract. It is a striking and elegant fact (proved independently by Furstenberg and Sárközy) that in any subset of the natural numbers of positive upper density there necessarily exist two distinct elements whose difference is given by a perfect square. In this article we present a new and simple proof of this result by adapting an argument originally developed by Croot and Sisask to give a new proof of Roth's theorem.

Dedicated to Steve Wainger on the occasion of his retirement

1. Introduction

Let $D(N)$ denote the maximum size of a subset of $\{1,\dots,N\}$ that contains no perfect (non-zero) square differences. In this note we shall be concerned with the behavior of this quantity for large values of N and at the outset we encourage the reader to convince herself of the essentially trivial upper and lower bounds for $D(N)$ of approximate quality $N/3$ and $\sqrt{N}$ respectively, and if possible to try and improve on these bounds, particularly the upper bound. In Appendix A we give full justification for the following specific bounds

$$\sqrt{N}-1 \leq D(N) \leq (N+34)/3. \tag{1}$$

It was conjecture by Lovász that $D(N) \leq \delta N$ for any $\delta > 0$, provided that N is sufficiently large, or equivalently that in any subset of the natural numbers of positive upper density[1] there necessarily exist two distinct elements (and hence infinitely many pairs of distinct elements) whose difference is given by a perfect square. This conjecture was subsequently proven to be correct, independently, by Sárközy and Furstenberg.

Theorem 1 (Sárközy [16]/Furstenberg [3])**.**

$$\lim_{N\to\infty} \frac{D(N)}{N} = 0$$

The purpose of this note is to give a new and simple proof of this result by adapting an argument that was originally developed by Croot and Sisask [2] to give a new proof of Roth's theorem on three term arithmetic progressions. In particular we will establish the following result, which clearly implies Theorem 1.

Theorem 2. *Let $M, N \in \mathbb{N}$, then*

$$\frac{D(N)}{N} \leq \frac{3}{4}\frac{D(M)}{M}$$

provided $N \geq e^{CM^7}$, for some absolute constant $C > 0$, and M is sufficiently large.

Remark on quantitative bounds. Although its proof is simple, Theorem 2 patently leads to quantitative upper bounds of the quality $N/\log_* N$ for $D(N)$ that are extremely weak in comparison to the current best known upper bound, namely

$$D(N) \leq CN/(\log N)^{\frac{1}{12}\log\log\log\log N} \tag{2}$$

for some absolute constant $C > 0$, which was established by Pintz, Steiger and Szemerédi in [14] using an ingenious and intricate Fourier analytic argument. For extremely readable accounts of easier arguments leading to intermediate bounds of the quality $N/(\log\log N)^{1/11}$ and $N\log\log N/\log N$, see Green [4] and Lyall and Magyar [11], respectively.

2000 *Mathematics Subject Classification.* 11B30.

[1] Recall that $A \subseteq \mathbb{N}$ is said to have positive upper density whenever $\limsup_{N\to\infty} |A \cap \{1,\dots,N\}|/N > 0$.

We further note that it is conjectured that $D(N) \geq N^{1-\varepsilon}$ for any $\varepsilon > 0$, provided N is sufficiently large (with respect to ε), and that Ruzsa [15] has demonstrated this conjecture to be true for all $\varepsilon \geq 0.267$.

Remark on other polynomial differences. At this point the reader is presumably curious to know what is so special about square differences. The following Theorem gives a complete answer to this question.

Theorem 3 (Kamae and Mendès France [7])**.** *Let $P \in \mathbb{Z}[n]$ and $D(P,N)$ denote the maximum size of a subset of $\{1,\dots,N\}$ that contains no two distinct elements whose difference is given by $P(n)$ for some $n \in \mathbb{Z}$. Then,*

$$\lim_{N\to\infty} \frac{D(P,N)}{N} = 0 \tag{3}$$

if and only if P has a root modulo m for every $m \geq 2$.

The methods used to prove Theorem 2 can in fact be extended to establish a result almost as general as Theorem 3, namely that (3) holds whenever P is a polynomial in $\mathbb{Z}[n]$ with at least one integer root. This is less general than Theorem 3, since while it is clear that any polynomial P in $\mathbb{Z}[n]$ with an integer root plainly has a solution to the congruence $P(n) \equiv 0 \pmod m$ for every intreger $m \geq 2$, there do in fact exist polynomials without an integer root that also have this property, for example $(n^3-19)(n^2+n+1)$.

However, it is not the objective of this note to try and prove the most general possible theorem, and as such we shall focus our attention almost exclusively on the case of square differences and proving Theorem 2, relegating further discussion of more general polynomial differences, including best known quantitative bounds and a brief outline of how to extend the proof of Theorem 2 in the direction alluded to above, to Appendix B.

2. Proof of Theorem 2

Let $A \subseteq \{1,\dots,N\}$ with no square differences and $|A| = D(N)$. Key to the argument we present is to construct, from this extremal set A, a new set $B \subseteq \{1,\dots,N\}$ with the following properties:

(i) $|B| \geq \frac{5}{3}|A|$

(ii) # of square differences in $B \leq \frac{C_0}{\sqrt{\log N}} N^{3/2}$, for some absolute constant $C_0 > 0$.

This construction, which will amount to defining B to be $A \cup (A + t^2)$ for some appropriate (large) value of t, will be carried out in Section 2.2 below. Having constructed a set with such properties we will then establish Theorem 2 by combining this with the following lower bound on the number of square differences contained in any given set $B \subseteq \{1,\dots,N\}$.

Lemma 1. *Given any $B \subseteq \{1,\dots,N\}$ and $1 \leq M \leq N$*

$$\#\text{ of square differences in } B \geq \left(\frac{|B|/N - (D(M)+2)/M}{M^{5/2}}\right) N^{3/2}.$$

The proof of this result is a straightforward exercise using ideas that where first exploited by Varnavides [17] in the context of counting three term arithmetic progressions. While, in our context of counting square differences, this quantitative result can easily be deduced by adapting the proof of Theorem 3.1 in [6] (for example) we will, for the sake of completeness, include a proof of Lemma 1 in Section 3.1 below.

We should also note at this point that the standard application Varnavides' argument is to show that Theorem 1 is equivalent to the statement that for any $\delta > 0$ and $B \subseteq \{1,\dots,N\}$ with $|B| \geq \delta N$

$$\#\text{ of square differences in } B \geq \lfloor c(\delta) N^{3/2} \rfloor,$$

for some $c(\delta) > 0$. In other words, provided N is sufficiently large, B will contain not only one square difference, but a positive proportion of all the square differences in $\{1,\dots,N\}$. This result clearly follows easily from Lemma 1.

2.1. **Proof of Theorem 2.** It follows immediately from the upper bound on the number of square differences in B given by property (ii) and the lower bound given by Lemma 1, that

$$\frac{|B|}{N} \leq \frac{D(M)}{M} + \frac{2}{M} + \frac{C_0 M^{5/2}}{\sqrt{\log N}}.$$

Assuming that N satisfies $C_0 M^{7/2} \leq \sqrt{\log N}$, it follows that

$$\frac{|B|}{N} \leq \frac{D(M)}{M} + \frac{3}{M}$$

and hence, using the trivial lower bound $D(M) \geq \sqrt{M} - 1$ (see Section A.2), that

$$\frac{|B|}{N} \leq \frac{5}{4}\frac{D(M)}{M}$$

provided that M is sufficiently large. Combining this observation with the inequality

$$\frac{|B|}{N} \geq \frac{5}{3}\frac{|A|}{N} = \frac{5}{3}\frac{D(N)}{N}$$

which follows immediately from property (i) of our constructed set B, gives the desired inequality. □

2.2. **Construction of the set B.** Given any set $B \subseteq \{1, \dots, N\}$, it is easy to see that

$$\#\text{ of square differences in } B = \sum_{n=1}^{\sqrt{N}} \sum_{x \in \mathbb{Z}} B(x)B(x-n^2) \tag{4}$$

where $B(x) = 1_B(x)$ denotes the indicator function of the set B. Using the familiar orthogonality relation

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

we can, as is standard, express our count (4) on the "transform side" as

$$\#\text{ of square differences in } B = \int_0^1 |\widehat{B}(\alpha)|^2 \widehat{S}(\alpha)\, d\alpha \tag{5}$$

where

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

denotes the Fourier transform (on $\mathbb{Z}$) of the set B and

$$\widehat{S}(\alpha) = \sum_{n=1}^{\sqrt{N}} e^{-2\pi i n^2 \alpha} \tag{6}$$

is the Fourier transform of the set of perfect squares contained in $\{1, \dots, N\}$.

Key to our proof (and essentially the only true "machinary" used in the proof) is the following well-known estimate for the Weyl sum $\widehat{S}(\alpha)$, which states that the only possible obstruction to cancellation in this exponential sum arises if α is "close" to a rational with "small" denominator.

Proposition 1. *Let $\varepsilon > 0$ and*

$$\mathbf{M}_{a/q}(\varepsilon) = \left\{ \alpha \in [0,1] \,:\, \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{\varepsilon^2 N} \right\}.$$

If $\alpha \notin \mathbf{M}_{a/q}(\varepsilon)$ for any $(a,q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, then

$$|\widehat{S}(\alpha)| \leq 6\varepsilon N^{1/2}$$

provided N is sufficiently large.

We are now ready to define our set B. Recalling that $A \subseteq \{1, \dots, N\}$ is an extremal set with no square differences, we define (for a value of $\varepsilon > 0$ to de determined)

$$B := A' \cup (A' + q_\varepsilon^2) \tag{7}$$

where $q_\varepsilon = \mathrm{lcm}\{1 \leq q \leq \varepsilon^{-2}\}$ and $A' = A \cap \{1, \dots, N - q_\varepsilon^2\}$.

Using the fact that $|A| = D(N) \geq \sqrt{N} - 1$ it follows that $|A'| \geq 5|A|/6$, and consequently also that property (i) for our set B will hold, provided $\varepsilon > 0$ is chosen large enough for

$$q_\varepsilon^2 \ll \sqrt{N}. \tag{8}$$

In order to see what actual restriction this places on our choice of $\varepsilon > 0$, we recall, as one can verify using only elementary properties of the prime numbers, that $q_\varepsilon = \exp(C\varepsilon^{-2})$ and hence that inequality (8) will hold whenever

$$\varepsilon^{-2} \ll \log N.$$

Remark (on "$\ll$ notation"). Whenever we write $E \ll F$ for any two quantities E and F we shall mean that $E \leq cF$, for some some sufficiently small constant $c > 0$.

We therefore now fix

$$\varepsilon := C_1 (\log N)^{-1/2} \tag{9}$$

with $C_1 > 0$ a sufficiently large (but absolute) constant. In order to to establish that our set B also satisfies property (ii) it will suffice to show, for this choice of $\varepsilon > 0$, that

$$\#\text{ of square differences in } B \leq 24\,\varepsilon N^{3/2} \tag{10}$$

for all sufficiently large N.

To establish (10) we first note that since $A' \subseteq A$ contains no square differences, it follows that

$$B(x) = A'(x) + A(x - q_\varepsilon^2)$$

and hence, using the familiar and easily verified property that Fourier transformation takes translations to modulations, that

$$\widehat{B}(\alpha) = \widehat{A'}(\alpha)(1 + e^{-2\pi i q_\varepsilon^2 \alpha}).$$

Multiplying this expression for $\widehat{B}(\alpha)$ by its complex conjugate, we see that

$$\int_0^1 |\widehat{B}(\alpha)|^2 \widehat{S}(\alpha)\, d\alpha = 2 \int_0^1 |\widehat{A'}(\alpha)|^2 (\cos(2\pi q_\varepsilon^2 \alpha) + 1) \widehat{S}(\alpha)\, d\alpha.$$

In light of (5), and the fact that A' contains no square differences, it follows that

$$\int_0^1 |\widehat{A'}(\alpha)|^2 \widehat{S}(\alpha)\, d\alpha = 0$$

and hence that

$$\begin{aligned} \#\text{ of square differences in } B &= 2 \int_0^1 |\widehat{A'}(\alpha)|^2 (\cos(2\pi q_\varepsilon^2 \alpha) - 1) \widehat{S}(\alpha)\, d\alpha \\ &\leq 2 \int_0^1 |\widehat{A'}(\alpha)|^2 \underbrace{|\cos(2\pi q_\varepsilon^2 \alpha) - 1||\widehat{S}(\alpha)|}_{(\star)}\, d\alpha. \end{aligned}$$

A crucial observation at this point, which completes the proof of inequality (10), is the fact that

$$(\star) \leq 12\,\varepsilon \sqrt{N} \tag{11}$$

uniformly in α, and hence

$$\#\text{ of square differences in } B \leq 24\,\varepsilon \sqrt{N} \int_0^1 |\widehat{A'}(\alpha)|^2\, d\alpha \leq 24\,\varepsilon N^{3/2}$$

where to establish the final inequality we have invoked the Plancherel identity, namely

$$\int_0^1 |\widehat{A'}(\alpha)|^2 \, d\alpha = \sum_{x\in\mathbb{Z}} |A'(x)|^2$$

whose validity in this setting can be easily verified (using orthogonality), together with the simple observation that

$$\sum_{x\in\mathbb{Z}} |A'(x)|^2 = |A'| \leq N.$$

It remains to verify the uniform estimate (11). Since $|\cos(2\pi q_\varepsilon^2\alpha) - 1| \leq 2$ for all $\alpha \in [0,1]$, it follows from Proposition 1 that (11) will hold whenever $\alpha \notin \mathbf{M}_{a/q}(\varepsilon)$ for any $(a,q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, provided N is sufficiently large. While if $\alpha \in \mathbf{M}_{a/q}(\varepsilon)$ for some $(a,q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, then by definition we know that $|\alpha - a/q| \leq \varepsilon^{-2}N^{-1}$. Moreover, since $q|q_\varepsilon^2$ (by the definition of q_ε) it follows that

$$\cos\left(2\pi q_\varepsilon^2\alpha\right) = \cos\left(2\pi q_\varepsilon^2\left(\alpha - a/q\right)\right)$$

and hence, by the Mean Value Theorem, we see that

$$\begin{aligned} |\cos(2\pi q_\varepsilon^2\alpha) - 1| &= |\cos(2\pi q_\varepsilon^2\left(\alpha - a/q\right)) - 1| \\ &\leq 2\pi q_\varepsilon^2 |\alpha - a/q| \\ &\leq 2\pi q_\varepsilon^2 \varepsilon^{-2} N^{-1}. \end{aligned}$$

The result then follows, provided the constant C_1 in our choice of fixed $\varepsilon > 0$ is chosen sufficiently large, since

$$2\pi q_\varepsilon^2 \varepsilon^{-2} N^{-1} \leq \varepsilon$$

whenever $\varepsilon^{-2} \ll \log N$ (again) and we trivially know that $|\widehat{S}(\alpha)| \leq \sqrt{N}$ for all $\alpha \in [0,1]$. □

This completes the proof of Theorem 2 modulo Lemma 1 and Proposition 1. The proof of these two results are given in Section 3 below.

3. Proof of Lemma 1 and Proposition 1

3.1. **Proof of Lemma 1.** Let $B \subseteq \{1,\dots,N\}$ and $1 \leq M \leq N$. We proceed by covering {1,...,N} by the collection of all square-difference progressions of length M of the form

$$P_{a,r} = \{a + r^2, \dots, a + Mr^2\}$$

with $1 \leq r \leq R := \sqrt{N}/M$ and $1 \leq a \leq N - MR^2$. We will say that such a progression $P_{a,r}$ is *good* if

$$|B \cap P_{a,r}| \geq D(M) + 1$$

since, by virtue of the fact that square differences are preserved under translations and dilations by a perfect square, each such progression clearly contributes at least one square difference in B.

A simple counting argument, which we give below, shows that

$$\#\text{ of } \textit{good} \text{ progressions } P_{a,r} \geq \left(\frac{|B|}{N} - \frac{D(M)+2}{M}\right) RN. \tag{12}$$

Now while, as noted above, each of these good progressions contributes at least one square difference in B, it is of course also the case that some of these square differences could be getting over counted. However, as we shall also see below, each square difference in B is being over counted at most $M^{3/2}$ times, from which it follows that

$$\#\text{ of square differences in } B \geq \left(\frac{|B|/N - (D(M)+2)/M}{M^{5/2}}\right) N^{3/2}$$

as required. We are thus left with the straightforward tasks of verifying (12) and the claim that the each square difference in B is being over counted in this argument at most $M^{3/2}$ times.

We will address the over counting argument first. Suppose we are given a pair $\{b, b+n^2\}$ in B. If this pair is contained in $P_{a,r}$, then r must be a divisor of n and moreover $n^2 \leq Mr^2$. It therefore follows that

there are at most $\sqrt{M}$ choices for r and it is easy to see that each choice of r fixes a in at most M ways, thus each square difference is indeed over counted at most $M^{3/2}$ times.

Finally, we verify (12). By combining the upper bound

$$\sum_{r=1}^{R}\sum_{a=1}^{N-MR^2}|B\cap P_{a,r}| \leq \sum_{\substack{a,r\\ \text{good } P_{a,r}}} M \;+\; \sum_{\substack{a,r\\ \underline{\text{not}} \text{ good } P_{a,r}}} D(M) \leq (\#\text{ of } \textit{good} \text{ progressions } P_{a,r})\, M + D(M)RN$$

with the lower bound

$$\sum_{r=1}^{R}\sum_{a=1}^{N-MR^2}|B\cap P_{a,r}| \geq M\sum_{r=1}^{R}|B\cap\{Mr^2,\dots,N-Mr^2\}| \geq MR\big(|B|-2MR^2\big)$$

it follows that

$$\#\text{ of } \textit{good} \text{ progressions } P_{a,r} \geq \left(\frac{|B|}{N}-\frac{2MR^2}{N}-\frac{D(M)}{M}\right)RN$$

from which (12) follows. □

3.2. **Proof of Proposition 1.** We first recall Dirichlet's (pigeonhole) principle:

Given any $\alpha\in\mathbb{R}$ and $Q\in\mathbb{N}$, there exist $(a,q)=1$ with $1\leq q\leq Q$ such that

$$\left|\alpha-\frac{a}{q}\right| \leq \frac{1}{qQ} \leq \min\Big\{\frac{1}{q^2},\frac{1}{Q}\Big\}.$$

The proof of the following key result is completely standard, see for example [13] or [5].

Proposition 2 (The Weyl inequality)**.** *If $|\alpha-a/q|\leq q^{-2}$ and $(a,q)=1$, then*

$$|\widehat{S}(\alpha)| \leq 40\sqrt{N}\log N(1/q+1/\sqrt{N}+q/N)^{1/2}.$$

We note (by Dirichlet's principle) that for any given $\alpha\in\mathbb{R}$ and $Q\in\mathbb{N}$, there always exist $(a,q)=1$ with $1\leq q\leq Q$ that satisfies the hypothesis of the Weyl inequality. Moreover, it is easy to see that this inequality gives a non-trivial conclusion whenever $N^{\mu}\leq q\leq N^{1-\mu}$ for some $0<\mu<1/2$. For the purposes of this exposition we shall take $Q=N^{1-\mu}$ with $\mu=1/20$ and define

$$\mathbf{M}'_{a/q}=\left\{\alpha\in[0,1]\,:\,\left|\alpha-\frac{a}{q}\right|\leq\frac{1}{N^{19/20}}\right\}.$$

It is customary to say that α is in a *major arc* if $\alpha\in\mathbf{M}'_{a/q}$ for some $(a,q)=1$ with $1\leq q\leq N^{1/20}$, and call the complement of these major arcs, the *minor arcs*. If α is in one of these minor arcs, then it follows from Dirichlet's principle that there must exist a reduced fraction a/q with $N^{1/20}\leq q\leq N^{19/20}$ such that $|\alpha-a/q|\leq q^{-2}$, and hence, by the Weyl inequality, that

$$|\widehat{S}(\alpha)| \leq 80N^{19/40}\log N \leq \varepsilon\sqrt{N}$$

for any $\varepsilon>0$, provided N is sufficiently large. This accounts for one of the $\varepsilon\sqrt{N}$ terms in Proposition 1.

In order to obtain the full conclusion of Proposition 1, which is valid on a subset of $[0,1]$ which is strictly larger than the collection of classical minor arcs defined above, we must perform a careful analysis of the behavior our exponential sum $\widehat{S}(\alpha)$ on the major arcs. In particular, we will invoke the following.

Lemma 2 (Major arc estimate)**.** *If $\alpha\in\mathbf{M}'_{a/q}$ for some $(a,q)=1$ with $1\leq q\leq N^{1/20}$, then*

$$|\widehat{S}(\alpha)| \leq 5\sqrt{N}\,q^{-1/2}(1+N|\alpha-a/q|)^{-1/2}.$$

It now follows immediately from this Lemma that for any given $\varepsilon>0$ and $\alpha\in\mathbf{M}'_{a/q}$, our exponential sum will satisfy

$$|\widehat{S}(\alpha)| \leq 5\varepsilon\sqrt{N}$$

provided $(a,q)=1$ and either $\varepsilon^{-2}\leq q\leq N^{1/20}$ or $\varepsilon^{-2}N^{-1}\leq|\alpha-a/q|\leq N^{-19/20}$, as required. □

The proof of Lemma 2 is standard, but for the sake of completeness we have chosen to included a proof in Appendix C below. Before doing this, we first present our justification of the trivial bounds for $D(N)$ that were purported at the beginning of the introduction and conclude our brief discussion of more general polynomial differences that was initiated at the end of the introduction.

Appendix A. Justification of inequality (1): the purported trivial bounds for $D(N)$

A.1. **Upper bound.** Let $A \subseteq \{1, \dots, N\}$ with no square differences.

It clearly follows that $A \cap (A + t^2) = \emptyset$ for all $t \in \mathbb{N}$ and in particular that

$$|A| \leq (N+1)/2$$

since $|(A+1) \cap \{1, \dots, N\}| \geq |A| - 1$ and hence

$$2|A| - 1 \leq |(A \cup (A+1)) \cap \{1, \dots, N\}| \leq N.$$

In order to obtain the superior bound (at least when $N \geq 65$) of

$$|A| \leq (N+34)/3$$

claimed in the introduction, one can use the further observation that if (r, s, t) form a Pythagorean triple with $r^2 + s^2 = t^2$, then

$$A \cap (A + s^2) = A \cap (A + t^2) = (A + s^2) \cap (A + t^2) = \emptyset.$$

In particular, taking $s = 3$ and $t = 5$, it follows that

$$3|A| - 34 \leq |\,(A \cup (A+9) \cup (A+25)) \cap \{1, \dots, N\}| \leq N,$$

as required, since clearly $|(A+9) \cap \{1, \dots, N\}| \geq |A| - 9$ and $|(A+25) \cap \{1, \dots, N\}| \geq |A| - 25$.

A.2. **Lower bound.** We now show that given any subset H of the natural numbers and any $N \in \mathbb{N}$, there always exists a set $A \subseteq \{1, \dots, N\}$ such that $(A - A) \cap H = \emptyset$ and

$$|A| \geq \frac{N-1}{|H \cap \{1, \dots, N\}| + 1}. \tag{13}$$

Taking H to be the set of square numbers, this corresponds to the desired lower bound

$$D(N) \geq \sqrt{N} - 1.$$

We construct the set A recursively as follows: Select $a_1 = 1$ to be the first element in A. Having selected $a_1, \dots, a_k$, with $k \geq 1$, we define $X_k = \{a_1, \dots, a_k\} + H \cap \{1, \dots, N\}$ and select a_{k+1} to be the smallest element in $\{1, \dots, N\} \setminus \{a_1, \dots, a_k, X_k\}$. In order to guarantee the existence of such an element a_{k+1}, we clearly must have $|\{a_1, \dots, a_k, X_k\}| \leq N - 1$, and since it is possible that $|\{a_1, \dots, a_k, X_k\}| = k\,(|H \cap \{1, \dots, N\}| + 1)$, this corresponds to the restriction that

$$k \leq \left\lfloor \frac{N-1}{|H \cap \{1, \dots, N\}| + 1} \right\rfloor$$

from which (13) immediately follows.

Appendix B. Other Polynomial Differences

Recall that for a given $P \in \mathbb{Z}[n]$, we define $D(P, N)$ to denote the maximum size of a subset of $\{1, \dots, N\}$ that contains no two distinct elements whose difference is given by $P(n)$ for some $n \in \mathbb{Z}$. The purpose of this section is to outline how one may extend the proof of Theorem 2 to give a new proof of the following special case of Theorem 3.

Theorem 4 (Kamae and Mendès France [7])**.** *If $P \in \mathbb{Z}[n]$ with at least one integer root, then*

$$\lim_{N \to \infty} \frac{D(P, N)}{N} = 0.$$

In order to do this we will make use of the observation, which originates (in a more general form) from [9] (see also [12]), that it suffices to consider the analogous problem, for monomial curves, in higher dimensions.

Before stating this observation more precisely (Lemma 3 below) we introduce some new notation. Let

$$Q_N = \{1, N^{2/(k+1)}\} \times \{1, N^{4/(k+1)}\} \times \cdots \times \{1, N^{2k/(k+1)}\} \subseteq \mathbb{Z}^k$$

noting that $|Q_N| = N^k$, and $D_k(N)$ denote the maximum size of a subset of Q_N that contains no monomial difference, that is no distinct elements whose difference is given by $\gamma(n) = (n, n^2, \ldots, n^k)$ for some $n \in \mathbb{Z}$.

Lemma 3 (Lyall and Magyar [9])**.** *If $P \in \mathbb{Z}[n]$ with degree $k \geq 2$ and at least one integer root, then*

$$\frac{D(P,N)}{N} \leq C_P \frac{D_k(N)}{N^k}.$$

In light of Lemma 3, whose proof we include in Section B.1 below, Theorem 4 will be an immediate consequence of the following higher dimensional analogue of Sárközy's theorem (Theorem 1).

Theorem 5 (Lyall and Magyar [9])**.**

$$\lim_{N\to\infty} \frac{D_k(N)}{N^k} = 0.$$

The methodology developed to prove Theorem 2 extends in a natural way to give a proof, which we choose to only sketch in Section B.2 below, of the following result (the analogue of Theorem 2 in this context) and hence a new proof of Theorems 5 and 4 (albeit with weak quantitative bounds).

Theorem 6. *Let $M, N \in \mathbb{N}$, then*

$$\frac{D_k(N)}{N^k} \leq \frac{3}{4}\frac{D_k(M)}{M^k}$$

provided $N \geq \exp(CM^{3k+4/(k+1)})^k$, for some constant $C > 0$, and M is sufficiently large.

Remark on quantitative bounds. While the methods of Pintz, Steiger and Szemerédi were extended by Balog, Pelikán, Pintz and Szemerédi [1] to show that

$$D(n^k, N) \leq C_k N/(\log N)^{c \log\log\log\log N},$$

the current best known upper bounds for general polynomials in $\mathbb{Z}[n]$ are due to Lucier [8], who showed that

$$D(P,N) \leq C_P N \left(\frac{(\log\log N)^\mu}{\log N}\right)^{1/(k-1)} \tag{14}$$

whenever P has a root modulo m for every $m \geq 2$, where $k = \deg(P)$ and $\mu = 3$ if $k = 2$ and $\mu = 2$ if $k \geq 3$.

In [10] the author and Magyar show that in the special case of polynomials in $\mathbb{Z}[n]$ of degree k with at least one integer root, one can in fact take $\mu = 1$ in (14) for all $k \geq 2$. This was achieved by first establishing

$$D_k(N) \leq C_k N^k \left(\frac{\log\log N}{\log N}\right)^{1/(k-1)} \tag{15}$$

for some absolute constant $C_k > 0$, and then invoking Lemma 3.

B.1. **Proof of Lemma 3.** Let $P \in \mathbb{Z}[n]$ of degree $k \geq 2$ with at least one integer root and $A \subseteq \{1, \ldots, N\}$ with no two distinct elements whose difference is given by $P(n)$ for some $n \in \mathbb{Z}$. By relabeling, we may assume, without loss in generality, that our polynomial has a root at zero and that $P(n) = c_k n^k + \cdots + c_1 n$.

Let $\mathcal{P} : \mathbb{Z}^k \to \mathbb{Z}$ denote the mapping given by

$$\mathcal{P}(b) = c_1 b_1 + \cdots + c_k b_k.$$

It follows from the pigeonhole principle that

$$\left|\mathcal{P}(\mathbb{Z}^k) \cap (A - m)\right| \geq |A|/\gcd(c_1, \ldots, c_k)$$

for some $1 \leq m \leq \gcd(c_1, \ldots, c_k)$. Thus, if we choose N' to be a sufficiently large multiple of $N^{2k/(k+1)}$ and define

$$B' = \left\{b \in \{-N', \ldots, N'\}^k \,:\, \mathcal{P}(b) \in A - m\right\},$$

it follows that

$$\frac{|B'|}{(2N'+1)^k} \geq c\,\frac{|A|}{N}$$

for some small, but absolute constant $c > 0$ depending only on the polynomial P. By partitioning $\{-N', \dots, N'\}^k$ using translates of Q_N, it then follows, again by the pigeonhole principle, that there must exist $B \subseteq Q_N$, a translate of some subset of B', with the property that

$$\frac{|B|}{N^k} \geq c\,\frac{|A|}{N}.$$

The key observation now is that since $\mathcal{P}(B') \subseteq A - m$ and $(A-A) \cap P(\mathbb{Z}) = \emptyset$ (by assumption), it follows that $(B'-B') \cap \gamma(n) = \emptyset$, and hence also that $(B-B) \cap \gamma(n) = \emptyset$, for all $n \in \mathbb{Z}$. It therefore follows that

$$\frac{D(P,N)}{N} \leq \frac{1}{c}\frac{D_k(N)}{N^k}$$

as required. □

B.2. **Sketch proof of Theorem 6.** As with the proof of Theorem 2 we begin with an extremal set $A \subseteq Q_N$ that contains no monomial differences and proceed to define, for a value $\varepsilon > 0$ fixed to be a sufficiently large multiple of $(\log N)^{-1/k}$, a new set

$$B = A' \cup (A' + \gamma(q_\varepsilon))$$

where $q_\varepsilon = \operatorname{lcm}\{1 \leq q \leq \varepsilon^{-k}\} \ll N^{1/(k+1)}$ and $A' = A \cap \{1, N^{2/(k+1)} - q_\varepsilon\} \times \cdots \times \{1, N^{2k/(k+1)} - q_\varepsilon^k\}$.

It is easy to then see that this set B has the property that $|B| \geq 5|A|/3$ and, by mimicking the arguments in Section 2.2, but using Fourier analysis on $\mathbb{Z}^k$ and invoking Lemma 5 from [9] (the analogue of Proposition 1 in this context), one can also show that

$$\#\text{ of monomial differences in } B \leq \frac{C_0}{(\log N)^{1/k}} N^{k+2/(k+1)}$$

for some absolute constant $C_0 > 0$.

Theorem 6 then follows, as in the proof of Theorem 2, by combining these two properties of set B with the following lower bound on the number of monomial differences in any given set $B \subseteq Q_N$ (the analogue of Lemma 1 in this context), whose proof we leave as an exercise.

Lemma 4. *There exists a constant $C_k > 0$ such that for any given $B \subseteq Q_N$ and $1 \leq M \leq N$*

$$\#\text{ of monomial differences in } B \geq \left(\frac{|B|/N^k - (D_k(M)+C_k)/M^k}{(M^{k+2/(k+1)})^2}\right) N^{k+2/(k+1)}.$$

Appendix C. Proof of Lemma 2 (Major arc estimate)

The proof of Lemma 2 hinges on the key observation that for each α in a major arc corresponding to a rational a/q, our exponential sum $\widehat{S}(\alpha)$ breaks naturally into an arithmetic part $S(a,q)$ and a continuous part $I_N(\alpha - a/q)$, up to a manageable error term. In particular we have

Lemma 5. *If $\alpha \in \mathbf{M}'_{a/q}$ with $1 \leq q \leq N^{1/20}$, then*

$$\widehat{S}(\alpha) = \sqrt{N}\, q^{-1} S(a,q) I_N(\alpha - a/q) + O(N^{1/10}) \tag{16}$$

where

$$S(a,q) = \sum_{r=0}^{q-1} e^{-2\pi i a r^2/q} \quad \text{and} \quad I_N(\beta) = \int_0^1 e^{-2\pi i N \beta x^2} dx.$$

Remark (on "big O notation"). Whenever we write $E = O(F)$ for any two quantities E and F we shall mean that $|E| \leq CF$, for some constant $C > 0$.

Proof. We can write $\alpha = a/q + \beta$ where $|\beta| \leq 1/N^{19/20}$ and $1 \leq q \leq N^{1/20}$. We can also write each $1 \leq d \leq \sqrt{N}$ uniquely as $d = mq + r$ with $1 \leq r \leq q$ and $0 \leq m \leq \sqrt{N}/q$. It then follows that

$$\begin{aligned}\widehat{S}(\alpha) &= \sum_{r=1}^{q} \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i(a/q+\beta)(mq+r)^2} + O(q) \\ &= \sum_{r=1}^{q} e^{-2\pi i a r^2/q} \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i \beta (mq+r)^2} + O(q).\end{aligned}$$

Since

$$\left| e^{-2\pi i(mq+r)^2\beta} - e^{-2\pi i m^2 q^2 \beta} \right| \leq \left| e^{-2\pi i(2mqr+r^2)\beta} - 1 \right| \leq Cdr|\beta| \leq CqN^{-9/20}$$

and

$$\begin{aligned}\Big| \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i m^2 q^2 \beta} - \int_0^{\sqrt{N}/q} e^{-2\pi i x^2 q^2 \beta} dx \Big| &\leq \sum_{m=0}^{\sqrt{N}/q} \int_m^{m+1} \left| e^{-2\pi i m^2 q^2 \beta} - e^{-2\pi i x^2 q^2 \beta} \right| dx \\ &\leq \sum_{m=0}^{\sqrt{N}/q} 2\pi(2m+1)q^2|\beta| \\ &\leq 20N^{1/20}\end{aligned}$$

it follows that

$$\left| \widehat{S}(\alpha) - \sqrt{N}\, q^{-1} S(a,q) I_N(\beta) \right| \leq CN^{1/10}. \qquad \square$$

Lemma 2 follows almost immediately from this and the two basic lemmas below.

Lemma 6 (Gauss sum estimate)**.** *If $(a,q) = 1$, then $|S(a,q)| \leq \sqrt{2q}$. More precisely,*

$$|S(a,q)| = \begin{cases} \sqrt{q} & \text{if } q \text{ odd} \\ \sqrt{2q} & \text{if } q \equiv 0 \mod 4 \\ 0 & \text{if } q \equiv 2 \mod 4 \end{cases}.$$

Lemma 7 (Oscillatory integral estimate)**.** *For any $\lambda \geq 0$*

$$\left| \int_0^1 e^{2\pi i \lambda x^2} dx \right| \leq \min\{1, 2\lambda^{-1/2}\} \leq 2\sqrt{2}(1+\lambda)^{-1/2}.$$

Proof of Lemma 2. Lemmas 6 and 7 imply that the main term in (16)

$$\sqrt{N}\, q^{-1} S(a,q) I_N(\alpha - a/q) \leq 4\sqrt{N} q^{-1/2} (1 + N|\alpha - a/q|)^{-1/2}$$

and since $q^{-1/2} \geq N^{-1/40}$ and $N\,|\alpha - a/q| \leq N^{1/20}$, it follows that

$$N^{1/10} \ll \sqrt{N}\, q^{-1/2} (1 + N|\alpha - a/q|)^{-1/2}. \qquad \square$$

Proof of Lemma 6. Squaring-out $S(a,q)$ we obtain

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

Letting $r = s + t$ and using the fact that $(a,q) = 1$ and

$$\sum_{s=0}^{q-1} e^{2\pi i a(2st)/q} = \begin{cases} q & \text{if } \quad 2at \equiv 0 \mod q \\ 0 & \text{otherwise} \end{cases}$$

it follows that

$$|S(a,q)|^2 = \sum_{t=0}^{q-1} e^{2\pi i a t^2/q} \sum_{s=0}^{q-1} e^{2\pi i a(2st)/q} = \begin{cases} q & \text{if } q \text{ odd} \\ q\left(e^{2\pi i a(q/4)} + 1\right) & \text{if } q \text{ even} \end{cases}. \qquad \square$$

Proof of Lemma 7. We need only consider the case when $\lambda \geq 1$. We write

$$\int_0^1 e^{2\pi i\lambda x^2}dx = \int_0^{\lambda^{-1/2}} e^{2\pi i\lambda x^2}dx + \int_{\lambda^{-1/2}}^1 e^{2\pi i\lambda x^2}dx =: I_1 + I_2.$$

It is easy to then see that $|I_1| \leq \lambda^{-1/2}$, while integration by parts gives that

$$\begin{aligned} |I_2| &= \left| \int_{\lambda^{-1/2}}^1 \frac{1}{4\pi i\lambda x}\Big(\frac{d}{dx}e^{2\pi i\lambda x^2}\Big)dx \right| \\ &\leq \frac{1}{4\pi\lambda}\left| \Big[\frac{1}{x}\,e^{2\pi i\lambda x^2}\Big]_{\lambda^{-1/2}}^1 + \int_{\lambda^{-1/2}}^1 \frac{1}{x^2}\,e^{2\pi i\lambda x^2}dx \right| \\ &\leq \lambda^{-1/2}. \end{aligned}$$

□

References

[1] A. Balog, J. Pelikán, J. Pintz, E. Szemerédi, *Difference sets without κ-th powers*, Acta Math. Hungar. 65 (1994), 165-187.

[2] E. Croot and O. Sisask, *A new proof of Roth's theorem on arithmetic progressions*, Proc. Amer. Math. Soc. 137 (2009), no. 3, 805809.

[3] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), pp. 204–256.

[4] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. Jour., 114, (2002) (2), 215–238.

[5] W. T. Gowers, *Additive and Combinatorial Number Theory*, `www.dpmms.cam.ac.uk/∼wtg10/addnoth.notes.dvi`

[6] M. Hamel and I. Łaba, *Arithmetic structures in random sets*, Integers: Electronic Journal of Combinatorial Number Theory 8 (2008), #4

[7] T. Kamae and M. Mendès France, *van der Corput's difference theorem*, Israel J. Math. 31 (1978), no. 3-4, 335-342.

[8] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. 123 (2006), no. 1, 57-95.

[9] N. Lyall and Á. Magyar, *Polynomial configurations in difference sets*, J. Num. Theory, v. 129/2, pp. 439-450, 2009.

[10] N. Lyall and Á. Magyar, *Polynomial configurations in difference sets (Revised version)*, `arxiv.org/abs/0903.4504`.

[11] N. Lyall and Á. Magyar, *Sárközy's Theorem*, `www.math.uga.edu/l̃yall/Research/Sarkozy.pdf`.

[12] N. Lyall and Á. Magyar, *Simultaneous polynomial recurrence*, `arxiv.org/abs/1009.0766`, to appear in the Bulletin of the London Math. Soc.

[13] H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics, 84.

[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), 219-231.

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

[16] A. Sárzözy, *On difference sets of sequences of integers III*, Acta Math. Acad. Sci. Hungar. 31 (1978), pp. 355–386.

[17] P. Varnavides, *On certain sets of positive density*, Journal London Math. Soc., 34 (1959), 358360

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

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