On Approximating the Covering Radius and Finding Dense Lattice Subspaces

Daniel Dadush
Centrum Wiskunde & Informatica (CWI)

ICERM April 2018
Outline

1. Integer Programming and the Kannan-Lovász (KL) Conjecture.

2. $\ell_2$ KL Conjecture & the Reverse Minkowski Conjecture.

3. Finding dense lattice subspaces.
Integer Programming (IP)

\[
\begin{align*}
\text{min } c x \\
\text{s.t. } A x & \leq b \\
x & \in \mathbb{Z}^n
\end{align*}
\]

\(n\) variables, \(m\) constraints

Open Question: Is there a \(2^{O(n)}\) time algorithm?

First result: \(2^{O(n^2)}\) \([\text{Lenstra `83}]\)

Best known complexity: \(n^{O(n)}\) \([\text{Kannan `87}]\)
Main Dichotomy

\[ \mu(K, \mathbb{Z}^n) := \text{smallest scaling } s \text{ such that every shift } sK + t \text{ contains an integer point.} \]

Either covering radius \( \mu(K, \mathbb{Z}^n) \leq 1 \).
Main Dichotomy

\[ \mu(K, \mathbb{Z}^n) := \text{smallest scaling } s \text{ such that every shift } sK + t \text{ contains an integer point.} \]

Either covering radius \( \mu(K, \mathbb{Z}^n) \leq 1 \).
Main Dichotomy

\[ \mu(K, \mathbb{Z}^n) := \text{smallest } s \text{ such that every shift } sK + t \text{ contains an integer point.} \]

Either covering radius \( \mu(K, \mathbb{Z}^n) \leq 1. \)
Main Dichotomy

$$\mu(K, \mathbb{Z}^n) := \text{smallest} \text{ scaling } s \text{ such that every shift } sK + t \text{ contains an integer point.}$$

$$\mu(K, \mathbb{Z}^2) = \frac{2}{3}$$

Either covering radius $$\mu(K, \mathbb{Z}^n) \leq 1.$$
Main Dichotomy

Either covering radius $\mu(K, \mathbb{Z}^n) \leq 1$.

Can find integer point in $2^{O(n)}$ time [D. 12].

Diagram of points in $\mathbb{Z}^2$ with a region marked $K$. The text explains that one of two cases must hold: either the covering radius is less than or equal to 1, or there exists an integer point within $2^{O(n)}$ time.
Main Dichotomy

Or $K$ is “flat”:

There exists rank $k \geq 1$ integer projection $P \in \mathbb{Z}^{n \times k}$ such that $\frac{1}{k} \text{vol}_k(PK)^1$ is small.
Main Dichotomy

Or $K$ is “flat”:

There exists rank $k \geq 1$ integer projection $P \in \mathbb{Z}^{n \times k}$ such $\text{vol}_k(PK)^{\frac{1}{k}}$ is small.
Main Dichotomy

Or $K$ is “flat”:

There exists rank $k \geq 1$ integer projection $P \in \mathbb{Z}^{n \times k}$ such that $\text{vol}_k(PK)^{\frac{1}{k}}$ is small.
Duality Relation

\[ 1 \leq \mu(K, \mathbb{Z}^n) \min_{P \in \mathbb{Z}^{k \times n}} \text{vol}_k(PK)^{\frac{1}{k}} \leq ? \]

Either covering radius \( \mu(K, \mathbb{Z}^n) \) is small or \( K \) is “flat”. 
$1 \leq \mu(K, \mathbb{Z}^n) \min_{\mathbf{p} \in \mathbb{Z}^{1 \times n}} \text{vol}_1(PK) \leq \tilde{O}(n^{4/3})$

[Khinchine `48, Babai `86, Hastad `86, Lenstra-Lagarias-Schnorr `87, Kannan-Lovasz `88, Banaszczyk `93-96, Banaszczyk-Litvak-Pajor-Szarek `99, Rudelson `00]
Kannan-Lovász Flatness Theorem

$$1 \leq \mu(K,\mathbb{Z}^n) \min_{P \in \mathbb{Z}^{k \times n}} \frac{1}{k} \text{vol}_k(PK)^{\frac{1}{k}} \leq n$$

[Kannan `87, Kannan-Lovász `88]
Kannan-Lovász (KL) Conjecture

\[ 1 \leq \mu(K, \mathbb{Z}^n) \min_{P \in \mathbb{Z}^{k \times n}} \text{vol}_k(PK)^{1/k} \leq O(\log n) \]
Faster Algorithm for IP?

\[ 1 \leq \mu(K, \mathbb{Z}^n) \min_{P \in \mathbb{Z}^{k \times n}} \frac{\text{vol}_k(PK)^1}{k} \leq O(\log n) \]

D. `12: Assuming KL conjecture

+ \( P \) computable in \((\log n)^{O(n)}\) time

then there is \((\log n)^{O(n)}\) time algorithm for IP.
\ell_2 \text{ Kannan-Lovász Conjecture}

Does the conjecture hold for ellipsoids?

An ellipsoid is $E = TB_2^n$
$\ell_2$ Kannan-Lovász Conjecture

Answer: YES* [Regev-S.Davidowitz 17]

* up to polylogarithmic factors
\( \ell_2 \) Kannan-Lovász Conjecture

Can we compute the projection \( P \)?

THIS TALK: YES, in \( 2^{O(n)} \) time.
Outline

1. Integer Programming and the Kannan-Lovász (KL) Conjecture.

2. $\ell_2$ KL Conjecture & the Reverse Minkowski Conjecture.

3. Finding dense lattice subspaces.
Easier to think of Euclidean ball vs general lattice.
A lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is $B \mathbb{Z}^n$ for a basis $B = (b_1, \ldots, b_n)$.

$L(B)$ denotes the lattice generated by $B$.

Note: a lattice has many equivalent bases.
A lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is $B\mathbb{Z}^n$ for a basis $B = (b_1, \ldots, b_n)$.

$\mathcal{L}(B)$ denotes the lattice generated by $B$.

The determinant of $\mathcal{L}$ is $|\det(B)|$. 

\[ b_1 \quad b_2 \]
A lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is $B\mathbb{Z}^n$ for a basis $B = (b_1, \ldots, b_n)$.

$\mathcal{L}(B)$ denotes the lattice generated by $B$.

The determinant of $\mathcal{L}$ is $|\det(B)|$.

Equal to volume of any tiling set.
\( \ell_2 \) Covering Radius

\[
\mu(\mathcal{L}) := \mu(B_2^n, \mathcal{L})
\]

Distance of farthest point to the lattice \( \mathcal{L} \).

Voronoi cell \( \mathcal{V} := \) all points closer to 0
Volumetric Lower Bounds

\[
\text{vol}_n \left( B_2^n \mu(\mathcal{L}) \right) \geq \text{vol}_n(\mathcal{V}) = \det(\mathcal{L})
\]

Voronoï cell \( \mathcal{V} \) := all points closer to \( 0 \)
Volumetric Lower Bounds

\[ \mu(\mathcal{L}) \geq \text{vol}_n(B_2^n)^{-\frac{1}{n}} \det(\mathcal{L})^{\frac{1}{n}} \]

Voronoi cell \( \mathcal{V} \) := all points closer to 0
Volumetric Lower Bounds

$$\mu(\mathcal{L}) \geq \sqrt{n} \det(\mathcal{L})^{\frac{1}{n}}$$

Voronoi cell $$\mathcal{V} :=$$ all points closer to 0
Volumetric Lower Bounds

\[ \mu(\mathcal{L}) \geq \mu(\mathcal{L}_{\perp W}) \]

\[ \mathcal{L}_{\perp W} \text{ projection onto } W \]
Volumetric Lower Bounds

\[ \mu(\mathcal{L}) \geq \mu(\mathcal{L}_{\downarrow W}) \geq \sqrt{k} \det(\mathcal{L}_{\downarrow W})^{\frac{1}{k}} \]

\[ \mathcal{L}_{\downarrow W} \text{ projection onto } W \]

\[ \dim(W) = k \geq 1 \]
Volumetric Lower Bounds

$$\mu(\mathcal{L}) \gtrsim \max_{\dim(W) = k \geq 1} \sqrt{k} \det(\mathcal{L}_{\downarrow W})^{\frac{1}{k}}$$

$\mathcal{L}_{\downarrow W}$ projection onto $W$

$\dim(W) = k \geq 1$
\( \ell_2 \) Kannan-Lovász Conjecture

Define \( C_{KL,2}(n) \) to be smallest number such that

\[
\mu(\mathcal{L}) \leq C_{KL,2}(n) \max_{\dim(W) = k \geq 1} \sqrt{k} \det(\mathcal{L}_{\downarrow W})^{1/k}
\]

for all lattices of dimension at most \( n \).

\[
C_{KL,2}(n) = \Omega(\sqrt{\log n})
\]

Lower bound for \( \mathcal{L} \) with basis \( e_1, \frac{1}{\sqrt{2}} e_2, \ldots, \frac{1}{\sqrt{n}} e_n \).
KL Bounds

\[ \mu(\mathcal{L}) \leq C_{KL,2}(n) \max_{\text{dim}(W)=k \geq 1} \sqrt{k} \det(\mathcal{L}_{\downarrow W})^{\frac{1}{k}} \]

Kannan-Lovász `88: \( \sqrt{n} \)

D. Regev `16: \( \log^{O(1)} n \)

Assuming Reverse Minkowski Conjecture.

Regev, S. Davidowitz `17: \( \log^{3/2} n \)

Reverse Minkowski Conjecture is proved!
Our Results

\( n \) dimensional lattice \( \mathcal{L} := \mathcal{L}(B) \)

1. Can compute subspace \( \mathcal{W}, \dim(\mathcal{W}) = k \geq 1 \)

\[
\mu(\mathcal{L}) \leq O(\log^{2.5} n) \sqrt{k} \det(\mathcal{L}_{\downarrow \mathcal{W}})^{\frac{1}{k}}
\]

in \( 2^{O(n)} \) time with high probability.

Prior work:
Kannan Lovász `88: \( \sqrt{n} \) in \( 2^{O(n)} \) time.
D. Micciancio `13: best subspace in \( n^{O(n^2)} \) time.
Our Results

$n$ dimensional lattice $\mathcal{L} := \mathcal{L}(B)$

2. Can combine lower bounds over different subspaces to certify $\mu(L)$ up to the slicing constant $L_n$ for “stable” Voronoi cells*.

* If $\text{vol}_n(\mathcal{V}) = 1$
  can find hyperplane $H$ s.t.
  $\text{vol}_{n-1}(\mathcal{V} \cap H) = \Omega\left(\frac{1}{L_n}\right)$
Our Results

$n$ dimensional lattice $\mathcal{L} := \mathcal{L}(B)$

2. Can combine lower bounds over different subspaces to certify $\mu(L)$ up to the slicing constant $L_n$ for “stable” Voronoi cells*.

Slicing Conjecture:

$L_n = O(1)$ for all convex bodies!

For “stable” Voronoi cells:

$L_n = O(\log n)$ \[RS \ '17\]
Notation

$M \subseteq \mathcal{L}$ sublattice of dimension $k$

Convention: $M = \{0\}$ then $\det(M) := 1$.

Normalized Determinant:

$\text{nd}(M) := \det(M)^{1/k}$

Projected Sublattice:

$\mathcal{L}/M := \mathcal{L}$ projected onto $\text{span}(M)^\perp$
Lower Bounds for Chains

Theorem [D. 17]:
For \( \{0\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_k = \mathcal{L} \) then

\[
\mu(\mathcal{L})^2 \gtrsim \sum_{i=1}^{k} \dim(\mathcal{L}_i/\mathcal{L}_{i-1}) \operatorname{nd}(\mathcal{L}/\mathcal{L}_{i-1})^2
\]

Only “missing ingredient”:
Combined with techniques from [R.S. `17] easily get tightness within slicing constant \( L_n \).
Lower Bounds for Chains

Theorem [D. 17]:
For \( \{0\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_k = \mathcal{L} \) then

\[
\mu(\mathcal{L})^2 \succsim \sum_{i=1}^k \dim(\mathcal{L}_i / \mathcal{L}_{i-1}) \text{nd}(\mathcal{L} / \mathcal{L}_{i-1})^2
\]

Proof Idea:
1. Establish SDP based lower bound: [D.R. `16]
   \[
   \mu(\mathcal{L})^2 \succsim \max \sum_i \text{rk}(P_i) \text{nd}(P_i \mathcal{L})^2
   \]
   s.t. \( \sum_i P_i^* P_i \preceq I_n \)

2. Build solution to above starting from any chain.
Lattice Density

\[
\lim_{r \to \infty} \frac{|\mathcal{L} \cap rB_2^n|}{\text{vol}_n(rB_2^n)} = \frac{1}{\det(\mathcal{L})}
\]
Lattice Density

$$\lim_{r \to \infty} \frac{|\mathcal{L} \cap rB_2^n|}{\text{vol}_n(rB_2^n)} = \frac{1}{\det(\mathcal{L})}$$

Global density of lattice points per unit volume
Minkowski’s First Theorem

\[ |\mathcal{L} \cap rB_2^n| \geq 2^{-n} \frac{\text{vol}_n(rB_2^n)}{\det(\mathcal{L})} \]

Global density implies “local density”
Reverse Minkowski Theorem

Regev-S. Davidowitz `17:
\( \mathcal{L} \) lattice dimension \( n \).
If all sublattices of \( \mathcal{L} \)
have determinant at least 1 then:

\( \mathcal{L} \) has at most \( 2^{O(\log^2 n r^2)} \) points at distance \( r \).

Almost tight: \( \mathbb{Z}^n \) has \( n^{\Omega(k)} \) points at distance \( r \)
for \( k \ll n \).
Outline

1. Integer Programming and the Kannan-Lovász (KL) Conjecture.

2. $\ell_2$ KL Conjecture & the Reverse Minkowski Conjecture.

3. Finding dense lattice subspaces.
Notation

\[ M \subseteq \mathcal{L} \text{ sublattice of dimension } k \]

Convention: \( M = \{0\} \) then \( \det(M) := 1 \).

Normalized Determinant:
\[ \text{nd}(M) := \det(M)^{1/k} \]

Projected Sublattice:
\[ \mathcal{L}/M := \mathcal{L} \text{ projected onto } \text{span}(M)^\perp \]
Densest Subspace Problem

\[ \text{nd}^*(\mathcal{L}) := \min_{M \subseteq \mathcal{L}, M \neq \{0\}} \text{nd}(M) \]

**\(\alpha\)-DSP:** Given \(\mathcal{L}\) find \(M \subseteq \mathcal{L}, M \neq \{0\}\) such that \(\text{nd}(M) \leq \alpha \text{ nd}^*(\mathcal{L})\).

**Remark:** dimension of \(M\) is not fixed!

Key primitive for finding sparse lattice projections. Will focus on this problem.
Densest Subspace Problem

Theorem:
Can solve $O(\log n)$-DSP in $2^{O(n)}$ time with high probability.

High Level Approach:
If $\mathcal{L}$ is not approximate minimizer:
find $y \neq 0$, orthogonal to actual minimizer, and recurse on $\mathcal{L} \cap y^\perp$
Canonical Polytope [Stuhler 76]

Let $\mathcal{L}$ be an $n$-dimensional lattice. The canonical polytope $\mathcal{P}(\mathcal{L})$ is the convex hull of the points $((k, \log \det(M)) : \text{sublattice } M \subseteq \mathcal{L}, \dim(M) = k)$.
Canonical Filtration [Stuhler 76]

$n$ dimensional lattice $\mathcal{L}$

Form Chain: $\{0\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_k = \mathcal{L}$
Canonical Filtration [Stuhler 76]

Form Chain: \( \{0\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_k = \mathcal{L} \)

Log det: \((0,0)\)

\(n\) dimensional lattice \(\mathcal{L}\)

Slope: \(\ln \text{nd}(\mathcal{L}_2/\mathcal{L}_1)\)
Stable Lattice [Stuhler 76]

$n$ dimensional lattice $\mathcal{L}$ is stable

I.e. no dense sublattices

If canonical filtration is trivial: $\{0\} \subset \mathcal{L}$
Stable Lattice [Stuhler 76]

Example: $\mathcal{L} = \mathbb{Z}^n$

$\mathbb{Z}^n$ has trivial filtration: $\{0\} \subset \mathbb{Z}^n$
1. Form Chain: \( \{0\} = \mathcal{L}_0 \subset \mathcal{L}_1 \subset \cdots \subset \mathcal{L}_k = \mathcal{L}. \)
2. Blocks \( \mathcal{L}_i / \mathcal{L}_{i-1} \) are stable.
3. Slope increasing: \( \text{nd}(\mathcal{L}_i / \mathcal{L}_{i-1}) < \text{nd}(\mathcal{L}_{i+1} / \mathcal{L}_i) \).
Densest Subspace Problem

\[ n \text{ dimensional lattice } \mathcal{L} \]

Want sublattice with approx. minimum slope.
Densest Subspace Problem

High Level Approach:
If $\mathcal{L}$ is not approximate minimizer:
find $y \neq 0$, orthogonal to actual minimizer,
and recurse on $\mathcal{L} \cap y^\perp$

Q: Where to find $y$?
A: The dual lattice $\mathcal{L}^*$

Q: How to find it in $\mathcal{L}^*$?
A: Discrete Gaussian sampling
A lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is $B\mathbb{Z}^n$ for a basis $B = (b_1, \ldots, b_n)$.

The dual lattice is
$$\mathcal{L}^* = \{y \in \text{span}(\mathcal{L}) : y^T x \in \mathbb{Z} \ \forall x \in \mathcal{L}\}$$
$\mathcal{L}^*$ is generated by $B^{-T}$.

Remark: $(\mathbb{Z}^n)^* = \mathbb{Z}^n$
A lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is $B\mathbb{Z}^n$ for a basis $B = (b_1, \ldots, b_n)$.

The dual lattice is

$$\mathcal{L}^* = \{y \in \text{span}(\mathcal{L}) : y^T x \in \mathbb{Z} \ \forall x \in \mathcal{L}\}$$

$\mathcal{L}^*$ is generated by $B^{-T}$.

$$\det(\mathcal{L}^*) = 1/\det(\mathcal{L})$$
Discrete Gaussian Distribution

\[ D_{\mathcal{L},s} := \Pr[y] \propto e^{-\|y\|^2 / s^2} \]

\[ s = 10 \]
Discrete Gaussian Distribution

\[ D_{\mathcal{L},s} := \Pr[y] \propto e^{-\|y\|^2/s^2} \]

**ADRS `15:**
Can sample in \(2^{n+o(n)}\) time for any parameter.

\[ s = 4 \]
Main Procedure

Repeat until $\mathcal{L} = \{0\}$

$s \leftarrow \text{nd}(\mathcal{L})$

Update $M \leftarrow \mathcal{L}$ if $\text{nd}(M) > s$

Sample $y \sim D_{\mathcal{L}^*, \frac{c}{s}}$ until $y \neq 0$

$\mathcal{L} \leftarrow \mathcal{L} \cap y^\perp$

Main Lemma: At any iteration, if $\mathcal{L}$ not $O(\log n)$ approximate minimizer, then $\mathcal{L} \cap y^\perp$ contains minimizer w.p. $\Omega(1)$.

Proc. finds apx minimizer with prob. $2^{-O(n)}$. 
Proof of Main Lemma

wlog \( \det(\mathcal{L}) = \det(\mathcal{L}^*) = 1 \)

\( \mathcal{L}_1 \subseteq \mathcal{L} \) densest sublattice

sample \( y \sim D_{\mathcal{L}^*,c} \)

If \( \text{nd}(\mathcal{L}_1) \ll \frac{1}{\log n} \)

must show that \( y \neq 0 \) and \( y \perp \mathcal{L}_1 \) w.p. \( \Omega(1) \).
\[ \det(\mathcal{L}) = \det(\mathcal{L}^*) = 1 \]
\[ \mathcal{L}_1 \subseteq \mathcal{L} \text{ densest sublattice, } \text{nd}(\mathcal{L}_1) \ll \frac{1}{\log n} \]

Sample \( y \sim D_{\mathcal{L}^*,c} \)

Want:
1. \( \Pr[y = 0] \leq \epsilon \)
2. \( \Pr[y \in \mathcal{L}^* \cap \mathcal{L}_1^\perp] \geq 1 - \epsilon \)
\[ \det(\mathcal{L}) = \det(\mathcal{L}^*) = 1 \]

1. \[ \Pr_{y \sim \mathcal{D}_{\mathcal{L}^*,c}}[y = 0] = \frac{1}{\rho_c(\mathcal{L}^*)} \leq \frac{1}{|\mathcal{L}^* \cap \sqrt{n}B_2^n| e^{-n/c^2}} \leq \frac{1}{2ne^{-n/c^2}} = o(1) \]

(By Minkowski)

\[ \rho_c(A) := \sum_{x \in A} e^{-\|x/c\|^2} \]
\[
\det(\mathcal{L}) = \det(\mathcal{L}^*) = 1
\]
\[
\mathcal{L}_1 \subseteq \mathcal{L} \text{ densest sublattice}, \text{ nd}(\mathcal{L}_1) \ll 1/\log n
\]
\[
W := \mathcal{L}_1^\perp
\]

2. \[
\Pr_{y \sim D_{\mathcal{L}^*, c}} [y \in W] = \frac{\rho_c(\mathcal{L}^* \cap W)}{\rho_c(\mathcal{L}^*)}
\]
(ortho. is worst-case) \[
\geq \frac{\rho_c(\mathcal{L}^* \cap W)}{\rho_c(\mathcal{L}^* \cap W) \rho_c(\mathcal{L}^*/W)\rho_c(\mathcal{L}^*/W)} = \frac{1}{\rho_c(\mathcal{L}^*/W)}
\]

\[
\rho_c(A) := \sum_{x \in A} e^{-\|x/c\|^2}
\]
\[ \det(\mathcal{L}) = \det(\mathcal{L}^*) = 1 \]

\( \mathcal{L}_1 \subseteq \mathcal{L} \) densest sublattice, \( \text{nd}(\mathcal{L}_1) \ll 1/\log n \)

\( W := \mathcal{L}_1^\perp \)

2. Need to show \( \rho_c(\mathcal{L}^*/W) \leq 1 + o(1) \)

Key: \( \text{nd}^*(\mathcal{L}^*/W) = 1/\text{nd}(\mathcal{L}_1) \gg \log n \)

Reverse-Minkowski \( \Rightarrow \)

\[ |(\mathcal{L}^*/W) \cap rB_2^n| \ll e^{o(r^2)}, \forall r \geq 0 \]

\[
\rho_c(A) := \sum_{x \in A} e^{-\|x/c\|^2}
\]
Canonical Polytope of $\mathcal{L}^*$?

Assumption: $\det(\mathcal{L}) = 1$

Log det

Slope: $\ln \operatorname{nd}(\mathcal{L}_1)$

$\mathcal{L}_1$

$\mathcal{L}_2$

$(0,0)$

$\{0\}$

$(n,0)$

Assumption: $\det(\mathcal{L}) = 1$
Canonical Polytope of $\mathcal{L}^*$?

$\det(\mathcal{L}^*) = 1$

Map $M \rightarrow \mathcal{L}^* \cap M^\perp$
 Canonical Polytope of $\mathcal{L}^*$?

$$\det(\mathcal{L}^*) = 1$$

Slope: $-\ln \text{nd}(\mathcal{L}_1)$

$\mathcal{P}(\mathcal{L}^*)$ is “reflection” of $\mathcal{P}(\mathcal{L})$
Conclusions

1. Algorithmic version of $\ell_2$ Kannan-Lovász conjecture via discrete Gaussian sampling.
2. Lower bound certificates for covering radius that are tight within $O(1)$ under slicing conjecture.

Open Problem

1. Prove KL conjecture for general convex bodies.
2. Prove Slicing conjecture for Voronoi cells.