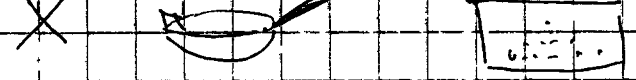
Day 4 Talk 1

Oded Regev

"~~Dimension Reduction for Matrices~~" /

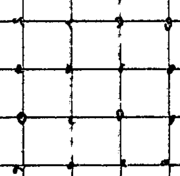
"A reverse Minkowski theorem"

Joint w. Daniel Dadush & Noah Stephens-Davidowitz

Puzzle: 

<u>Def</u> Lattice: $\mathcal{L} = \{ \sum_{i=1} a_i b_i \mid a_i \in \mathbb{Z} \}$

b_i vectors



square lattice

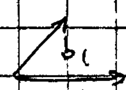
- Motivations: many applications (e.g. Sphere packing)

Problem: - Counting problem

$$\# \Lambda \cap B(0,R) = ?$$

- Shortest vector problem $(\sup R \text{ s.t. } \# \Lambda \cap B(0,R) = 1)$

Def $\det(\Lambda) = \lim_{r \to \infty} \frac{\text{Vol}(\text{Ball}(r))}{\# \Lambda \cap \text{Ball}(r)}$ coincides with determinant

$= \det(B)$ 

$\longrightarrow B$

Minkowski Thm: if $\det(\Lambda) = 1$ $\Rightarrow \#\{\Lambda \cap \text{Ball}(\sqrt{n})\} \geq 2^n$

Proof by pidgeon whole

Show $\# \Lambda \cap Ball(\sqrt{n}) \geq 2$, assume not.

Then $\underbrace{B(\lambda, \sqrt{n})}_{vol > 1}$ disjoint for $\lambda \in \Lambda$

$\rightsquigarrow$ volume bound leads to contradiction.

Reverse Minkowski? First attempt (see slides) doesn't work.

2^{nd} attempt: if dense $\rightsquigarrow \exists$ sublattice / subspace where $\det \leq 1$

precisely:

<u>Thm</u> if all sublattices of L has $\det \geq 1$ then $\forall r > 0$

$$\# \{ B(0, r) \cap \Lambda \} \leq e^{c \log^2 n \, r^2}$$

- this has many applications.

Few remarks about proof: (switch to blackboard)

<u>Thm</u> If $L \subset \mathbb{R}^n$ st. $L' \subseteq L$ $\det(L') \geq 1$, and $\det(L) = 1$, then

(replace counting with Gaussians, "weighted sum" "smoothed out sum") $\rho(L) = \sum_{x \in L} e^{-\|x\|^2} \leq 2^n$ ignoring log factor

Proof idea: Goal upper-bound $\rho(L)$

on

stable lattices $\{L \subset \mathbb{R}^n : \det L = 1$
$\forall L' \subset L, \det L' \geq 1\}$

If there are no local maxima, then ρ attains it's maximum on the boundary.

$\rightsquigarrow$ Assume no local maxima. Look for maximum on the bdry. Lies on the bdry if sublattice $\det(L') = 1$

$\rightsquigarrow$ iteration / induction.

How?

$$\rho(L) \leq \rho(\underset{\substack{\nearrow \\ \text{sub-lattice with } \det(L')=1}}{L'} \oplus L/L')$$

(picture on slides)

By Gram-schmidt direct sum ~~for~~ simplified, numbers different

$$= \underset{\substack{\nearrow \\ \text{stable}}}{\rho(L')}\ \underset{\substack{\nearrow \\ \text{stable}}}{\rho(L/L')} \leq 2^d\, 2^{n-d} = 2^n$$

$\rightsquigarrow$ induction

By continuing in dimension reduction, would get
$\rho(L) \leq \rho(\mathbb{Z}^n)$ don't know

- But local maxima may exist...

Computing laplacian, in dim ≤ 4 no local maxima, but unclear in higher dimensions.

How to fix?

Maybe using local maximum could also be analyzed? (For example $\nabla \rho(L) = 0 \ldots$)

Hard!

(2) Instead let's work with

$$\psi(L) = \gamma(\mathrm{Vor}(L)) \doteq \int_{\mathrm{Vor}(L)} e^{-\|x\|^2} dx$$

γ: Gaussian mass

$\mathrm{Vor}(L)$: ~~defn~~ voronoi cell of the origin, see slides.

- In a sense $\psi(L) \approx \frac{1}{\rho(L)}$ [CDLP'13] have an inequality.

if ψ has no local minima

$$\psi(L) \geq \psi(L' \oplus L/L') = \psi(L')\,\psi(L/L')$$

again Gram-Schmidt etc ... same as before

graphical rep. on slides

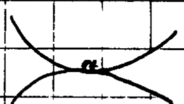
idea find domain for voronoi cell $L' \oplus L/L'$ is also fundamental for L, but "closer" to the origin than $\mathrm{Vor}(L)$ & of same volume.

- Maybe Local minima not so bad? Can be done.

Main Proposition

$$\nabla_A \gamma(\underbrace{\mathrm{Vor}(AL)}_{\text{voronoi cell of transformed lattice}})\Big|_{A=\mathrm{Id}_n} \neq \nabla_A \gamma(\underbrace{A\cdot \mathrm{Vor}(L)}_{\text{linearly transformed voronoi cell}})\Big|_{A=\mathrm{Id}}$$

see slides

 ← Idea: $\gamma(A\cdot\mathrm{Vor}(L)) \leq \gamma(\mathrm{Vor}(AL))$

+ differentiability argument

+ equal at a pt.

Rk: $A\,\mathrm{Vor}(L)$ & $\mathrm{Vor}(AL)$ fundamental domains of AL.

Note taker note:

<u>Def</u> $S \subset \mathbb{R}^n$ fundamental domain for L if

(S convex set) & $LS = \bigcup_{\lambda \in L} \lambda S = \mathbb{R}^n$ &

some other regularity assumption

$\lambda S \cap \lambda' S = \emptyset$ for $\lambda \neq \lambda'$ (or intersect only on bdry).

<u>Thm</u> if $K \subseteq \mathbb{R}^n$ symm. convex body of $\mathrm{Vol}(K) = (\log n)^n$ for which $\gamma|_K$ is isotropic, then $\gamma(K) \geq \frac{1}{2}$

source of $\log n$

[Bobkov, Cordero-Erausquin, Fradelisi, Maurey],

[Figiel, ..., Pisier] ℓ-position, (B)-conjecture

Summary: - Use the correct function: φ

- on bdry decompose
- for local minima can analyze using Thm above + critical point property

Open Qs: $\varphi'(L) = \int_{\mathrm{Vor}(L)} \|x\|^2 \, dx$

- could we do the same for $\varphi'(L)$.
- related to slicing conjecture

Reverse Minkowski: BANFF 2016/9/6

Journey through mathematics: Markov chains, dynamical systems, additive combinatorics, number theory, functional analysis, convex geometry

Thm 1 If $L \subset \mathbb{R}^n$ is s.t. $\forall L' \subseteq L$, $\det L' \geq 1$, then

$$\cancel{\Psi_0(L)} := |L \cap \sqrt{n} B_2| \leq 2^n$$

$$\rho(L) := \sum \exp(-\pi \|x\|^2) \leq 2^n \quad \text{(We actually prove this)}$$

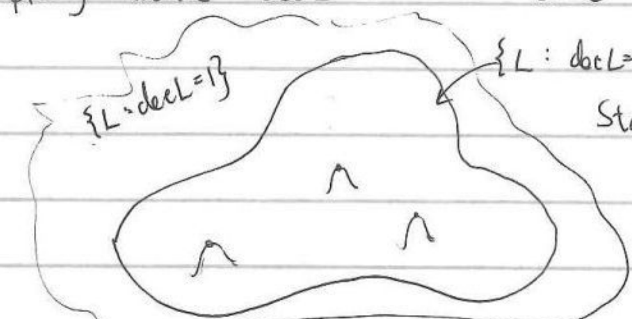
(implies $|L \cap \sqrt{n} B_2| \leq 2^n \cdot e^{\pi n} = (2 \cdot e^{\pi})^n$)

$\rho(10 \log n \cdot L) \leq 2$

Nice because Eight: gives NP-witness.

Proof structure suggested by [Shapira & Weiss].

For simplicity assume $\det L = 1$ (can reduce to this case).



$\{L : \det L = 1, \forall L' \subseteq L, \det L' \geq 1\}$

Stable lattices (algebraic-geometry origin, Harder-Narasimhan)

① Replace Ψ with a ~~continuous~~ smooth function $\Psi_1(L) = \sum_{x \in L} \exp(-\|x\|^2)$

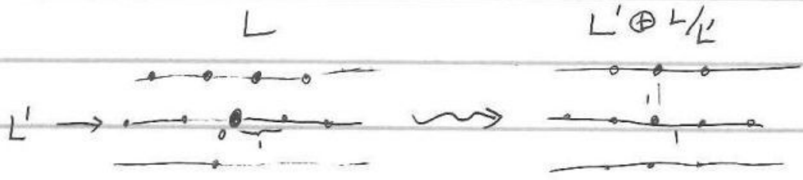
② Assume there are no local maxima. Then it suffices to bound $\Psi(L)$ for L on the boundary, which means that $\exists L' \subsetneq L$ s.t. $\det L' = 1$.

Then we are done by induction since

$$\Psi(L) \leq \Psi(L' \oplus L/L') = \Psi(L') \cdot \Psi(L/L') \leq 2^d \cdot 2^{n-d} = 2^n$$

since L' and L/L' are stable

where $d = \operatorname{rank} L'$.



This process shows that $\mathbb{Z}^n$ is densest among all lattices!

(3) Do local maxima exist? • [Dutour Sikirić, Schürmann, Vallentin 12] : local maxima exist for μ.

• [SARNAK STROMBERGSSON 06] : Epstein's zeta function, height, automorphic forms, [TERRAS] eigen~~values~~ functions of Laplacian. If Laplacian always ~~negative~~ positive no local maxima can exist.

Maybe local maxima are not so evil?

We don't know how to analyze local maxima of Ψ. So we use a different proxy for # points: Gaussian mass of Voronoi cell :

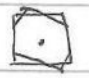
$$\Psi_2^*(L) = \overbrace{\int_{V_2(L)} \exp(-\pi\|x\|^2)\, dx}^{\gamma(\mathrm{Vor}(L))} \qquad \Psi(L) \approx \frac{1}{\rho(L)} \qquad \Psi(L) \geq \Psi(L' \oplus L/L') = \Psi(L') \cdot \Psi(L/L')$$

which is morally the reciprocal of $\rho(L)$. [Chung Dadush Liu Peikert '13]

We still can't rule out local minima of Ψ_2! Induction still works for Ψ_2.

What can we say about local minima of Ψ_2?

These are lattices ~~whose Voronoi cell, is isotropic Gaussian~~ for which the Gaussian measure, when restricted to the Voronoi cell, is isotropic. $\gamma|_{\mathrm{Vor}(L)}$,

<u>Proposition</u> $\nabla_A \gamma(\mathrm{Vor}(AL))|_{A=I_n} = \nabla_A \gamma(A \cdot \mathrm{Vor}(L))|_{A=I_n}$ 

<u>Thm 2</u> If $K \subseteq \mathbb{R}^n$ is a symmetric convex body of $\mathrm{vol}(K) = (\log n)^{n}$ (10) for which $\gamma|_K$ is isotropic, then $\gamma(K) \geq \frac{1}{2}$

i.e. $\int_{\mathrm{Vor}(L)} \exp(-\pi\|x\|^2)\, x x^t\, dx \propto I_n$

(Using Bobkov, B-conjecture, ℓ-position)

Cordero-Erausquin-Fradelizi-Maurey Figiel-Tomczak-Jaegermann-Pisier

 $K = [-c\sqrt{\log n}, c\sqrt{\log n}]^n$

$\gamma(K) = 1/2$

(Not clear that proof needs to involve convex geometry)

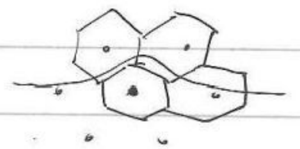
Open questions:

1. Is $\mathbb{Z}^n$ really densest?
2. Application to Integer Programming
3. Solve Minkowski conjecture (strong slicing conjecture would almost be there)
4. Coding theory analogue
5. More applications
6. Strong reverse Minkowski

Lemma [CHUNG DADUSH LIU PEIKERT 13]

$$\rho(\mathcal{L}) \cdot \gamma(\mathcal{V}(\mathcal{L})) \leq 1$$

Proof:



$$\begin{aligned}
1 &= \int_{\mathbb{R}^n} e^{-\pi\|x\|^2} dx \\
&= \sum_{y\in\mathcal{L}} \int_{V(\mathcal{L})} e^{-\pi\|y+t\|^2} dt \\
&= \sum_{y\in\mathcal{L}} e^{-\pi\|y\|^2} \int_{V(\mathcal{L})} e^{-\pi\|t\|^2} \cdot e^{2\pi\langle y,t\rangle} dt \\
&= \sum_{y\in\mathcal{L}} \rho(y) \int_{V(\mathcal{L})} e^{-\pi\|t\|^2} \cdot \cosh(2\pi\langle y,t\rangle)\, dt \\
&\geq \sum_{y\in\mathcal{L}} \rho(y) \int_{V(\mathcal{L})} e^{-\pi\|t\|^2} dt = \rho(\mathcal{L}) \cdot \gamma(V(\mathcal{L})).
\end{aligned}$$

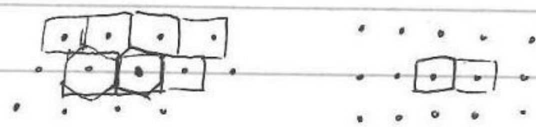
$\forall y \in \mathbb{R}^n,\ \gamma(V+y) \geq \gamma(V)\cdot\rho(y)$

$1 = \gamma(\mathbb{R}^n) = \sum_{y\in L} \gamma(V+y)$

$\geq \gamma(V)\cdot\rho(L)$

$\square$

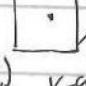
Lemma $\gamma(V(L)) \geq \gamma(V(L' \oplus L/L'))$



Figiel-Tomczak Jaegermann, Pisier $\quad$ vol $K = (10\log n)$,

<u>Thm 3</u> $\forall$ symmetric convex body $K \subset \mathbb{R}^n$, $\exists A$, $\det A = 1$, s.t.

$$\gamma(10\sqrt{\log n}\, AK) \geq 1/2$$



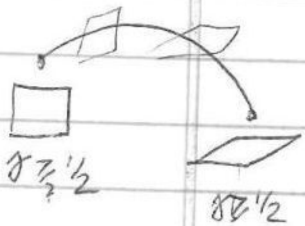
$\gamma([-t,t]^n) =$ Need $t \approx \sqrt{\log n}$ for $\gamma \geq 1/2$.

~~Proof~~ (Actual statement talks about ℓ norm or actually $\ell \cdot \ell^{(n)}$, uses K-convexity) $\quad \gamma([-t,t])^n$

<u>Thm 4</u> [Cordero-Erausquin, Fradelizi, Maurey '04] $\forall$ symmetric convex body $K \subset \mathbb{R}^n$, the function $\gamma(e^D K)$ where D ranges over diagonal $n \times n$ matrices is log-concave.

<u>Cor</u> For any orthogonal U, V, the func. $\gamma(U e^D V K)$ where D —"— is log concave.

<u>Proof of Thm 2:</u>



By Thm 3, $\exists A \in \mathbb{R}^{n \times n}$, $\det(A) = 1$, s.t.

$$\gamma(AK) \geq 1/2.$$

Using the singular value decompos., $A = UDV$ ~~So~~ ~~and define $K' = VK$.~~ with $\det D = 1$.

~~$\gamma(DVK) = \gamma(AK) \geq 1/2$.~~ Assume wlog that A is diagonal (Write $A = UDV$, then clearly DV also satisfies $\gamma(DVK) \geq 1/2$; can also assum

The assumption that $\gamma|_K$ is isotropic is equivalent to

$$\nabla_B \gamma(BK)\big|_{I_n} \propto I_n$$

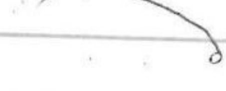
So the function $r \xmapsto{h} \gamma(e^{r \log A} K)$ satisfies

$$h(0) = \gamma(K)$$
$$h(1) = \gamma(AK) \geq 1/2$$

and by Thm 4 is log-concave. Moreover, since $\gamma|_K$ is isotropic, ~~so is $\gamma|_{VK}$~~, which is equivalent to

$$\nabla_B \gamma(BK)\big|_{B = I_n} \propto I_n$$

implying that $h'(0) = 0$, since $\operatorname{Tr} \log A = 0$.



Covering radius

Def $\mu(L) = \max_{x \in \mathbb{R}^n} \text{dist}(x, L)$ **Ex** $\mu(\mathbb{Z}^n) = \frac{\sqrt{n}}{2}$

Can we upper bound μ for stable lattices? Is $\frac{\sqrt{n}}{2}$ the maximum?

(if true, this would imply Minkowski's Conjecture) [ShapiraWeiss 16]

Also gives the ℓ_2 case of the Kannan-Lovasz conjecture [KL88].

We can try the same framework as before. ~~Local maxima are known to exist.~~ Induction works well:

$$\mu(L)^2 \le \mu(L')^2 + \mu(L/L')^2$$

Local maxima are known to exist. ~~They correspond to~~

Notice that $\mu(L) = R(\text{Vor}(L))$ where $R(K)$ is the circum radius of K,

$$R(K) = \max_{x \in K} \|x\|$$

A local maximum corresponds to a Voronoi cell in "John position" i.e., a position that minimizes circum radius. Can we hope that for K, $\text{vol}(K) = 1$ the John position has $R(K) \le \sqrt{n}/2$? Unfortunately, not: $K = c \cdot n \cdot B_1^n$ has $\text{vol}(K) = 1$ but $R(K) = c \cdot n$.

Instead, we use

$$\bar{\mu}(L) = \mathbb{E}_{x \sim \mathbb{R}^n}[\text{dist}(x, L)^2]^{1/2}$$

or equivalently,

$$\bar{\mu}(L) = Z_2(\text{Vor}(L)) := \mathbb{E}_{x \sim \text{Vor}(L)}[\|x\|^2]^{1/2}$$

Claim [GuruMiccR 04] $\forall L$, $\bar{\mu}(L) \le \mu(L) \le 2\bar{\mu}(L)$.

(Why bother if it's the same? This deals with ℓ_1-ball). Shows that ℓ_1 balls cannot be Voronoi cells; all we know about Vcells

Proof We will show that

$$\Pr_{x \in \mathbb{R}^n}\left[\text{dist}(x, L) \ge \frac{\mu(L)}{2}\right] \ge 1/2$$

Assume not. Then, $\forall y$,

$$\Pr_x\left[\text{dist}(x, L) < \frac{\mu(L)}{2}\right] > 1/2$$

$$\Pr_x\left[\text{dist}(x+y, L) < \frac{\mu(L)}{2}\right] > 1/2 \Rightarrow \exists x \text{ s.t. } \text{dist}(x, L), \text{dist}(x+y, L) < \frac{\mu}{2}$$

$$\Downarrow$$

$\text{dist}(y, L) < \mu$. Contr. ∎

Local maxima of $\bar{\mu}(L)$ correspond to Voronoi cells in isotropic position.
(one that minimizes Z_2)

Conj (Slicing conj.) If K, $vol(K)=1$, is in isotropic position, then

$$Z_2(K) \leq C \cdot \sqrt{n}.$$

Thm Assuming Slicing, $\forall$ stable L, $\mu(L) \leq 2C \cdot \sqrt{n}$.
(if we assume cube is tight for symmetric slicing we get $\mu(L) \leq \frac{\sqrt{n}}{\sqrt{3}}$, nearly answering [SW16])
Unfortunately, best known bound on C is $O(n^{1/4})$
[BOURGAIN '91, KLARTAG '06]

THM $\forall$ stable L, $\mu(L) \leq 20 \log n \cdot \sqrt{n}$.

PROOF Since L is stable, so is L^*. $\left(\forall L' \subseteq L^*.\ \det(L') = \det(L^*) / \det(L^*/L') = (\det(L^*/L'))^{-1} = \det(\underbrace{(L^*/L')^*}_{\subseteq L}) \geq 1. \right)$

Therefore, by main thm,

$$\rho(10 \log n \cdot L^*) \leq 3/2.$$

This means that L has smoothing parameter $\leq 10 \log n$,
which is known to imply $\mu(L) \leq 10 \log n \cdot \sqrt{n}$.
(since using PSF, the function $x \mapsto \rho(\frac{L}{10 \log n} + x)$ is nearly constant). ∎

A Reverse Minkowski Theorem

Daniel Dadush
(CWI, Amsterdam)

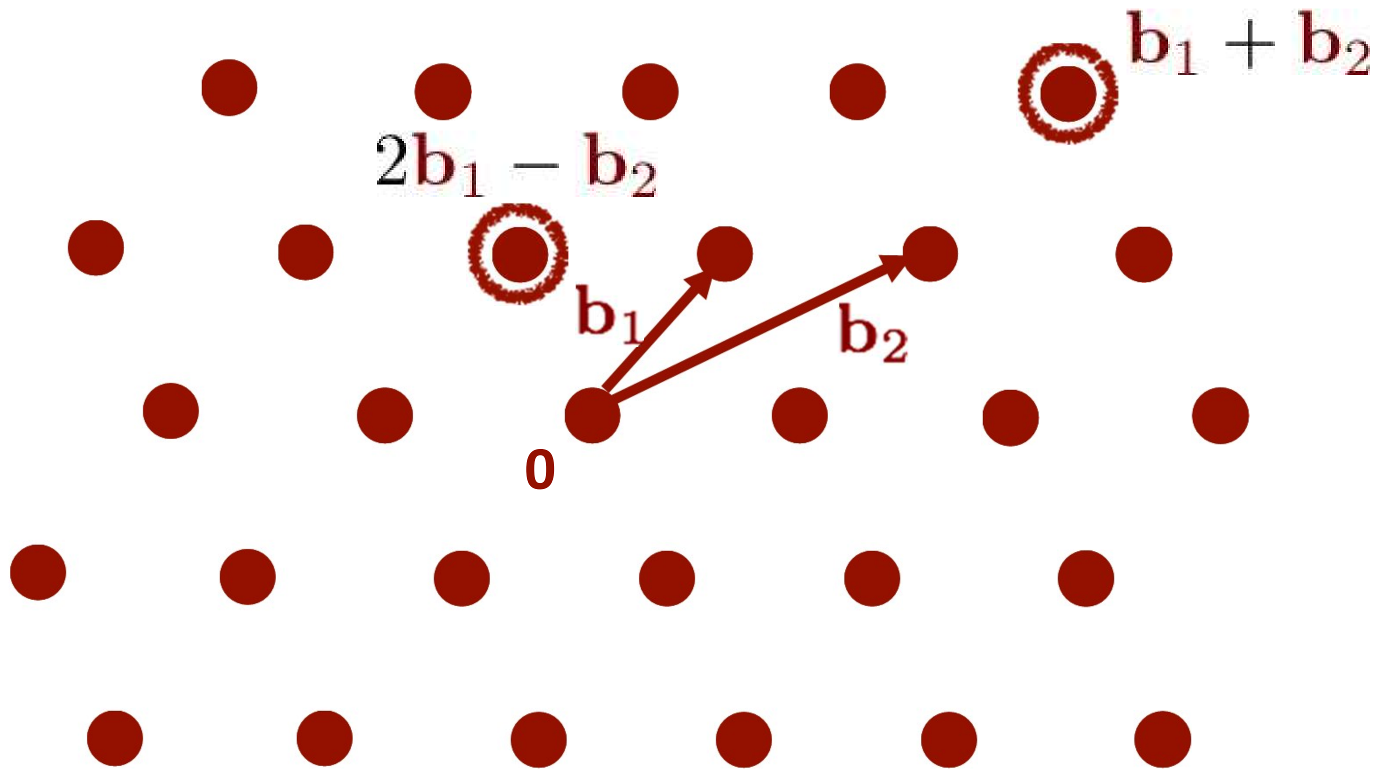
Oded Regev
(NYU)

Noah
Stephens-Davidowitz
(NYU)

X

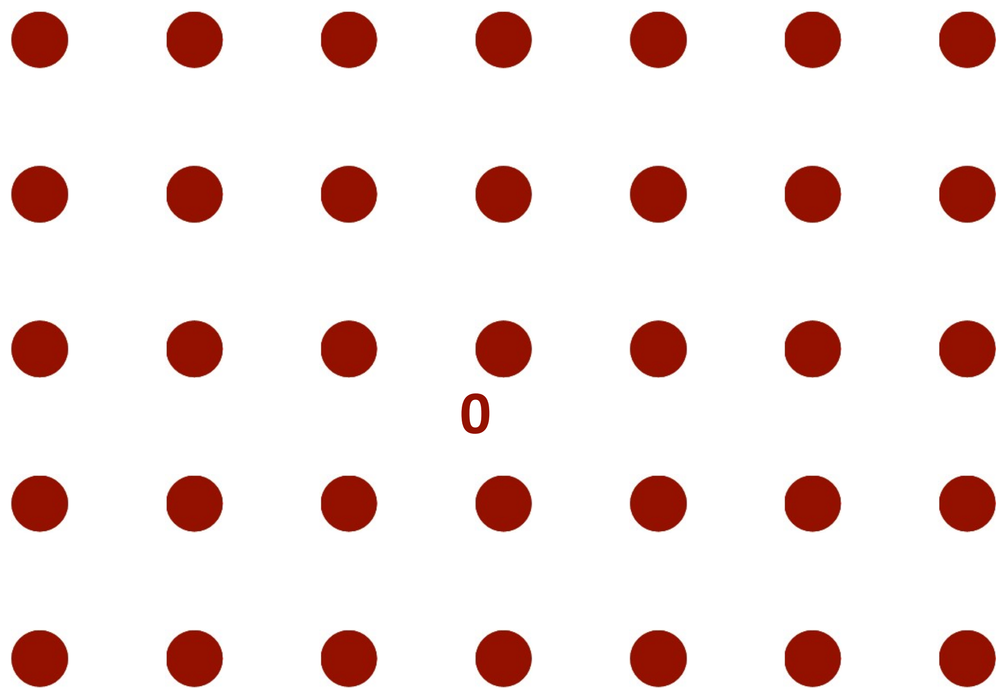
Lattices

- $\mathcal{L} = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_i \in \mathbb{Z}\}$
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of linearly independent vectors



Lattices

$$\mathbb{Z}^n = \{(z_1, \ldots, z_n) \; : \; z_i \in \mathbb{Z}\}$$

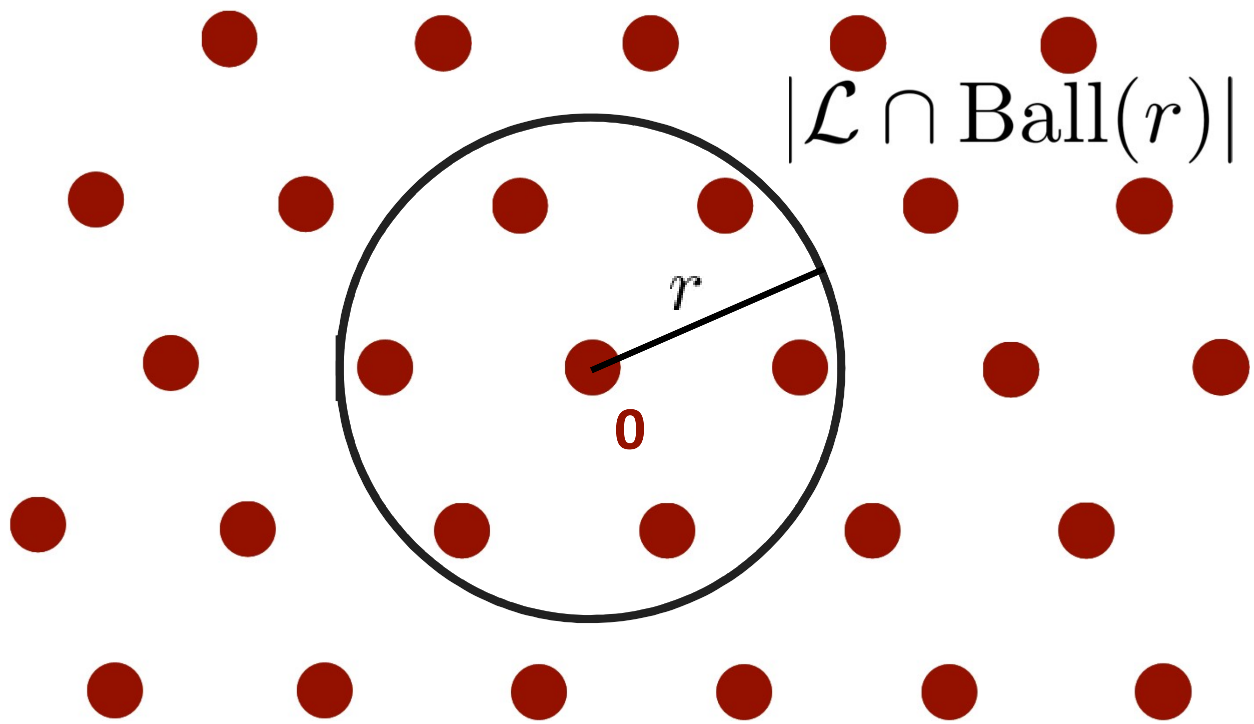


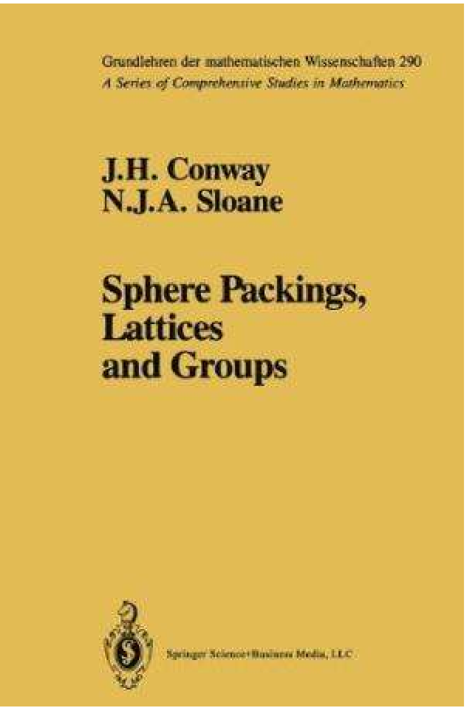
Applications

- Sphere packings
- (Algebraic) number theory, diophantine approximation,…
- Crystallography
- Coding theory, wireless communication,…
- Integer programming
- Computational complexity
- Cryptography
- Global warming
- And more…

Counting Lattice Points

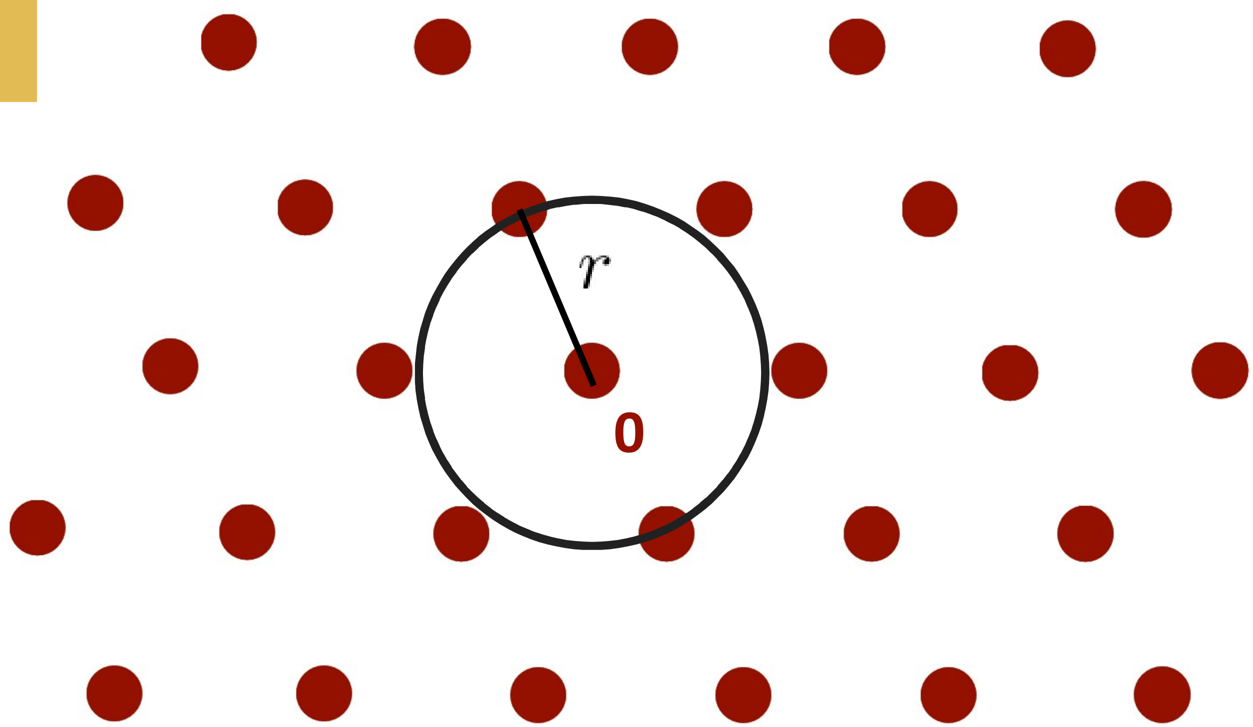
How many lattice points are there in a ball of radius r?





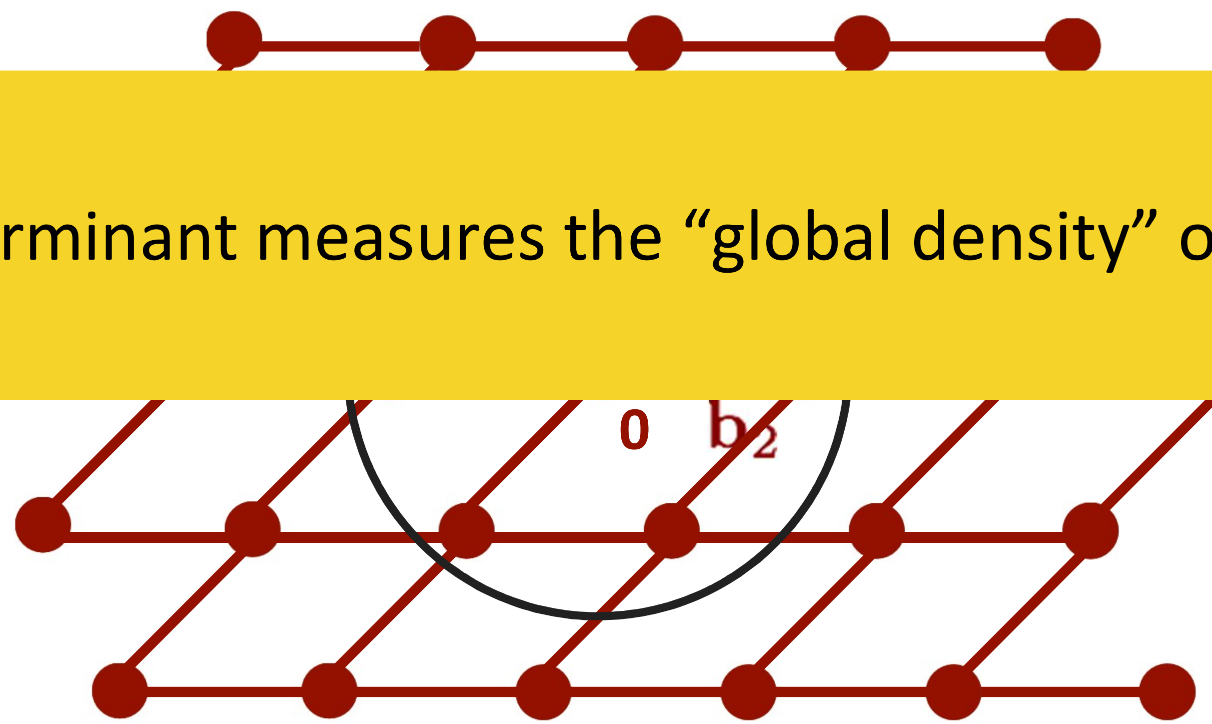
Shortest Vector / Sphere Packing

[Kepler 1611, Gauss 1831, Hales1998,Viazovska2016,...]



Determinant of a Lattice

$$\det(\mathcal{L}) = \lim_{r\to\infty} \frac{\mathrm{Vol}(\mathrm{Ball}(r))}{\mathcal{L} \cap \mathrm{Ball}(r)}$$
$$= \left|\det(B)\right|$$



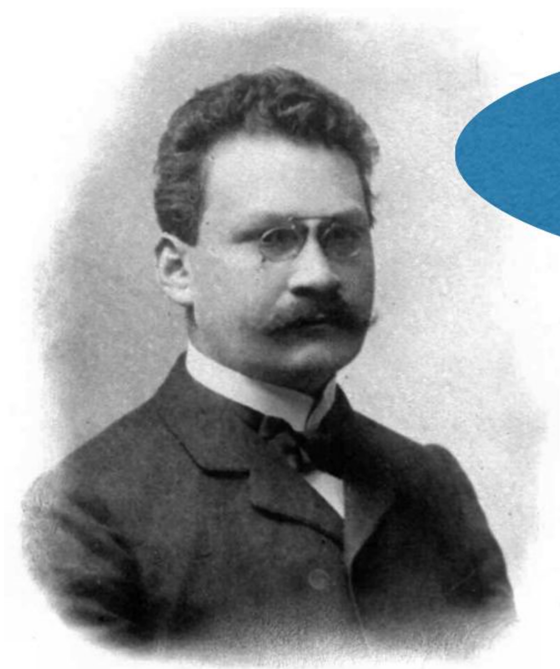
The determinant measures the "global density" of the lattice

Minkowski's Theorem

[Blichfeldt, van der Corput'36]

Thm: For any L with detL=1,

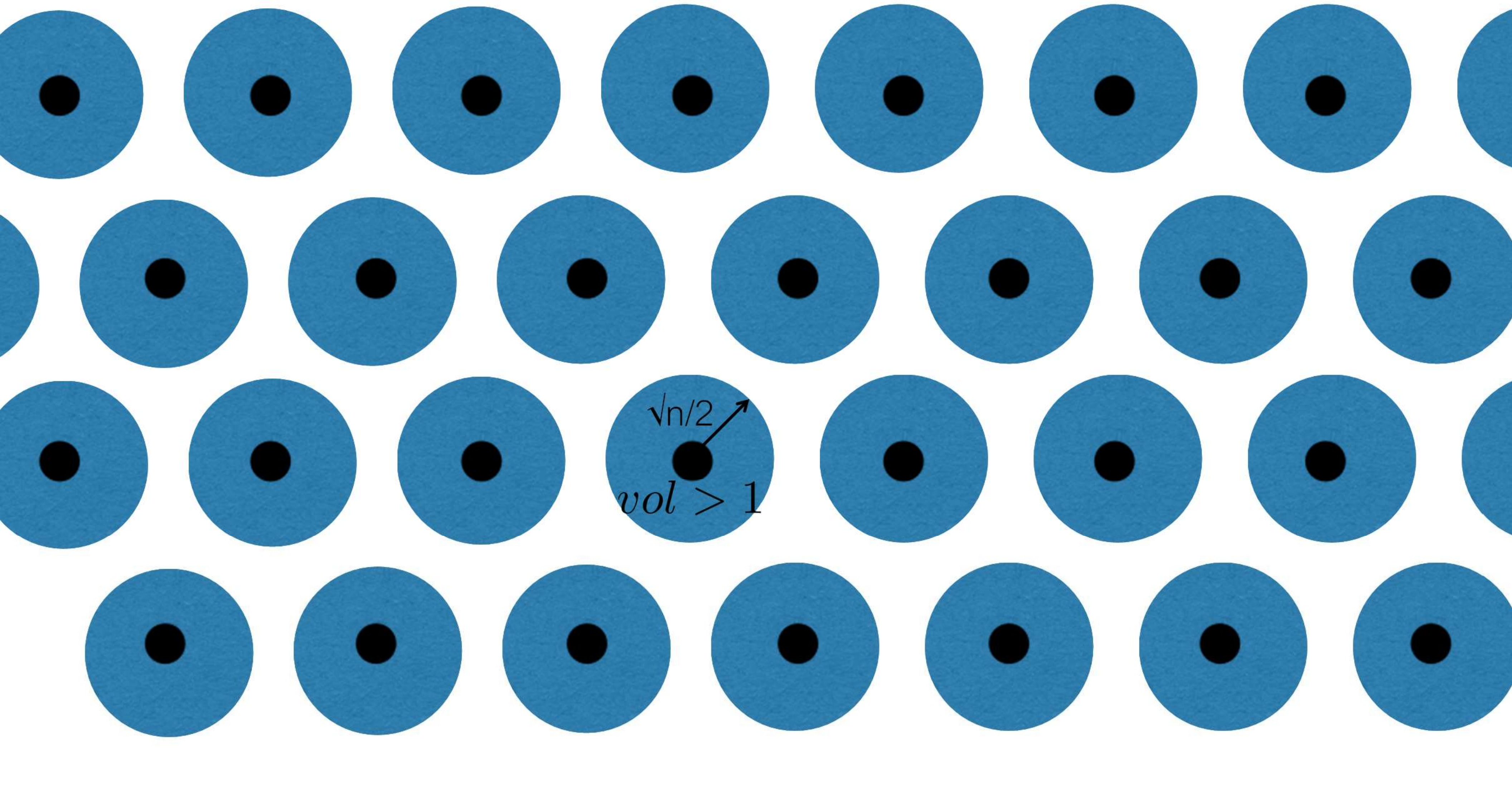
$$|\mathcal{L} \cap \mathrm{Ball}(\sqrt{n})| \geq 2^n$$



1891: **Global density implies local density!**

Minkowski's Theorem

Thm: For any L with detL=1, $|\mathcal{L} \cap \mathrm{Ball}(\sqrt{n})| \geq \cancel{2^n}$ 2



Converse?

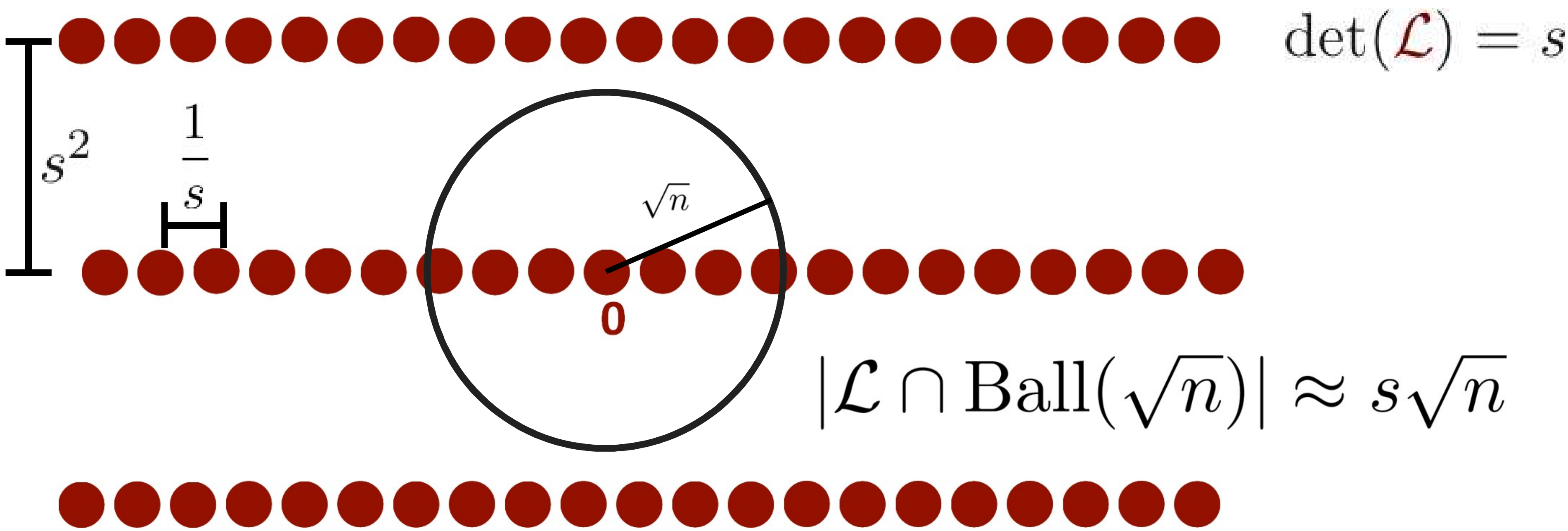
1891: **Global density implies local density!**

2012: Does local density imply global density?

Reverse Minkowski: First Attempt

If a lattice has more than 2^n points in a ball of radius $\sqrt{n}$, does it necessarily have determinant less than one?

No!



Reverse Minkowski: Second Attempt

If a lattice has more than 2^n points in a ball of radius $\sqrt{n}$, does it necessarily have a **sublattice** of determinant less than one?

THIS IS DADUSH'S CONJECTURE

MAIN THEOREM: YES!
Local density implies global density in a subspace!

Reverse Minkowski: The Theorem

Thm: If all sublattices of L have det ≥ 1, then $\forall r>0$, L has at most $\exp(C\cdot\log^2 n\cdot r^2)$ points of norm at most r

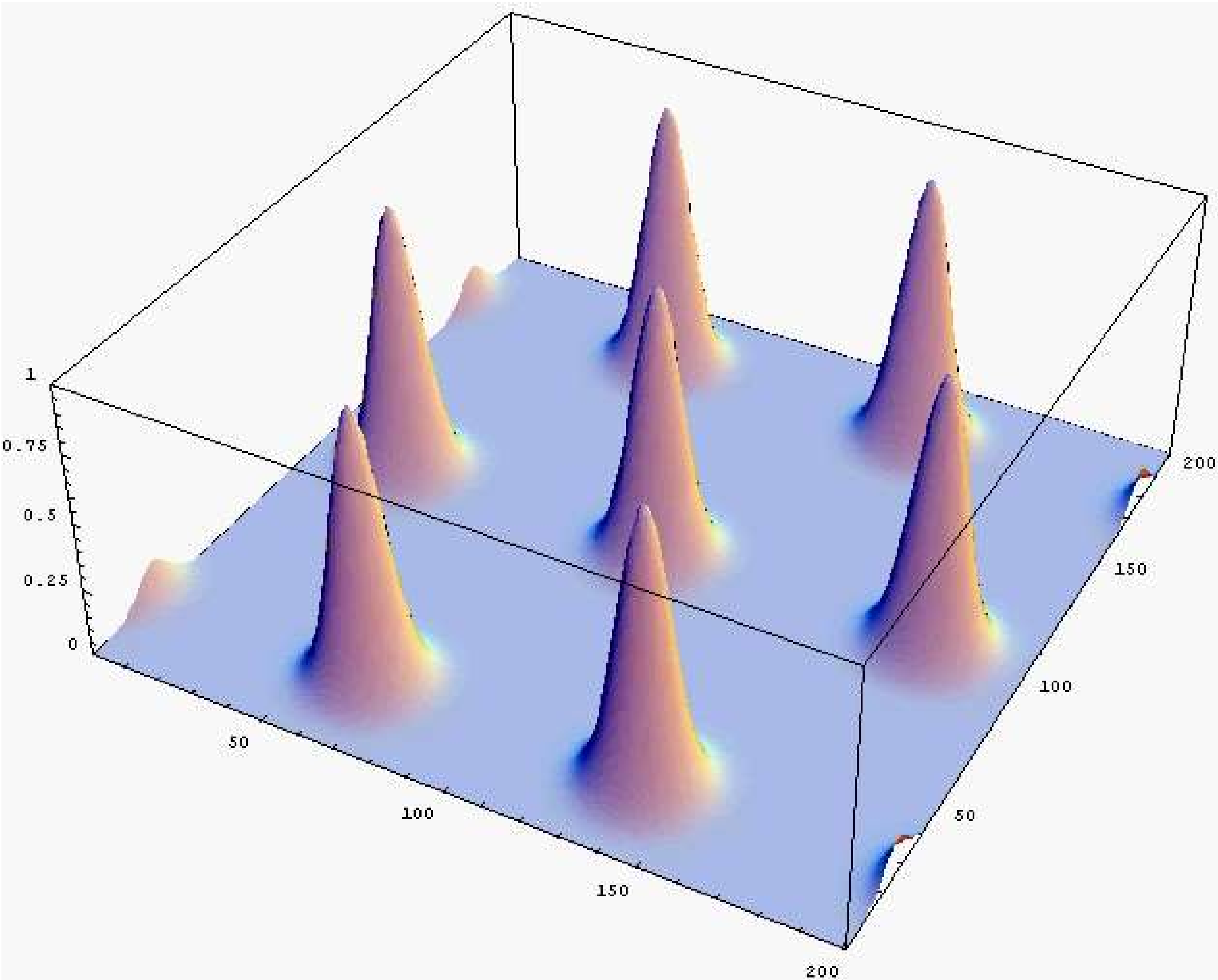
Remarks:

1. This is nearly tight for Z^n which has $\exp(c\cdot\log n\cdot r^2)$ points of norm at most r
2. Is Z^n the densest lattice?
3. Usually one cares about the "best" packing/covering/etc.; we care about the "worst"

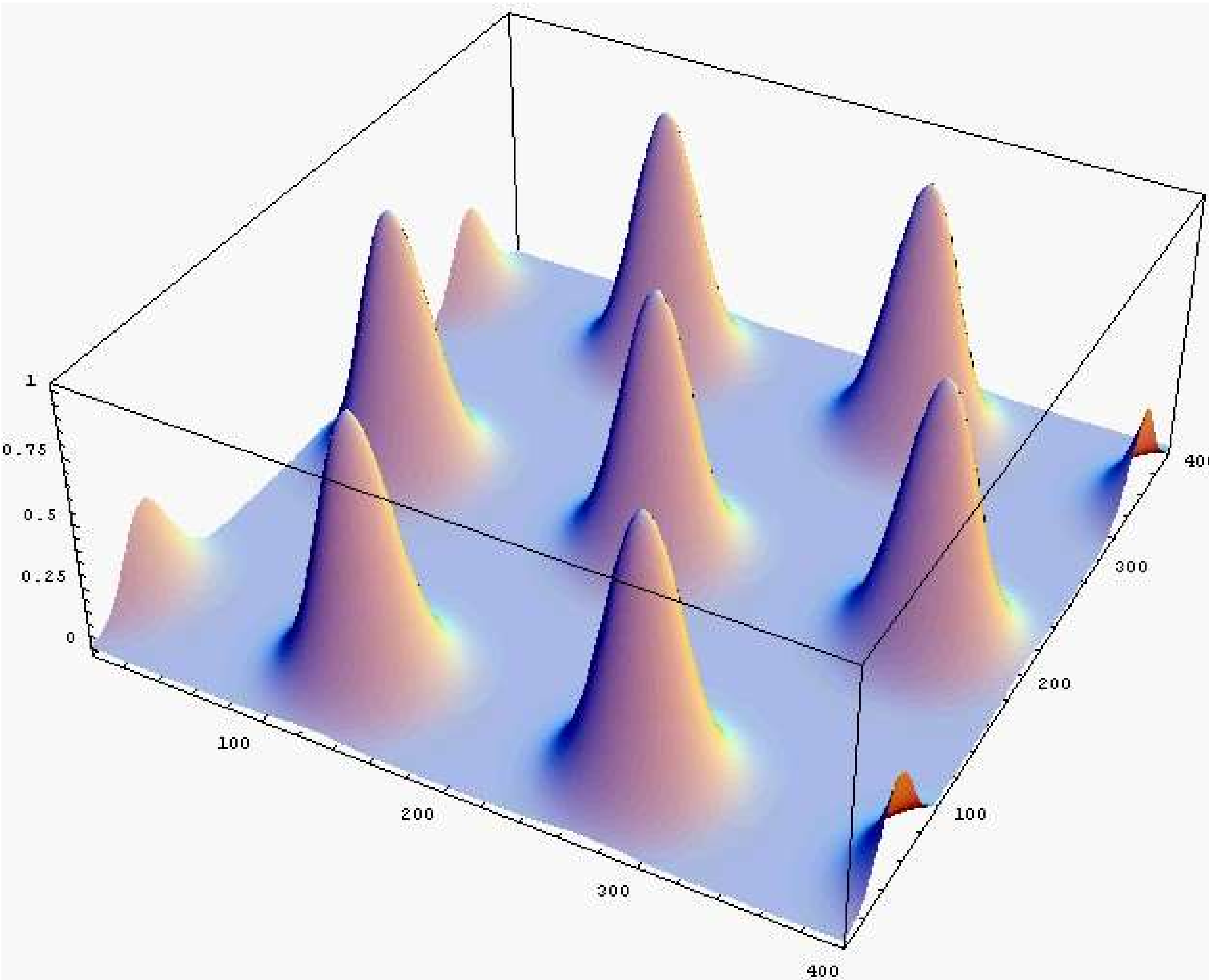
Applications of Reverse Minkowski [DadushR, FOCS'16]

- L_2 case of Kannan-Lovasz conjecture [KL88]
  - Characterizes *covering radius* in terms of determinants of sublattices
  - Motivation comes from Integer Programming
- Computational Complexity of lattice problems
  - NP certificate for "lots of lattice points"
- New hardness reductions in cryptographic applications
- Brownian motion on flat tori (question of Saloff-Coste)
  - ℓ_1 mixing time $\approx \ell_\infty$ mixing time

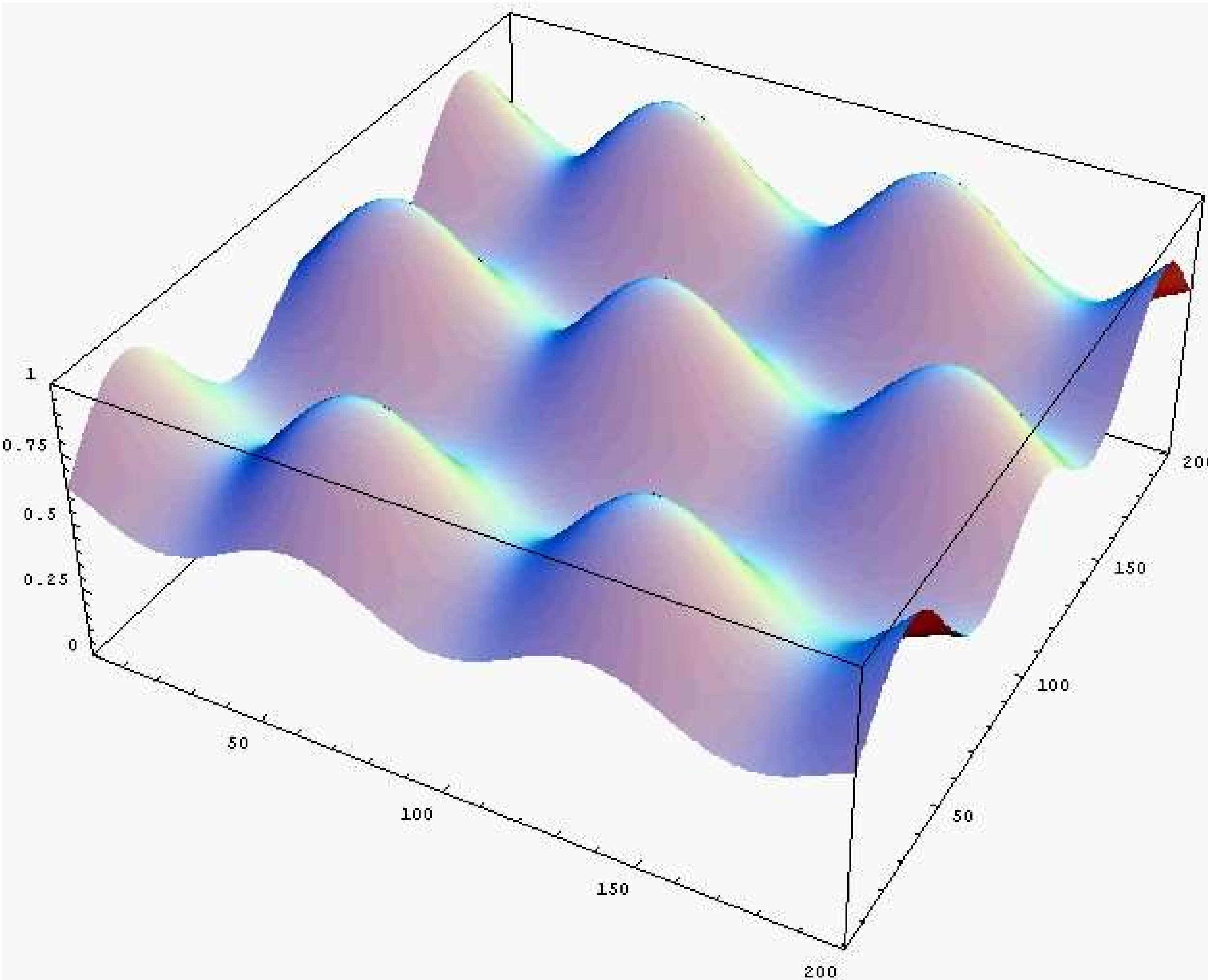
Mixing Time on Flat Tori



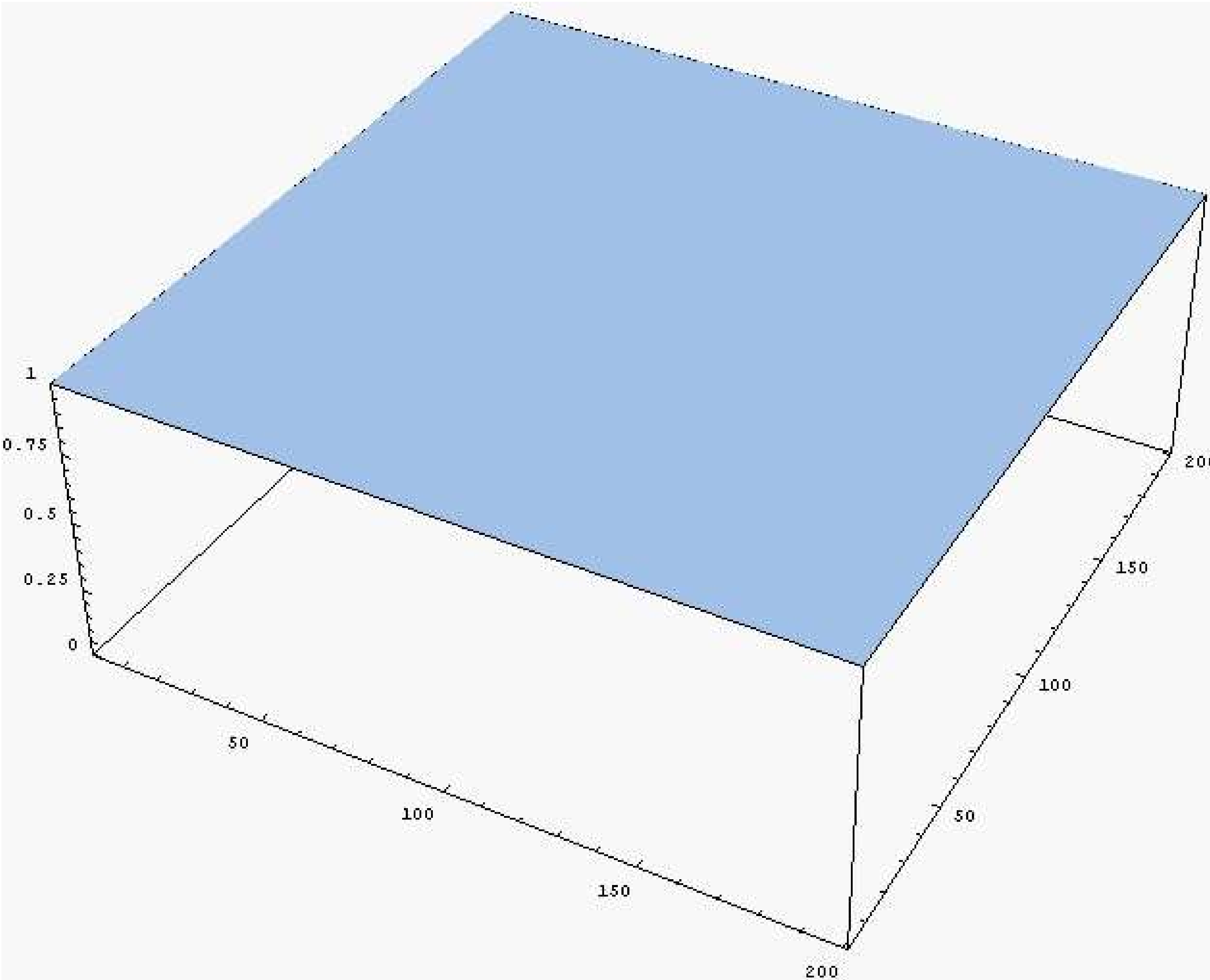
Mixing Time on Flat Tori



Mixing Time on Flat Tori



Mixing Time on Flat Tori



Applications of Reverse Minkowski [DadushR, FOCS'16]

- L_2 case of Kannan-Lovasz conjecture [KL88]
  - Characterizes *covering radius* in terms of determinants of sublattices
  - Motivation comes from Integer Programming
- Computational Complexity of lattice problems
  - NP certificate for "lots of lattice points"
- New hardness reductions in cryptographic applications
- Brownian motion on flat tori (question of Saloff-Coste)
  - ℓ_1 mixing time $\approx \ell_\infty$ mixing time

- Counterexample to strong variant of Freiman-Ruzsa conjecture over the integers (question of Ben Green) [LovettR16]
- New proof systems for lattice problems [AlamatiPeikertStephensdavid17]
- Connections with slicing conjecture [Dadush17]

The Proof