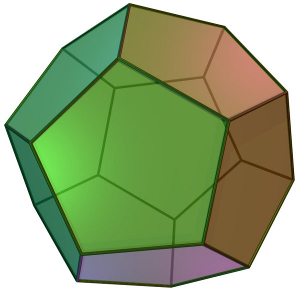
# Fooling Polytopes

Li-Yang Tan (Stanford)

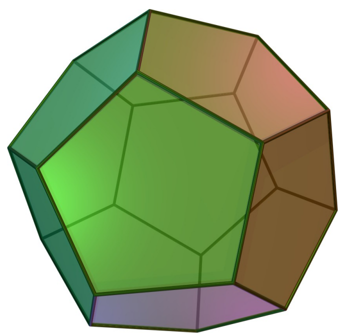
Joint work with

Ryan O'Donnell (CMU) and Rocco Servedio (Columbia)

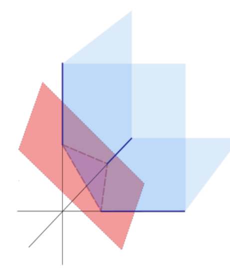


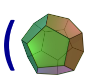
# Polytopes over $\{0,1\}^n$
# = Intersections of boolean halfspaces

$$F(x) = h_1(x) \wedge \cdots \wedge h_m(x) \qquad x \in \{0,1\}^n$$



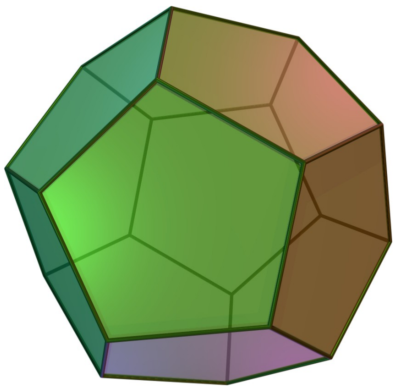
Halfspace:
$\mathrm{sign}(w \cdot x - \theta)$



- Within CS: optimization ( = {0,1}-integer programs $Ax \leq b$), complexity theory, learning theory, …
- Beyond CS: Large body of work in combinatorics, high-dimensional geometry, …

# Main complexity measure for this talk: **# of facets**

$$F(x) = h_1(x) \wedge \cdots \wedge h_m(x) \qquad x \in \{0,1\}^n$$



*m* = number of facets of polytope

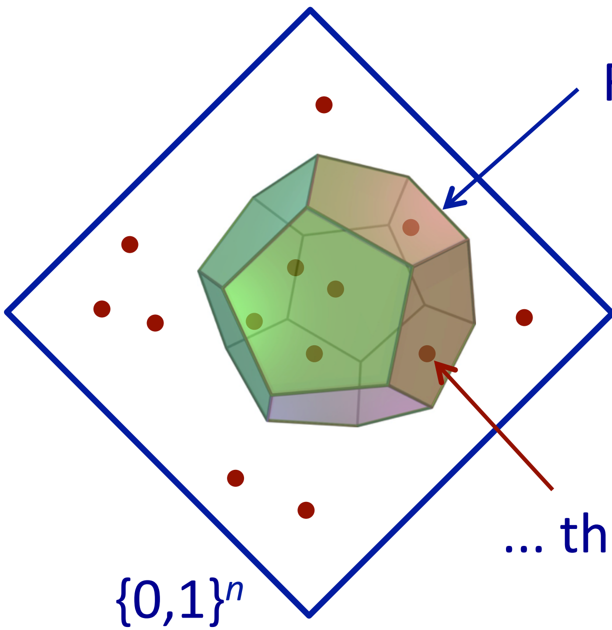
= number of halfspaces

$1 \leq m \leq 2^n$

**This talk:** think of $m$ = poly($n$), say $n^{10}$

# This talk: **Discrepancy Sets** for Polytopes

Want **small** set of points ● in $\{0,1\}^n$ such that:



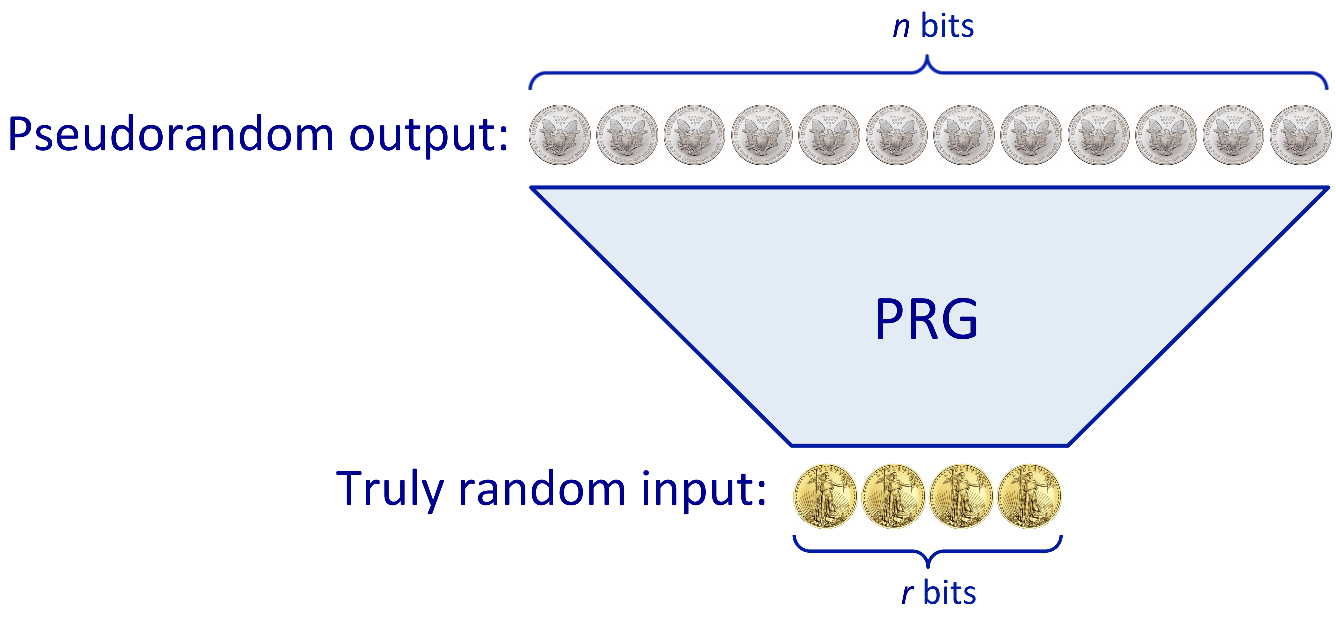

For all $m$-facet polytopes $F$,

if $F$ accepts $\Delta$ fraction of inputs in $\{0,1\}^n$ …

… then $F$ accepts $(\Delta \pm 0.01)$ fraction of points ●

*Random* set of points works great. Want **explicit** set.

# Pseudorandom Generators
## for Polytopes

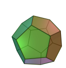


# Pseudorandom Generators

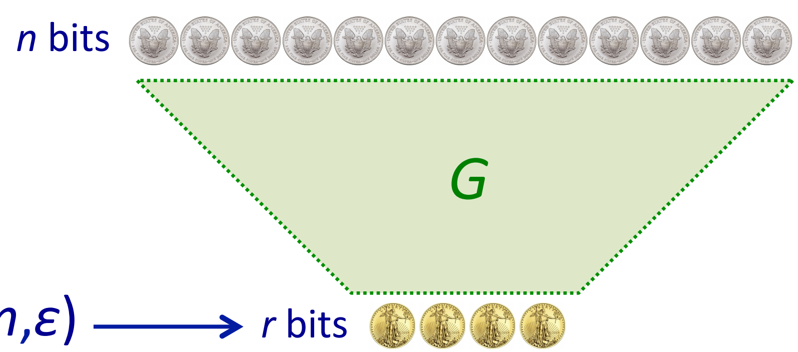
Definition: An **$\varepsilon$-PRG** for a class $C$ is an explicit function $G : \{0,1\}^r \rightarrow \{0,1\}^n$ such that: for every function $F$ in $C$,

$$\left| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\{0,1\}^n}[F(\boldsymbol{x})] - \mathop{\mathbb{E}}_{\boldsymbol{s}\sim\{0,1\}^r}[F(G(\boldsymbol{s}))] \right| \le \varepsilon$$

**This work:**

$C$ = { $m$-facet polytopes  }

**Goal:** minimize seed length $r(n,m,\varepsilon)$ →

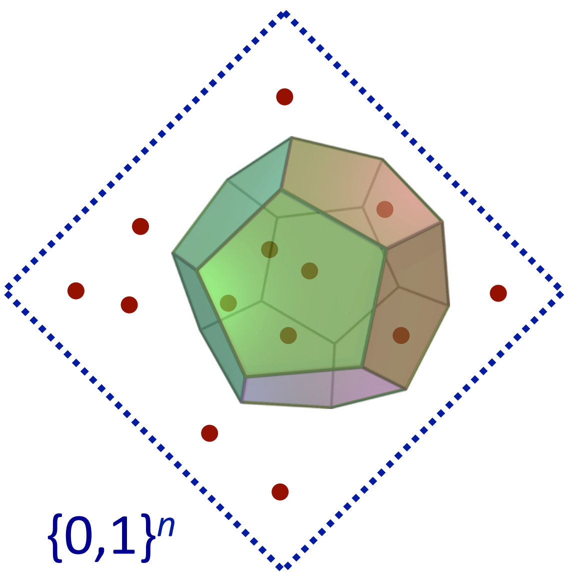


# Our main result: PRG for polytopes

An $\varepsilon$-PRG for $m$-facet polytopes over $\{0,1\}^n$ with seed length:

$$\mathrm{poly}(\log m, 1/\varepsilon) \cdot \log n$$

- Previous best seed length had linear dependence on $m$




**Equivalently:**

Discrepancy set of size $n^{\mathrm{polylog}(m)}$

(Previous best: $n^{O(m)}$)

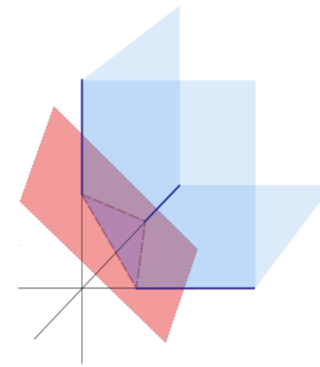
# Comparison with prior results

| **Class of functions:** | **Seed length:** |
| --- | --- |
| **Any function** of $m$ general halfspaces<br>[Gopalan, O'Donnell, Wu, Zuckerman 10] | $\tilde{O}(m \log(1/\varepsilon)) \cdot \log n$ |
| Intersections of $m$ "**regular**" halfspaces<br>[Harsha, Klivans, Meka 10] | $\mathrm{poly}(\log m, 1/\varepsilon) \cdot \log n$ |
| Intersections of $m$ **low-weight** halfspaces<br>[Servedio, T. 17] | $\mathrm{poly}(\log m, 1/\varepsilon) \cdot \mathrm{polylog}\, n$ |
| Intersections of $m$ **general** halfspaces<br>(This work) | $\mathrm{poly}(\log m, 1/\varepsilon) \cdot \log n$ |

# PRGs for halfspaces and their generalizations

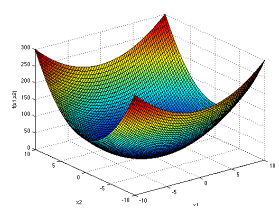
## Halfspaces

- Diakonikolas, Gopalan, Jaiswal, Servedio, Viola 2009
- Meka, Zuckerman 2009
- Karnin, Rabani, Shpilka 2011
- Kothari, Meka 2015
- Gopalan, Kane, Meka 2015



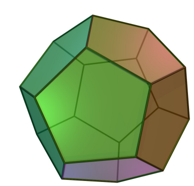
## **Polynomial** threshold functions

- Meka, Zuckerman 2009
- Diakonikolas, Kane, Nelson 2009
- Kane 2011
- Kane 2011
- Kane, Meka 2013
- Kane 2014



## **Intersections of** halfspaces

- Harsha, Klivans, Meka 2010
- Gopalan, O’Donnell, Wu, Zuckerman 2010
- Servedio, T. 2017
- **This work**



# Structure of this talk

- **Part I:** The connection to **Central Limit Theorems**
  - Versatile and powerful framework for designing PRGs

    [Meka, Zuckerman 09] [Harsha, Klivans, Meka 10]

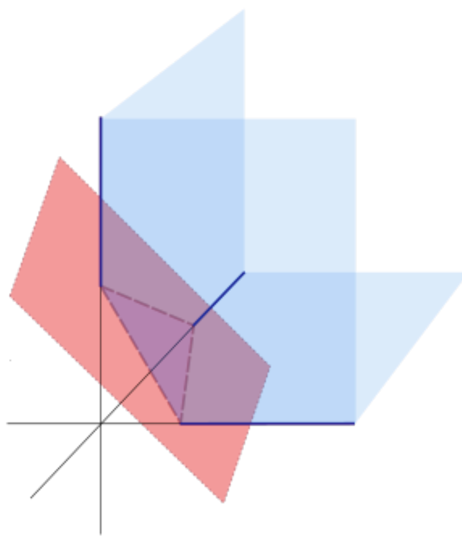
  - Especially effective for analyzing "**regular**" halfspaces

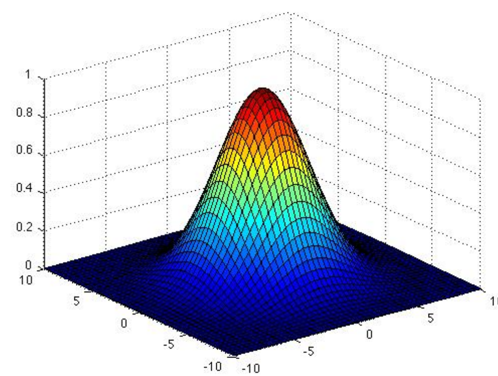
- **Part II:** Our work
  - Challenges in dealing with **general** halfspaces
  - New ideas and ingredients in our work
    - New Littlewood–Offord theorem for polytopes

**Chalk talk tomorrow!**

Part I: Background and Context

# PRGs via Central Limit Theorems






Illustrative example: Fooling a single “regular” halfspace [MZ10]

# Central Limit Theorems

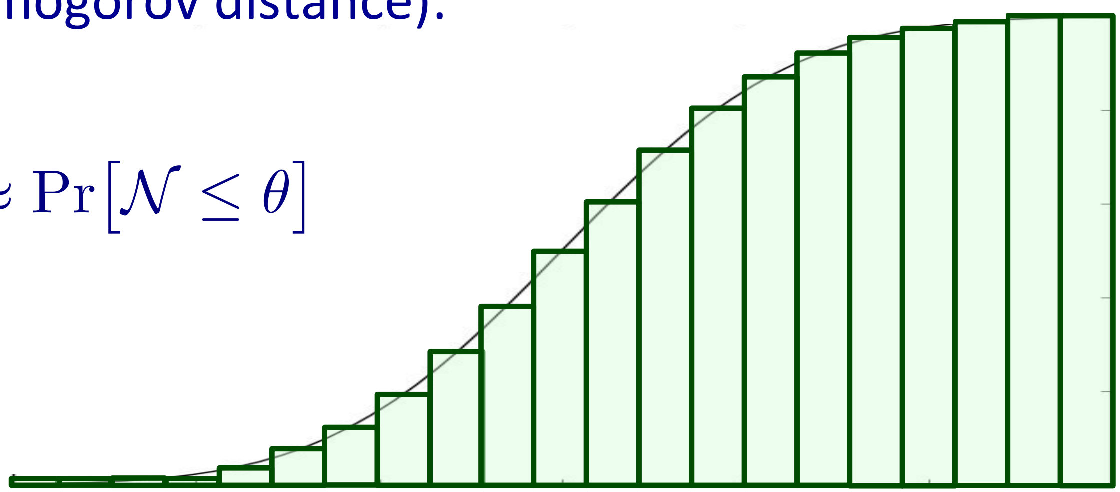
The sum of many independent "reasonable" random variables converges to **Gaussian** (of same mean and variance).

$$\boldsymbol{S} = \boldsymbol{X}_1 + \cdots + \boldsymbol{X}_n \ \approx\ \mathcal{N}(\mu, \sigma^2)$$

CDF distance (= Kolmogorov distance):

For all $\theta$ in R,

$$\Pr\big[\boldsymbol{S} \le \theta\big] \approx \Pr\big[\mathcal{N} \le \theta\big]$$



CDFs of ***S*** vs. Gaussian

# Regularity and the Berry–Esséen CLT

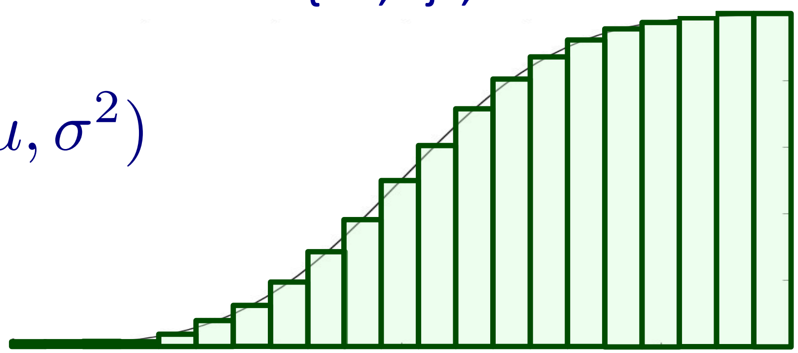
Definition: An "$\varepsilon$-regular" linear form $S : \mathbb{R}^n \to \mathbb{R}$

$$S(x) = w_1 x_1 + \cdots + w_n x_n$$

is one in which **no weight is too dominant:** $|w_i| \leq \varepsilon \cdot \|w\|_2$

**Berry–Esséen CLT:** For ***x*** uniform from $\{-1,1\}^n$,

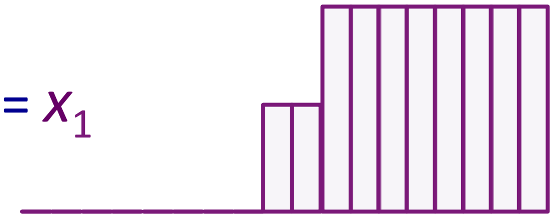
$$S(\boldsymbol{x}) \underset{\varepsilon}{\approx} \mathcal{N}(\mu, \sigma^2)$$



Observation:

Regularity crucial; consider $S(x) = x_1$

CDF of $x_1 \neq$ Gaussian



# The connection between CLTs and pseudorandomness

Regular linear form: $S(\boldsymbol{x}) = w_1\boldsymbol{x}_1 + \cdots + w_n\boldsymbol{x}_n$ (***x*** uniform $\{-1,1\}^n$)

**CLT:** $S(\boldsymbol{x})$ converges to Gaussian in CDF distance

$$\Pr_{\text{uniform } \boldsymbol{x} \sim \{\pm 1\}^n}\left[S(\boldsymbol{x}) \le \theta\right] \approx \Pr\left[\mathcal{N} \le \theta\right] \qquad \text{(for all } \theta\text{)}$$

*versus*

**Pseudorandomness:** Fool the regular halfspace sign($S(\boldsymbol{x})-\theta$)

$$\Pr_{\text{uniform } \boldsymbol{x} \sim \{\pm 1\}^n}\left[S(\boldsymbol{x}) \le \theta\right] \approx \Pr_{\text{pseudo } \boldsymbol{y} \sim \{\pm 1\}^n}\left[S(\boldsymbol{y}) \le \theta\right]$$

*Pseudorandom* version of Berry–Esséen CLT?

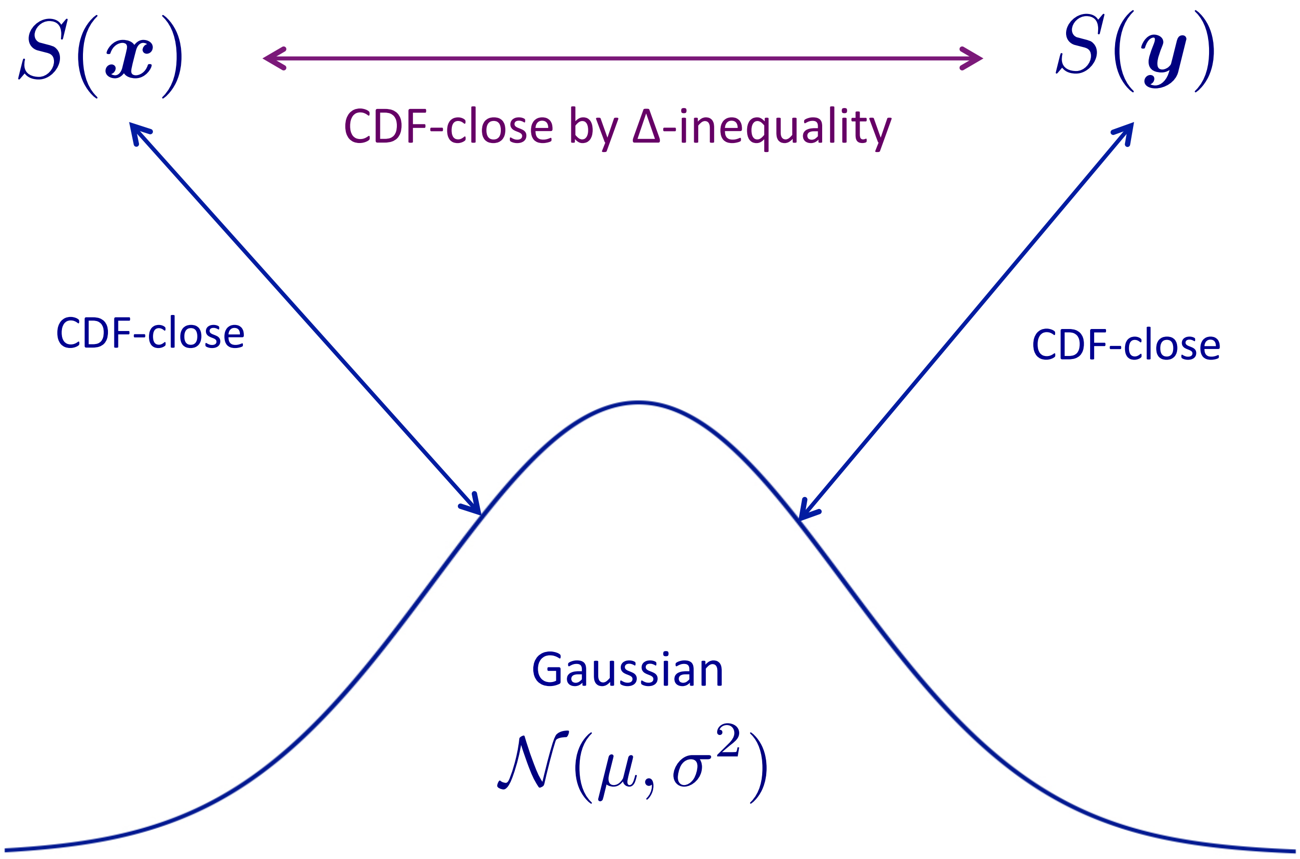
# Meka–Zuckerman: PRGs for regular halfspaces via CLTs

Berry–Esséen CLT

Uniform $\boldsymbol{x} \sim \{-1,1\}^n$

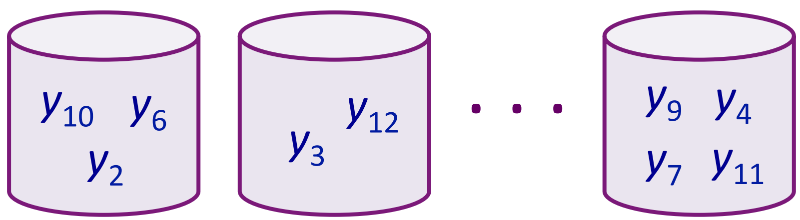
[MZ]'s **derandomization** of BE

*Pseudorandom* $\boldsymbol{y} \sim \{-1,1\}^n$



# Meka–Zuckerman's PRG for regular halfspaces

1. Pseudorandomly hash $n$ variables into $1/\varepsilon^2$ buckets
2. Assign values within each bucket according to $O(1)$-wise independent distribution (independently across buckets)




$1/\varepsilon^2$ buckets

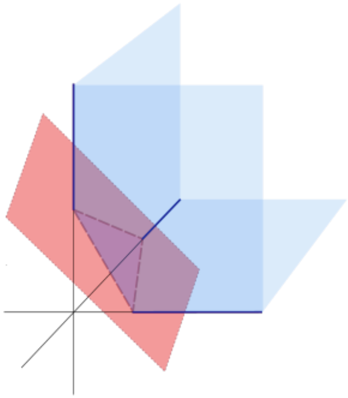
[Meka–Zuckerman 10]

- **Theorem:** Berry–Esséen CLT holds for this distribution
- **Corollary:** This is an $\varepsilon$-PRG for $\varepsilon$-regular halfspaces with seed length $O((\log n)/\varepsilon^2)$.

This talk: All PRGs = this [MZ] generator

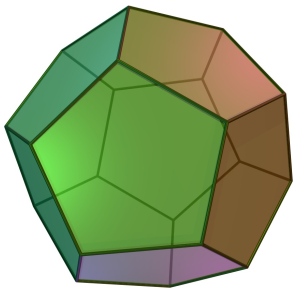
(possibly with different parameters)

# Next: Fooling **Intersections of** regular halfspaces



Regular halfspaces

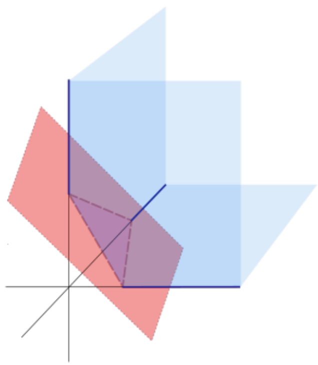
[Meka, Zuckerman 09]



**Intersections of** regular halfspaces

[Harsha, Klivans, Meka 10]

Same overall framework, but many cool new ideas and ingredients...

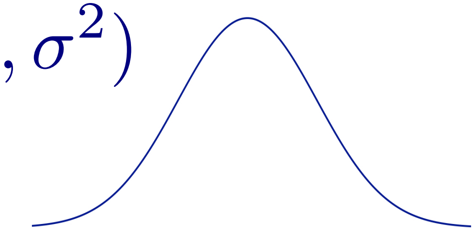


1 regular halfspace

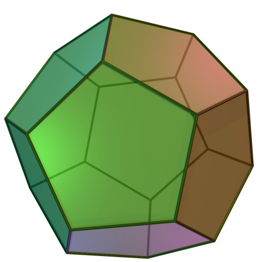
[Meka, Zuckerman 09]

## Berry-Esséen CLT

$$\underbrace{\sum_{i=1}^{n} \boldsymbol{X}_i}_{} \longrightarrow \mathcal{N}(\mu, \sigma^2)$$



Sum of real-valued r.v.'s,
none too dominant

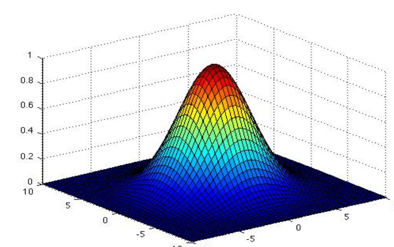


Intersection of *m*
regular halfspaces

[Harsha, Klivans, Meka 10]

## [HKM10] **multidimensional** CLT

$$\underbrace{\sum_{i=1}^{n} \vec{\boldsymbol{X}}_i}_{} \longrightarrow \mathcal{N}(\vec{\mu}, \Sigma)$$



Sum of $\mathsf{R}^m$-valued r.v.'s,
none too dominant

convergence in
multidimensional CDF distance

# HKM's PRG via their multidimensional CLT

Let *A* be an *m* x *n* matrix, where every row of *A* is regular

(row = weights of a regular halfspace)

Uniform $\boldsymbol{x} \sim \{-1,1\}^n$

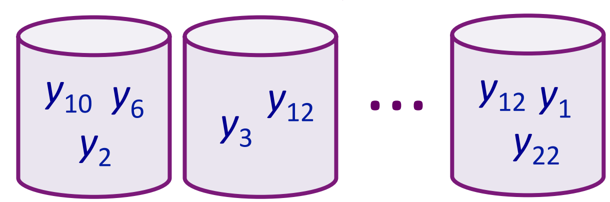
*Pseudorandom* $\boldsymbol{y} \sim \{-1,1\}^n$

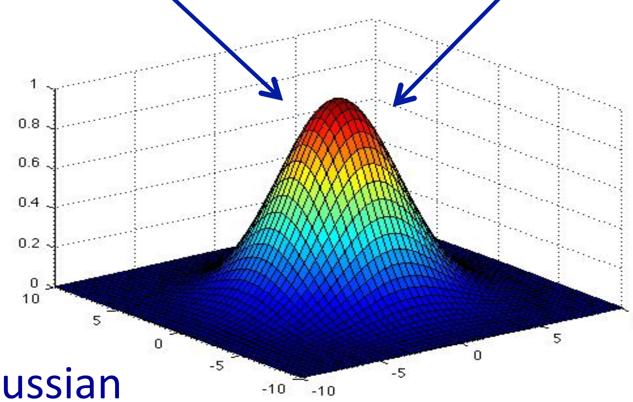
$A\boldsymbol{x}$ $\longleftrightarrow$ $A\boldsymbol{y}$

CDF-close by Δ-inequality

CDF-close

CDF-close

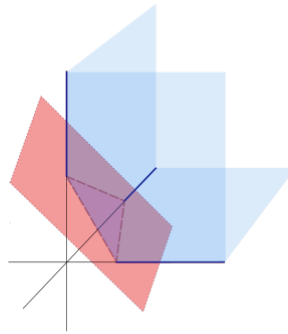



*m*-dimensional Gaussian

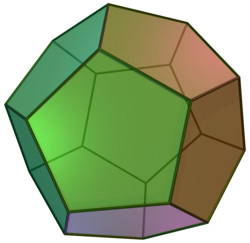
PRGs via Central Limit Theorems

Part I: ✓



Regular halfspaces

[Meka, Zuckerman 09]

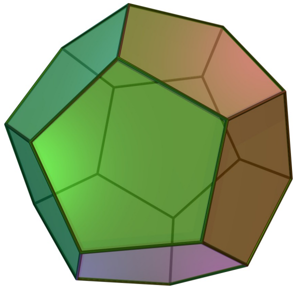


Intersections of regular halfspaces

[Harsha, Klivans, Meka 10]

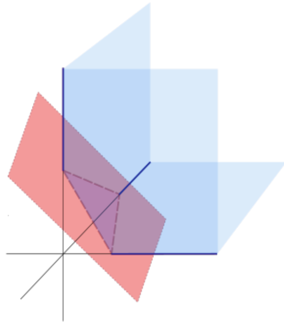
Part II:

(Our work)

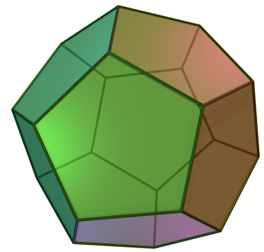


Intersections of **general** halfspaces

**Part I:**

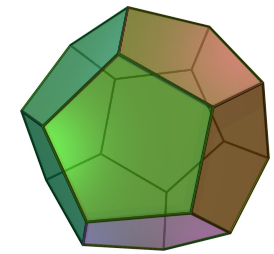


Regular halfspaces



Intersections of *m* regular halfspaces

**Part II:**



Intersections of *m* general halfspaces

## Other relevant works not discussed in Part I:

- 1 general halfspace [Meka, Zuckerman 09]
- **Any function** of *m* general halfspaces, but seed length $\tilde{O}(m)$ [Gopalan, O'Donnell, Wu, Zuckerman 10]
- Intersection of *m* **low-weight** halfspaces, seed length polylog($m$) [Servedio, T. 17]

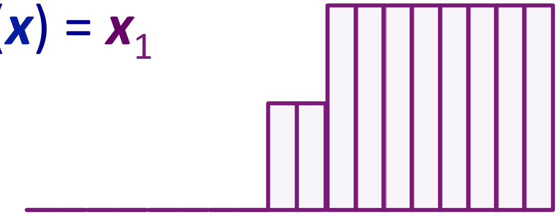
# Main challenge:
# CLTs and **regularity** go hand in hand

<u>Central Limit Theorem **false** without regularity assumption</u>

$$S(\boldsymbol{x}) = w_1 \boldsymbol{x}_1 + \cdots + w_n \boldsymbol{x}_n \not\longrightarrow \mathcal{N}(\mu, \sigma^2)$$

if there are dominant $w_i$'s

Recall simple example: $S(\boldsymbol{x}) = \boldsymbol{x}_1$



Not close to CDF of any Gaussian

# This work: bypassing Gaussian middleperson (by necessity)

Let *A* be **general** *m* x *n* matrix

(row = weights of **general** halfspace, not necessarily regular)

Uniform $\boldsymbol{x} \sim \{-1,1\}^n$

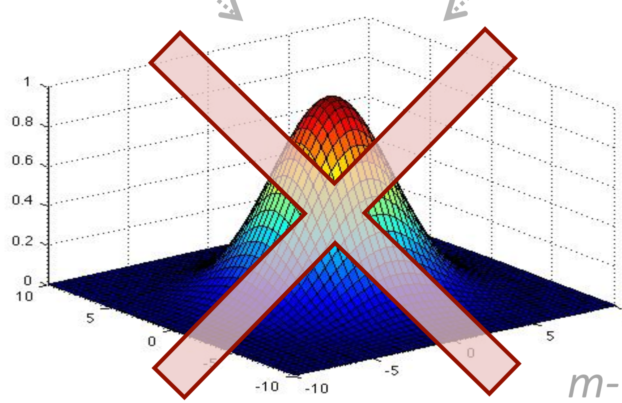
Pseudorandom $\boldsymbol{y} \sim \{-1,1\}^n$

$$A\boldsymbol{x} \longleftrightarrow A\boldsymbol{y}$$

CDF-close?

**Not** CDF-close

**Not** CDF-close




*m*-dimensional Gaussian

# But—will still employ CLT proof techniques

## (even though CLT does not hold!)

$$A\boldsymbol{x} \xleftrightarrow{\text{CDF-close!}} A\boldsymbol{y}$$

Uniform $\boldsymbol{x} \sim \{-1,1\}^n$ Pseudorandom $\boldsymbol{y} \sim \{-1,1\}^n$

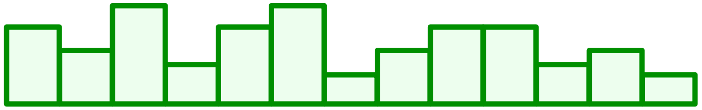
- Lindeberg replacement method
  - Powerful technique for proving CLTs [Lindeberg 22]
  - [MZ, HKM]'s strategy for the all-regular case
- Non-regularity necessitates new ideas and ingredients:
  - PRGs for CNF formulas [AW85, Nis92, Baz07, ... ]
  - New Littlewood–Offord theorem for polytopes

## Outline of the rest of the talk
## (= the structure of our proof)

1. A useful decomposition of polytopes
2. “Smooth version” of the problem
3. Proving the smooth version
4. Going from smooth version to actual version

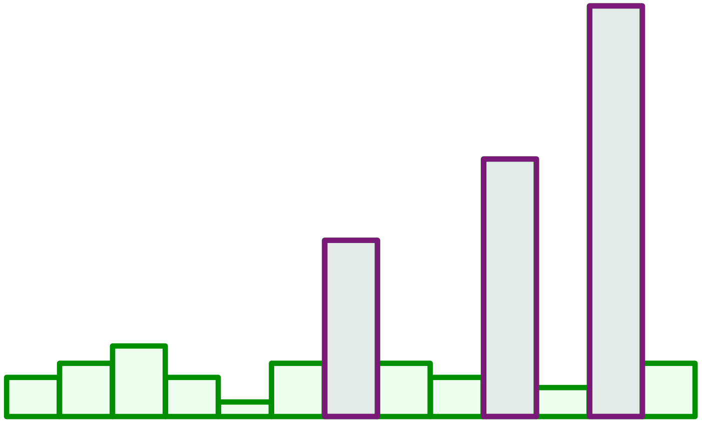
# Regularity lemma for a single halfspace

Weights of **regular** halfspace:



(No weight too dominant)

Weights of **general** halfspace:

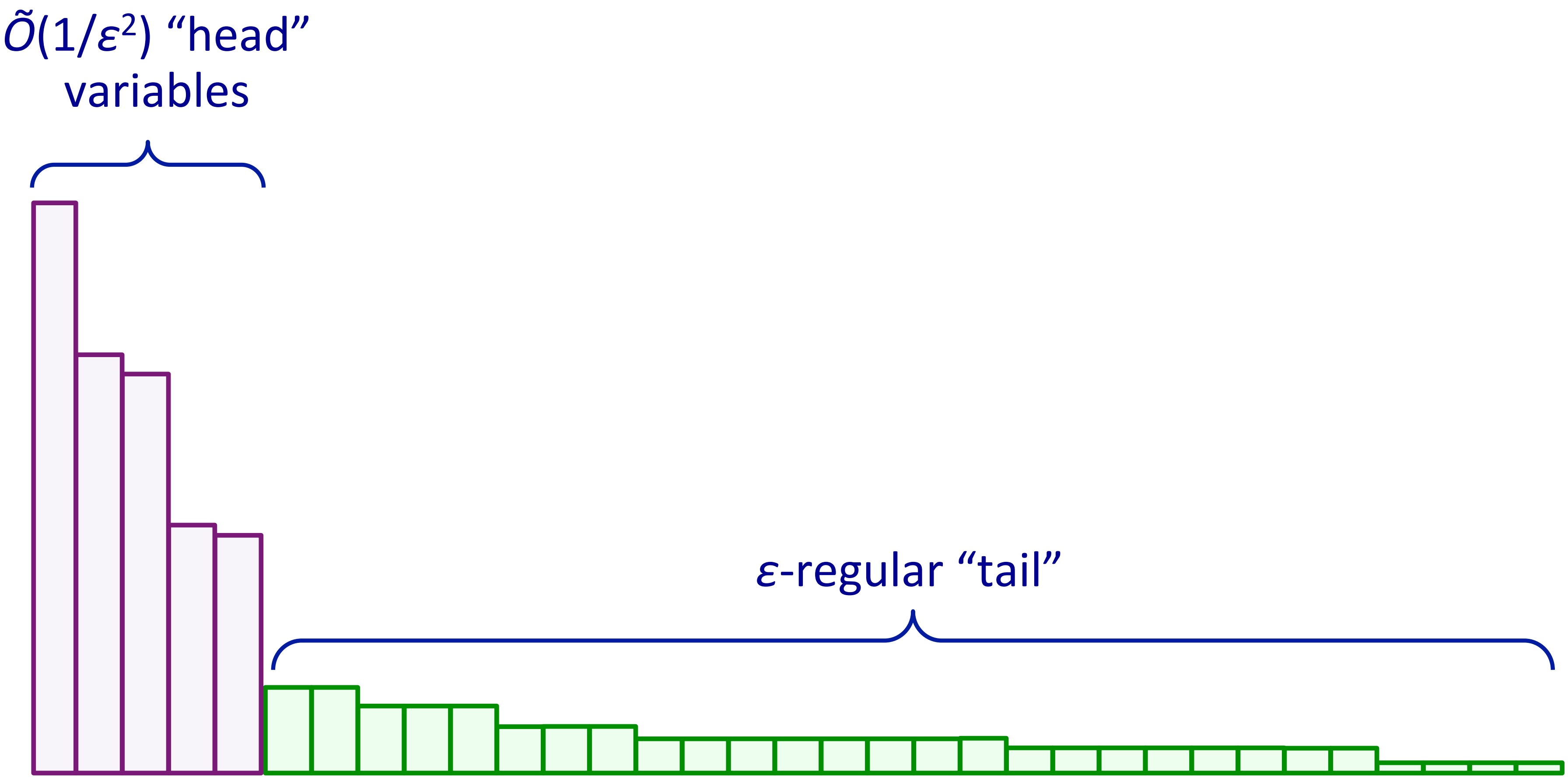


**Halfspace Regularity Lemma**
[Servedio 07]

Every halfspace can be made regular* by restricting a small number of variables

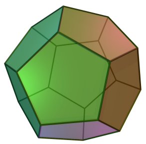
*or very close to constant

# Halfspace Regularity Lemma as a picture




Weights of a general halfspace sorted by magnitude

# Applying the regularity lemma to *m* halfspaces

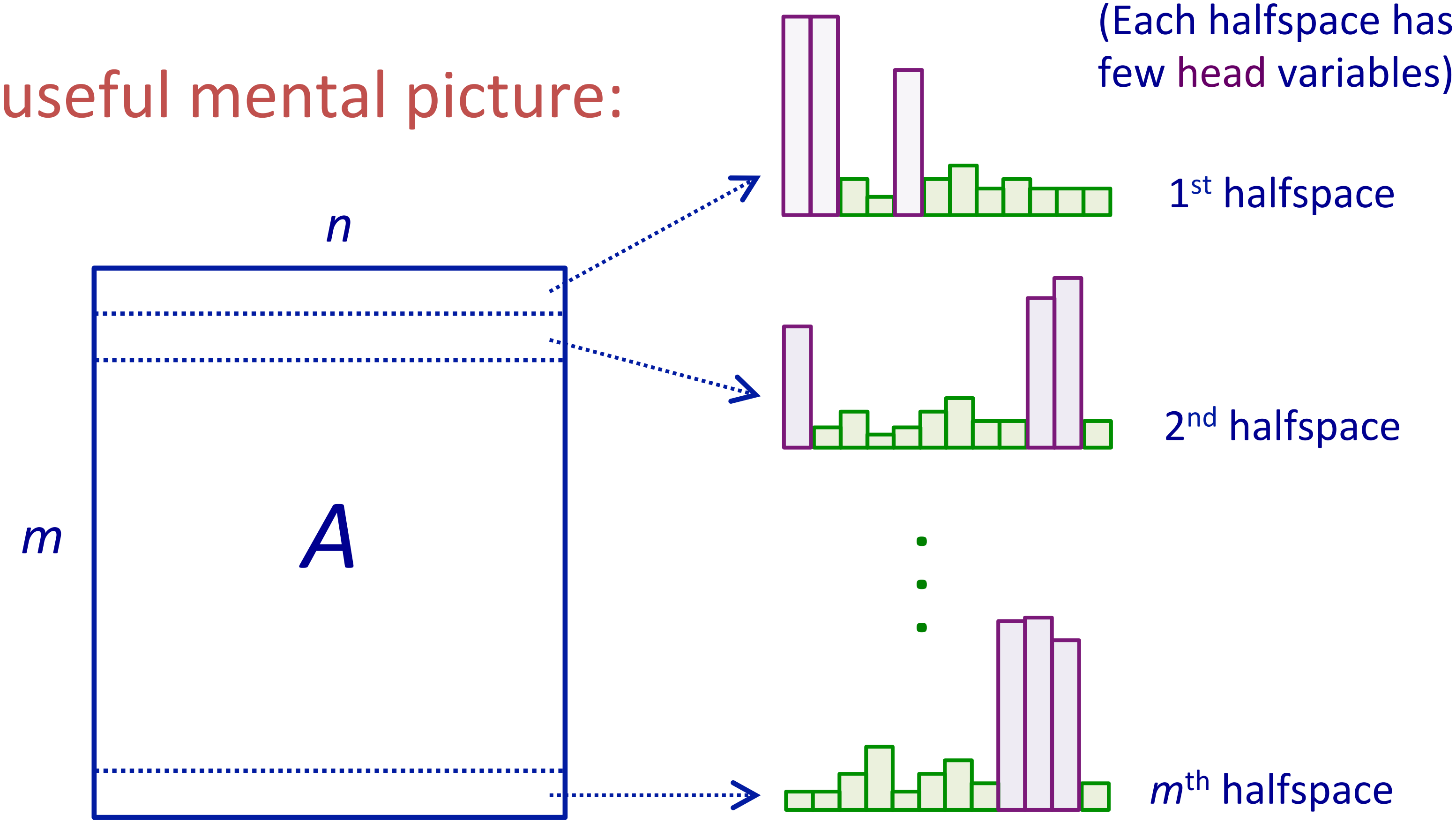


1st halfspace   2nd halfspace   . . .   ($m$-1)st halfspace   $m$th halfspace

Remark:

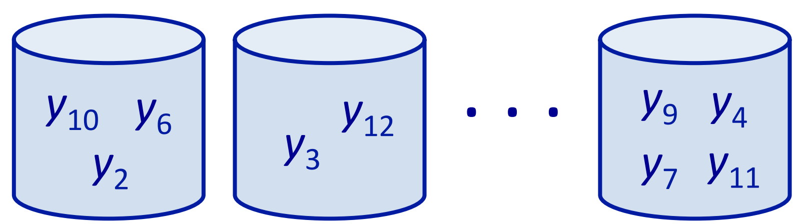
- Each head small, but union of all $m$ heads could cover $[n]$
- So the natural strategy of reducing to the all-regular case – by "restricting away" all head variables – does not work

# A useful mental picture:




**Goal:** $Ax$ and $Ay$ are close in multidimensional CDF distance

- $\boldsymbol{x} \sim \{-1,1\}^n$ uniform
- $\boldsymbol{y} \sim \{-1,1\}^n$ pseudorandom:



# Outline of the rest of the talk
# (= the structure of our proof)

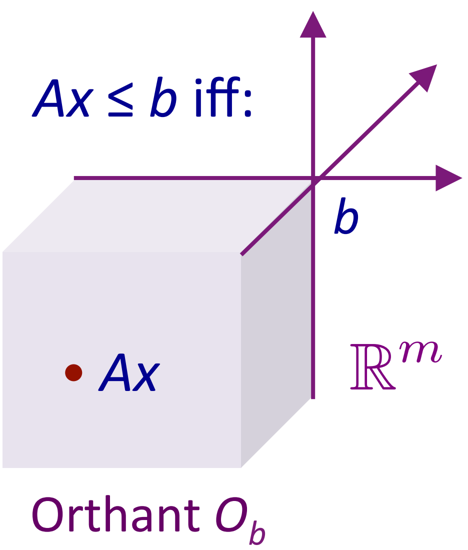
1. A useful decomposition of polytopes
2. **"Smooth version" of the problem**
3. Proving the smooth version
4. Going from smooth version to actual version

# A smooth version of CDF distance

$$\begin{aligned} & A\boldsymbol{x} \text{ and } A\boldsymbol{y} \text{ are CDF-close} \\ \iff & \Pr[A\boldsymbol{x} \le b] \approx \Pr[A\boldsymbol{y} \le b] \quad \text{for all } b \in \mathbb{R}^m \\ \iff & \mathbb{E}[\mathcal{O}_b(A\boldsymbol{x})] \approx \mathbb{E}[\mathcal{O}_b(A\boldsymbol{y})] \quad \text{for all } b \in \mathbb{R}^m \end{aligned}$$

$O_b$ = {0,1}-indictor of orthant defined by $b$

Discontinuous function!




We will first show:

$$\mathbb{E}[\widetilde{\mathcal{O}}_b(A\boldsymbol{x})] \approx \mathbb{E}[\widetilde{\mathcal{O}}_b(A\boldsymbol{y})]$$

where

$$\widetilde{\mathcal{O}}_b : \mathbb{R}^m \to [0,1]$$

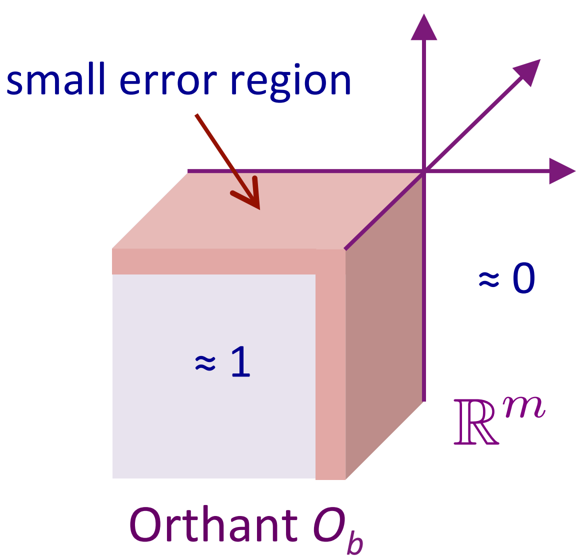
is **smooth approximator** of $\mathcal{O}_b : \mathbb{R}^m \to \{0,1\}$

"mollifier"

# Smooth approximators of orthants

Standard way of mollifying a function: adding Gaussian noise

$$\widetilde{\mathcal{O}}_b(v) = \mathop{\mathbb{E}}_{\boldsymbol{G}\sim\mathcal{N}(0,1)^m}\left[\mathcal{O}_b(v+\lambda\boldsymbol{G})\right]$$




Two important properties of $\tilde{O}_b$ [Bentkus 90]:

1. Good approximation of $O_b$
2. Small derivatives: for all $c > 1$,

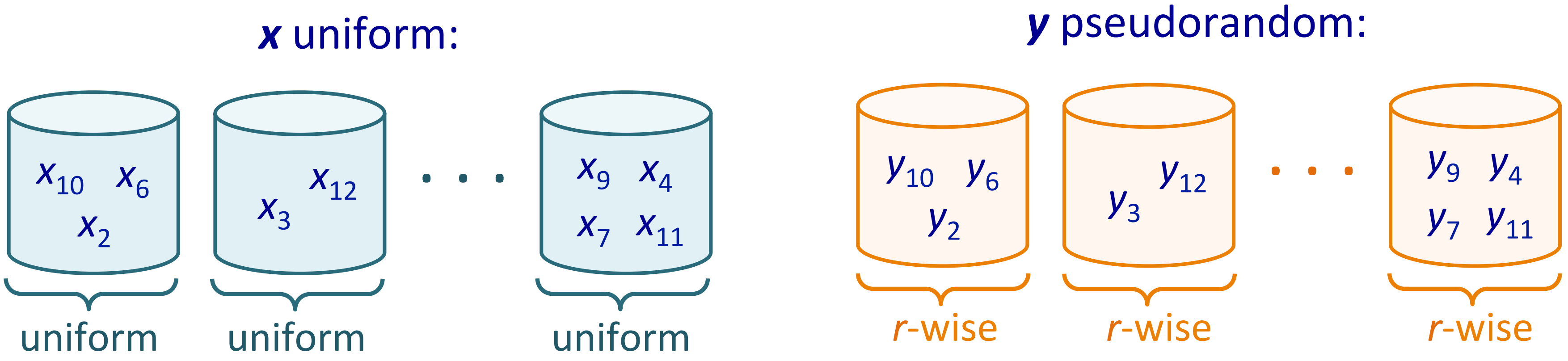
$$\sup_{v\in\mathbb{R}^m}\left\{\underbrace{\sum_{|\alpha|=c}}_{m^c \text{ many partial derivatives}} \left|\partial_\alpha \widetilde{\mathcal{O}}_b(v)\right|\right\} \lesssim \frac{(\log m)^{c/2}}{\lambda^c}$$

# Outline of the rest of the talk
# (= the structure of our proof)

1. A useful decomposition of polytopes
2. "Smooth version" of the problem
3. **Proving the smooth version**
4. Going from smooth version to actual version

# Proving the smooth version via a **hybrid argument**

Goal is to "fool" the orthant mollifier: $\mathop{\mathbb{E}}_{\boldsymbol{x}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{y})]$




Bucket-wise hybrid argument [MZ, HKM]:

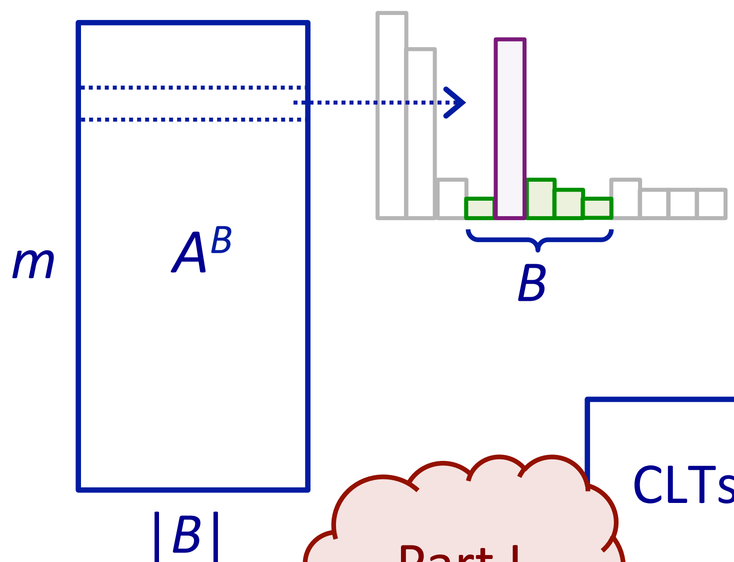
- Start will all buckets filled in uniformly (i.e. start with ***x***)
- Bucket by bucket, "swap out" uniform bits for *r*-wise independent bits
- Argue that each swap incurs small error

# **Single swap** in the hybrid argument

Fix bucket $B \subseteq [n]$ of variables. Let $A^B$ = $A$ restricted to columns in $B$.

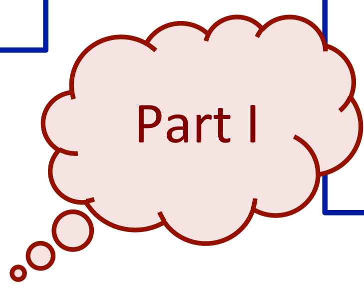
Want to show: $\displaystyle \mathop{\mathbb{E}}_{\boldsymbol{x}}[\widetilde{\mathcal{O}}_b(A^B\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\widetilde{\mathcal{O}}_b(A^B\boldsymbol{y})]$

$$\iff \mathop{\mathbb{E}}_{\boldsymbol{x}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{x}+T\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{y}+T\boldsymbol{y})]$$




Write $A^B$ = $H$ + $T$, where:

- $H$ contains only the head variables
- $T$ contains only the tail variables



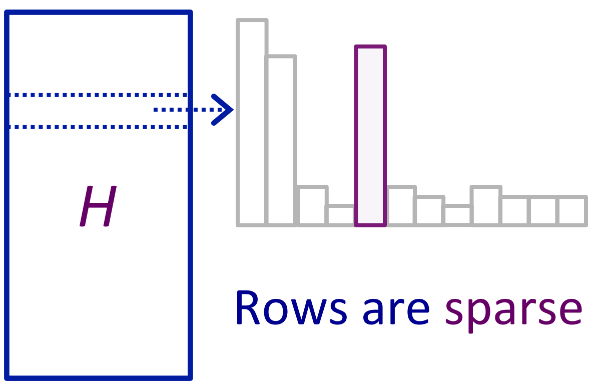

CLTs (e.g. [HKM]) deal with regular linear forms;

Presence of $H$ = our main challenge

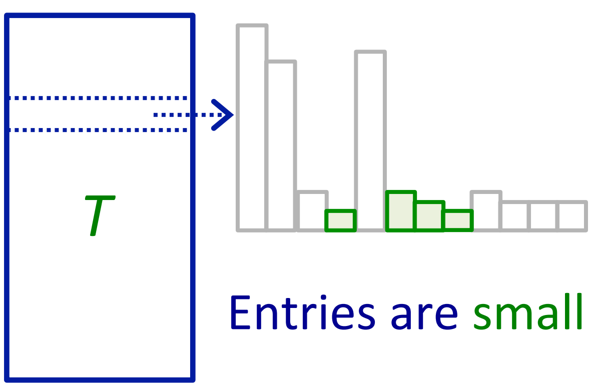
# Multidimensional Taylor expansion

**Claim:** $\underset{\boldsymbol{x}}{\mathbb{E}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{x}+T\boldsymbol{x})] \approx \underset{\boldsymbol{y}}{\mathbb{E}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{y}+T\boldsymbol{y})]$

Equivalently, ***y*** fools the function $z \mapsto \widetilde{\mathcal{O}}_b(Hz + Tz)$




Rows are sparse




Entries are small

Multidimensional Taylor expansion:

$$\widetilde{\mathcal{O}}_b(Hz) + \sum_{|\alpha|=1}^{c-1} \frac{1}{\alpha!} \partial_\alpha \widetilde{\mathcal{O}}_b(Hz)(Tz)^\alpha \pm \mathrm{err}$$

**Warmup:** Does ***y*** fool the *zeroth*-order term?

$$\underset{\boldsymbol{x}}{\mathbb{E}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{x})] \approx \underset{\boldsymbol{y}}{\mathbb{E}}[\widetilde{\mathcal{O}}_b(H\boldsymbol{y})]$$

(Observation: trivial when *H* = 0)

# Warmup: fooling the zeroth-order term

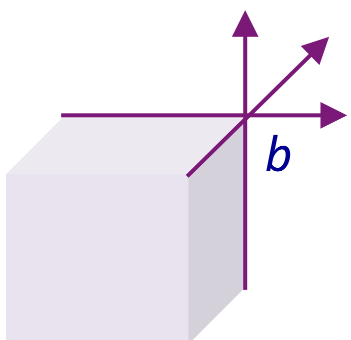
**Claim:** ***y*** fools the function $z \mapsto \widetilde{\mathcal{O}}_b(Hz)$

Recalling the definition of $\tilde{O}_b$,

$$\widetilde{\mathcal{O}}_b(Hz) = \mathop{\mathbb{E}}_{\boldsymbol{G}}[\underbrace{\mathcal{O}_b(Hz+\lambda \boldsymbol{G})}]$$

$$= \prod_{i=1}^{m} \mathbf{1}[(Hz+\lambda\boldsymbol{G})_i \le b_i]$$


Rows are sparse




Orthant $O_b$

Product structure of $\tilde{O}_b$ + Sparsity of *H*

$\Downarrow$

Suffices for ***y*** to fool small-width CNFs

Simple but key idea: product of *k*-juntas = width-*k* CNF

# Back to the Taylor expansion

**Claim:** ***y*** fools the function $z \mapsto \widetilde{\mathcal{O}}_b(Hz + Tz)$

We consider the multidimensional Taylor expansion:

$$\widetilde{\mathcal{O}}_b(Hz) + \underbrace{\sum_{1 \le |\alpha| \le c} \frac{1}{\alpha!} \partial_\alpha \widetilde{\mathcal{O}}_b(Hz)(Tz)^\alpha}_{} \pm \mathrm{err}$$

Previous slide

More complicated, but same key ideas:

- Product structure of $\partial_\alpha \widetilde{O}_b$
- Sparsity of *H*

$\Longrightarrow$ Suffices for ***y*** to fool CNFs

---

To bound error term, use fact that $\tilde{O}_b$ has small derivatives (same as [HKM]):

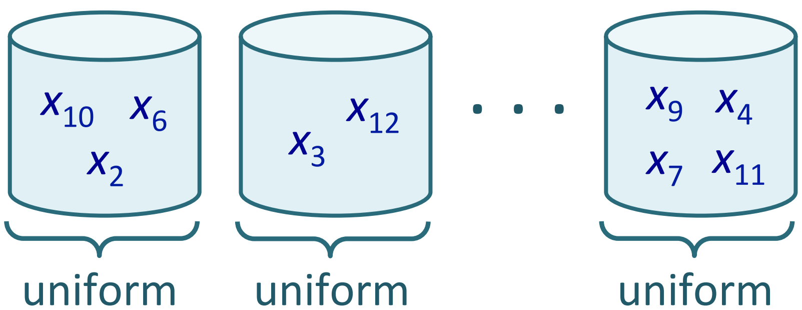
$$\sup_{v \in \mathbb{R}^m} \left\{ \sum_{|\alpha| = c} \left| \partial_\alpha \widetilde{\mathcal{O}}_b(v) \right| \right\} \lesssim \frac{(\log m)^{c/2}}{\lambda^c}$$

[Bentkus 90]

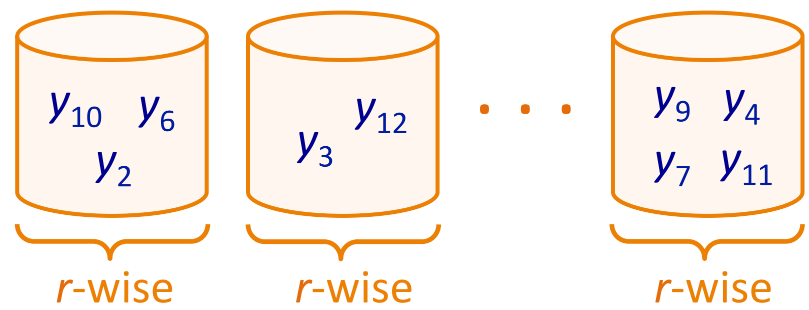
# Recap

Goal is to "fool" the orthant mollifier: $\mathop{\mathbb{E}}_{\boldsymbol{x}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{y})]$

***x*** uniform:

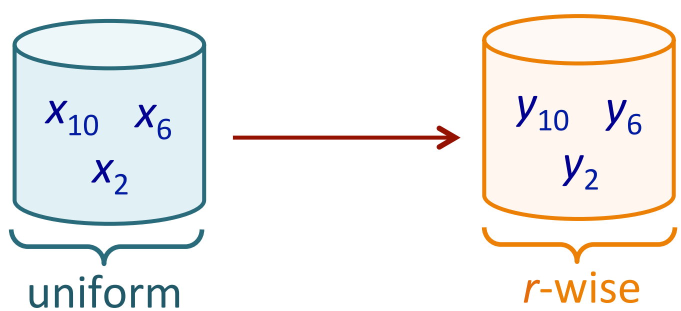



***y*** pseudorandom:




<u>What we just sketched</u>

Bounding error incurred by a single swap:

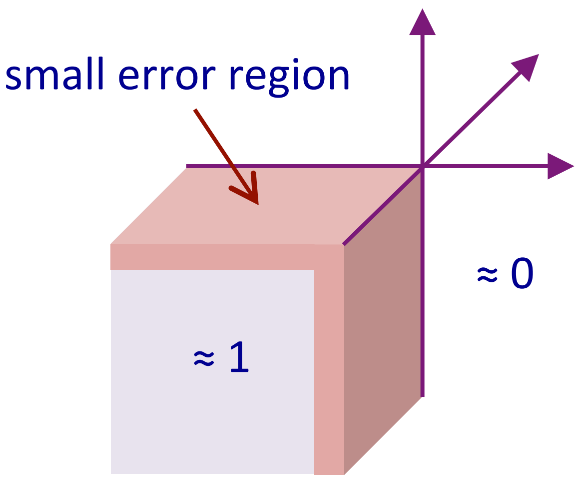


# Outline of the rest of the talk
# (= the structure of our proof)

1. A useful decomposition of polytopes
2. "Smooth version" of the problem
3. Proving the smooth version
4. **Going from smooth version to actual version**

## What we've shown:

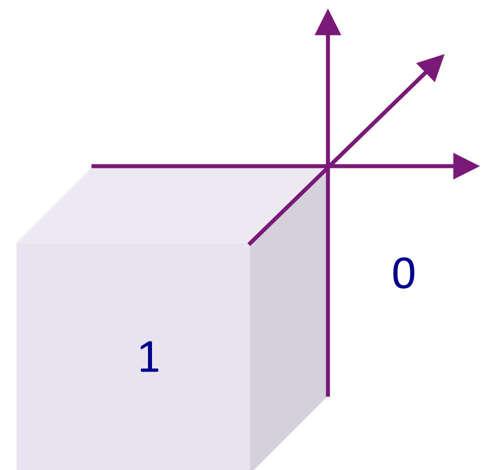
$$\mathop{\mathbb{E}}_{\boldsymbol{x}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\widetilde{\mathcal{O}}_b(A\boldsymbol{y})]$$




$$\widetilde{\mathcal{O}}_b : \mathbb{R}^m \to [0,1]$$

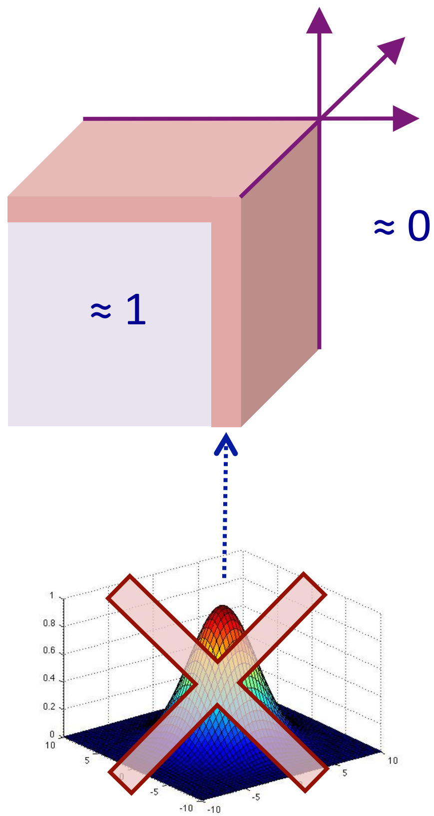
## What we'd like to show:
## (closeness in CDF distance)

$$\mathop{\mathbb{E}}_{\boldsymbol{x}}[\mathcal{O}_b(A\boldsymbol{x})] \approx \mathop{\mathbb{E}}_{\boldsymbol{y}}[\mathcal{O}_b(A\boldsymbol{y})]$$




$$\mathcal{O}_b : \mathbb{R}^m \to \{0,1\}$$

# Another conceptual difference/challenge: Boolean vs. Gaussian anticoncentration




Proofs of CLTs (e.g. [HKM]):
Gaussian anticoncentration
$\boldsymbol{A G}, \quad \boldsymbol{G} \sim N(0,1)^n$

Since we are bypassing Gaussians:

Have to instead reason about **Boolean** anticoncentration

(Fact: Boolean anticoncentration

$$\Downarrow$$

Gaussian anticoncentration)

# Littlewood–Offord anticoncentration inequality

Let $w \in \mathbb{R}^n$ where $|w_i| \geq 1$ for all $i$.
For all open intervals $I \subset \mathbb{R}$ of radius 2,

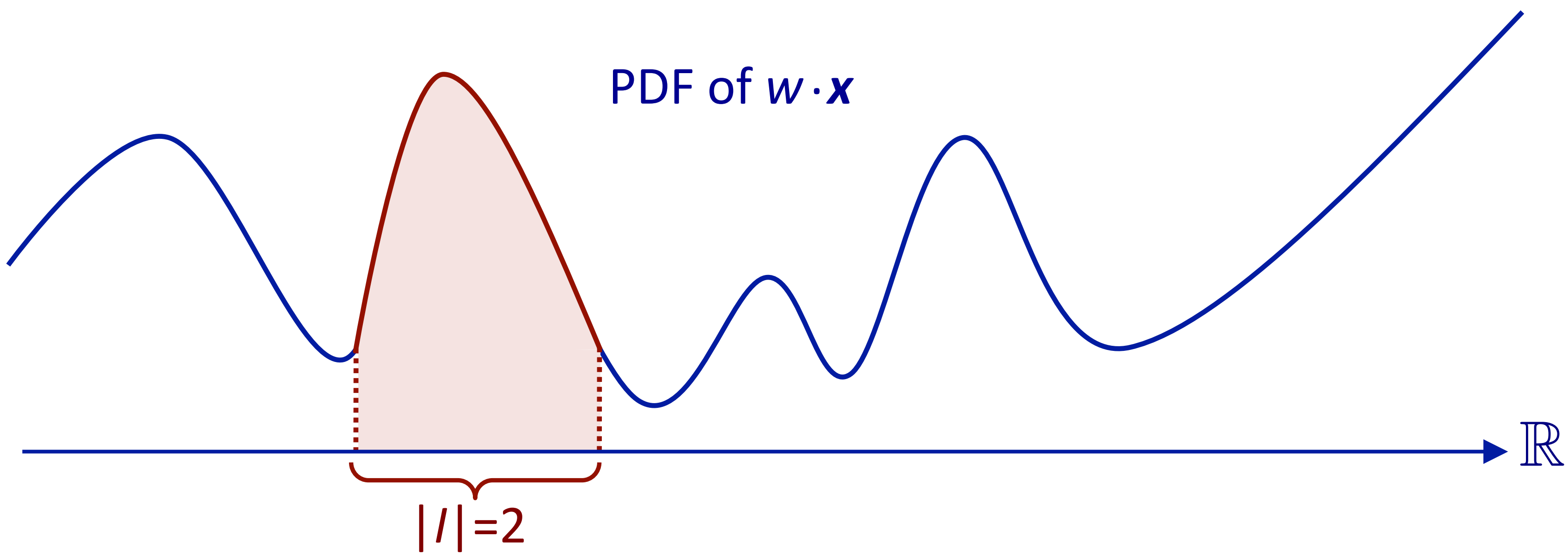
$$\Pr_{\boldsymbol{x}\sim\{\pm 1\}^n}[\, w \cdot \boldsymbol{x} \in I \,] \lesssim \frac{1}{\sqrt{n}}.$$

In fact:

$$\leq \binom{n}{\lfloor n/2 \rfloor} \cdot 2^{-n}$$

[Erdős 45]

(Exactly tight for $w = 1^n$)

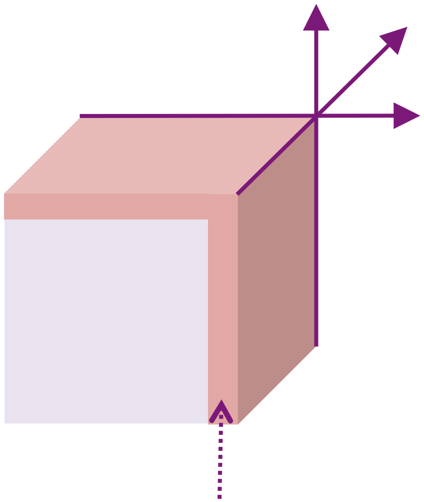


# A **high-dimensional** Littlewood–Offord inequality

## (LO: *m*=1 case)

Let $A \in \mathbb{R}^{m \times n}$ where $|A_{ij}| \geq 1$ for all $i, j$.
For all orthant boundaries $B \subset \mathbb{R}^m$ of width 2,

$$\Pr_{\boldsymbol{x} \sim \{\pm 1\}^n} [\, A\boldsymbol{x} \in B \,] \lesssim \; ?$$



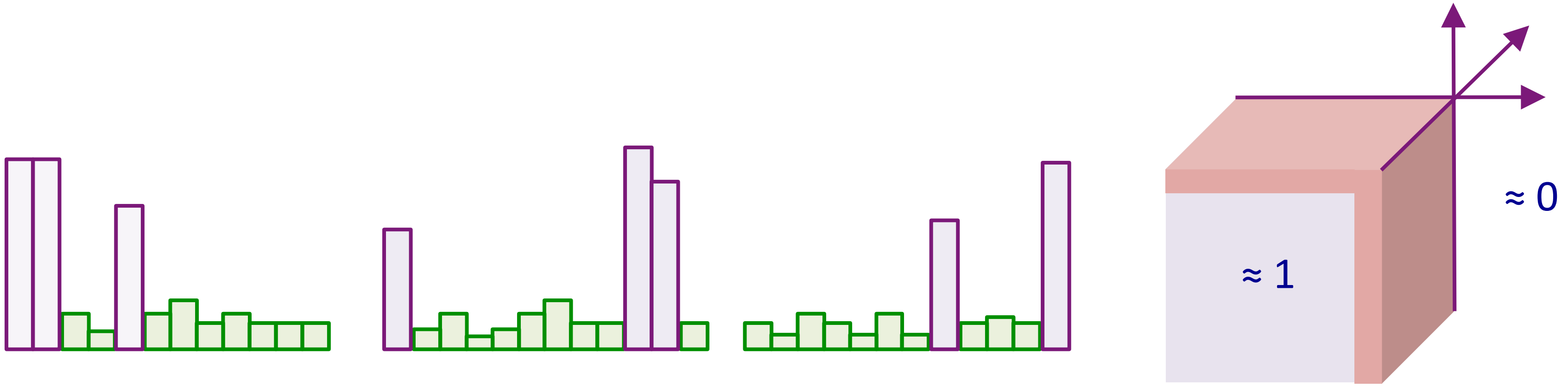
{ *x* : *Ax* ≤ *b* } \ { *x* : *Ax* ≤ *b*−$\vec{2}$ }

- 1-dimensional LO + union bound: $O(m/\sqrt{n})$
- We prove $O(\sqrt{\log m}/\sqrt{n})$, which we show is tight
- Need various technical extensions for our purposes

**Chalk talk tomorrow!**

# Recap of proof structure

1. A useful decomposition of polytopes
2. “Smooth version” of the problem
3. Proving the smooth version
4. Going from smooth version to actual version



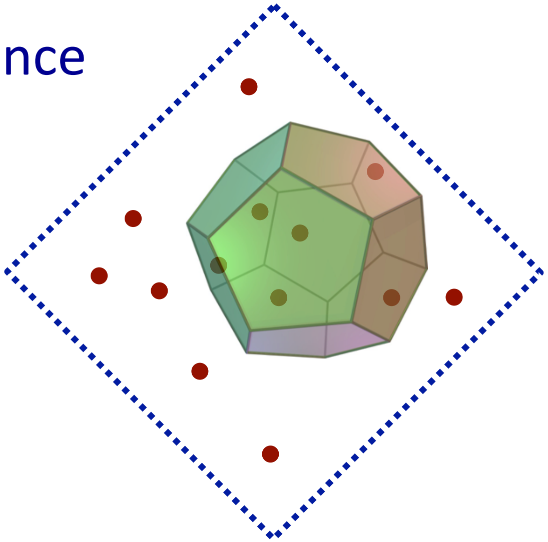
# Summary

**Our main result**

An $\varepsilon$-PRG for $m$-facet polytopes over $\{0,1\}^n$ with seed length:

$$\text{poly}(\log m, 1/\varepsilon) \cdot \log n$$

- Previous best seed length had linear dependence on $m$
- Many interesting future directions:
  - Seed length $\text{poly}(\log m, \log(1/\varepsilon)) \cdot \log n$
  - PRGs for other geometric sets?
    - PRG for all convex sets?



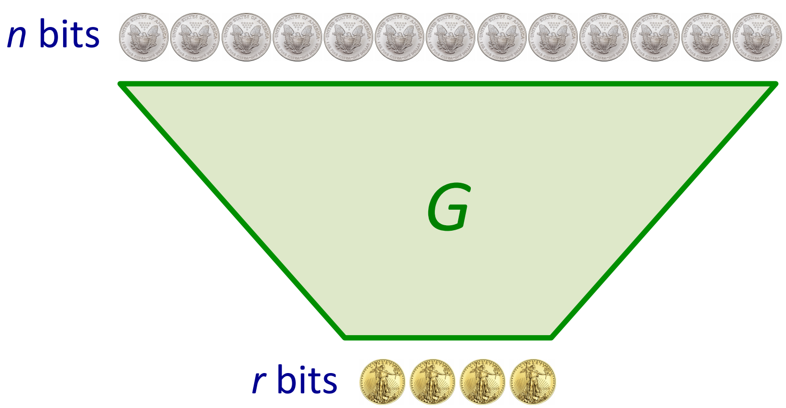
Discrepancy set of size $n^{\text{polylog}(m)}$

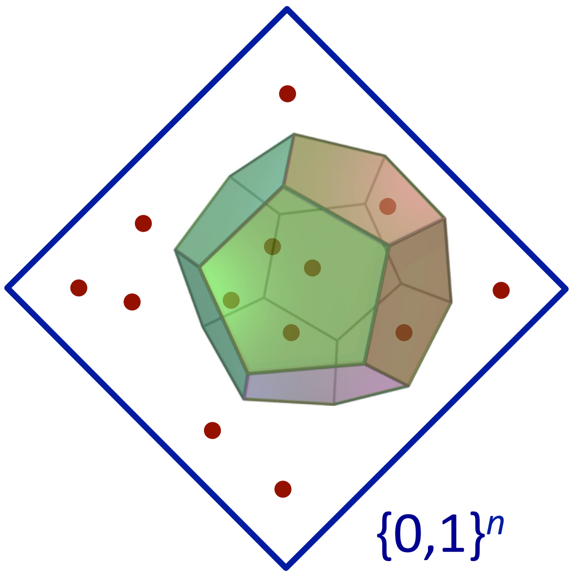
# Thanks!

# Image of PRG = Discrepancy Set

Let $G : \{0,1\}^r \rightarrow \{0,1\}^n$ be an $\varepsilon$-PRG for the class $m$-facet polytopes

Consider $\{ G(s) : s \in \{0,1\}^r \}$ $\longrightarrow$ A set of $2^r$ points ● in $\{0,1\}^n$



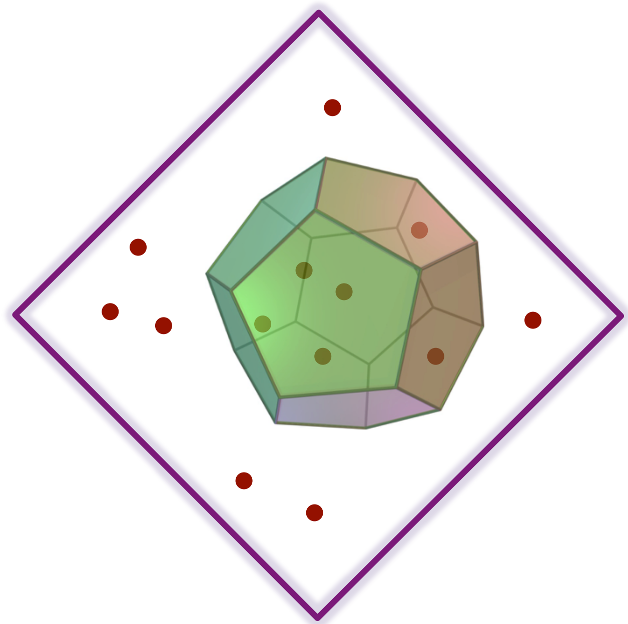




Discrepancy set for the class of $m$-facet polytopes

# Analogous results for other domains

$\{0,1\}^n$

Standard reductions



- Solid cube $[0,1]^n$
- Hypergrid $\{0,1,\ldots,k\}^n$
- Gaussian space ($\mathbb{R}^n$ under $N(0,1)^n$) [HKM10]
- ...

# One algorithmic application:
# Counting # of solutions of {0,1}-integer programs

maximize $c^{\mathrm{T}}x$

subject to $Ax \leq b$

and $x \in \{0,1\}^n$

Given as input a {0,1}-IP with $m$ constraints, there is a deterministic algorithm that runs in time

$$n^{\mathrm{poly}(\log m,\ 1/\varepsilon)}$$

and outputs an estimate of the **fraction of feasible solutions**, accurate to $\pm\ \varepsilon$.

PRG = **input-oblivious** algorithm

Average w.r.t. fixed discrepancy set works for all possible inputs (all possible {0,1}-IPs)