BEHREND'S EXAMPLE

NEIL LYALL

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

Proof. The proof relies on the geometrical observation that a straight line can intersect a sphere in $\mathbb{Z}^n$ in at most two points. In other words the set

$$\{x \in \mathbb{Z}^n : |x| = r\}$$

cannot contain an arithmetic progression of length three, for any $r > 0$ and $n \geq 1$.

Now we have to map this example back to $\{1, \dots, N\}$. Let n, M be large integers which we shall determine later, and consider the set

$$S(r) = \{x \in \{1, \dots, M\}^n : x_1^2 + \cdots + x_n^2 = r^2\}.$$

Note that as r^2 ranges from n to nM^2 these sets cover the cube $\{1, \dots, M\}^n$, which is of cardinality M^n. It therefore follows from the 'principle of the pigeons' that there exist a radius $\sqrt{n} \leq R \leq \sqrt{n}M$ such that the sphere $S := S(R)$ in $\{1, \dots, M\}^n$ has cardinality

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

Now we must map S to $\{1, \dots, N\}$. To this end we define the mapping

$$P(x) = P(x_1, \dots, x_n) = \frac{1}{2M}\sum_{k=1}^{n} x_k(2M)^k.$$

It is then easy to check that

(i) P is a one-one mapping
(ii) $x + y = 2z$ whenever $P(x) + P(y) = 2P(z)$
(iii) $\max_{x\in S} P(x) \leq (2M)^n$.

Therefore, if we set $M = \lfloor N^{1/n}/2 \rfloor$ it follows that $P(S) \subset \{1, \dots, N\}$ and contains no arithmetic progressions of length three. Setting $n = \sqrt{\log N}$ we see that $P(S)$ has cardinality

$$|P(S)| = |S| \geq \frac{N^{1-2/n}}{n2^n} \geq N\exp(-\log n - n\log 2 - \tfrac{2}{n}\log N) = N\exp(-C\sqrt{\log N}). \qquad \square$$

[1] If we let $r(N)$ denote the maximal cardinality of a subset $A \subset [1,N]$ which does not contain any arithmetic progressions of length three, then combining Behrend's theorem with the bounds obtained by Roth, we see that

$$N\exp(-c\sqrt{\log N}) \leq r(N) \leq CN/\log\log N.$$

The best know upper bound of $c_1 N\sqrt{\log\log N/\log N}$ for $r(N)$ is due to Bourgain.
Alternatively, if for a given $0 < \delta < 1$ we define $R(\delta)$ to be the smallest number R such that if $N \geq R$ then any $A \subset [1,N]$ with $|A| = \delta N$ contains an arithmetic progression of length three, then the corresponding inequality is

$$\exp(1/c \cdot \log 1/\delta)^2 \leq R(\delta) \leq \exp\exp(C/\delta).$$

Here Bourgain's result corresponds to the upper bound of $\exp(c_2/\delta^{2+\epsilon})$ *for* $R(\delta)$.