Behrend's Construction

Bryan Gillespie, Pennsylvania State University

June 31, 2010

The following is a detailed discussion of Behrend's construction of a large set of integers which lacks three-term arithmetic progressions. It is based on a proof sketch introduced to me at the 2010 University of Georgia REU in mathematics, which in turn was based on Behrend's original manuscript [1].

Theorem 1 (Behrend's Theorem, 1946). *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 $x = (x_1, x_2, \ldots, x_n) \in [1, M]^n$. We know that there are M^n such points, and for each point we have that $r^2 := x_1^2 + \ldots + x_n^2$ is integer-valued in the interval $[n, nM^2]$. Thus by the pigeonhole principle, there must exist a sphere $S_n(M)$ with radius r which contains at least

$$|S_n(M)| \geq \left\lceil \frac{M^n}{nM^2 - n + 1} \right\rceil \geq \frac{M^n}{n(M^2 - 1)} > \frac{M^{n-2}}{n}$$

points.

We would now like to map $S_n(M)$ to the integers. We define $P : \mathbb{Z}^n \to \mathbb{Z}$ by

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

This mapping has a number of desirable properties which will be useful:

I. P is integer-valued;

II. $1 \leq P(x) \leq (2M)^n$ for each $x \in [1, M]^n$;

III. P is linear;

IV. P is one-to-one in the domain $[1, M]^n$; and

V. $P(z) - P(y) = P(y) - P(x) \implies z - y = y - x$ for all $x, y, z \in [1, M]^n$.

Property I is clear because each summand in P includes a factor of $2M$.

Property II follows because each summand is strictly increasing with each of the coordinates x_i. Thus we have that for $x \in [1, M]^n$,

$$P(x) \leq P((M, M, \ldots, M)) = \frac{1}{2M} \sum_{i=1}^{n} M(2M)^i$$
$$= M \sum_{i=1}^{n-1} (2M)^i = M \frac{(2M)^n - 1}{2M - 1} \leq M \frac{(2M)^n}{M} = (2M)^n.$$

The lower bound is trivial since each summand $x_i(2M)^{i-1}$ is greater than or equal to 1.

Property III is straightforward from the definition of P, for if $x, y \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$, we have

$$P(ax + by) = \frac{1}{2M} \sum_{i=1}^{n} (ax_i + by_i)(2M)^i$$
$$= a \left(\frac{1}{2M} \sum_{i=1}^{n} x_i(2M)^i \right) + b \left(\frac{1}{2M} \sum_{i=1}^{n} y_i(2M)^i \right) = aP(x) + bP(y).$$

To see that Properties IV and V hold, we make use of the following lemma.

Lemma 1.1. *Let $x \in (-2M, 2M)^n$. Then $P(x) = 0$ if and only if $x = 0$.*

Proof. If $x = 0$, then clearly $P(x) = 0$ by the definition of P. Now suppose by way of contradiction that $P(x) = 0$ but $x \neq 0$. In this case, there is a least coordinate j such that $x_j \neq 0$. Then we have

$$P(x) = \frac{1}{2M} \sum_{i=1}^{n} x_i(2M)^i = \frac{1}{2M} \sum_{i=j}^{n} x_i(2M)^i = 0,$$

and this implies that

$$x_j = \sum_{i=j+1}^{n} x_i(2M)^{i-j} = 2M \sum_{i=0}^{n-(j+1)} x_{i+(j+1)}(2M)^i = 2M \cdot k,$$

where k is an integer. But we are assuming that $0 < |x_j| < 2M$, and this implies that $0 < k < 1$, which is ridiculous. Thus our original assumption must have been false, and we must conclude that $x = 0$. $\square$

Now to see that Property IV holds, suppose that $P(x) = P(y)$ for $x, y \in [1, M]^n$. Then we have $P(x) - P(y) = P(x - y) = 0$, and since $x - y \in (-M, M)^n \subseteq (-2M, 2M)^n$, this implies by the lemma that $x - y = 0$, or $x = y$. Thus P is one-to-one.

Finally, to see that Property V holds, suppose that $P(z) - P(y) = P(y) - P(x)$ for $x, yz \in [1, M]^n$. Then we have

$$P(z) - 2P(y) + P(x) = P(z - 2y + x) = 0,$$

and we notice that $z - 2y + x \in (-2M, 2M)^n$. So again by the lemma, we find that $z - 2y + x = 0$, or $z - y = y - x$, as we wished to show.

Now take $n = \lceil \sqrt{\log N} \rceil$ and $M = \lfloor N^{1/n}/2 \rfloor$, and define $A := P(S_n(M))$. Then $A \subseteq [1, (2M)^n] \subseteq [1, N]$ because P is integer valued into the domain $[1, (2M)^n]$, and $|A| = |S_n(M)|$ because P is one-to-one. Finally, we notice that A contains no arithmetic progressions of length 3, because by

Property V, any non-trivial 3-term arithmetic progression in A corresponds to such a progression in S, which is impossible because a line can intersect with a Euclidean sphere in at most 2 points. To see that A is large enough, we calculate (assuming N exceeds some trivial lower bounds):

$$\begin{aligned}\frac{|A|}{N} = \frac{|S|}{N} \geq \frac{M^{n-2}}{nN} = \frac{\left\lfloor N^{1/n}/2 \right\rfloor^{n-2}}{nN} \geq \frac{\left(N^{1/n}/e\right)^{n-2}}{nN} = e^{2-n} \cdot N^{-2/n} \cdot \frac{1}{n} \\ = e^{\left(2-\left\lceil \sqrt{\log N} \right\rceil\right)} \cdot N^{\left(-2/\left\lceil \sqrt{\log N} \right\rceil\right)} \cdot \frac{1}{\left\lceil \sqrt{\log N} \right\rceil} \\ \geq e^{\left(2-\left(\sqrt{\log N}-1\right)\right)} \cdot N^{\left(-2/\sqrt{\log N}\right)} \cdot \frac{1}{\sqrt{\log N}+1} \\ \geq e^{\left(1-\sqrt{\log N}\right)} \cdot e^{\left(-2\log N/\sqrt{\log N}\right)} \cdot e^{-1-\sqrt{\log N}} = e^{-4\sqrt{\log N}}\end{aligned}$$

Thus A satisfies the bounds required by the theorem.

□

References

[1] Behrend, Felix A. *On the sets of integers which contain no three in arithmetic progression.* Proceedings of the National Academy of Sciences, 23:331-332, 1946.