Bounds on the density of nearly uniform lattice coverings

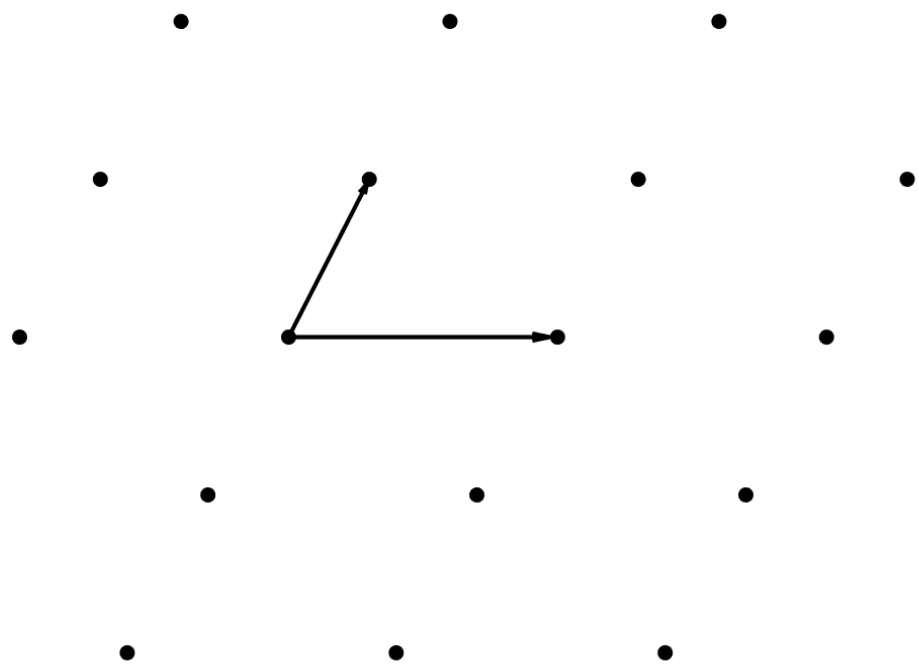
Or Ordentlich (Hebrew University of Jerusalem)
Joint work with Oded Regev (NYU) and Barak Weiss (TAU)

May 20, 2024

Definitions

- A **lattice** $L \subset \mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$
- It can be (non-uniquely) identified with a full-rank **generating matrix** $g = [g_1 | \cdots | g_n] \in \mathbb{R}^{n \times n}$, as

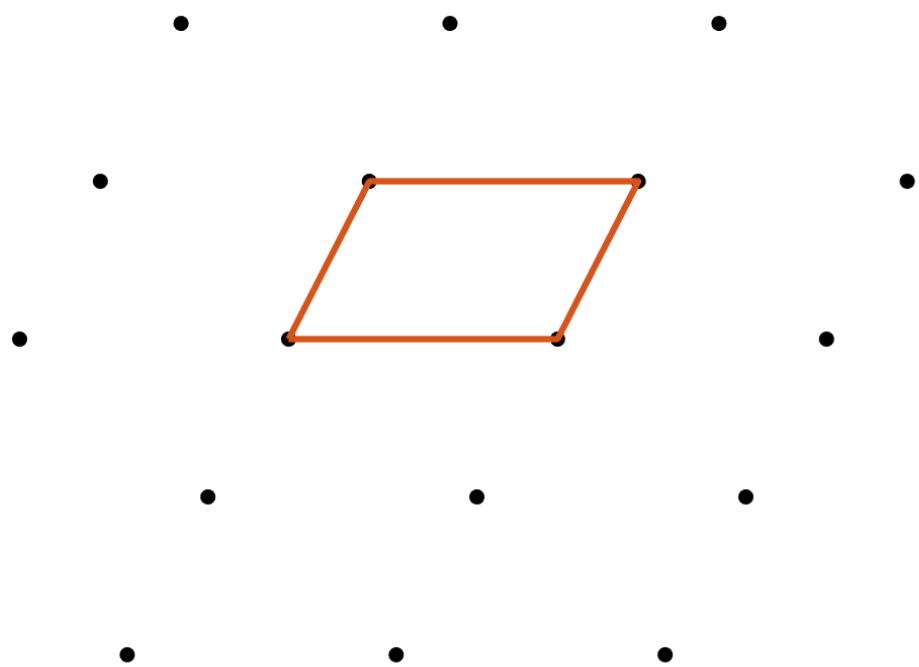
$$L = g\,\mathbb{Z}^n = \mathrm{span}_{\mathbb{Z}}(g_1, \ldots, g_n)$$



Definitions

- A **lattice** $L \subset \mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$
- It can be (non-uniquely) identified with a full-rank **generating matrix** $g = [g_1 | \cdots | g_n] \in \mathbb{R}^{n \times n}$, as

$$L = g\,\mathbb{Z}^n = \mathrm{span}_{\mathbb{Z}}(g_1, \ldots, g_n)$$



- **co-volume** of $L = |\det(g)|$ (volume of fundamental cell)

Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

- Let $\mathcal{B} \subset \mathbb{R}^n$ be a Euclidean ball
- The **covering density** of L is

$$\Theta(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\},$$

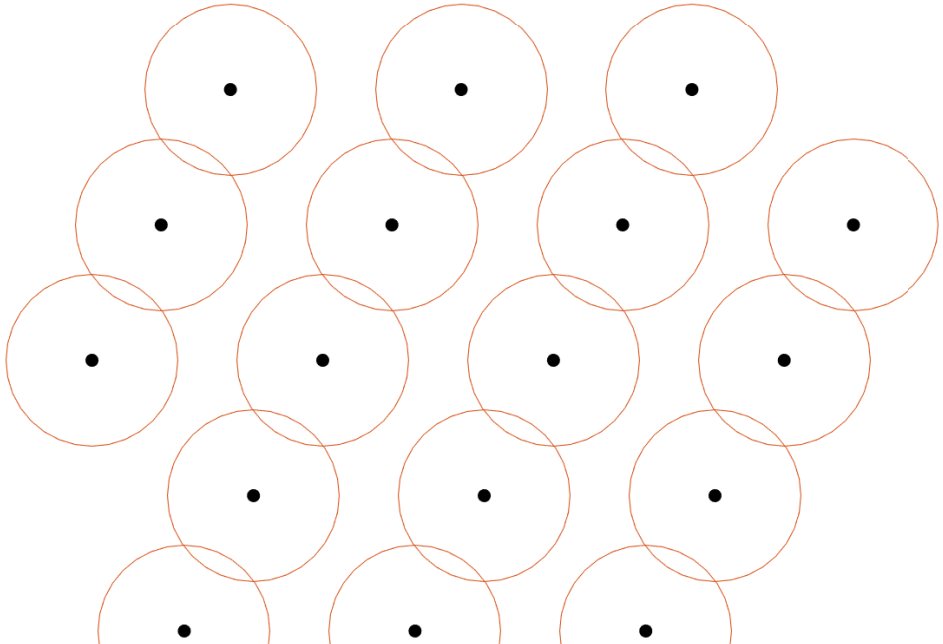
Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

- Let $\mathcal{B} \subset \mathbb{R}^n$ be a Euclidean ball
- The **covering density** of L is

$$\Theta(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\},$$



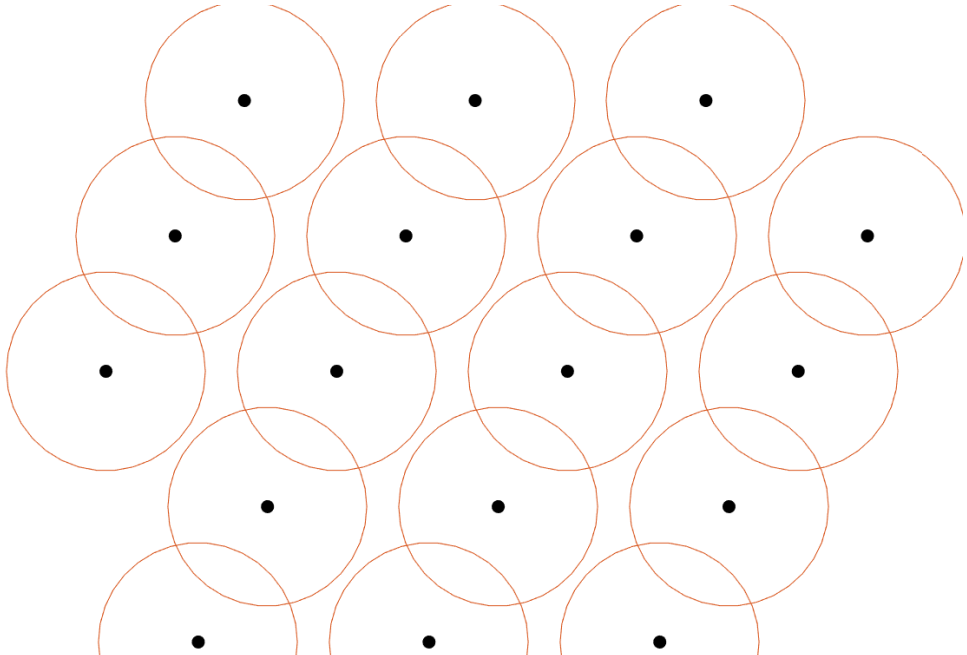
Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

- Let $\mathcal{B} \subset \mathbb{R}^n$ be a Euclidean ball
- The **covering density** of L is

$$\Theta(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\},$$



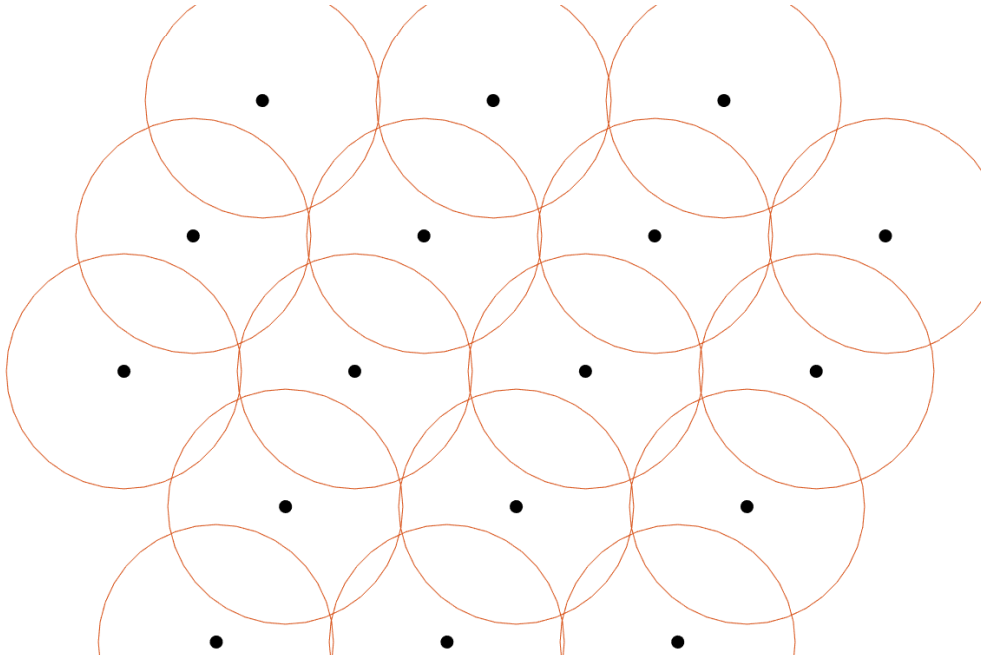
Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

- Let $\mathcal{B} \subset \mathbb{R}^n$ be a Euclidean ball
- The **covering density** of L is

$$\Theta(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\},$$



Definitions

The lattice covering problem:

Find the most "economical" way to cover $\mathbb{R}^n$ with balls around each lattice point

- Let $\mathcal{B} \subset \mathbb{R}^n$ be a Euclidean ball
- The **covering density** of L is

$$\Theta(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\},$$

- $\alpha L + \alpha r\mathcal{B} = \mathbb{R}^n \Leftrightarrow L + r\mathcal{B} = \mathbb{R}^n, \quad \forall \alpha \neq 0$
  $\Rightarrow$ Can assume WLOG that $L \in \mathcal{L}_n \triangleq \{g\,\mathbb{Z}^n \ : \ \det(g) = 1\}$

- The **optimal covering density** is

$$\Theta_n \triangleq \inf_{L \in \mathcal{L}_n} \Theta(L)$$

Definitions

More generally

- Let Conv_n denote the set of compact convex subsets of $\mathbb{R}^n$
- For $\mathcal{K} \in \mathrm{Conv}_n$ we define

$$\Theta_{\mathcal{K}}(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\}$$

and

$$\Theta_{n,\mathcal{K}} \triangleq \inf_{L \in \mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

Definitions

More generally

- Let Conv_n denote the set of compact convex subsets of $\mathbb{R}^n$
- For $\mathcal{K} \in \mathrm{Conv}_n$ we define

$$\Theta_{\mathcal{K}}(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\}$$

and

$$\Theta_{n,\mathcal{K}} \triangleq \inf_{L \in \mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

Note that clearly $\Theta_{n,\mathcal{K}} \geq 1$ for any $\mathcal{K}$

Definitions

More generally

- Let Conv_n denote the set of compact convex subsets of $\mathbb{R}^n$
- For $\mathcal{K} \in \mathrm{Conv}_n$ we define

$$\Theta_{\mathcal{K}}(L) \triangleq \inf \{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\}$$

and

$$\Theta_{n,\mathcal{K}} \triangleq \inf_{L \in \mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

Note that clearly $\Theta_{n,\mathcal{K}} \geq 1$ for any $\mathcal{K}$

- Many applications in EECS: placing cellular basestations ($n = 3$), lossy compression ($n \gg 1$), enforcing power constraint in communication, derivation of upper/lower bounds through covering numbers...

Previous Bounds

$$\Theta(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\right\}, \ \Theta_n \triangleq \inf_{L\in\mathcal{L}_n} \Theta(L)$$

$$\Theta_{\mathcal{K}}(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\right\}, \ \Theta_{n,\mathcal{K}} \triangleq \inf_{L\in\mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

What was known?

Previous Bounds

$$\Theta(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\right\}, \ \Theta_n \triangleq \inf_{L\in\mathcal{L}_n} \Theta(L)$$

$$\Theta_{\mathcal{K}}(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\right\}, \ \Theta_{n,\mathcal{K}} \triangleq \inf_{L\in\mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

What was known?

- **Rogers'59,Coxeter-Few-Rogers'59:** $c_2 n < \Theta_n < n(\log(n))^{c_3}$
- **Gritzmann'85:** If $\mathcal{K} \in \mathrm{Conv}_n$ is "symmetric enough" $\Theta_{n,\mathcal{K}} < n(\log(n))^{c_3}$
- **Rogers'59:** $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < n^{\log_2 \log n + c_1}$

Previous Bounds

$$\Theta(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{B}) \ : \ L + r\mathcal{B} = \mathbb{R}^n\right\}, \ \Theta_n \triangleq \inf_{L\in\mathcal{L}_n} \Theta(L)$$

$$\Theta_{\mathcal{K}}(L) \triangleq \inf\left\{\mathrm{vol}(r\mathcal{K}) \ : \ L + r\mathcal{K} = \mathbb{R}^n\right\}, \ \Theta_{n,\mathcal{K}} \triangleq \inf_{L\in\mathcal{L}_n} \Theta_{\mathcal{K}}(L)$$

What was known?

- **Rogers'59,Coxeter-Few-Rogers'59:** $c_2 n < \Theta_n < n(\log(n))^{c_3}$
- **Gritzmann'85:** If $\mathcal{K} \in \mathrm{Conv}_n$ is "symmetric enough" $\Theta_{n,\mathcal{K}} < n(\log(n))^{c_3}$
- **Rogers'59:** $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < n^{\log_2 \log n + c_1}$

Theorem 1 [O.-Regev-Weiss, JAMS22]

$$\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < cn^2$$

A “Typical” Lattice

What can we say about a typical lattice?

A "Typical" Lattice

What can we say about a typical lattice?
Actually, how should we define a typical lattice?

A "Typical" Lattice

What can we say about a typical lattice?
Actually, how should we define a typical lattice?

Recall:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} : \det(t) = 1\}$
- Any $L \in \mathcal{L}_n$ can be written as $L = g\,\mathbb{Z}^n$ for some $g \in \mathrm{SL}_n(\mathbb{R})$
- But, for any $t \in \mathrm{SL}_n(\mathbb{Z})$ we also have $L = g\,t\,\mathbb{Z}^n$
  $\Longrightarrow \mathcal{L}_n \cong \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$

A "Typical" Lattice

What can we say about a typical lattice?
Actually, how should we define a typical lattice?

Recall:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} \ : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} \ : \det(t) = 1\}$
- Any $L \in \mathcal{L}_n$ can be written as $L = g\,\mathbb{Z}^n$ for some $g \in \mathrm{SL}_n(\mathbb{R})$
- But, for any $t \in \mathrm{SL}_n(\mathbb{Z})$ we also have $L = g\,t\,\mathbb{Z}^n$
  $\Longrightarrow \mathcal{L}_n \cong \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$

A measure μ_n on $\mathcal{L}_n$ is $\mathrm{SL}_n(\mathbb{R})$-invariant if:

$$\mu_n(gE) = \mu_n(E) \ : \forall E \subset \mathcal{L}_n, \forall g \in \mathrm{SL}_n(\mathbb{R})$$

A "Typical" Lattice

What can we say about a typical lattice?
Actually, how should we define a typical lattice?

Recall:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} \ : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} \ : \det(t) = 1\}$
- Any $L \in \mathcal{L}_n$ can be written as $L = g\,\mathbb{Z}^n$ for some $g \in \mathrm{SL}_n(\mathbb{R})$
- But, for any $t \in \mathrm{SL}_n(\mathbb{Z})$ we also have $L = g\,t\,\mathbb{Z}^n$
  $\Longrightarrow \mathcal{L}_n \cong \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$

A measure μ_n on $\mathcal{L}_n$ is $\mathrm{SL}_n(\mathbb{R})$-invariant if:

$$\mu_n(gE) = \mu_n(E) \ : \forall E \subset \mathcal{L}_n, \forall g \in \mathrm{SL}_n(\mathbb{R})$$

There is a unique $\mathrm{SL}_n(\mathbb{R})$-invariant probability measure μ_n on $\mathcal{L}_n$. We call it the Haar-Siegel measure.

Covering Density of a Typical Lattice

For $L \sim \mu_n$ the covering density $\Theta_{\mathcal{K}}(L)$ is a random variable
What can we say about it?

- Easy fact (from [O.-Regev-Weiss, JAMS'22]): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

Covering Density of a Typical Lattice

For $L \sim \mu_n$ the covering density $\Theta_{\mathcal{K}}(L)$ is a random variable
What can we say about it?

- Easy fact (from [O.-Regev-Weiss, JAMS'22]): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

But this doesn't imply that a typical lattice has large $\Theta_{\mathcal{K}}(L)$
What can we say about the tail $\Pr(\Theta_{\mathcal{K}}(L) > M)$?

Covering Density of a Typical Lattice

For $L \sim \mu_n$ the covering density $\Theta_{\mathcal{K}}(L)$ is a random variable
What can we say about it?

- Easy fact (from [O.-Regev-Weiss, JAMS'22]): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

But this doesn't imply that a typical lattice has large $\Theta_{\mathcal{K}}(L)$
What can we say about the tail $\Pr(\Theta_{\mathcal{K}}(L) > M)$?
What was known? **Strömbergsson'12:**

- Easy corollary from Rogers'58: for any $\mathcal{K} \in \mathrm{Conv}_n$ and $1 < V < c_1 n$ we have $\Pr(\Theta_{\mathcal{K}}(L) > 2^n V) < c_2 e^{-V}$
- Improvement: $\Pr(\Theta_{\mathcal{K}}(L) > (1.756\ldots)^n) < c_3 e^{-c_4 n}$

Covering Density of a Typical Lattice

For $L \sim \mu_n$ the covering density $\Theta_{\mathcal{K}}(L)$ is a random variable
What can we say about it?

- Easy fact (from [O.-Regev-Weiss, JAMS'22]): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

But this doesn't imply that a typical lattice has large $\Theta_{\mathcal{K}}(L)$
What can we say about the tail $\Pr(\Theta_{\mathcal{K}}(L) > M)$?
What was known? **Strömbergsson'12:**

- Easy corollary from Rogers'58: for any $\mathcal{K} \in \mathrm{Conv}_n$ and $1 < V < c_1 n$ we have $\Pr(\Theta_{\mathcal{K}}(L) > 2^n V) < c_2 e^{-V}$
- Improvement: $\Pr(\Theta_{\mathcal{K}}(L) > (1.756\ldots)^n) < c_3 e^{-c_4 n}$

Theorem 2 [O.-Regev-Weiss, JAMS'22]

For any $n \in \mathbb{N}$, $\mathcal{K} \in \mathrm{Conv}_n$ and $M \in [n^2, n^3]$ we have

$$\Pr(\Theta_{\mathcal{K}}(L) > M) < c_5 e^{-\frac{c_6 M}{n^2}}$$

Covering Density of a Typical Lattice - Cont.

Theorem 2 [O.-Regev-Weiss, JAMS'22]

For any $n \in \mathbb{N}$, $\mathcal{K} \in \mathrm{Conv}_n$ and $M \in [n^2, n^3]$ we have

$$\Pr\left(\Theta_{\mathcal{K}}(L) > M\right) < c_5 e^{-\frac{c_6 M}{n^2}}$$

Corollaries:

1. $\exists c > 0$ such that $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Pr\left(\Theta_{\mathcal{K}}(L) > cn^2\right) < 1$
   $\Longrightarrow \sup_{\mathcal{K}\in\mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < cn^2$ which is our Theorem 1
2. $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Pr\left(\Theta_{\mathcal{K}}(L) > \omega(n^2)\right) = o(1)$
3. $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Pr\left(\Theta_{\mathcal{K}}(L) > cn^3\right) < c_7 e^{-c_8 n}$
   Improves previous result of Strömbergsson with n^3 instead of $(1.756\ldots)^n$.

Nearly Uniform Covering

Stronger requirement than covering:

All $x \in \mathbb{R}^n$ should be covered roughly the same number of times by $L + r\mathcal{K}$.

Nearly Uniform Covering

Stronger requirement than covering:

All $x \in \mathbb{R}^n$ should be covered roughly the same number of times by $L + r\mathcal{K}$.

- The number of times a point is covered is denoted by

$$N(L, \mathcal{K}, x) \stackrel{\text{def}}{=} |(L - x) \cap \mathcal{K}| = |\{y \in L \ : \ x \in y - \mathcal{K}\}|$$

- "On average" a point is covered $\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)$ times:

$$\mathbb{E}_{X \sim \mathrm{Unif}(\mathbb{R}^n/L)} N(L, r\mathcal{K}, X) = \mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)$$

- Furthermore, for all $x \in \mathbb{R}^n$ we have that

$$\lim_{r \to \infty} \frac{N(L, r\mathcal{K}, x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} = 1$$

Nearly Uniform Covering - Cont.

How large does $\mathrm{vol}(r\mathcal{K})$ have to be for $\frac{N(L,r\mathcal{K},x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} \approx 1$ to hold for all $x \in \mathbb{R}^n$?

Nearly Uniform Covering - Cont.

How large does $\mathrm{vol}(r\mathcal{K})$ have to be for $\frac{N(L,r\mathcal{K},x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} \approx 1$ to hold for all $x \in \mathbb{R}^n$?

Definitions:

- Covering smoothness:

$$\eta(r\mathcal{K}, L) \stackrel{\mathrm{def}}{=} \sup_{x\in\mathbb{R}^n} \left| \frac{N(L, r\mathcal{K}, x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} - 1 \right|$$

Note: $\eta(r\mathcal{K}, L) < 1$ implies that $L + r\mathcal{K} = \mathbb{R}^n$

Nearly Uniform Covering - Cont.

How large does $\mathrm{vol}(r\mathcal{K})$ have to be for $\frac{N(L,r\mathcal{K},x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} \approx 1$ to hold for all $x \in \mathbb{R}^n$?

Definitions:

- Covering smoothness:

$$\eta(r\mathcal{K}, L) \stackrel{\mathrm{def}}{=} \sup_{x\in\mathbb{R}^n} \left| \frac{N(L, r\mathcal{K}, x)}{\mathrm{vol}(r\mathcal{K})/\mathrm{covol}(L)} - 1 \right|$$

- Since $r \mapsto \eta(r\mathcal{K}, L)$ is not monotone, we also define

$$\Phi_{\mathcal{K},L}(\varepsilon) \stackrel{\mathrm{def}}{=} \sup \left\{ \frac{\mathrm{vol}(r\mathcal{K})}{\mathrm{covol}(L)} \ : \ r > 0 \text{ satisfies } \eta(r\mathcal{K}, L) > \varepsilon \right\}.$$

Nearly Uniform Covering: Results for μ_n

Theorem [O.-Regev-Weiss'23]

Let $n > 25$, let $\mathcal{K} \in \mathrm{Conv}_n$, and let $\delta, \varepsilon \in (0,1)$ and assume $\mathrm{vol}(\mathcal{K}) > c_1 \left(\frac{1}{\varepsilon\delta}\right)^{6.5} n^3$. Then, for $L \sim \mu_n$ we have

$$\Pr\left(\eta(\mathcal{K}, L) > \varepsilon\right) < \delta.$$

Nearly Uniform Covering: Results for μ_n

Theorem [O.-Regev-Weiss'23]

Let $n > 25$, let $\mathcal{K} \in \mathrm{Conv}_n$, and let $\delta, \varepsilon \in (0,1)$ and assume $\mathrm{vol}(\mathcal{K}) > c_1 \left(\frac{1}{\varepsilon\delta}\right)^{6.5} n^3$. Then, for $L \sim \mu_n$ we have

$$\Pr\left(\eta(\mathcal{K}, L) > \varepsilon\right) < \delta.$$

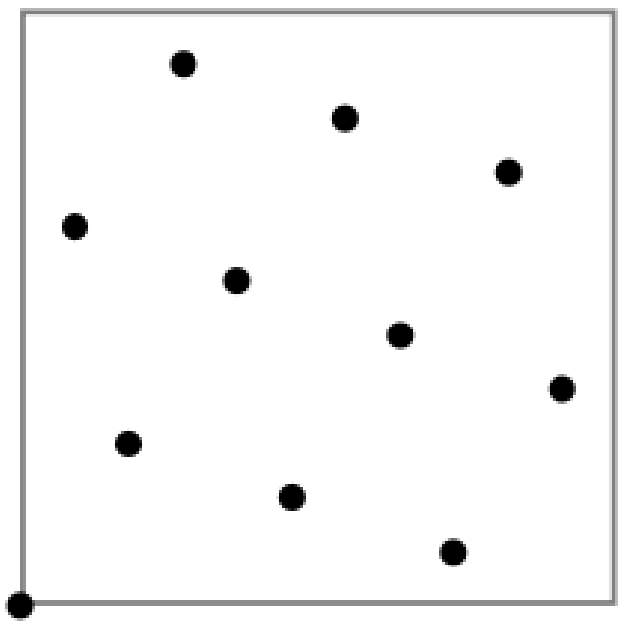
Theorem [O.-Regev-Weiss'23]

Let $n > 25$, let $\mathcal{K} \in \mathrm{Conv}_n$, and let $\delta, \varepsilon \in (0,1)$. Then, for $L \sim \mu_n$ we have

$$\Pr\left(\Phi_{\mathcal{K},L}(\varepsilon) > c_2 \left(\frac{1}{\varepsilon^2\delta}\right)^{6.5} n^3\right) < \delta.$$

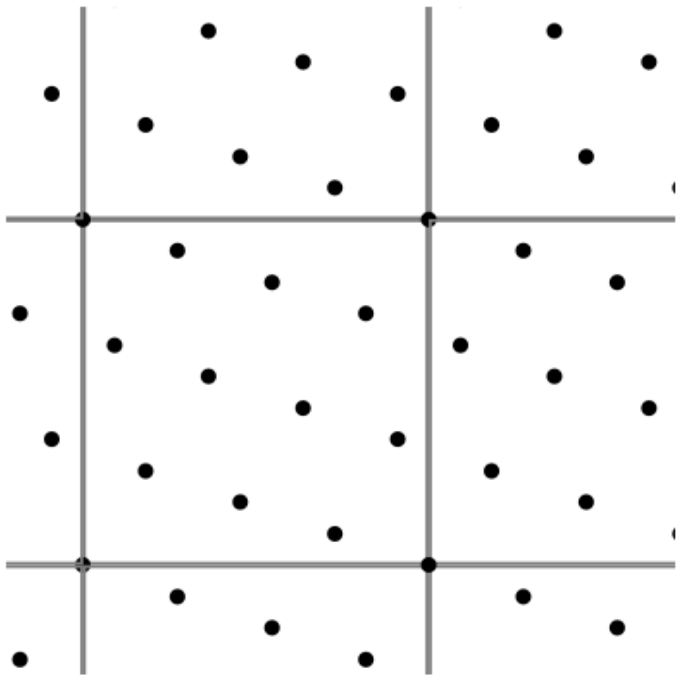
Nearly Uniform Covering: Results for Construction A

- For a prime p denote by $\mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the collection of subspaces of dimension r in $\mathbb{F}_p^n$
- $\pi_p : \mathbb{Z}^n \to \mathbb{F}_p^n$ is the natural mapping, and π_p^{-1} its inverse
- For $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the corresponding construction A lattice is $L = \pi_p^{-1}(S)$



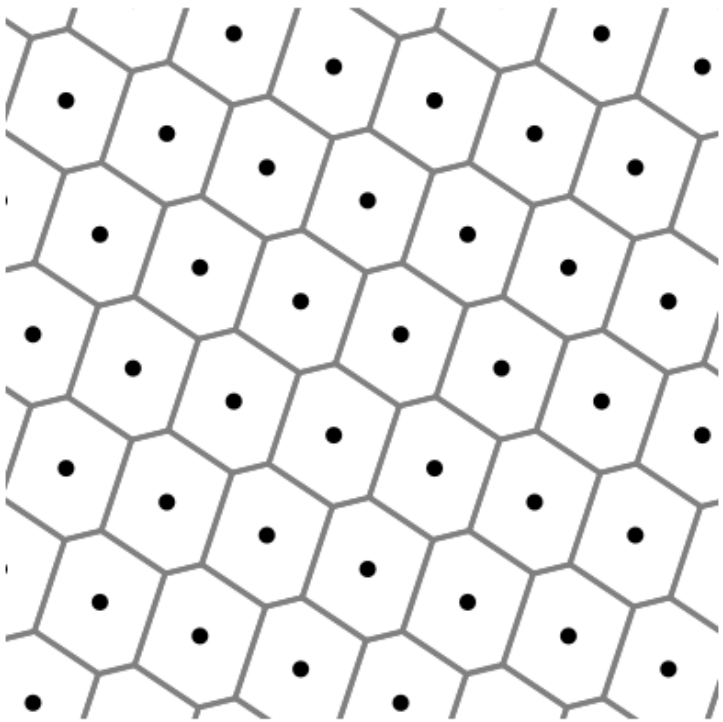
Nearly Uniform Covering: Results for Construction A

- For a prime p denote by $\mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the collection of subspaces of dimension r in $\mathbb{F}_p^n$
- $\pi_p : \mathbb{Z}^n \to \mathbb{F}_p^n$ is the natural mapping, and π_p^{-1} its inverse
- For $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the corresponding construction A lattice is $L = \pi_p^{-1}(S)$



Nearly Uniform Covering: Results for Construction A

- For a prime p denote by $\mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the collection of subspaces of dimension r in $\mathbb{F}_p^n$
- $\pi_p : \mathbb{Z}^n \to \mathbb{F}_p^n$ is the natural mapping, and π_p^{-1} its inverse
- For $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$ the corresponding construction A lattice is $L = \pi_p^{-1}(S)$



Nearly Uniform Covering: Results for Construction A

Theorem [O.-Regev-Weiss'23]

Let $n > 25$, and let $\delta, \varepsilon \in (0,1)$. Let $\mathcal{B}$ be a Euclidean ball with $\mathrm{vol}(\mathcal{B}) \geq c_3 \left(\frac{1}{\varepsilon\delta}\right)^6 n^6$. Let p be a prime number satisfying

$$\frac{1024}{(\varepsilon\delta)^2} n^2 \leq p \leq \frac{2048}{(\varepsilon\delta)^2} n^2,$$

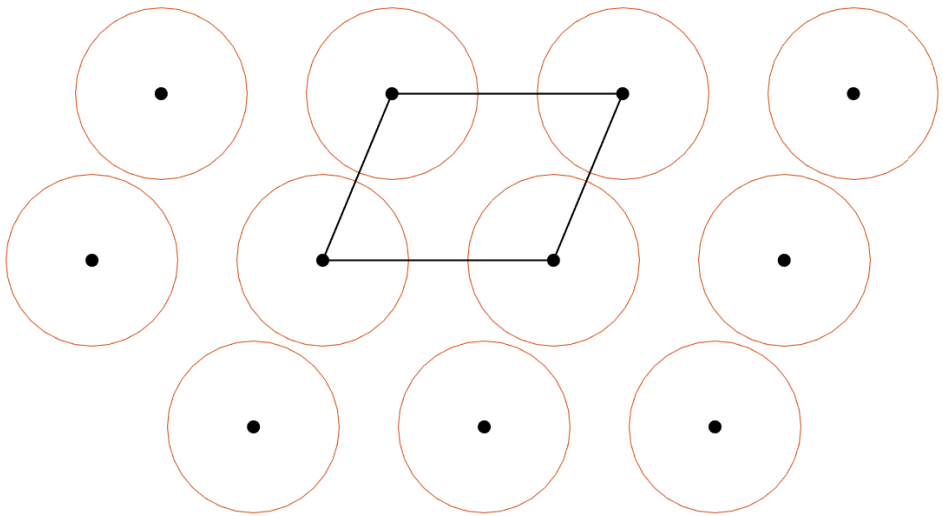
and $r = 3 + \left\lceil \frac{n}{\log p} \left(\frac{1}{2} \log 9n\right) \right\rceil$. Then if L is drawn from the (p, r) random construction A ensemble (so that $\mathrm{covol}(p^{r/n} L) = 1$), we have

$$\Pr\left(\eta(\mathcal{B}, p^{r/n} L) > \varepsilon\right) \leq \delta.$$

Main Thm : Proof Outline

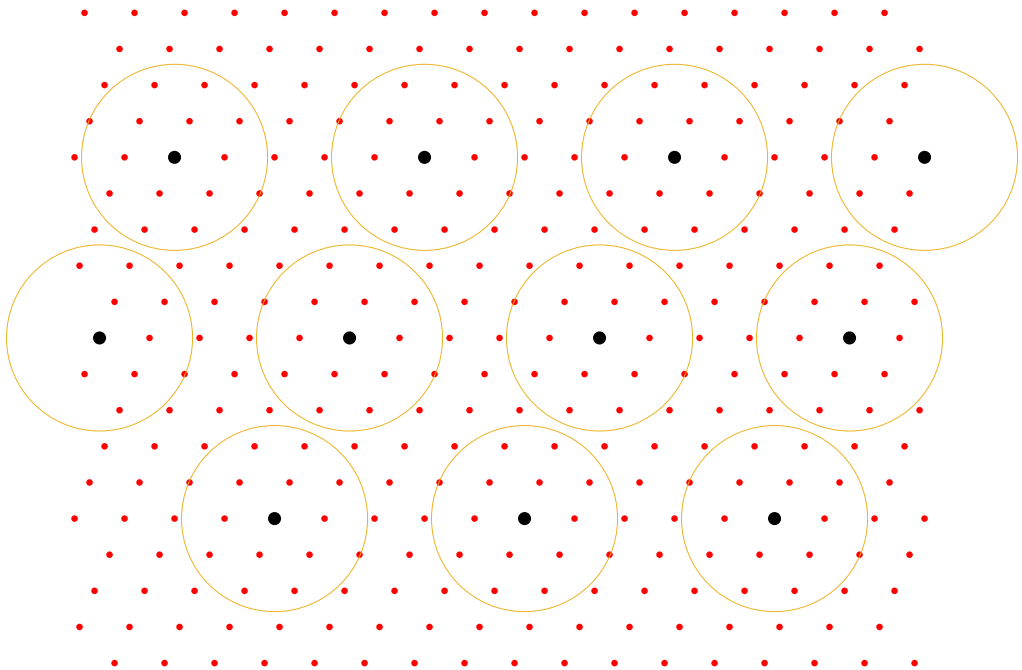
Step 1 - packing and "rough" covering:

- We dilate $\mathcal{K}$ such that $\mathrm{vol}(\mathcal{K}) = 5^{-n}$
  Thus, $\mathrm{vol}(\mathcal{K} - \mathcal{K}) < (4/5)^n < 1$ (Rogers-Shephard'57)
- By Siegel's summation formula, if $L \sim \mu_n$ it forms a packing w.r.t. $\mathcal{K}$ w.h.p.
- Furthermore, $L + 11\mathcal{K} = \mathbb{R}^n$ w.h.p. $(\mathrm{vol}(11\mathcal{K}) > 2^n)$



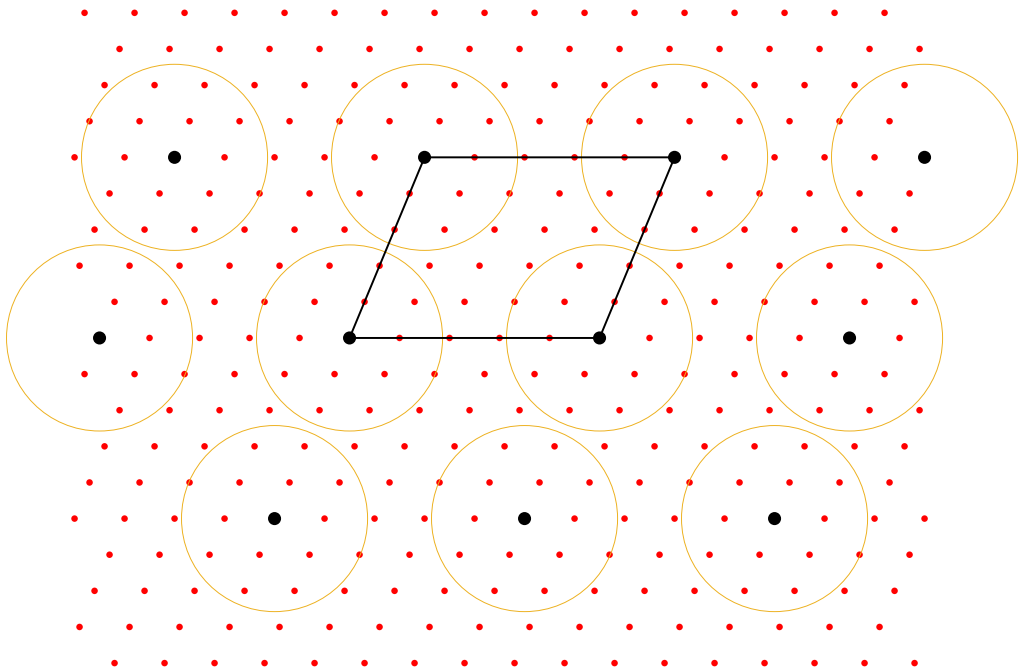
Main Thm : Proof Outline

Step 2 - discretization: For a large prime p define $L_2 = \frac{1}{p}L$



Main Thm : Proof Outline

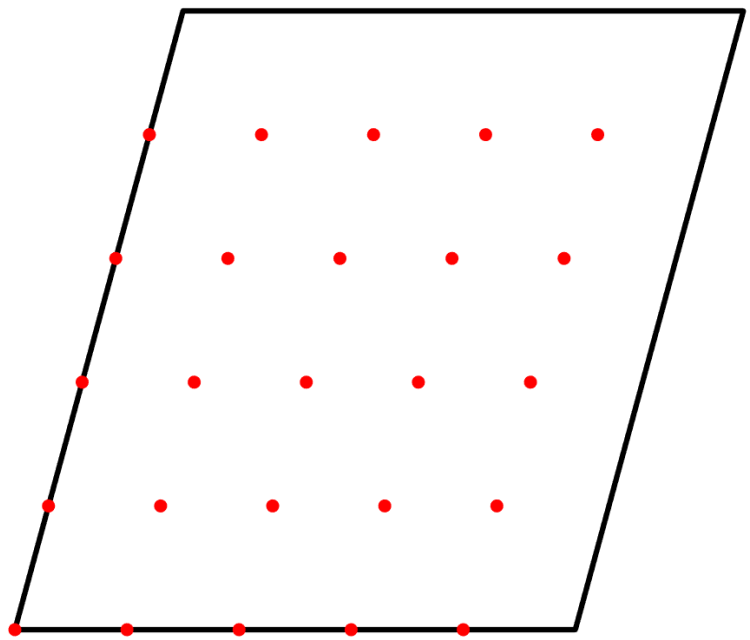
Step 2 - discretization: For a large prime p define $L_2 = \frac{1}{p}L$



$L_2/L \cong \mathbb{F}_p^n$

Main Thm : Proof Outline

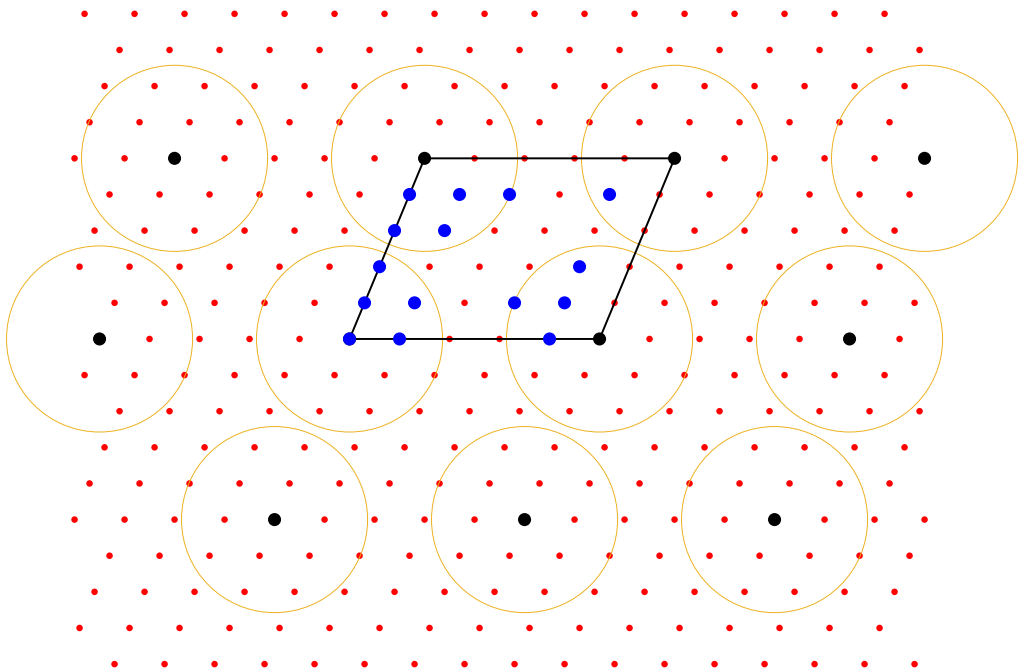
Step 2 - discretization: For a large prime p define $L_2 = \frac{1}{p}L$



$L_2/L \cong \mathbb{F}_p^n$

Main Thm : Proof Outline

Step 2 - discretization: For a large prime p define $L_2 = \frac{1}{p}L$

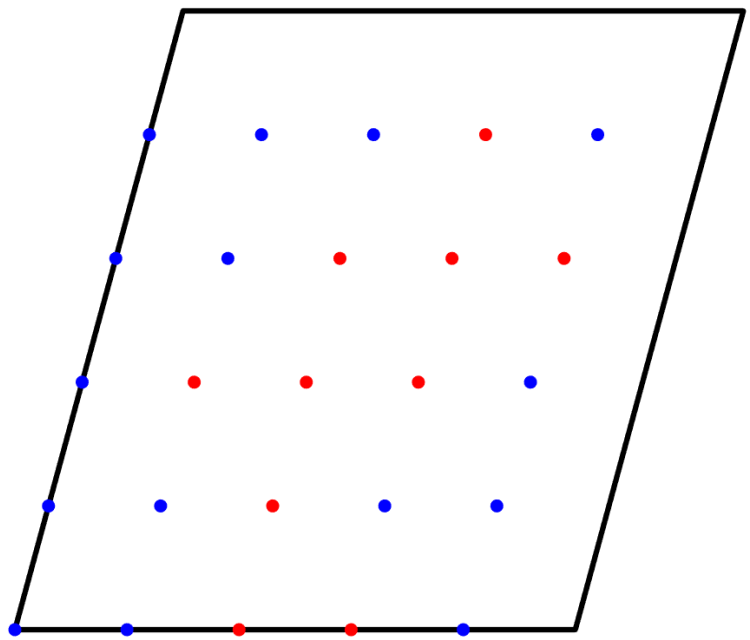


$L_2/L \cong \mathbb{F}_p^n$

Let $\mathcal{A} \subset \mathbb{F}_p^n$ be the set of covered points in the grid; let $\rho = 11/p$
$\Longrightarrow (1-\rho)^n \mathrm{vol}(\mathcal{K}) p^n \leq |\mathcal{A}| \leq (1+\rho)^n \mathrm{vol}(\mathcal{K}) p^n$

Main Thm : Proof Outline

Step 2 - discretization: For a large prime p define $L_2 = \frac{1}{p}L$



$L_2/L \cong \mathbb{F}_p^n$

Let $\mathcal{A} \subset \mathbb{F}_p^n$ be the set of covered points in the grid; let $\rho = 11/p$
$\Longrightarrow (1-\rho)^n \mathrm{vol}(\mathcal{K}) p^n \leq |\mathcal{A}| \leq (1+\rho)^n \mathrm{vol}(\mathcal{K}) p^n$

Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

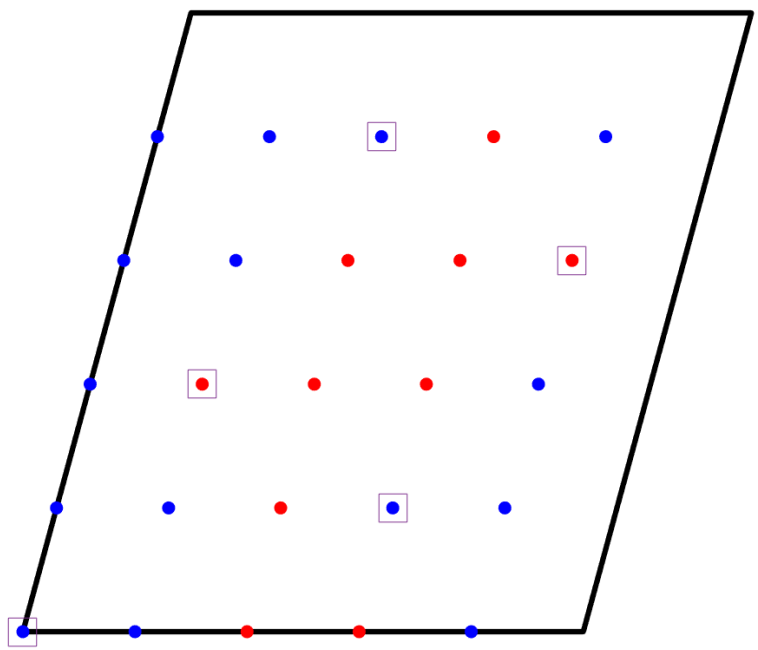
$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

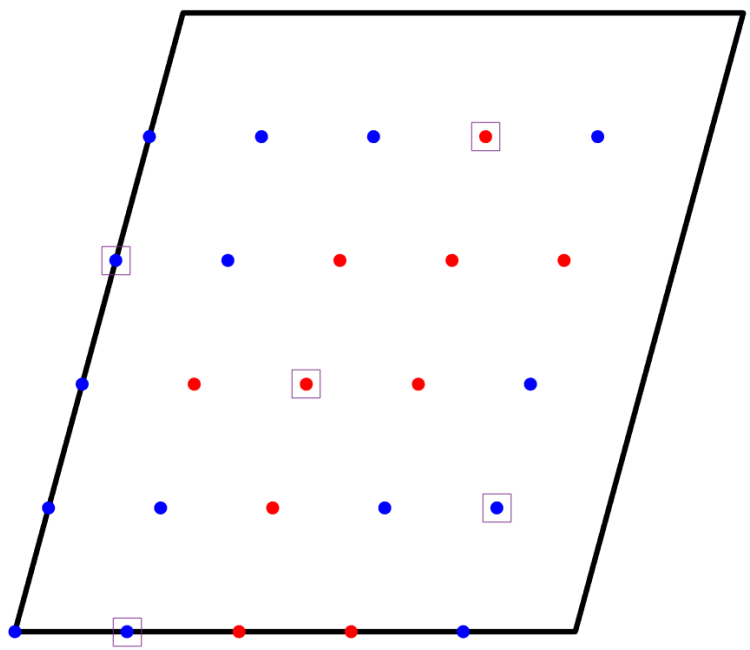


Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

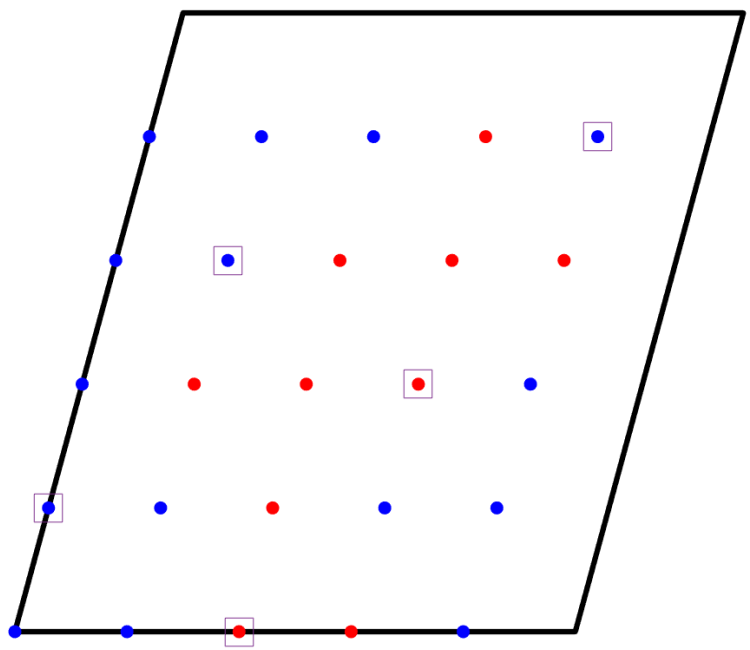


Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

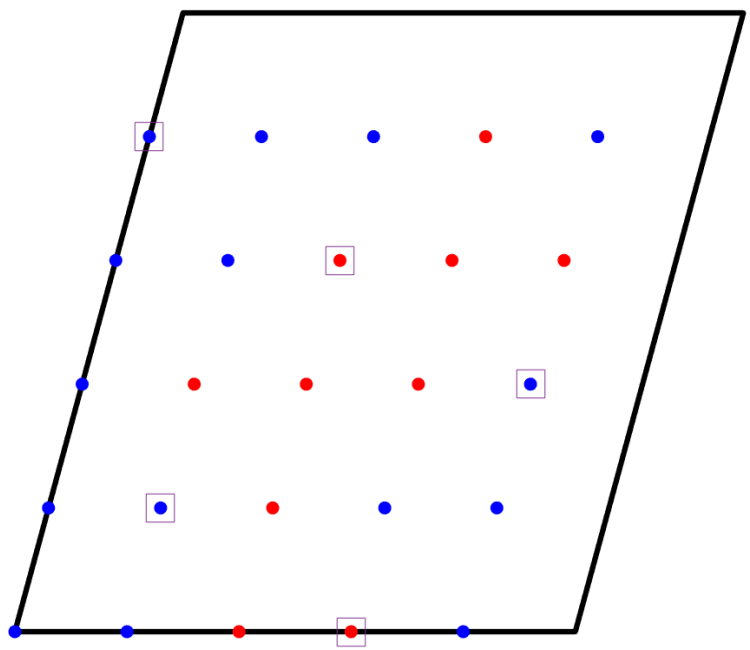


Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

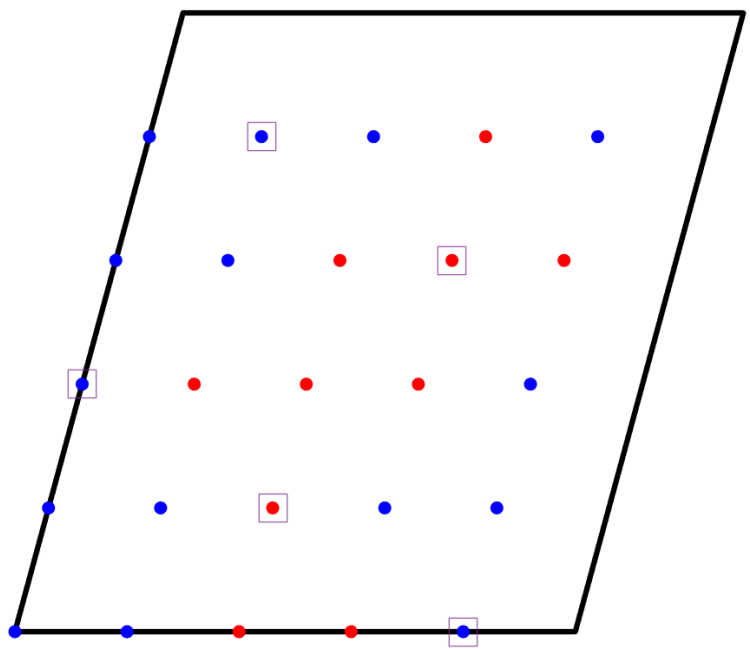


Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$



Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

How large should r be for this to be possible?
Clearly $r = n$ works, and we must have $|\mathcal{A}| p^r > p^n$

Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \approx |\mathcal{A}| p^{r-n}$$

How large should r be for this to be possible?
Clearly $r = n$ works, and we must have $|\mathcal{A}| p^r > p^n$

Theorem [Dhar-Dvir'22]

For any $\mathcal{A} \subset \mathbb{F}_p^n$ and integer $4 \leq r \leq n$ chosen such that $|\mathcal{A}| \cdot p^r > p^{n+3}$, a random subset $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$ smooths $\mathcal{A}$ w.h.p. provided that $p = \omega(n)$

Main Thm : Proof Outline

Step 3 - discrete smoothing:

Choose some subspace $S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)$, such that

$$\forall x \in \mathbb{F}_p^n \ : |(x+S) \cap \mathcal{A}| \in (1 \pm \varepsilon)|\mathcal{A}|p^{r-n}$$

More formally:

Theorem [Dhar-Dvir'22]

Let

- $n \geq 5$, $\delta, \varepsilon \in (0,1)$, and $p > 64n/(\varepsilon\delta)^2$
- $A \subset \mathbb{F}_p^n$, $|A| > p^4$ and $r > 3 + n - \log_p |A|$
- $S \sim \mathrm{Unif}\left(\mathrm{Gr}_{n,r}(\mathbb{F}_p)\right)$

Then,

$$\Pr\left(\max_{x \in \mathbb{F}_p^n} \left| \frac{|(x+S) \cap \mathcal{A}|}{|\mathcal{A}|p^{r-n}} - 1 \right| > \varepsilon \right) < \delta.$$

Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$

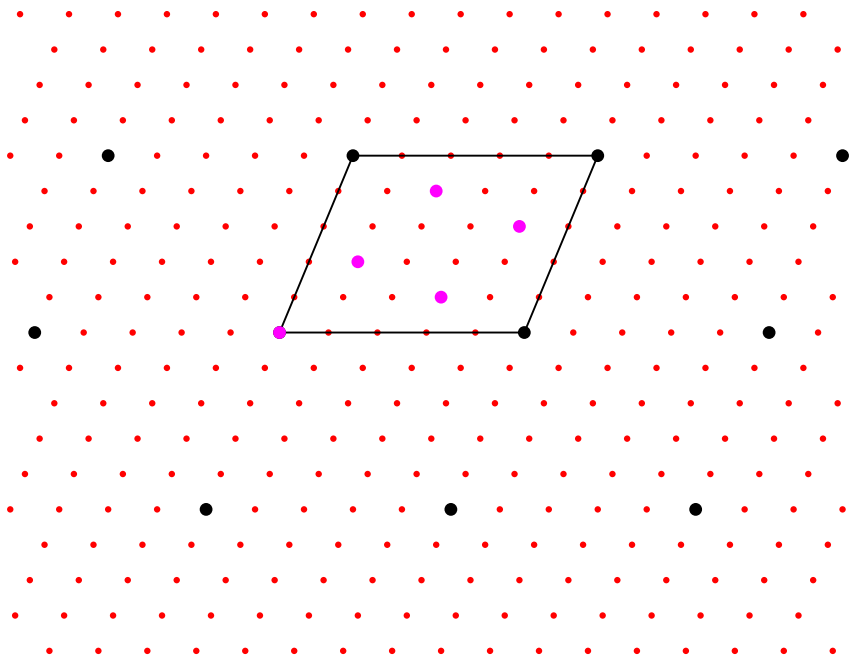
Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$



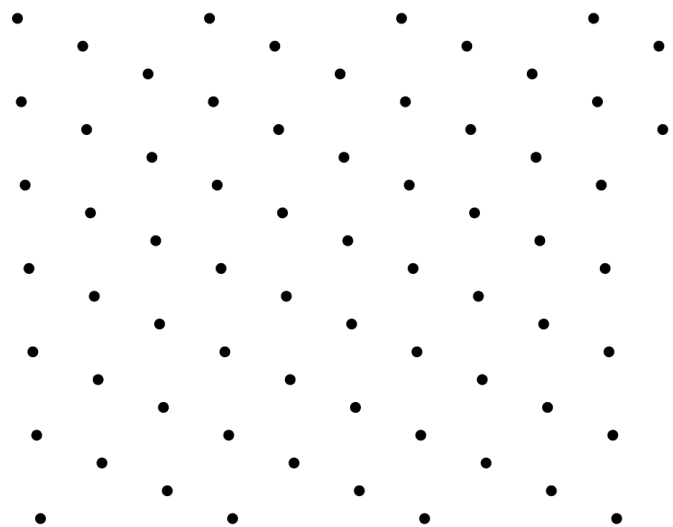
Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$



Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$

Proposition [O.-Regev-Weiss, JAMS'22]

If $L \sim \mu_n$ and $S \sim \mathrm{Unif}(\mathrm{Gr}_{n,r}(\mathbb{F}_p))$ are statistically independent, then $\alpha L(S) \sim \mu_n$ for $\alpha = p^{r/n}$.

Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$

Proposition [O.-Regev-Weiss, JAMS'22]

If $L \sim \mu_n$ and $S \sim \mathrm{Unif}(\mathrm{Gr}_{n,r}(\mathbb{F}_p))$ are statistically independent, then $\alpha L(S) \sim \mu_n$ for $\alpha = p^{r/n}$.

Proof: for any $g' \in \mathrm{SL}_n(\mathbb{R})$ we have

$$g' \cdot \{L(S) \ : \ S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)\} = \{(g'L)(S) \ : \ S \in \mathrm{Gr}_{n,r}(\mathbb{F}_p)\}$$

Thus, the probability measure governing $L(S)$ is $\mathrm{SL}_n(\mathbb{R})$-invariant

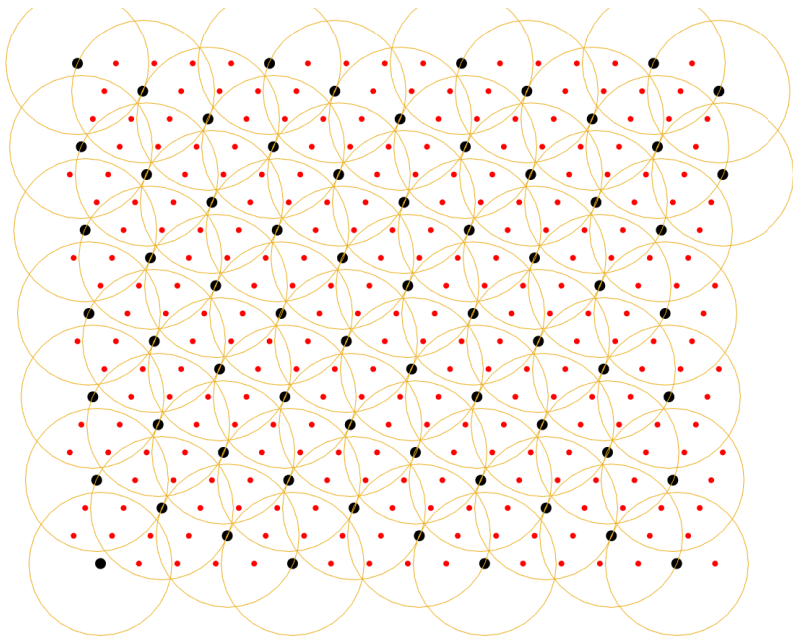
Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$



The points of $\frac{L}{p}$ are almost uniformly covered by $L(S) + \mathcal{K}$ w.h.p. over $L \sim \mu_n$ and $S \sim \mathrm{Unif}(\mathrm{Gr}_{n,r})$ [r chosen according to DD'22]

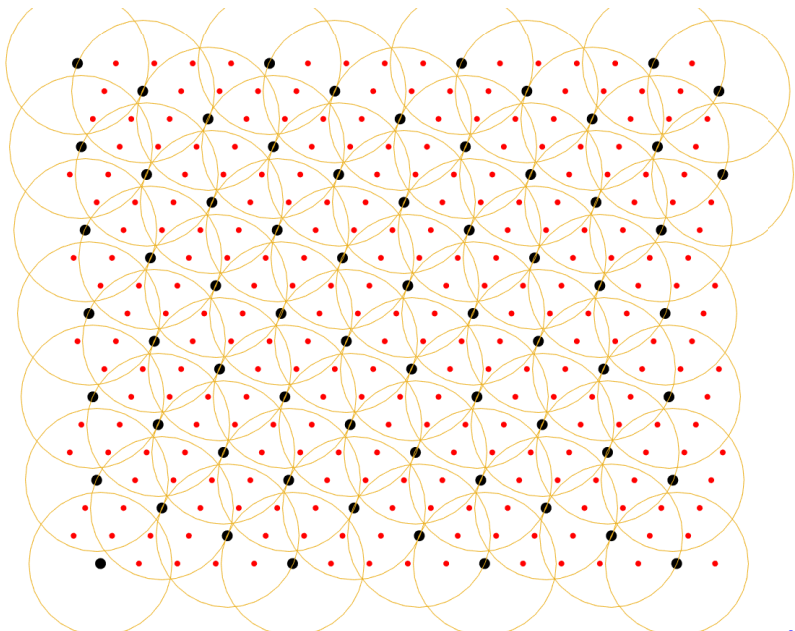
Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$



The points of $\frac{L}{p}$ are almost uniformly covered by $\tilde{L} + p^{r/n}\mathcal{K}$ w.h.p. over $\tilde{L} \sim \mu_n$ [r chosen according to DD'22]

Main Thm : Proof Outline

Step 4 - Create a denser lattice

Construct a lattice $L(S)$, such that $L \subset L(S) \subset \frac{L}{p}$ and $L(S)/\frac{L}{p} \cong S$

In particular, if g is the natural mapping from $\mathbb{F}_p^n$ to the fundamental cell

$$L(S) = g(S) + L$$

- Recall that by DD'22 $r \approx 3 + n - \log_p |\mathcal{A}|$ and $p = \Omega(n)$ suffice
- $|\mathcal{A}| \approx \mathrm{vol}(\mathcal{K})p^n$

Thus, we can choose p and r such that almost uniform covering is obtained w.h.p. and

$$\mathrm{vol}\left(p^{r/n}\mathcal{K}\right) = p^r \mathrm{vol}(\mathcal{K}) = O(n^3)$$

Main Thm : Proof Outline

Step 5 - From uniformly covering $\frac{L}{p}$ to uniformly covering $\mathbb{R}^n$

Lemma

Let $L, L' \subset \mathbb{R}^n$ be lattices, $\mathcal{K} \subset \mathbb{R}^n$ be a convex set, and assume $0 < \rho < 1$ is such that $L' + \rho\mathcal{K} = \mathbb{R}^n$. Then:

1. $\max_{x \in \mathbb{R}^n} N(L, \mathcal{K}, x) \leq \max_{x' \in L'} N(L, (1+\rho)\mathcal{K}, x')$;
2. $\min_{x \in \mathbb{R}^n} N(L, \mathcal{K}, x) \geq \min_{x' \in L'} N(L, (1-\rho)\mathcal{K}, x')$.

Main Thm : Proof Outline

Step 5 - From uniformly covering $\frac{L}{p}$ to uniformly covering $\mathbb{R}^n$

Lemma

Let $L, L' \subset \mathbb{R}^n$ be lattices, $\mathcal{K} \subset \mathbb{R}^n$ be a convex set, and assume $0 < \rho < 1$ is such that $L' + \rho\mathcal{K} = \mathbb{R}^n$. Then:

1. $\max_{x \in \mathbb{R}^n} N(L, \mathcal{K}, x) \leq \max_{x' \in L'} N(L, (1+\rho)\mathcal{K}, x')$;
2. $\min_{x \in \mathbb{R}^n} N(L, \mathcal{K}, x) \geq \min_{x' \in L'} N(L, (1-\rho)\mathcal{K}, x')$.

We apply this lemma with $L' = \frac{L}{p}$, and $\rho = \frac{11}{p} = O(1/n)$. Details are omitted.

Thanks for your attention!