Behrend's example

Theorem 1 (Behrend's Theorem, 1946 [1]). *Let N be a large integer. Then there exists a subset $A \subseteq [1, N]$ with $\frac{|A|}{N} \geq \exp(-c\sqrt{\log N})$ which does not contain any arithmetic progressions of length three.*

Proof. Behrend's construction relies on the observation that a line can intersect any sphere in at most two points.

Consider the points $x \in [1, M]^n$ We know that there are M^n such points. Let us consider the possible radii of these points x: for any $x \in [1, M]^n$, we have $r^2 := x_1^2 + \ldots x_n^2 \in [n, nM^2]$. Hence, by the pigeonhole principle, there must be some sphere, S, which contains at least

$$|S| \geq \frac{M^n}{n(M^2-1)} > \frac{M^{n-2}}{n}$$

points.

We would now like to map S to $[1, N]$. For any $x \in S$, we define

$$P(x) := \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i.$$

One can then show (check this!) that

(i) P is a one-one mapping

(ii) $x + y = 2z$ whenever $P(x) + P(y) = 2P(z)$

(iii) $\max_{x \in S} P(x) \leq (2M)^n$.

Let $A := \{\frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i : x \in S\}$. If we now take $M := \lfloor N^{1/n}/2 \rfloor$ and $n := \sqrt{\log N}$, then we see that $\frac{|A|}{N} \geq \exp(-C\sqrt{\log N})$. □

The following theorem, taken from Soundararajan [2], should be compared with Varnavides' variant of Roth's theorem.

Theorem 2. *Let $\delta > 0$ and let N be a large integer. Then there exists a subset $A \subseteq [1, N]$ such that $|A| \geq \delta N$ and has fewer than $\delta^{c \log(1/\delta)} N^2$ three term arithmetic progressions.*

Proof. Let $\delta > 0$. Let $B \subseteq [1, M]$ with density 2δ which contains no three term arithmetic progressions. Behrend's construction tells us that we can take $M = \exp(c \log^2(1/\delta))$. We will now define a set A using translates of B. For each $1 \leq x \leq 2MK$, we will say that $x \in A$ if $x \equiv b \pmod{2M}$ for some $b \in B$. Then

$$|A| \geq \delta(2KM).$$

Notice that if $x + z = 2y$, and $x, y, z \in A$, then we must have $x \equiv y \equiv z \pmod{2M}$. Hence, the maximum number of three term arithmetic progressions in A is bounded by $2\delta MK \cdot K$. Applying our choice of M gives the desired result. □

References

[1] F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U. S. A.*, 32:331–332, 1946.

[2] K. Soundararajan. Additive combinatorics: Winter 2007. `http://math.stanford.edu/~ksound/Notes.pdf`.