New Bounds on the Density of Lattice Coverings

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

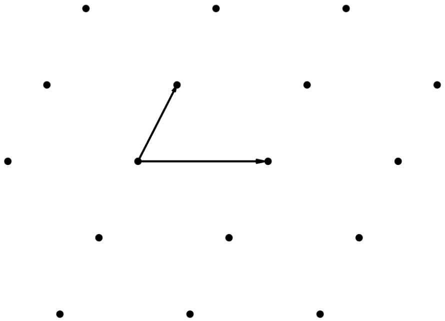
2020 Workshop on Coding, Cooperation, and Security in Modern Communication Networks (COCO 2020),

July 16, 2020

Definitions

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

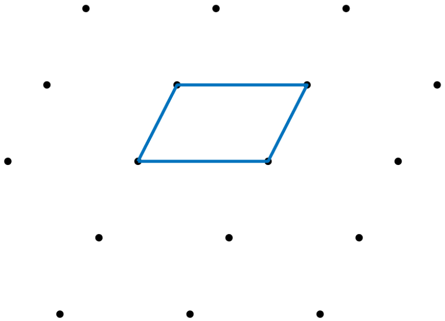
$$L = g\,\mathbb{Z}^n = \mathrm{span}_{\mathbb{Z}}(g_1, \ldots, g_n)$$



Definitions

- A **lattice** $L \subset \mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$
- It can be (non-uniquely) identified with a **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 an Euclidean ball
- The **covering density** of L is

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

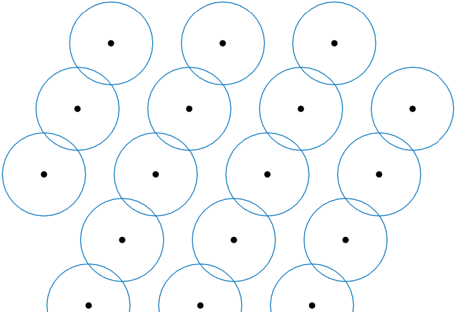
Definitions

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 an Euclidean ball
- The **covering density** of L is

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



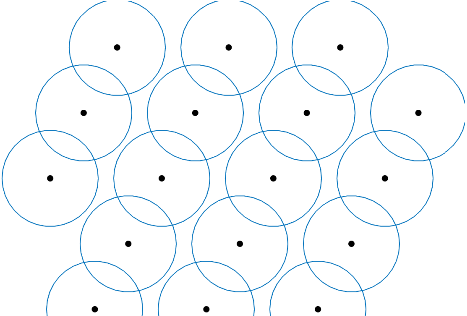
Definitions

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 an Euclidean ball
- The **covering density** of L is

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



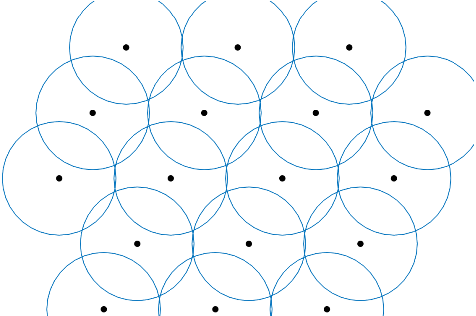
Definitions

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 an Euclidean ball
- The **covering density** of L is

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



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 an Euclidean ball
- The **covering density** of L is

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

- $\alpha L + \alpha r\mathcal{B} = \mathbb{R}^n \Leftrightarrow L + r\mathcal{B} = \mathbb{R}^n, \quad \forall \alpha \neq 0$
  $\Rightarrow$ 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

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

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

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

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 $\mathcal{K}$

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

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

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

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:** $\sup_{\mathcal{K} \in \mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < n^{\log_2 \log n + c_1}$

Our Theorem 1

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

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?

Some preliminary definitions are needed first:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} \ : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} \ : \det(t) = 1\}$
- 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?

Some preliminary definitions are needed first:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} \; : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} \; : \det(t) = 1\}$
- 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?

Some preliminary definitions are needed first:

- $\mathrm{SL}_n(\mathbb{R}) \triangleq \{g \in \mathbb{R}^{n\times n} \ : \det(g) = 1\}$
  $\mathrm{SL}_n(\mathbb{Z}) \triangleq \{t \in \mathbb{Z}^{n\times n} \ : \det(t) = 1\}$
- 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 $L = g\ t\ \mathbb{Z}^n$
  $\implies \mathcal{L}_n \cong \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$

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 our paper): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

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 our paper): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

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

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 our paper): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

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?

- **Corollary from Rogers'58:** for any $\mathcal{K} \in \mathrm{Conv}_n$ and $1 < V < c_1 n$ we have $\Pr(\Theta_{\mathcal{K}}(L) > 2^n V) < c_2 e^{-V}$
- **Strömbergsson'12:** $\Pr(\Theta_{\mathcal{K}}(L) > (1.756\ldots)^n) < c_3 e^{-c_4 n}$

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 our paper): $\mathbb{E}[\Theta_{\mathcal{K}}(L)] = \infty$

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?

- **Corollary from Rogers'58:** for any $\mathcal{K} \in \mathrm{Conv}_n$ and $1 < V < c_1 n$ we have $\Pr(\Theta_{\mathcal{K}}(L) > 2^n V) < c_2 e^{-V}$
- **Strömbergsson'12:** $\Pr(\Theta_{\mathcal{K}}(L) > (1.756\ldots)^n) < c_3 e^{-c_4 n}$

Our Theorem 2

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.

Our Theorem 2

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:

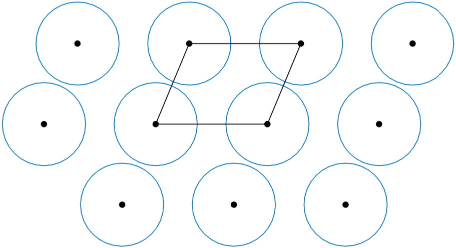
1. $\exists c > 0$ such that $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Pr\left(\Theta_{\mathcal{K}}(L) > cn^2\right) < 1$
$\Longrightarrow \sup_{\mathcal{K}\in\mathrm{Conv}_n} \Theta_{n,\mathcal{K}} < cn^2$ which is our Theorem 1
2. $\sup_{\mathcal{K}\in\mathrm{Conv}_n} \Pr\left(\Theta_{\mathcal{K}}(L) > \omega(n^2)\right) = o(1)$
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 $(1.756\ldots)^n$.

Thm 1 : Proof Outline

We dilate $\mathcal{K}$ to have volume $1 < V < cn$ (WLOG)

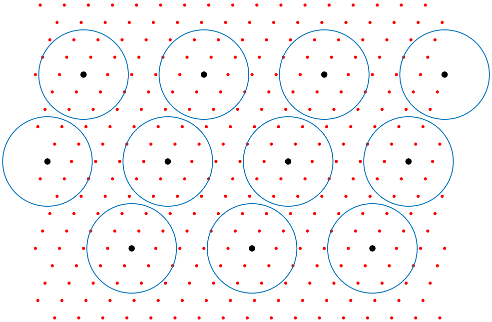
Step 1 - almost perfect covering: Find a lattice $L \in \mathcal{L}_n$ such

that at least $1 - \epsilon$ of the fundamental cell (torus) is covered
Rogers'58: if $L \sim \mu_n$, this happens with probability $\gtrapprox 1 - \epsilon^{-1}e^{-V}$



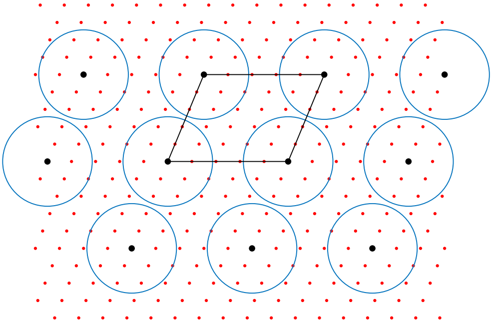
Thm 1 : Proof Outline

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



Thm 1 : Proof Outline

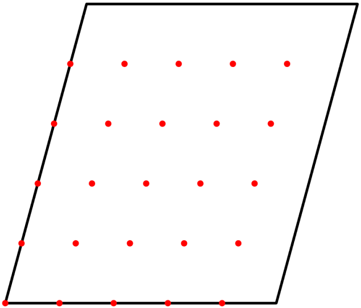
Step 2 - discretization: For a prime $n \le p \le 2n$ define $L_2 = \frac{1}{p} L$



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

Thm 1 : Proof Outline

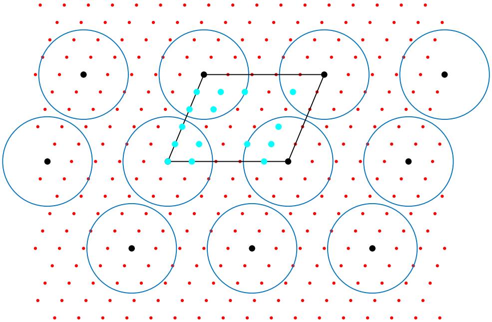
Step 2 - discretization: For a prime $n \leq p \leq 2n$ define $L_2 = \frac{1}{p}L$



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

Thm 1 : Proof Outline

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

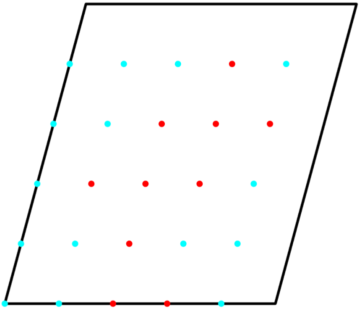


$L_2/L \cong \mathbb{F}_p^n$

Let $\mathcal{A} \subset \mathbb{F}_p^n$ be the set of covered points in the grid
$\implies |\mathcal{A}| \geq (1-\epsilon)p^n$ (after a shift)

Thm 1 : Proof Outline

Step 2 - discretization: For a prime $n \leq p \leq 2n$ 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
$\implies |\mathcal{A}| \geq (1-\epsilon)p^n$ (after a shift)

Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

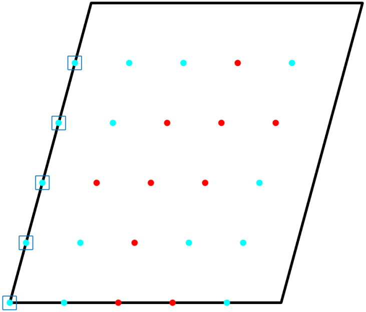
This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

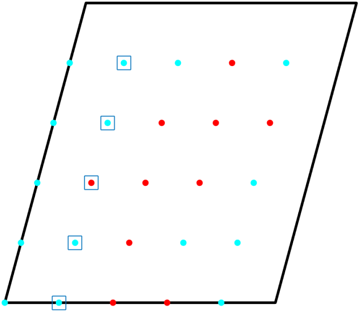


Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

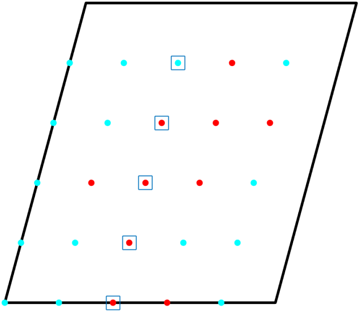


Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

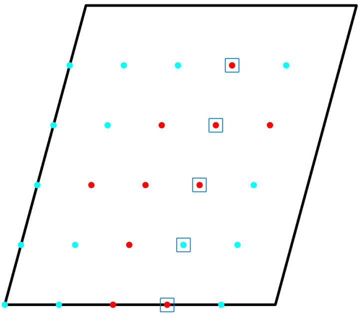


Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

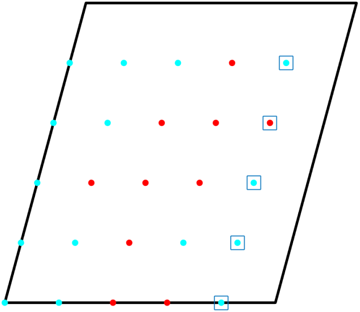


Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r



Thm 1 : Proof Outline

Step 3 - discrete covering problem: Choose some subspace $S \subset \mathbb{F}_p^n$ of dimension r, such that

$$\forall x \in \mathbb{F}_p^n \ : x + S \not\subset \mathcal{A}^c$$

This is possible if $\mathcal{A}^c$ is **not** a **Kakaeya-set of rank** r

Theorem [Dvir,Kopparty,Lev,Saraf,Sudan 2009-2013]

If $|\mathcal{A}^c| < e^{-n/p} p^n$ it is not a Kakeya-set of rank 2.

For our probabilistic theorem, we prove a soft version of this
Recall that $|\mathcal{A}^c| < \epsilon p^n$, thus if $\epsilon < e^{-1}$ we can find such S

Thm 1 : Proof Outline

Step 4 - Use S to kill the discrete hole:

Construct a lattice L_1, such that $L \subset L_1 \subset L_2$ and $L_1/L_2 \cong S$

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

$$L_1 = g(S) + L$$

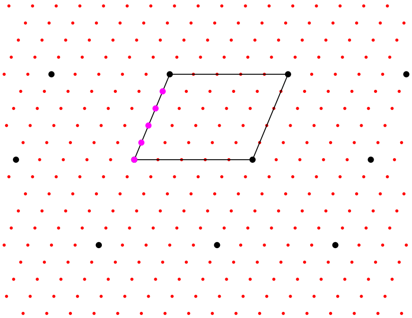
Thm 1 : Proof Outline

Step 4 - Use S to kill the discrete hole:

Construct a lattice L_1, such that $L \subset L_1 \subset L_2$ and $L_1/L_2 \cong S$

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

$$L_1 = g(S) + L$$



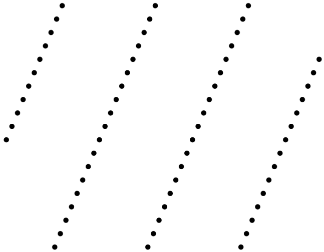
Thm 1 : Proof Outline

Step 4 - Use S to kill the discrete hole:

Construct a lattice L_1, such that $L \subset L_1 \subset L_2$ and $L_1/L_2 \cong S$

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

$$L_1 = g(S) + L$$



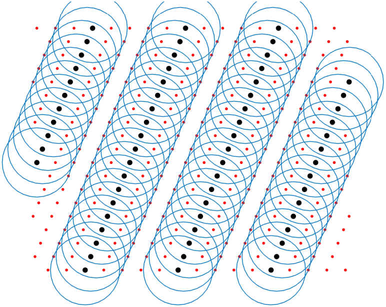
Thm 1 : Proof Outline

Step 4 - Use S to kill the discrete hole:

Construct a lattice L_1, such that $L \subset L_1 \subset L_2$ and $L_1/L_2 \cong S$

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

$$L_1 = g(S) + L$$



The good: $L_2 \subset L_1 + \mathcal{K}$, The bad: $\frac{\text{co-volume of}(L_1)}{\text{co-volume of}(L)} = p^{-r}$

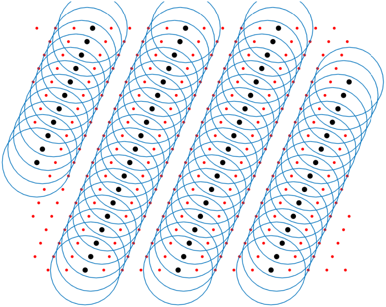
Thm 1 : Proof Outline

Step 4 - Use S to kill the discrete hole:

Construct a lattice L_1, such that $L \subset L_1 \subset L_2$ and $L_1/L_2 \cong S$

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

$$L_1 = g(S) + L$$



Remark: If $L \sim \mu_n$ and S is a a uniform subspace, then $p^{r/n} L_1 \sim \mu_n$

Thm 1 : Proof Outline

Step 5 - From covering L_2 to covering $\mathbb{R}^n$

Fact:
If $L + \mathcal{K}$ covers more than 1/2 of the space, then $L + 2\mathcal{K} = \mathbb{R}^n$

$\implies L_2 + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 = \frac{1}{p}L$)

$\implies L_1 + \mathcal{K} + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 \subset L_1 + \mathcal{K}$)

$\implies L_1 + \left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$ (since $\mathcal{K}$ is convex)

$\implies p^{r/n}L_1 + p^{r/n}\left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$, and $p^{r/n}L_1 \in \mathcal{L}_n$

Thm 1 : Proof Outline

Step 5 - From covering L_2 to covering $\mathbb{R}^n$

Fact:
If $L + \mathcal{K}$ covers more than $1/2$ of the space, then $L + 2\mathcal{K} = \mathbb{R}^n$

$\implies L_2 + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 = \frac{1}{p}L$)

$\implies L_1 + \mathcal{K} + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 \subset L_1 + \mathcal{K}$)

$\implies L_1 + \left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$ (since $\mathcal{K}$ is convex)

$\implies p^{r/n}L_1 + p^{r/n}\left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$, and $p^{r/n}L_1 \in \mathcal{L}_n$

$$\Theta_{\mathcal{K}}(p^{r/n}L_1) \leq \mathrm{Vol}\left(p^{r/n}\left(1 + \frac{2}{p}\right)\mathcal{K}\right) = p^r\left(1 + \frac{2}{p}\right)^n \mathrm{Vol}(\mathcal{K}) < p^r e^2 V$$

Thm 1 : Proof Outline

Step 5 - From covering L_2 to covering $\mathbb{R}^n$

Fact:
If $L + \mathcal{K}$ covers more than 1/2 of the space, then $L + 2\mathcal{K} = \mathbb{R}^n$

$\implies L_2 + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 = \frac{1}{p}L$)

$\implies L_1 + \mathcal{K} + \frac{2}{p}\mathcal{K} = \mathbb{R}^n$ (since $L_2 \subset L_1 + \mathcal{K}$)

$\implies L_1 + \left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$ (since $\mathcal{K}$ is convex)

$\implies p^{r/n}L_1 + p^{r/n}\left(1 + \frac{2}{p}\right)\mathcal{K} = \mathbb{R}^n$, and $p^{r/n}L_1 \in \mathcal{L}_n$

$$\Theta_{\mathcal{K}}(p^{r/n}L_1) \leq \mathrm{Vol}\left(p^{r/n}\left(1 + \frac{2}{p}\right)\mathcal{K}\right) = p^r\left(1 + \frac{2}{p}\right)^n \mathrm{Vol}(\mathcal{K}) < p^r e^2 V$$

We used $r = 2$, $n < p < 2n$ and all arguments hold with $V = \text{const}$
$\implies \Theta_{\mathcal{K}}(p^{r/n}L_1) < cn^2$

Thanks for your attention!