

+

+

An Improved Construction of Progression-Free Sets

Michael Elkin

Ben-Gurion University

+

1

The Problem

Numbers i, j, ℓ form an

arithmetic triple if

$$i = \frac{j+\ell}{2} \text{ or } j = \frac{i+\ell}{2} \text{ or } \ell = \frac{i+j}{2}.$$

A subset $S \subseteq \{1, 2, \dots, n\}$ is

progression-free if it contains

no arithmetic triple.

$\nu(n)$ - the largest size of a
progression-free subset $S \subseteq \{1, 2, \dots, n\}$.

$$\nu(n) = ?$$

Previous Research - Lower Bounds

[van der Waerden, 1927]

Closely related problem.

$\forall k, \ell \exists n = n(k, \ell)$ such that
 \forall partition $S_1 \cup S_2 \cup \dots \cup S_k = \{1, 2, \dots, n\}$
 $\exists S_i$ that contains an arithmetic
progression of length ℓ .

[Erdos, Turan, 1936]

Introduced $\nu(n)$ and showed that

$$\nu(n) = \Omega(n^{\log_3 2})$$

Previous Research - Lower Bounds (Cont.)

[Salem, Spencer, 1942]

$$\nu(n) = \Omega\left(\frac{n}{\frac{c \log n}{2^{\log \log n}}}\right),$$

for a constant $c > 0$.

[Behrend, 1946]

$$\nu(n) = \Omega\left(\frac{n}{2^{2\sqrt{2}\sqrt{\log_2 n}} \cdot \log^{1/4} n}\right)$$

No improvement since then!

Previous Research

Upper Bounds:

[Roth, 1953]

$$\nu(n) = O\left(\frac{n}{\log \log n}\right)$$

[Bourgain, 1999, 2007]

$$\nu(n) = O\left(\frac{n}{\log^{2/3} n} (\log \log n)^2\right)$$

Related work:

[Rankin, 1960] - excluding arithmetic progressions of length $k \geq 4$.

[Ruzsa, 1993], [Shapira, 2006], [Koester, 2008] - excluding more general subsequences.

[Szemerédi, 1975] - any dense subset of integers contains an infinitely long arithmetic progression.

[Green, Tao, 2004] - primes contain an infinitely long arithmetic progression.

Our Result

$$\nu(n) = \Omega\left(\frac{n}{2^{2\sqrt{2}\sqrt{\log_2 n}}} \cdot \log^{1/4} n\right)$$

Improves the result of Behrend
by a factor of $\Theta(\sqrt{\log n})$.

Proves that

- Behrend's construction is *not optimal*.
- $\frac{n}{2^{2\sqrt{2}\sqrt{\log_2 n}}}$ is *not the right expression*.

Consequent Work

- [Green,Wolf] Arxiv, Oct. 2008
“A Note on Elkin’s Improvement of Behrend’s Construction”

Alternative (much shorter) proof of our result.

Citing [Green,Wolf]:

“The only advantage of our approach is its brevity: it is based on ideas morally close to those of Elkin, and moreover, his argument is more constructive than ours.”

- [O’Bryant] Arxiv, Nov. 2008

Combines our (and Green-Wolf’s) technique with that of [Rankin,60].

Gets slightly improved bounds on sets without k -term arithmetic progressions, for $k \geq 4$.

Was anticipated in [Elkin] Arxiv, Jan. 2008.

The Geometric Application

$C_k(R)$ - maximum size of a convexly independent set (CIS) U of k -dimensional integer vectors of norm $\leq R$.

[Jarnik,1925] $C_2(R) = \Theta(R^{2/3})$.

[Arnold,80],[Balog,Barany,91]

More precise estimates for $C_2(R)$.

[Andrews,63] $C_k(R) = O(R^{k-2+\frac{2}{k+1}})$, $\forall k \geq 3$.

[Barany, Larman, 98]

$$C_k(R) = \Omega(R^{k-2+\frac{2}{k+1}}), \quad \forall k \geq 3.$$

Quite elaborate proof - uses results from the approximation theory of smooth convex bodies by polytopes, and Khintchine's Flatness Theorem.

Not constructive!

Our result: a constructive algorithmic proof that

$$\forall k \geq 5: C_k(R) = \Omega(R^{k-2+\frac{2}{k+1}})$$

$$k = 4: C_4(R) = \Omega\left(\frac{R^{12/5}}{(\log \log R)^{2/5}}\right)$$

$$k = 3: C_3(R) = \Omega(R^{3/2-\epsilon}), \quad \forall \epsilon > 0$$

Elementary, self-contained, except for standard estimates on discrepancy between volume and number of integer points in large balls.

+

+

The Geometric Application (Cont.)

The computational version: $B(R)$ - the set of integer points of the k -ball of radius R , centered at 0.

Compute a CIS $U \subseteq B(R)$ of large size.

The naive solution: compute $\text{ConvHull}(B(R))$.

Running time $\geq n = |B(R)| = R^k$.

$k = 3$: Preparata-Hong's algorithm has running time $O(n \log n)$.

$k \geq 4$: Chan's algorithm has running time $n^{2-O(1/k)}$.

Our running time: $O(n^{1-\frac{1}{k+1}})$, $\forall k \geq 3$

(*Sublinear* in n , but not in $|U|$.)

(Our set's size is slightly suboptimal for $k \in \{3, 4\}$.)

+

9

Additional Applications

Our construction of progression-free sets can be implemented in $\frac{n}{2^{\Omega(\sqrt{\log n})}}$ time.



Our construction can be used instead of Behrend's construction in all applications.

Matrix Multiplication:

[Coppersmith, Winograd, 90]

$$n^w \cdot \zeta(n), \quad w < 2.376, \quad \zeta(n) = n^{o(1)}.$$

Using our construction inside the algorithm of Coppersmith-Winograd one gets running time $n^w \cdot \zeta(n) \cdot \frac{1}{\log^\eta n}$, for some constant $\eta > 0$.

Overview of Behrend's Construction

k - a positive integer parameter.

$$y = \frac{n^{1/k}}{2}.$$

Select an integer point v
uniformly at random from $C = \{0, 1, \dots, y - 1\}^k$.

$$Z = \|v\|^2$$

$$\mu_Z \approx \frac{k}{3} \cdot y^2$$

$$\sigma_Z = \Theta(\sqrt{k} \cdot y^2)$$

Behrend's Construction (Cont.)

By Chebyshev inequality

$$\mathbb{P}(|Z - \mu_Z| > 2\sigma_Z) \leq \frac{1}{4}$$

↓

$\geq \frac{3}{4} \cdot |C|$ of all vectors of C
belong to the annulus $\hat{\mathcal{S}}$ given by

$$\hat{\mathcal{S}} = \{v : \mu_Z - 2\sigma_Z \leq \|v\|^2 \leq \mu_Z + 2\sigma_Z\}.$$

Let $K = C \cap \hat{\mathcal{S}}$.

$$|K| \geq \frac{3}{4} \cdot |C| = \frac{3}{4}y^k.$$

Since every $v \in K$ is an integer point,
 $\|v\|^2$ may accept $\leq 4\sigma_Z + 1$ values
between $\mu_Z - 2\sigma_Z$ and $\mu_Z + 2\sigma_Z$.

By PHP, $\exists T$ such that

$$\mu_Z - 2\sigma_Z \leq T \leq \mu_Z + 2\sigma_Z$$

$$\text{and } \geq \frac{|K|}{4\sigma_Z+1} \geq \frac{3}{4} \cdot \frac{1}{4\sigma_Z+1} \cdot |C| = \frac{3}{4} \cdot \frac{y^k}{4\sigma_Z+1} = \Omega\left(\frac{y^k}{\sigma_Z}\right)$$

vectors $v \in K$ satisfy $\|v\|^2 = T$.

\mathcal{S} - the set of integer points of C that belong to the sphere P of squared norm T .

Since $\sigma_Z = \Theta(\sqrt{k} \cdot y^2)$,

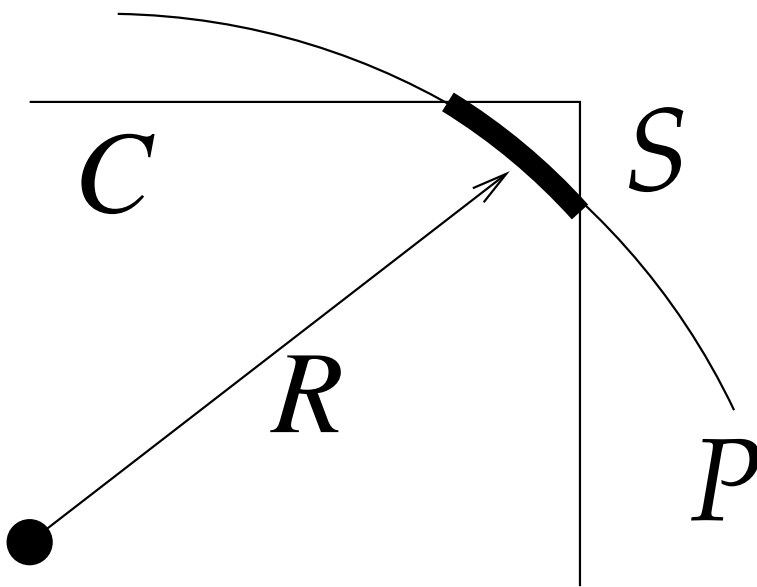
$$|\mathcal{S}| = \Omega\left(\frac{y^k}{\sigma_Z}\right) = \Omega\left(\frac{1}{\sqrt{k} \cdot y^2} \cdot y^k\right) = \Omega\left(\frac{y^{k-2}}{\sqrt{k}}\right).$$

$$R = \sqrt{T} \approx \sqrt{\mu_Z \pm 2\sigma_Z} \approx \sqrt{\frac{k}{3}} \cdot y.$$

Set $k = \sqrt{2 \cdot \log_2 n}$.



$$|S| = \Omega\left(\frac{y^{k-2}}{\sqrt{k}}\right) = \Omega\left(\frac{n}{2^{2\sqrt{2}} \sqrt{\log_2 n} \cdot \log^{1/4} n}\right).$$



Via Freiman isomorphism, construct a progression-free $S \subseteq \{1, 2, \dots, n\}$, with $|S| = |S|$. Hence

$$|S| = \Omega\left(\frac{y^{k-2}}{\sqrt{k}}\right) = \Omega\left(\frac{n}{2^{2\sqrt{2}} \sqrt{\log_2 n} \cdot \log^{1/4} n}\right).$$

Behrend Construction versus Our Construction

Behrend: Points are on a *sphere*.

Our construction: Replace the sphere by a *thin annulus*.

A hurdle: A set \mathcal{A} of integer points in an annulus is *not* necessarily convexly independent.

Our solution: Construct a large convexly independent subset (CIS) $Q = \text{Ext}(\mathcal{A})$ of \mathcal{A} .

The annulus is sufficiently thin so that

$$|Q| \geq \frac{|\mathcal{A}|}{2} .$$

+

+

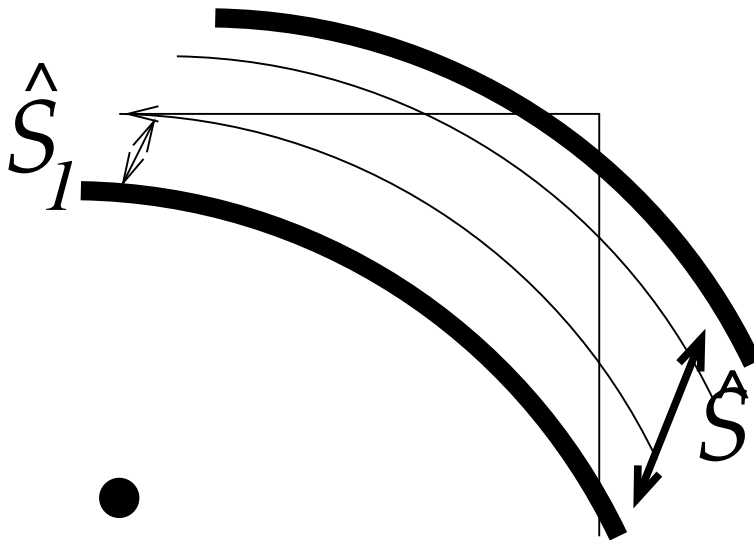
Constructing the Thin Annulus

The rv Z : the squared norm of a point selected uniformly at random from $C = \{0, 1, \dots, y - 1\}^k$.

The (thick) annulus $\hat{\mathcal{S}}$: integer points of squared norm between $\mu_Z - 2 \cdot \sigma_Z$ and $\mu_Z + 2 \cdot \sigma_Z$.

$$|\hat{\mathcal{S}}| = \Omega(y^k).$$

Partition $\hat{\mathcal{S}}$ into disjoint thin annuli $\hat{\mathcal{S}}_1, \hat{\mathcal{S}}_2, \dots$ of (squared) width $g = \epsilon \cdot k$, $\epsilon > 0$.



+

+

+

Constructing the Annulus (Cont.)

Each $\hat{\mathcal{S}}_i$ has (squared) width g :

$$\hat{\mathcal{S}}_1 = \{v : \mu_Z - 2\sigma_Z \leq \|v\|^2 < \mu_Z - 2\sigma_Z + g\}$$

$$\hat{\mathcal{S}}_2 = \{v : \mu_Z - 2\sigma_Z + g \leq \|v\|^2 < \mu_Z - 2\sigma_Z + 2g\}$$

⋮

$$\#\text{annuli} \approx \frac{4\sigma_Z}{g}$$

Pick $\hat{\mathcal{S}}_i$ that contains the largest number of integer points of $\hat{\mathcal{S}}$.

By PHP, $\exists i$ such that

$$\begin{aligned} |\hat{\mathcal{S}}_i| &= \Omega\left(\frac{|\hat{\mathcal{S}}|}{4\sigma_Z/g}\right) = \Omega\left(\frac{y^k}{\sigma_Z} \cdot g\right) \\ &= \Omega\left(\frac{y^k}{\sqrt{k} \cdot y^2} \cdot \epsilon k\right) = \Omega(y^{k-2}\sqrt{k}). \end{aligned}$$

+

- \sqrt{k} is in the numerator!



The factor of $k = \Theta(\sqrt{\log n})$ is gained!

- But $\hat{\mathcal{S}}_i = \tilde{\mathcal{S}}$ is *not* convexly independent.
- We show that $\tilde{\mathcal{S}}$ contains a CIS $\check{\mathcal{S}}$ such that

$$\begin{aligned} |\check{\mathcal{S}}| &= |\text{Ext}(\tilde{\mathcal{S}})| \geq \frac{|\tilde{\mathcal{S}}|}{2} = \Omega(y^{k-2} \cdot \sqrt{k}) \\ &= \Omega\left(\frac{n}{2^{2\sqrt{2}\sqrt{\log_2 n}}} \cdot \log^{1/4} n\right). \end{aligned}$$

- Via Freiman isomorphism, this CIS translates into a progression-free set S , $|S| = |\check{\mathcal{S}}|$.

+

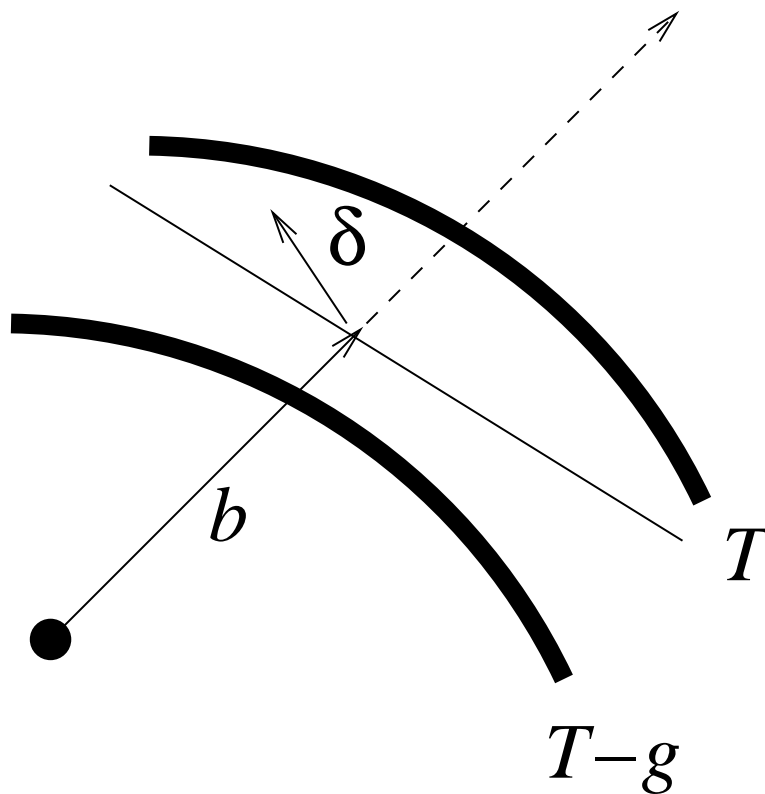
+

A Key Lemma

$B = B(\sqrt{T})$ - the set of integer points of the k -ball of squared radius T , centered at the origin.

$Ext(B)$ - the exterior set of B .

Lemma: Let $b \in B \setminus Ext(B)$ such that $T - g \leq \|b\|^2 \leq T$.
Then \exists integer vector $\delta \neq 0$ such that $0 \leq \langle b, \delta \rangle \leq g$ and $0 < \|\delta\|^2 \leq g$.



+

Wiping off Points

By the Lemma, there is a collection of hyperplanes $\mathcal{H}(\delta, h) = \{b \mid \langle b, \delta \rangle = h\}$, integer h, δ , $0 \leq h \leq g$, $0 < \|\delta\|^2 \leq g$, that contains all points b of $B \setminus \text{Ext}(B)$ that are “close” to the surface of B .

(“Close” means $T - g \leq \|b\|^2 \leq T$.)

Intuition: There are “few” hyperplanes, and each wipes off only a small number of points.

So we are left with a large CIS.

Summary and Open Problems

- **Progression-free sets:**

Our lower bound is

$$\nu(n) = \Omega \left(\frac{n}{2^{2\sqrt{2}\sqrt{\log_2 n}}} \cdot \log^{1/4} n \right).$$

Bourgain's upper bound is

$$\nu(n) = O \left(\frac{n}{\log^{2/3} n} (\log \log n)^2 \right).$$

- **Large CIS of integer vectors of norm $\leq R$ in 3D:**

Naively: $\Omega(R^{3/2})$ vectors in $O(R^3 \log R)$ time.

Our bound: $\Omega(R^{3/2-\epsilon})$ vectors in $O(R^{9/4})$ time.

Open: $\Omega(R^{3/2})$ vectors in $O(R^{3/2})$ time?