Limits on the Hardness of Lattice Problems in ℓ_p Norms

Chris Peikert

SRI International

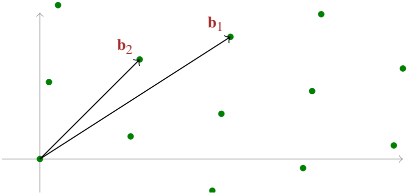
Complexity 2007

Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$

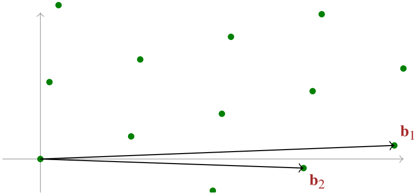


Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$

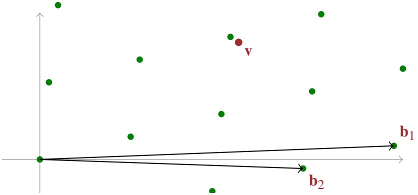


Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Close Vector Problem (CVP$_\gamma$)

Approximation factor $\gamma = \gamma(n)$, in some norm $\|\cdot\|$.

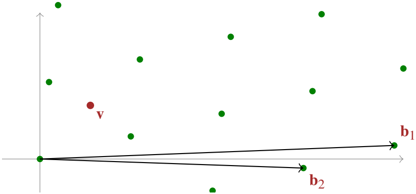
- Given basis $\mathbf{B}$ and point $\mathbf{v} \in \mathbb{R}^n$, distinguish $\text{dist}(\mathbf{v}, \mathcal{L}) \leq 1$ from $\text{dist}(\mathbf{v}, \mathcal{L}) > \gamma$ (otherwise, don't care.)

Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Close Vector Problem (CVP_γ)

Approximation factor $\gamma = \gamma(n)$, in some norm $\|\cdot\|$.

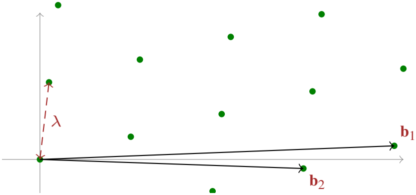
- Given basis $\mathbf{B}$ and point $\mathbf{v} \in \mathbb{R}^n$, distinguish
  $\text{dist}(\mathbf{v}, \mathcal{L}) \le 1$ from $\text{dist}(\mathbf{v}, \mathcal{L}) > \gamma$ (otherwise, don't care.)

Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} \quad = \quad \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Short Vector Problem (SVP_γ)

Define minimum distance $\lambda = \min \|\mathbf{v}\|$ over all $0 \neq \mathbf{v} \in \mathcal{L}$.

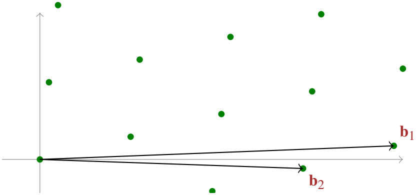
- Given basis $\mathbf{B}$, distinguish
  $\lambda \leq 1$ from $\lambda > \gamma$ (otherwise, don't care.)

Lattices and Their Problems

Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ be linearly independent.

The n-dim lattice $\mathcal{L}$ having basis $\mathbf{B}$ is:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Short Vector Problem (SVP$_\gamma$)

Define minimum distance $\lambda = \min \|\mathbf{v}\|$ over all $0 \neq \mathbf{v} \in \mathcal{L}$.

- Given basis $\mathbf{B}$, distinguish
  $\lambda \leq 1$ from $\lambda > \gamma$ (otherwise, don't care.)

Usually use ℓ_p norm: $\|\mathbf{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$.

Algorithms and Hardness

Algorithms for SVP$_\gamma$ & CVP$_\gamma$

- $\gamma(n) \sim 2^n$ approximation in poly-time [LLL,Babai,Schnorr]
- Time/approximation tradeoffs: $\gamma(n) \sim n^c$ in time $\sim 2^{n/c}$ [AKS]

Algorithms and Hardness

Algorithms for SVP$_\gamma$ & CVP$_\gamma$

- $\gamma(n) \sim 2^n$ approximation in poly-time [LLL,Babai,Schnorr]
- Time/approximation tradeoffs: $\gamma(n) \sim n^c$ in time $\sim 2^{n/c}$ [AKS]

NP-Hardness **(some randomized reductions...)**

- In any ℓ_p norm, SVP$_\gamma$ hard for any $\gamma(n) = O(1)$ [Ajt,Micc,Khot,ReRo]
- In any ℓ_p norm, CVP$_\gamma$ hard for any $\gamma(n) = n^{O(1/\log\log n)}$ [DKRS,Dinur]
- Many other problems (CVPP, SIVP) hard as well ...

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\mathrm{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\mathrm{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]
- In ℓ_2 norm, $\mathrm{CVP}_\gamma \in$ coNP for $\gamma \sim \sqrt{n}$ [AharonovRegev]

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]
- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coNP for $\gamma \sim \sqrt{n}$ [AharonovRegev]
- CVP_γ is as hard as many other lattice problems [GMSS,GMR]

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]
- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coNP for $\gamma \sim \sqrt{n}$ [AharonovRegev]
- CVP_γ is as hard as many other lattice problems [GMSS,GMR]

Neat. What else?

- In ℓ_2 norm, $\text{SVP}_\gamma \leq$ avg-problems for $\gamma \sim n$ [Ajtai,...,MR,Regev]
- For lattice problems, ℓ_2 norm is easiest [RegevRosen]
- Much, much more... [LLM,PR]

‘Positive’ Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]
- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coNP for $\gamma \sim \sqrt{n}$ [AharonovRegev]
- CVP_γ is as hard as many other lattice problems [GMSS,GMR]

Neat. What else?

- In ℓ_2 norm, $\text{SVP}_\gamma \leq$ avg-problems for $\gamma \sim n$ [Ajtai,...,MR,Regev]
- For lattice problems, ℓ_2 norm is easiest [RegevRosen]
- Much, much more... [LLM,PR]

'Positive' Results (Limits on Hardness)

Could problems be NP-hard for much larger $\gamma(n)$?
Probably not.

- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coAM for $\gamma \sim \sqrt{n/\log n}$ [GoldreichGoldwasser]
- In ℓ_2 norm, $\text{CVP}_\gamma \in$ coNP for $\gamma \sim \sqrt{n}$ [AharonovRegev]
- CVP_γ is as hard as many other lattice problems [GMSS,GMR]

Neat. What else?

- In ℓ_2 norm, $\text{SVP}_\gamma \leq$ avg-problems for $\gamma \sim n$ [Ajtai,...,MR,Regev]
- For lattice problems, ℓ_2 norm is easiest [RegevRosen]
- Much, much more... [LLM,PR]

(Can generalize to ℓ_p norms, but lose up to $\sqrt{n}$ factors.)

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\text{CVP}_\gamma \in \text{coNP}$ for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\text{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\text{CVP}_\gamma \in \text{coNP}$ for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\text{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\mathrm{CVP}_\gamma \in$ coNP for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\mathrm{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\mathrm{CVP}_\gamma \in \mathrm{coNP}$ for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\mathrm{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\mathrm{CVP}_\gamma \in \mathrm{coNP}$ for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\mathrm{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Techniques

- New analysis of prior algorithms [AharRegev,MiccRegev,Regev,...]
- General analysis of discrete Gaussians over lattices
- Introduce ideas from [Ban95] to complexity

Our Results

- Extend positive results to ℓ_p norms, $p \geq 2$, for same factors $\gamma(n)$.

New Limits on Hardness

- In ℓ_p norm, $\mathsf{CVP}_\gamma \in \mathsf{coNP}$ for $\gamma = c_p \cdot \sqrt{n}$
- In ℓ_p norm, $\mathsf{SVP}_\gamma \leq$ avg-problems for $\gamma \sim c_p \cdot n$
- Generalize to norms defined by arbitrary convex bodies

Techniques

- New analysis of prior algorithms [AharRegev,MiccRegev,Regev,...]
- General analysis of discrete Gaussians over lattices
- Introduce ideas from [Ban95] to complexity

A Bit Odd

- Can't show anything new for $1 \leq p < 2$...

Interpretation and Open Problems

1. Partial converse of [RegevRosen] ("ℓ_2 is easiest").

Interpretation and Open Problems

1. Partial converse of [RegevRosen] ("ℓ_2 is easiest").

2. Weakens assumptions for lattice-based cryptography.

Interpretation and Open Problems

1. Partial converse of [RegevRosen] ("ℓ_2 is easiest").
2. Weakens assumptions for lattice-based cryptography.
3. What's going on with $p < 2$?
   (Beating $n^{1/p}$ for even a single p has implications for codes.)

Interpretation and Open Problems

1. Partial converse of [RegevRosen] ("ℓ_2 is easiest").
2. Weakens assumptions for lattice-based cryptography.
3. What's going on with $p < 2$?

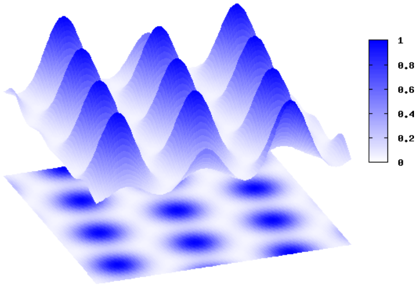
   (Beating $n^{1/p}$ for even a single p has implications for codes.)
4. Are all ℓ_p norms ($p \geq 2$) equivalent?

Gauss meets Lattices

Define Gaussian function $\rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2)$ over $\mathbb{R}^n$.

Gauss meets Lattices

Define Gaussian function $\rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2)$ over $\mathbb{R}^n$.

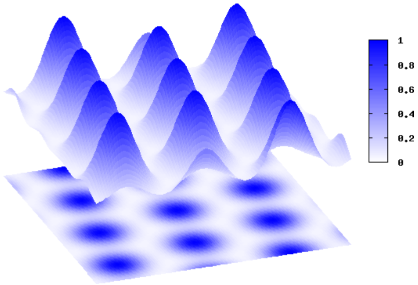


Define

$$f(\mathbf{x}) = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x}-\mathbf{v})}{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{v})} = \frac{\rho(\mathcal{L}-\mathbf{x})}{\rho(\mathcal{L})}.$$

Gauss meets Lattices

Define Gaussian function $\rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2)$ over $\mathbb{R}^n$.



Define

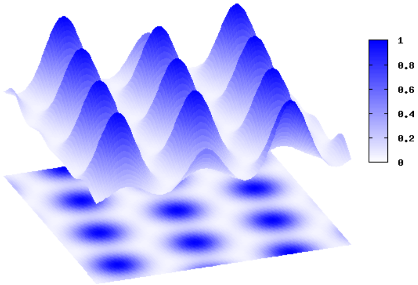
$$f(\mathbf{x}) = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x}-\mathbf{v})}{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{v})} = \frac{\rho(\mathcal{L}-\mathbf{x})}{\rho(\mathcal{L})}.$$

Properties of f

- If $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \le \frac{1}{10}$, then $f(\mathbf{x}) \ge \frac{1}{2}$. (Easy.)
- If $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) > \sqrt{n}$, then $f(\mathbf{x}) < 2^{-n}$. (Really hard. [Ban93])

Gauss meets Lattices

Define Gaussian function $\rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2)$ over $\mathbb{R}^n$.



Define

$$f(\mathbf{x}) = \frac{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{x}-\mathbf{v})}{\sum_{\mathbf{v}\in\mathcal{L}} \rho(\mathbf{v})} = \frac{\rho(\mathcal{L}-\mathbf{x})}{\rho(\mathcal{L})}.$$

Properties of f

- If $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \le \frac{1}{10}$, then $f(\mathbf{x}) \ge \frac{1}{2}$. (Easy.)
- If $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) > \sqrt{n}$, then $f(\mathbf{x}) < 2^{-n}$. (Really hard. [Ban93])

Enter Aharonov & Regev…

- A compact & verifiable representation of $f \Rightarrow \mathrm{CVP}_{10\sqrt{n}} \in \mathrm{coNP}$.

Measure Inequalities (for ℓ_2)

Lemma [Ban93]

For any lattice $\mathcal{L}$ and $\mathbf{x} \in \mathbb{R}^n$,

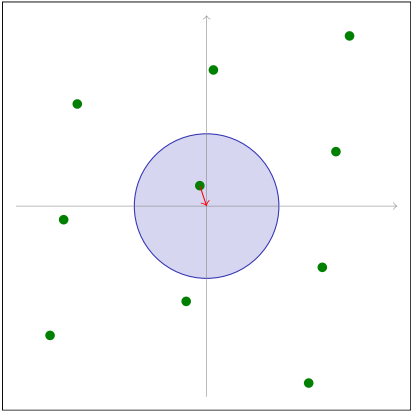
$$\frac{\rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)}{\rho(\mathcal{L})} < 2^{-n}.$$

Measure Inequalities (for ℓ_2)

Lemma [Ban93]

For any lattice $\mathcal{L}$ and $\mathbf{x} \in \mathbb{R}^n$,

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)}{\rho(\mathcal{L})} < 2^{-n}.$$

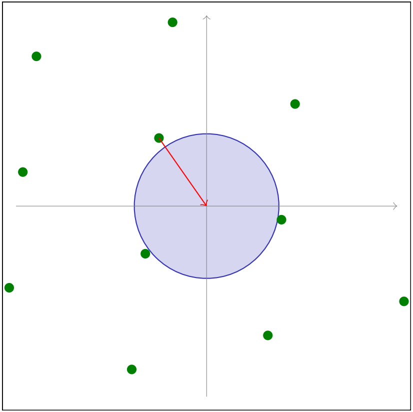


Measure Inequalities (for ℓ_2)

Lemma [Ban93]

For any lattice $\mathcal{L}$ and $\mathbf{x} \in \mathbb{R}^n$,

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)}{\rho(\mathcal{L})} < 2^{-n}.$$



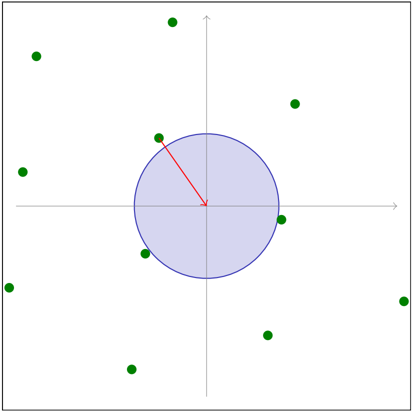
- Say $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) > \sqrt{n}$.
- Then $\rho(\mathcal{L} - \mathbf{x}) = \rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)$.
- Therefore $f(\mathbf{x}) = \frac{\rho(\mathcal{L} - \mathbf{x})}{\rho(\mathcal{L})} < 2^{-n}$.

Measure Inequalities (for ℓ_2)

Lemma [Ban93]

For any lattice $\mathcal{L}$ and $\mathbf{x} \in \mathbb{R}^n$,

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)}{\rho(\mathcal{L})} < 2^{-n}.$$



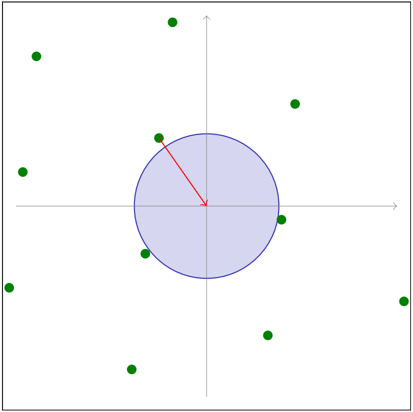
- Say $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) > \sqrt{n}$.
- Then
  $\rho(\mathcal{L} - \mathbf{x}) = \rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)$.
- Therefore $f(\mathbf{x}) = \frac{\rho(\mathcal{L} - \mathbf{x})}{\rho(\mathcal{L})} < 2^{-n}$.

Measure Inequalities (for ℓ_2)

Lemma [Ban93]

For any lattice $\mathcal{L}$ and $\mathbf{x} \in \mathbb{R}^n$,

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)}{\rho(\mathcal{L})} < 2^{-n}.$$



- Say $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) > \sqrt{n}$.
- Then $\rho(\mathcal{L} - \mathbf{x}) = \rho((\mathcal{L} - \mathbf{x}) \setminus \sqrt{n} \cdot \mathcal{B}_2)$.
- Therefore $f(\mathbf{x}) = \frac{\rho(\mathcal{L} - \mathbf{x})}{\rho(\mathcal{L})} < 2^{-n}$.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

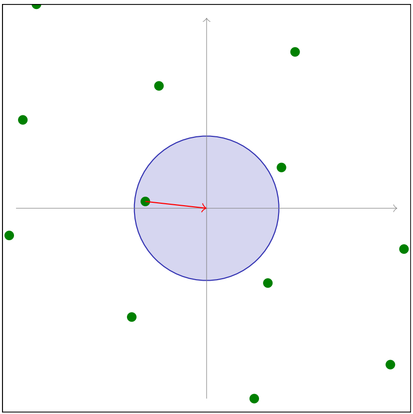
$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$

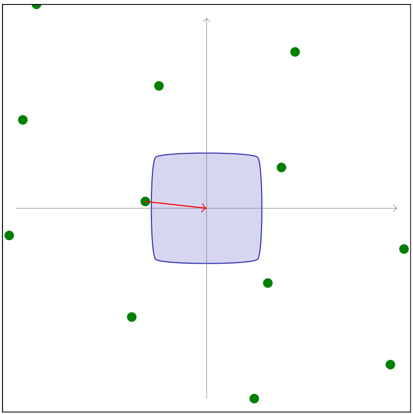


Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Say $p \geq 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

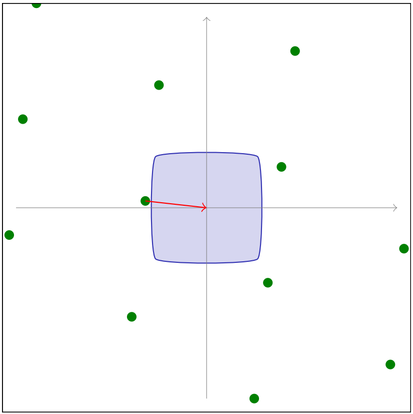
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- If $d \leq \frac{n^{1/p - 1/2}}{10}$, then $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, and $f(\mathbf{x}) \geq 1/2$.
- Therefore in ℓ_p norm, $\mathrm{CVP}_{10 c_p \sqrt{n}} \in \mathrm{coNP}$.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Say $p \geq 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

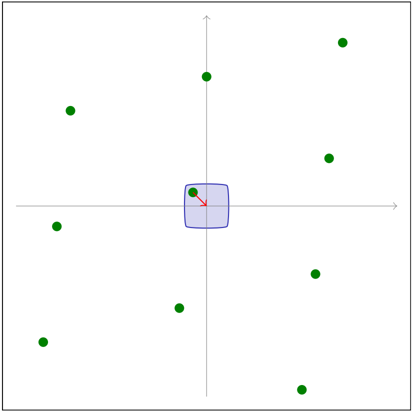
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- If $d \leq \frac{n^{1/p-1/2}}{10}$, then $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, and $f(\mathbf{x}) \geq 1/2$.
- Therefore in ℓ_p norm, $\mathrm{CVP}_{10 c_p \sqrt{n}} \in$ coNP.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Say $p \geq 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

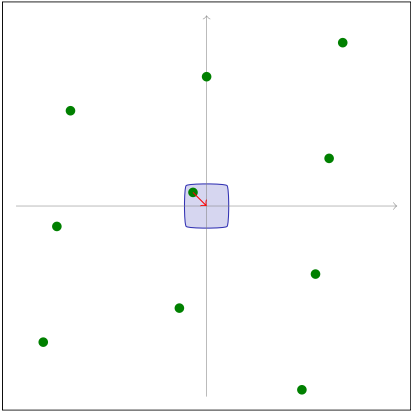
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- If $d \leq \frac{n^{1/p-1/2}}{10}$, then $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, and $f(\mathbf{x}) \geq 1/2$.
- Therefore in ℓ_p norm, $\mathrm{CVP}_{10 c_p \sqrt{n}} \in$ coNP.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Say $p \geq 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

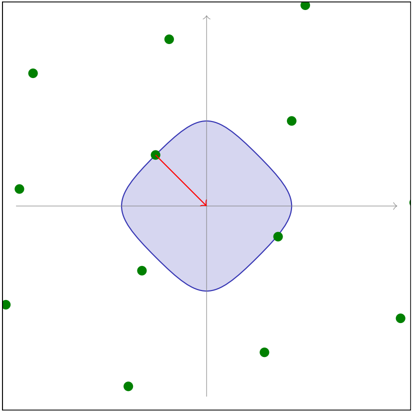
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- If $d \leq \frac{n^{1/p-1/2}}{10}$, then $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, and $f(\mathbf{x}) \geq 1/2$.
- Therefore in ℓ_p norm, $\mathrm{CVP}_{10 c_p \sqrt{n}} \in \mathrm{coNP}$.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Now say $p < 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

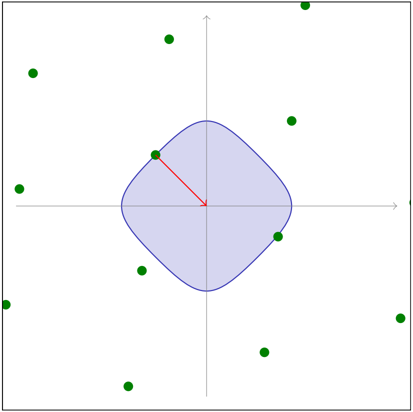
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- To guarantee $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, we need $d \leq \frac{1}{10}$.
- Only a $\sim n^{1/p}$ gap.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Now say $p < 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

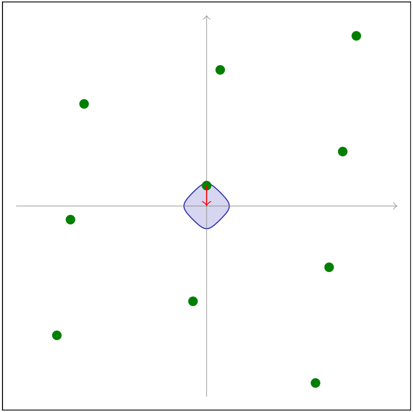
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- To guarantee $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, we need $d \leq \frac{1}{10}$.
- Only a $\sim n^{1/p}$ gap.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Now say $p < 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

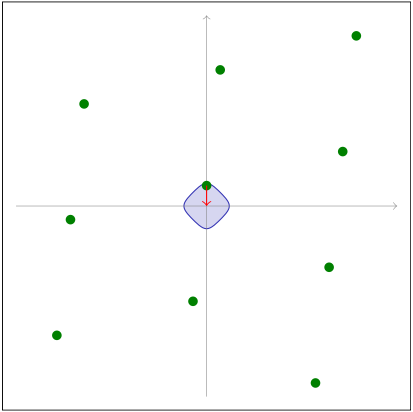
- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- To guarantee $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, we need $d \leq \frac{1}{10}$.
- Only a $\sim n^{1/p}$ gap.

Generalizing to ℓ_p Norms

Lemma [Ban95]

For any $p \in [1, \infty)$, there exists a constant c_p:

$$\frac{\rho((\mathcal{L} - \mathbf{x}) \backslash c_p \cdot n^{1/p} \cdot \mathcal{B}_p)}{\rho(\mathcal{L})} < \frac{1}{4}.$$



Now say $p < 2$. Let $d = \mathrm{dist}_p(\mathbf{x}, \mathcal{L})$.

- If $d > c_p \cdot n^{1/p}$, then $f(\mathbf{x}) < 1/4$.
- To guarantee $\mathrm{dist}_2(\mathbf{x}, \mathcal{L}) \leq \frac{1}{10}$, we need $d \leq \frac{1}{10}$.
- Only a $\sim n^{1/p}$ gap.

Discrete Gaussians

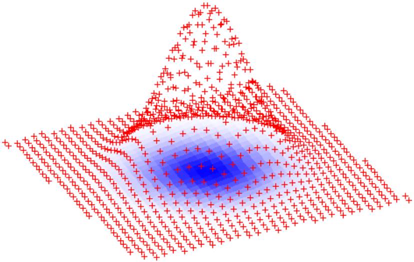
Define probability distribution $D_{\mathcal{L}}$ over lattice $\mathcal{L}$:

$$\text{For } \mathbf{x} \in \mathcal{L}, \quad D_{\mathcal{L}}(\mathbf{x}) \sim \rho(\mathbf{x}) = \exp(-\pi \left\| \mathbf{x} \right\|_2^2).$$

Discrete Gaussians

Define probability distribution $D_{\mathcal{L}}$ over lattice $\mathcal{L}$:

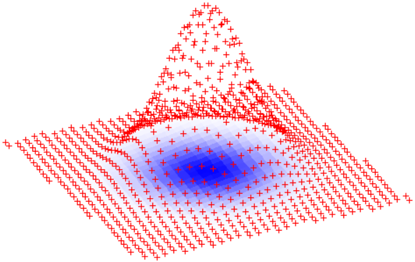
$$\text{For } \mathbf{x} \in \mathcal{L}, \quad D_{\mathcal{L}}(\mathbf{x}) \sim \rho(\mathbf{x}) = \exp(-\pi \left\|\mathbf{x}\right\|_2^2).$$



Discrete Gaussians

Define probability distribution $D_{\mathcal{L}}$ over lattice $\mathcal{L}$:

$$\text{For } \mathbf{x} \in \mathcal{L}, \quad D_{\mathcal{L}}(\mathbf{x}) \sim \rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2).$$

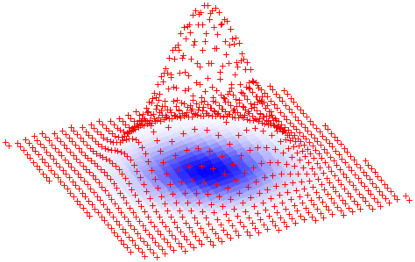


- Central role in worst-to-average reductions [MicciancioRegev,Regev]
- Reductions output (sums of) samples from $D_{\mathcal{L}}$

Discrete Gaussians

Define probability distribution $D_{\mathcal{L}}$ over lattice $\mathcal{L}$:

$$\text{For } \mathbf{x} \in \mathcal{L}, \quad D_{\mathcal{L}}(\mathbf{x}) \sim \rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2).$$



- Central role in worst-to-average reductions [MicciancioRegev,Regev]
- Reductions output (sums of) samples from $D_{\mathcal{L}}$

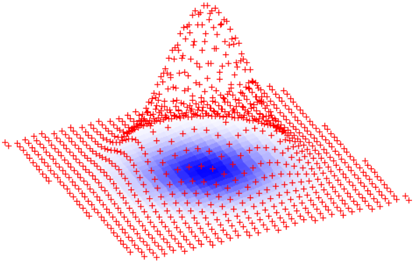
Main Question

Q: How do samples from $D_{\mathcal{L}}$ behave in ℓ_p norm?

Discrete Gaussians

Define probability distribution $D_{\mathcal{L}}$ over lattice $\mathcal{L}$:

$$\text{For } \mathbf{x} \in \mathcal{L}, \quad D_{\mathcal{L}}(\mathbf{x}) \sim \rho(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|_2^2).$$



- Central role in worst-to-average reductions [MicciancioRegev,Regev]
- Reductions output (sums of) samples from $D_{\mathcal{L}}$

Main Question

Q: How do samples from $D_{\mathcal{L}}$ behave in ℓ_p norm?

A: Just like those from a continuous Gaussian!

$$\mathop{\mathrm{E}}_{\mathbf{x} \sim D_{\mathcal{L}}} \left[\|\mathbf{x}\|_p \right] \approx \sqrt{p} \cdot n^{1/p}$$

Proof Highlights

Exponential Tail Inequality

For any $r \geq 0$,

$$\Pr_{\mathbf{x} \sim D_{\mathcal{L}}} [|x_i| > r] \quad \leq \quad \exp(-\pi r^2).$$

Proof Highlights

Exponential Tail Inequality

For any $r \geq 0$,

$$\Pr_{\mathbf{x} \sim D_{\mathcal{L}}} [|x_i| > r] \quad \leq \quad \exp(-\pi r^2).$$

Moments

$$\mathop{\mathrm{E}}_{\mathbf{x} \sim D_{\mathcal{L}}} [|x_i|^p] = \sum_{\mathbf{x} \in \mathcal{L}} |x_i|^p \Pr[\mathbf{x}] = \sum_{\mathbf{x} \in \mathcal{L}} p \int_{r=0}^{|x_i|} r^{p-1} \, dr \Pr[\mathbf{x}]$$

$$= p \int_{r=0}^{\infty} r^{p-1} \Pr_{\mathbf{x}}[|x_i| > r] \, dr \leq (\sqrt{p})^p.$$

Proof Highlights

Exponential Tail Inequality

For any $r \geq 0$,

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L}}}[|x_i| > r] \quad \leq \quad \exp(-\pi r^2).$$

Moments

$$\mathop{\mathrm{E}}_{\mathbf{x}\sim D_{\mathcal{L}}}[|x_i|^p] = \sum_{\mathbf{x}\in\mathcal{L}} |x_i|^p \Pr[\mathbf{x}] = \sum_{\mathbf{x}\in\mathcal{L}} p \int_{r=0}^{|x_i|} r^{p-1}\, dr \Pr[\mathbf{x}]$$

$$= p \int_{r=0}^{\infty} r^{p-1} \Pr_{\mathbf{x}}[|x_i| > r]\, dr \leq (\sqrt{p})^p.$$

Jensen & Linearity

$$\mathop{\mathrm{E}}_{\mathbf{x}\sim D_{\mathcal{L}}}\left[\|\mathbf{x}\|_p\right] \;\leq\; \left(\mathrm{E}\left[\|\mathbf{x}\|_p^p\right]\right)^{1/p} \;=\; (n \cdot \mathrm{E}[|x_i|^p])^{1/p} \;\leq\; \sqrt{p} \cdot n^{1/p}.$$

Conclusions

1. Gaussian techniques are even more powerful than we thought.

Conclusions

1. Gaussian techniques are even more powerful than we thought.
2. ℓ_p norms for $p \geq 2$ look surprisingly similar.

Conclusions

1. Gaussian techniques are even more powerful than we thought.
2. ℓ_p norms for $p \geq 2$ look surprisingly similar.
3. We should pay more attention to the ℓ_1 norm.