

+

+

# **An Improved Construction of Progression-Free Sets**

**Michael Elkin**

**Ben-Gurion University**

+

1

## The Problem

Numbers  $i, j, \ell$  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  $\ell$ .

[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 arithmetic progression of any length.

[Green, Tao, 2004] - primes contain an arithmetic progression of any length.

## 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

**Def:**  $U \subseteq \mathbb{R}^k$  is a *convexly independent set (CIS)* if  $\text{ConvHull}(U) = U$ .

$C_k(R)$  - maximum size of a CIS of integer  $k$ -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.

## 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 (thick) annulus  $\tilde{\mathcal{S}}$  given by

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

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

(Discrete cube intersected with  
the thick annulus.)

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

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

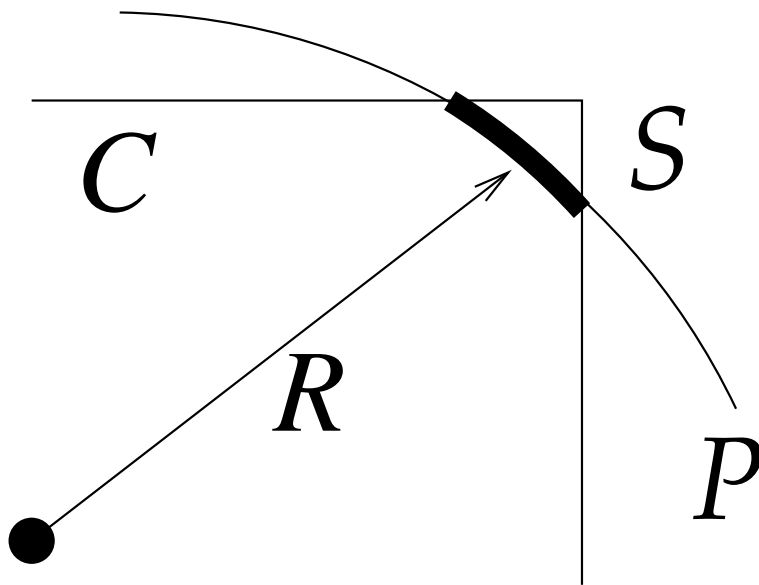
$$|\mathcal{S}| = \Omega\left(\frac{y^k}{\sigma_Z}\right) = \Omega\left(\frac{1}{\sqrt{k} \cdot y^2} \cdot y^k\right) = \Omega\left(\frac{y^{k-2}}{\sqrt{k}}\right).$$

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

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

↓

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



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

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

For Freiman isomorphism to work it is required that  $\mathcal{S}$  will be a CIS.

## Behrend Construction versus Our Construction

**Behrend:** Points are on a *sphere*.

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

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

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

The annulus is sufficiently thin so that

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

+

+

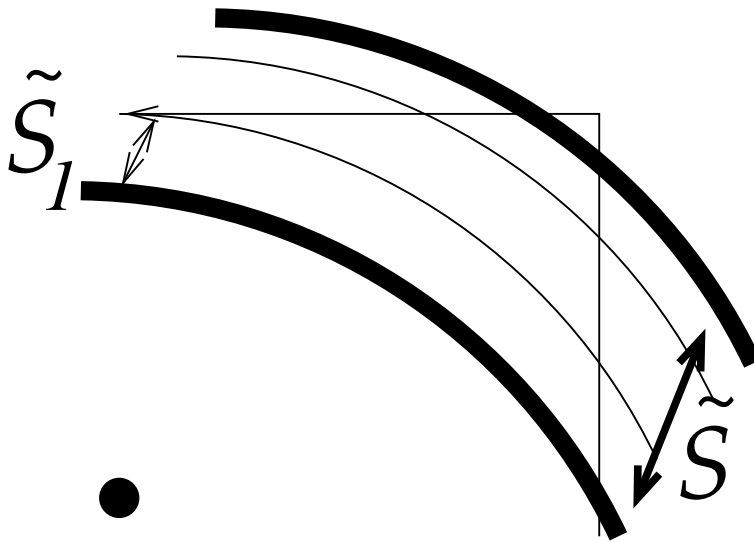
## Constructing the Thin Annulus

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

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

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

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



+

+

+

## Constructing the Annulus (Cont.)

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

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

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

⋮

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

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

By PHP,  $\exists i$  such that

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

+

- $\sqrt{k}$  is in the numerator!



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

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

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

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

It is left to construct a CIS  $\check{\mathcal{S}}$

of size  $|\check{\mathcal{S}}| \geq \frac{|\hat{\mathcal{S}}|}{2}$ .

+

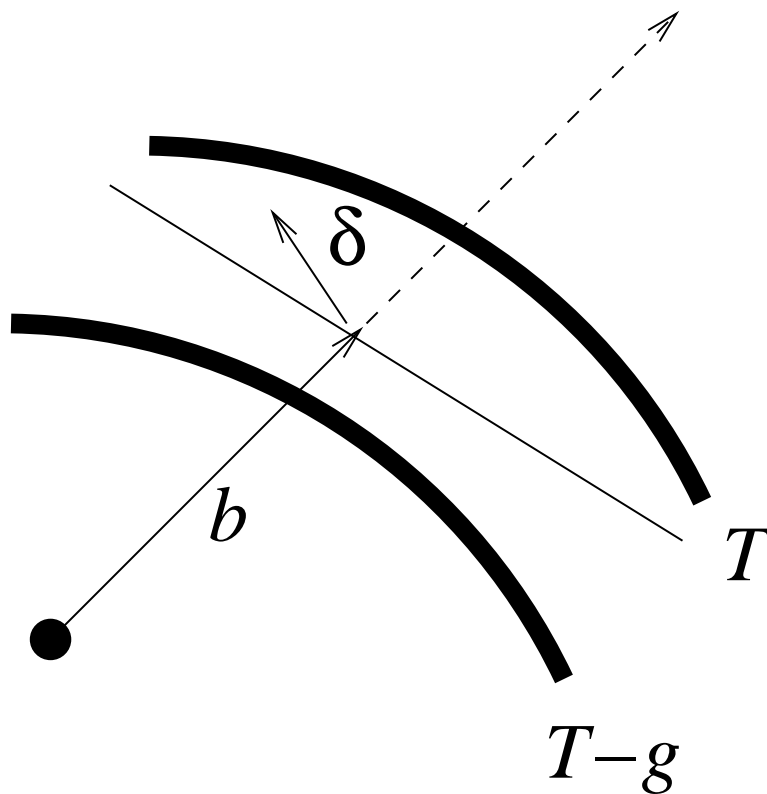
+

## 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  $h, \delta$ ,  $0 \leq h \leq g$ ,  $0 < \|\delta\|^2 \leq g$ , 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.

The set of points of  $\hat{\mathcal{S}}$  wiped off by a hyperplane  $\mathcal{H}(\delta, h)$  has dimension  $k - 1$ , while  $\hat{\mathcal{S}}$  has dimension  $k$ .

The “length” of  $\hat{\mathcal{S}}$  in each dimension is  $\approx R = \sqrt{T} \approx y$ . Thus each hyperplane wipes off  $\leq \frac{1}{y}$ -fraction of integer points of  $\hat{\mathcal{S}}$ .

+

$$\# \text{ hyperplanes} \leq (\#h) \cdot (\#\delta)$$

$$(\#h) = g + 1.$$

$$(\#\delta) \leq 2^{\eta \cdot k},$$

for an arbitrarily small  $\eta = \eta(\epsilon) > 0$ ,  $g = \epsilon \cdot k$ .

$\leq \left( \frac{2^{\eta(\epsilon) \cdot k} (g+1)}{y} \right)$ -fraction of points of  $\hat{\mathcal{S}}$   
is wiped off by *one of the hyperplanes*.

$$g \leq k = \Theta(\log y).$$

Set  $\epsilon > 0$  to be sufficiently small.  
 $\eta > 0$  becomes as small as we wish.

↓

$$\frac{2\eta(\epsilon) \cdot k(g+1)}{y} \leq \frac{1}{2}$$

Thus  $\leq \frac{1}{2}$ -fraction of points is wiped off.

↓

$$|Ext(\hat{\mathcal{S}})| \geq \frac{1}{2}|\hat{\mathcal{S}}|$$

$Ext(\hat{\mathcal{S}})$  is a CIS.

+

+

## Estimating $(\#\delta)$

$\delta$  is an integer  $k$ -vector  
s.t.  $0 < \|\delta\|^2 \leq g$ .

We prove that  $(\#\delta) \leq 2^{\eta \cdot k}$

### Proof:

$(\#\delta) \approx \text{Vol}(k\text{-ball of squared radius } g)$

$(\#\delta) \approx \beta_k \cdot g^{k/2},$

where  $\beta_k = \text{Vol}(\text{unit-radius } k\text{-ball}) = \frac{\pi^{k/2}}{\Gamma(k/2+1)}.$

$(\#\delta) \approx \frac{(\epsilon \cdot k)^{k/2} (\pi e)^{k/2}}{(k/2)^{k/2}} \approx (2\pi e \cdot \epsilon)^{k/2} = 2^{\eta(\epsilon) \cdot k}.$

QED

+

+

+

## A Hurdle

To prove that each hyperplane wipes off  $\leq \frac{1}{y}$ -fraction of  $\hat{\mathcal{S}}$ .

Not obvious because:

$\hat{\mathcal{S}}$  is the set of integer points of a *very thin* annulus  $\mathcal{A}$  ( $\mathcal{A} = \{b \in \mathbb{R}^k : T - g \leq \|b\|^2 \leq T\}$ ) intersected with the discrete cube  $C$  in a *very high dimension*.

Its squared radius is  $\frac{k}{3}y^2$ .

Its squared width is  $g = \epsilon \cdot k$ .

Its dimension is  $k = 2 \log y$ .

(The dimension grows *logarithmically* with the radius.)

+

17

We end up proving a weaker statement:  
each hyperplane wipes off  
 $\frac{2^{c \cdot k}}{y}$ -fraction of the set of integer points of  $\hat{\mathcal{S}}$   
for a *sufficiently* small  $c > 0$ . ( $0 < c < 1/2$ )

(Not for an *arbitrarily* small  $c > 0$ .)

Sufficient for our purposes.

## The Proof of the Lemma

**Lemma:** Let  $b \in B \setminus \text{Ext}(B)$  such that  $T - g \leq \|b\|^2 \leq T$ .

Then  $\exists \delta \neq 0$  such that  $0 \leq \langle b, \delta \rangle \leq g$  and  $0 < \|\delta\|^2 \leq g$ .

### Proof:

$\exists a, c \in B$  (integer points)

$\exists p, 0 < p < 1$  such that

$$b = p \cdot a + (1 - p) \cdot c.$$

$$\|a\|^2, \|c\|^2 \leq T.$$

If  $\langle a, b \rangle, \langle c, b \rangle < \|b\|^2$

then  $\langle b, b \rangle = p\langle a, b \rangle + (1 - p)\langle c, b \rangle < \|b\|^2$ ,  
contradiction.

Hence wlog  $\langle a, b \rangle \geq \|b\|^2$ .

↓

$$\langle a - b, b \rangle \geq 0.$$

Set  $\delta = a - b$ .

Hence  $\langle b, \delta \rangle \geq 0$ .

$\delta$  is an integer vector.

Since  $0 < p < 1$ ,  $\delta \neq 0$ .

$$T \geq \|a\|^2 = \|b + \delta\|^2 = \|b\|^2 + 2\langle b, \delta \rangle + \|\delta\|^2.$$

But  $\|b\|^2 \geq T - g$ .

↓

$$2\langle b, \delta \rangle + \|\delta\|^2 \leq g.$$

Since  $\langle b, \delta \rangle \geq 0$ ,

it follows that  $\langle b, \delta \rangle, \|\delta\|^2 \leq g$ .

QED

+

+

## Counting Points Wiped off by a Hyperplane

$$\mathcal{A} = \{b \in \mathbb{R}^k : T - g \leq \|b\|^2 \leq T\}$$

(continuous annulus)

$$\mathcal{C} = [0, y - 1]^k \text{ (continuous hypercube)}$$

$$\hat{\mathcal{S}} = \mathcal{A} \cap \mathcal{C} \text{ (continuous annulus}$$

intersected with *discrete* hypercube)

$$\mathcal{H} = \mathcal{H}(\delta, h) = \{b \mid \langle b, \delta \rangle = h\}$$

(we fix  $\delta$  and  $h$ ;  
 $\mathcal{H}$  is a fixed hyperplane)

$$\hat{\mathcal{W}} = \hat{\mathcal{W}}(\delta, h) = \hat{\mathcal{S}} \cap \mathcal{H} = (\mathcal{A} \cap \mathcal{C}) \cap \mathcal{H}$$

Our goal is to estimate  $|\hat{\mathcal{W}}|$ , i.e.,  
to show that  $\frac{|\hat{\mathcal{W}}|}{|\hat{\mathcal{S}}|} \leq \frac{2^{c \cdot k}}{y}$ ,  
for an appropriate sufficiently  
small constant  $c$ ,  $0 < c < 1/2$ .

( $y \approx 2^{k/2}$ ; so  $c$  should be  $< 1/2$ .)

+

+

+

## Counting (Cont.)

$$\mathcal{A}' = \mathcal{A} \cap \mathcal{H}$$

$\mathcal{A}'$  is a  $(k - 1)$ -dimensional annulus,  
 $\mathcal{A}' \subseteq \mathcal{H}$ , centered at  $\frac{h}{\|\delta\|^2} \cdot \delta$ ,  
 containing vectors  $b$  such that

$$\left(T - \frac{h^2}{\|\delta\|^2}\right) - g \leq \|b - \frac{h}{\|\delta\|^2} \cdot \delta\|^2 \leq \left(T - \frac{h^2}{\|\delta\|^2}\right).$$

$$T' = T - \frac{h^2}{\|\delta\|^2} \leq T$$

(the new squared radius).

We need to estimate

$$\widehat{W} = \widehat{\mathcal{S}} \cap \mathcal{H} = \mathcal{A} \cap \mathcal{C} \cap \mathcal{H} = \mathcal{A}' \cap \mathcal{C}.$$

Let  $\widetilde{W} = \mathcal{A}' \cap \mathcal{C}$  be the continuous analogue of  $\widehat{W}$ , i.e.,  $\widehat{W}$  is the set of integer points of  $\widetilde{W}$ .

We provide an upper bound on  $\text{Vol}(\widetilde{W})$ .

+

## The Strategy

- To use estimates on the discrepancy between volume and number of integer points to obtain an upper bound for  $\hat{W}$  using an upper bound for  $Vol(\tilde{W})$ .
- *But* the body  $\tilde{W} = \mathcal{A}' \cap \mathcal{C} = \mathcal{A} \cap \mathcal{H} \cap \mathcal{C}$  is complex; it is hard to compute its volume or the discrepancy between volume and number of integer points.
- We build a nicer body  $\tilde{Q}$  s.t.  $\tilde{W} \subseteq \tilde{Q}$ , estimate its volume and discrepancy, and get an upper bound for the number of integer points in  $\tilde{W}$ .

## The Body $\tilde{Q}$

- $\tilde{W} = \mathcal{A}' \cap \mathcal{C}$ .
- $\tilde{Q}$  is  $\mathcal{A}'$  intersected with a (relatively) small number of orthants, after the axes are appropriately rotated.
- The number of orthants will be  $2^{\epsilon \cdot k}$ .

Recall:  $g = \epsilon \cdot k$  is the squared width of  $\mathcal{A}$ ; i.e.,  $\epsilon$  is a parameter that we control.

## Crude Attempts

Taking  $\tilde{Q} = \mathcal{A}'$  is too crude.

Intuitively, we get an extra factor of roughly  $2^k \gg y = 2^{k/2}$ .

$2^k$  is the number of orthants.

$\mathcal{A}'$  contains points in all orthants in  $\mathbb{R}^{k-1}$ ;  
 ( $\mathcal{A}' \subseteq \mathcal{H}$ ; if we put the origin in the center of  $\mathcal{A}'$ , and use any orthonormal basis, then  $\mathcal{A}'$  intersects all orthants.)

$\tilde{W} = \mathcal{A}' \cap \mathcal{C}$  is contained in the positive orthant in  $\mathbb{R}^k$  (because  $\mathcal{C}$  is).

Using the  $k$ -volume of one orthant of  $\mathcal{A}$  (rather than  $(k-1)$ -volume of  $\mathcal{A}'$ ) is too crude either, as we pay an extra factor of  $y$ .

## Rotating the Space

To define the “right” superset  $\tilde{Q}$  of  $\tilde{W}$  (and subset of  $\mathcal{A}'$ ) we rotate the space.

- $\mathcal{H}' = \{\alpha \in \mathbb{R}^k \mid \langle \alpha, \delta \rangle = 0\}$  is the parallel hyperplane to  $\mathcal{H} = \{\alpha \in \mathbb{R}^k \mid \langle \alpha, \delta \rangle = h\}$  that passes through the origin.
- We'll build an orthonormal basis  $\Upsilon = \{\gamma_1, \gamma_2, \dots, \gamma_{k-1}\}$  for  $\mathcal{H}'$ .
- Recall:  $0 < \|\delta\|^2 \leq g = \epsilon \cdot k$ ,  $\delta \in \mathbb{R}^k$ ,  $\delta$  is an integer vector.



$\delta$  may have  $\leq \epsilon \cdot k$  non-zero entries.

$$I = \{i \in [k] : \delta_i \neq 0\}.$$

Let  $m = |I| \leq \epsilon \cdot k$ .

## Defining the Basis

- For each  $\alpha = (a_1, a_2, \dots, a_k) \in \mathcal{H}'$ ,

$$\sum_{i \in I} a_i \cdot \delta_i = \langle \delta, \alpha \rangle = 0 .$$

- $\{\gamma^{(1)}, \gamma^{(2)}, \dots, \gamma^{(m-1)}\}$  -  
an arbitrary orthonormal basis for the  
solution space of this equation.

$$\gamma^{(1)}, \gamma^{(2)}, \dots, \gamma^{(m-1)} \in \mathbb{R}^m ,$$

- Define  $\hat{\gamma}^{(1)}, \hat{\gamma}^{(2)}, \dots, \hat{\gamma}^{(m-1)} \in \mathbb{R}^k$  by:  
 $\hat{\gamma}^{(j)}$  agrees with  $\gamma^{(j)}$  in all coordinates  $i \in I$ ,  
and has 0 elsewhere.

- Also,  $\forall j \in [k] \setminus I$ ,  
we insert into the basis  $\Upsilon$  the vectors  
 $e_j = (0, 0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{R}^k$ ,  
with 1 in the  $j$ th entry.

+

+

## Properties of the New Basis

- $\# \text{vectors} = m - 1 + k - m = k - 1 = \dim(\mathcal{H}')$ .  
To complete it to the basis of  $\mathbb{R}^k$ ,  
add the vector  $\frac{\delta}{\|\delta\|}$ .
- $\forall j \in [k] \setminus I, e_j \in \mathcal{H}'$ ,  
because  $\delta$  has 0 in  $j$ th entry.
- All vectors have unit norm.
- $\langle \hat{\gamma}^{(i)}, e_j \rangle = 0$ ,  
because  $\hat{\gamma}^{(i)}$  has 0 in each entry  $j \in [k] \setminus I$ .
- Hence  $\Upsilon = (\hat{\gamma}^{(1)}, \dots, \hat{\gamma}^{(m-1)}) \circ (e_j \mid j \in [k] \setminus I)$   
is an orthonormal basis for  $\mathcal{H}'$ .
- We do not know much about the  
 $m - 1 \leq \epsilon \cdot k - 1$  vectors  $\hat{\gamma}^{(1)}, \hat{\gamma}^{(2)}, \dots, \hat{\gamma}^{(m-1)}$ .  
But the other  $k - m$  vectors of this basis  
are  $e_j$ 's,  $j \in [k] \setminus I$ .

+

## Changing the Axes

Notation:  $\Upsilon = \{\gamma_1, \gamma_2, \dots, \gamma_{k-1}\}$ .

- Move the origin to the point  $\frac{h}{\|\delta\|^2} \cdot \delta$  (the center of the annulus  $\mathcal{A}'$ ).
- Rotate the space so that the axes become colinear with vectors of  $\Upsilon$  and with  $\frac{\delta}{\|\delta\|}$ .
- This rotation is volume-preserving.
- For a vector  $\tau \in \mathcal{H}'$ ,  
 $\tau_1[\Upsilon], \tau_2[\Upsilon], \dots, \tau_{k-1}[\Upsilon]$  -  
the coordinates of  $\tau$  in the new basis.

$$\tau_i[\Upsilon] = \left\langle \tau - \frac{h}{\|\delta\|^2} \cdot \delta, \gamma_i \right\rangle$$

+

+

## Properties of $\Upsilon$

**Lemma:**  $\forall \tau \in \tilde{W} = \mathcal{A}' \cap \mathcal{C}$ , and  
 $\forall i \in \{m, m + 1, \dots, k - 1\}$ ,  
 $\tau_i[\Upsilon] \geq 0$ .

Hence in this basis  $\tau$  has  $\geq (1 - \epsilon) \cdot k$   
 non-negative coordinates.

**Proof:**  $\langle \tau - \frac{h}{\|\delta\|^2} \cdot \delta, \gamma_i \rangle = \langle \tau, \gamma_i \rangle$   
 (because  $\langle \delta, \gamma_i \rangle = 0$ , because  $\gamma_i \in \mathcal{H}'$ , and  $\mathcal{H}' \perp \delta$ )

Observe that  $\tau \in \mathcal{C}$ .

Thus, its coordinates are non-negative.

For  $i \in \{m, m + 1, \dots, k - 1\}$ ,  
 $\gamma_i = e_{j_i}$ , for some  $j_i \in [k] \setminus I$ .

Hence  $\langle \tau, \gamma_i \rangle = \langle \tau, e_{j_i} \rangle \geq 0$ . QED

+

## Defining $\tilde{Q}$

Recall:  $\tilde{Q}$  is a superset of  $\tilde{W}$   
 (but a subset of  $\mathcal{A}'$ ),  
 which is nicer to work with.

$$(\tilde{W} = \mathcal{A}' \cap \mathcal{C} = \mathcal{A} \cap \mathcal{H} \cap \mathcal{C})$$

$$\tilde{Q} = \{ \alpha \in \mathcal{A}' (= \mathcal{A} \cap \mathcal{H}) \mid \\ \forall i \in \{m, m+1, \dots, k-1\}, \alpha_i[\Upsilon] \geq 0 \}$$

Instead of intersecting  $\mathcal{A}'$  with the cube,  
 we intersect it with the  $2^{m-1}$   
 orthants of the rotated space.  
 The first  $m-1$  coordinates may be  
 either positive or negative;  
 the rest are non-negative.

By the last lemma,

$$\tilde{W} = \mathcal{A}' \cap \mathcal{C} \subseteq \tilde{Q}.$$

Let  $\mathcal{A}'' = (\mathbb{R}^+)^{k-1} \cap \mathcal{A}'$ ,  
(in the rotated basis).

$\mathcal{A}''$  is one single orthant  
of the annulus  $\mathcal{A}'$ .

$\tilde{Q}$  is  $2^{m-1}$  orthants of  $\mathcal{A}'$ .

Thus:

$$\text{Vol}(\tilde{Q}) = 2^{m-1} \cdot \text{Vol}(\mathcal{A}'') \leq 2^{\epsilon k - 1} \cdot \text{Vol}(\mathcal{A}'')$$

So  $\text{Vol}(\tilde{W}) \leq \text{Vol}(\tilde{Q}) \leq 2^{\epsilon k - 1} \text{Vol}(\mathcal{A}'')$ .

## Wrapping up

**Lm:**  $\text{Vol}(\mathcal{A}'') \leq g \cdot \left(\frac{\pi e}{6}\right)^{k/2} \cdot y^{k-3} \cdot 2^{O(\sqrt{k})}$ .

(The proof is by a direct calculation.)

Hence  $\text{Vol}(\tilde{W}) \leq 2^{\epsilon k} \left(\frac{\pi e}{6}\right)^{k/2} \cdot y^{k-3}$ .

It can be shown that

$$\hat{W} \leq 2^{\epsilon k} \left(\frac{\pi e}{6}\right)^{k/2} \cdot y^{k-3} \text{ too,}$$

where  $\hat{W}$  is the set of integer points in  $\tilde{W}$ .

(We argue that the #integer points in  $\tilde{Q}$  is at most this. This is easy because  $\tilde{Q}$  is “nice”, and so the discrepancy between volume and #integer points can be easily estimated. Then we conclude it for  $\tilde{W}$ , because  $\tilde{W} \subseteq \tilde{Q}$ .)

Recall that  $|\hat{\mathcal{S}}| = \Omega(\epsilon \cdot \sqrt{k} \cdot y^{k-2})$ ,

where  $\hat{\mathcal{S}} = \mathcal{A} \cap C$  is the original point set (from which  $\mathcal{H}$  wipes off the points of  $\hat{W}$ ).

We need to show that  $|\hat{W}|$  is a small fraction (ideally,  $\frac{1}{y}$ -fraction) of  $|\hat{\mathcal{S}}|$ .

+

+

## Wrapping Up (Cont.)

Roughly, we compare  $\left(\frac{\pi e}{6}\right)^{k/2}$  with  $y \approx 2^{k/2}$ .

$$\left(\frac{\pi e}{6}\right)^{k/2} \approx y^{0.51}.$$

So each hyperplane  $\mathcal{H}$  wipes off roughly  $\leq \frac{1}{\sqrt{y}}$ -fraction of all integer points of  $\widehat{\mathcal{S}}$ .

All the  $2^{\eta(\epsilon) \cdot k} = y^{2\eta(\epsilon)}$  hyperplanes wipe off  $\leq \frac{1}{y^{1/2-2\eta}}$ -fraction of all integer points of  $\widehat{\mathcal{S}}$ .

The set  $\check{\mathcal{S}}$  of the remaining points contains  $\geq \left(1 - \frac{1}{y^{1/2-2\eta}}\right)$ -fraction  $\geq$  half of all integer points of  $\widehat{\mathcal{S}}$ , and it is a CIS.

$\check{\mathcal{S}}$  translates into progression-free  $\check{\mathcal{S}}$  of the same cardinality, via Freiman isomorphism.

QED

+

## 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

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

- O'Bryant showed that these ideas can be extended to  $k$ -term progressions.

Does it extend to improve

*Ruzsa's construction?*

(Dense sets with no solutions to certain Diophantine equations.)