Johnson-Lindenstrauss Lemma and Lattices

Peter Ly

December 5, 2022

Shortest Vector Problem

Problem (GapSVP$_\gamma$)

Given a lattice, what is a "fairly" short non-zero vector in a given lattice $\mathcal{L}$? More precisely, find a non-zero vector $\mathbf{v}$ *such that* $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$

SVP parameters

- Dimension of the lattice
- Definition of "shortest"

Shortest Vector Problem

Problem (GapSVP$_\gamma$)

Given a lattice, what is a "fairly" short non-zero vector in a given lattice $\mathcal{L}$? More precisely, find a non-zero vector $\mathbf{v}$ *such that* $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$

SVP parameters

- Dimension of the lattice
- Definition of "shortest"

Norms

Definition (Norm)

Let X be a vector space over the field $\mathbb{R}$. A norm is a function $\|\cdot\| : X \to \mathbb{R}_{\geq 0}$ which satisfies the following properties:

- $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0 \in X$,
- $\|c\mathbf{x}\| = |c| \cdot \|\mathbf{x}\|$ for all $c \in \mathbb{R}$ and for all $\mathbf{x} \in X$,
- $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

Norms are generalizations of length for vectors.

Example

Problems seen in this class are often with respect to the ℓ_2 norm mapping $\mathbf{x} \mapsto \sqrt{\sum x_i^2}$.

Other norms are sometimes of interest - for example, if we need to guarantee that no single coefficient of a vector $\mathbf{x}$ grows too large, we are interested in a bound on the $\|\mathbf{x}\|_\infty$.

Norms

Definition (Norm)

Let X be a vector space over the field $\mathbb{R}$. A norm is a function $\|\cdot\| : X \to \mathbb{R}_{\geq 0}$ which satisfies the following properties:

- $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0 \in X$,
- $\|c\mathbf{x}\| = |c| \cdot \|\mathbf{x}\|$ for all $c \in \mathbb{R}$ and for all $\mathbf{x} \in X$,
- $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

Norms are generalizations of length for vectors.

Example

Problems seen in this class are often with respect to the ℓ_2 norm mapping $\mathbf{x} \mapsto \sqrt{\sum x_i^2}$.

Other norms are sometimes of interest - for example, if we need to guarantee that no single coefficient of a vector $\mathbf{x}$ grows too large, we are interested in a bound on the $\|\mathbf{x}\|_\infty$.

Norms

Definition (Norm)

Let X be a vector space over the field $\mathbb{R}$. A norm is a function $\|\cdot\| : X \to \mathbb{R}_{\geq 0}$ which satisfies the following properties:

- $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0 \in X$,
- $\|c\mathbf{x}\| = |c| \cdot \|\mathbf{x}\|$ for all $c \in \mathbb{R}$ and for all $\mathbf{x} \in X$,
- $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

Norms are generalizations of length for vectors.

Example

Problems seen in this class are often with respect to the ℓ_2 norm mapping $\mathbf{x} \mapsto \sqrt{\sum x_i^2}$.
Other norms are sometimes of interest - for example, if we need to guarantee that no single coefficient of a vector $\mathbf{x}$ grows too large, we are interested in a bound on the $\|\mathbf{x}\|_\infty$.

A simple result

Theorem

Let X be a finite dimensional vector space. Fix $\|\cdot\|_a$ and $\|\cdot\|_b$ to be norms for X. Then there exist constants C_1, C_2 such that for all $\mathbf{x} \in X$

$$C_1\|\mathbf{x}\|_a \leq \|\mathbf{x}\|_b \leq C_2\|\mathbf{x}\|_a.$$

In other words, the lengths of $\mathbf{x} \in X$ under any norm reveal partial information about lengths $\mathbf{x} \in X$ under any other norm.

In particular, by Hölder's inequality,

Theorem

Let $X = \mathbb{R}^n$. Then $\|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \sqrt{n}\|\mathbf{x}\|_p$.

So we can approximate lengths under the ℓ_2 norm if we pay $\sqrt{n}$ in approximation factor and have knowledge of the distances under the ℓ_p norm.

A simple result

Theorem

Let X be a finite dimensional vector space. Fix $\|\cdot\|_a$ and $\|\cdot\|_b$ to be norms for X. Then there exist constants C_1, C_2 such that for all $\mathbf{x} \in X$

$$C_1\|\mathbf{x}\|_a \leq \|\mathbf{x}\|_b \leq C_2\|\mathbf{x}\|_a.$$

In other words, the lengths of $\mathbf{x} \in X$ under any norm reveal partial information about lengths $\mathbf{x} \in X$ under any other norm.

In particular, by Hölder's inequality,

Theorem

Let $X = \mathbb{R}^n$. Then $\|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \sqrt{n}\|\mathbf{x}\|_p$.

So we can approximate lengths under the ℓ_2 norm if we pay $\sqrt{n}$ in approximation factor and have knowledge of the distances under the ℓ_p norm.

A simple result

Theorem

Let X be a finite dimensional vector space. Fix $\|\cdot\|_a$ and $\|\cdot\|_b$ to be norms for X. Then there exist constants C_1, C_2 such that for all $\mathbf{x} \in X$

$$C_1\|\mathbf{x}\|_a \leq \|\mathbf{x}\|_b \leq C_2\|\mathbf{x}\|_a.$$

In other words, the lengths of $\mathbf{x} \in X$ under any norm reveal partial information about lengths $\mathbf{x} \in X$ under any other norm.

In particular, by Hölder's inequality,

Theorem

Let $X = \mathbb{R}^n$. Then $\|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \sqrt{n}\|\mathbf{x}\|_p$.

So we can approximate lengths under the ℓ_2 norm if we pay $\sqrt{n}$ in approximation factor and have knowledge of the distances under the ℓ_p norm.

A simple result

Theorem

Let X be a finite dimensional vector space. Fix $\|\cdot\|_a$ and $\|\cdot\|_b$ to be norms for X. Then there exist constants C_1, C_2 such that for all $\mathbf{x} \in X$

$$C_1\|\mathbf{x}\|_a \leq \|\mathbf{x}\|_b \leq C_2\|\mathbf{x}\|_a.$$

In other words, the lengths of $\mathbf{x} \in X$ under any norm reveal partial information about lengths $\mathbf{x} \in X$ under any other norm.

In particular, by Hölder's inequality,

Theorem

Let $X = \mathbb{R}^n$. Then $\|\mathbf{x}\|_p \leq \|\mathbf{x}\|_2 \leq \sqrt{n}\|\mathbf{x}\|_p$.

So we can approximate lengths under the ℓ_2 norm if we pay $\sqrt{n}$ in approximation factor and have knowledge of the distances under the ℓ_p norm.

Johnson-Lindenstrauss type tool

Definition (Embedding families for $p < \infty$)

For any real $1 \leq p < \infty$ and integers $m \geq n$, we define a distribution $\mathcal{F}(p, n, m)$ over embedding functions $f : \ell_2^n \to \ell_p^m$. We can sample a function from $\mathcal{F}(p, n, m)$ by sampling n orthonormal vectors in S^{m-1} uniformly at random and let $\mathbf{A}$ be the $m \times n$ matrix whose columns are the orthonormal vectors. Then define $f(\mathbf{x}) \triangleq \nu_p(n, m) \cdot \mathbf{A}\mathbf{x}$ where $\nu_p(n, m)$ is a normalization factor.

Theorem ([FLM77])

There exists $\nu_p(n, m)$ such that for all $p < \infty$, $\varepsilon > 0$ and n there is m such that with probability at least $1 - 2^{-\Omega(n)}$, a randomly chosen embedding function $f \sim \mathcal{F}(p, n, m)$ satisfies that for all $\mathbf{x} \in \mathbb{R}^n$

$$(1 - \varepsilon)\|\mathbf{x}\|_2 \leq \|f(\mathbf{x})\|_p \leq (1 + \varepsilon)\|\mathbf{x}\|_2.$$

Johnson-Lindenstrauss type tool

Definition (Embedding families for $p < \infty$)

For any real $1 \leq p < \infty$ and integers $m \geq n$, we define a distribution $\mathcal{F}(p, n, m)$ over embedding functions $f : \ell_2^n \to \ell_p^m$. We can sample a function from $\mathcal{F}(p, n, m)$ by sampling n orthonormal vectors in S^{m-1} uniformly at random and let $\mathbf{A}$ be the $m \times n$ matrix whose columns are the orthonormal vectors. Then define $f(\mathbf{x}) \triangleq \nu_p(n, m) \cdot \mathbf{A}\mathbf{x}$ where $\nu_p(n, m)$ is a normalization factor.

Theorem ([FLM77])

There exists $\nu_p(n, m)$ such that for all $p < \infty$, $\varepsilon > 0$ and n there is m such that with probability at least $1 - 2^{-\Omega(n)}$, a randomly chosen embedding function $f \sim \mathcal{F}(p, n, m)$ satisfies that for all $\mathbf{x} \in \mathbb{R}^n$

$$(1 - \varepsilon)\|\mathbf{x}\|_2 \leq \|f(\mathbf{x})\|_p \leq (1 + \varepsilon)\|\mathbf{x}\|_2.$$

Asymmetric embeddings

Definition (Embedding families for $p = \infty$)

For any integers $m \geq n$, we define a distribution $\mathcal{F}(\infty, n, m)$ over embedding functions $f : \ell_2^n \to \ell_\infty^m$. We can sample a function from $\mathcal{F}(\infty, n, m)$ by taking $\mathbf{A} \leftarrow \mathcal{N}(0,1)^{m \times n}$. Then define $f(\mathbf{x}) \triangleq \nu_\infty \cdot \mathbf{A}\mathbf{x}$ where $\nu_\infty = (2 \ln(m/\sqrt{\ln m}))^{-1/2}$ is a normalization factor.

Theorem (Strengthened [Ind03] due to [RR06])

For any $\varepsilon > 0$, any large enough n, and any $\delta > 0$, the family $\mathcal{F}(\infty, n, m)$ for $m = (n \log n + \delta^{-1} + \varepsilon^{-1})^{O(1/\varepsilon)}$ satisfies the following:

$$\max_{\mathbf{v}} \Pr_{f \leftarrow \mathcal{F}(\infty,n,m)}[\|f(\mathbf{v})\|_p \geq (1+\varepsilon)\|\mathbf{v}\|_q] \leq \delta$$

$$\forall \mathbf{v} \in \mathbb{R}^n, \Pr[\|f(x)\|_\infty \geq (1-\varepsilon)\|\mathbf{v}\|_2] \leq 1 - m2^{-\Omega(n)}$$

Asymmetric embeddings

Definition (Embedding families for $p = \infty$)

For any integers $m \geq n$, we define a distribution $\mathcal{F}(\infty, n, m)$ over embedding functions $f : \ell_2^n \to \ell_\infty^m$. We can sample a function from $\mathcal{F}(\infty, n, m)$ by taking $\mathbf{A} \leftarrow \mathcal{N}(0,1)^{m \times n}$. Then define $f(\mathbf{x}) \triangleq \nu_\infty \cdot \mathbf{A}\mathbf{x}$ where $\nu_\infty = (2 \ln(m/\sqrt{\ln m}))^{-1/2}$ is a normalization factor.

Theorem (Strengthened [Ind03] due to [RR06])

For any $\varepsilon > 0$, any large enough n, and any $\delta > 0$, the family $\mathcal{F}(\infty, n, m)$ for $m = (n \log n + \delta^{-1} + \varepsilon^{-1})^{O(1/\varepsilon)}$ satisfies the following:

$$\max_{\mathbf{v}} \Pr_{f \leftarrow \mathcal{F}(\infty,n,m)}[\|f(\mathbf{v})\|_p \geq (1+\varepsilon)\|\mathbf{v}\|_q] \leq \delta$$

$$\forall \mathbf{v} \in \mathbb{R}^n, \Pr[\|f(x)\|_\infty \geq (1-\varepsilon)\|\mathbf{v}\|_2] \leq 1 - m2^{-\Omega(n)}$$

Complexity of GapSVP

We can improve the approximation factor loss from $\sqrt{n}$ to basically nothing.

Theorem ([RR06])

For all $\varepsilon > 0$ and for all $1 \leq p \leq \infty$, there is a randomized polynomial time reduction from GapSVP_γ *in the ℓ_2 norm to* $\text{GapSVP}_{(1+\varepsilon)\cdot\gamma}$ *in the ℓ_p norm.*

Informally, this tells us that GapSVP is easier in the ℓ_2 norm than in any other ℓ_p norm.

Proof sketch

For $1 \leq p < \infty$, apply [FLM77] in a straightforward way.
For $p = \infty$, apply strengthened [Ind03].
The main idea is that every vector does not shrink much w.h.p., and a $\gamma \cdot \lambda_1(\mathcal{L})$ length vector does not grow much w.h.p.

Complexity of GapSVP

We can improve the approximation factor loss from $\sqrt{n}$ to basically nothing.

Theorem ([RR06])

For all $\varepsilon > 0$ and for all $1 \leq p \leq \infty$, there is a randomized polynomial time reduction from GapSVP_γ *in the ℓ_2 norm to* $\text{GapSVP}_{(1+\varepsilon)\cdot\gamma}$ *in the ℓ_p norm.*

Informally, this tells us that GapSVP is easier in the ℓ_2 norm than in any other ℓ_p norm.

Proof sketch

For $1 \leq p < \infty$, apply [FLM77] in a straightforward way.
For $p = \infty$, apply strengthened [Ind03].
The main idea is that every vector does not shrink much w.h.p., and a $\gamma \cdot \lambda_1(\mathcal{L})$ length vector does not grow much w.h.p.

Other results from [RR06]

Theorem

For any $\varepsilon > 0$, $\gamma > 1$, and any $1 \leq p \leq \infty$, there is a randomized Karp reduction from GapCVP_γ *under the ℓ_2 norm to* $\mathrm{GapCVP}_{\gamma'}$ *under the ℓ_p norm.*

Theorem

For any $\varepsilon > 0$, $\gamma > 1$ and any $1 \leq p \leq \infty$, there is a reduction from $\mathrm{GapCVPP}_\gamma$ *to* $\mathrm{GapCVPP}_{\gamma'}$ *where* $\gamma' = \frac{1-\varepsilon}{1+\varepsilon} \cdot \gamma$.

Each of these results essentially follows the same proof as in the case of GapSVP, where we construct the embedding, and apply the embedding in a "black-box" manner.

Other results from [RR06]

Theorem

For any $\varepsilon > 0$, $\gamma > 1$, and any $1 \leq p \leq \infty$, there is a randomized Karp reduction from GapCVP_γ *under the ℓ_2 norm to* $\mathrm{GapCVP}_{\gamma'}$ *under the ℓ_p norm.*

Theorem

For any $\varepsilon > 0$, $\gamma > 1$ and any $1 \leq p \leq \infty$, there is a reduction from $\mathrm{GapCVPP}_\gamma$ *to* $\mathrm{GapCVPP}_{\gamma'}$ *where* $\gamma' = \frac{1-\varepsilon}{1+\varepsilon} \cdot \gamma$.

Each of these results essentially follows the same proof as in the case of GapSVP, where we construct the embedding, and apply the embedding in a "black-box" manner.

(Some) Collected results under arbitrary norms

The techniques of Regev and Rosen give inapproximability results for lattice problems under different norms (when combined with complexity assumptions).

Theorem

There is no efficient algorithm for $\mathrm{GapSVP}_{\Theta(1)}$ *under the* ℓ_1 *norm unless* $\mathrm{NP} \subseteq \mathrm{RP}$.

Theorem

There is no efficient algorithm for $\mathrm{GapSVP}_{\Theta(1)}$ *under the* ℓ_∞ *norm unless* $\mathrm{NP} \subseteq \mathrm{RP}$.

(Some) Collected results under arbitrary norms

The techniques of Regev and Rosen give inapproximability results for lattice problems under different norms (when combined with complexity assumptions).

Theorem

There is no efficient algorithm for $\mathsf{GapSVP}_{\Theta(1)}$ *under the* ℓ_1 *norm unless* $\mathsf{NP} \subseteq \mathsf{RP}$.

Theorem

There is no efficient algorithm for $\mathsf{GapSVP}_{\Theta(1)}$ *under the* ℓ_∞ *norm unless* $\mathsf{NP} \subseteq \mathsf{RP}$.

Continuing the work

Their techniques covered do not extend to all lattice problems over all ℓ_p norms!

Open Questions

- Is there a reduction from GapCRP_γ under the ℓ_2 norm to $\text{GapCRP}_{\gamma'}$ under the ℓ_∞ norm where $\gamma' = (1 - \varepsilon) \cdot \gamma$ for $\varepsilon > 0$?
- Are lattice problems equivalently difficult regardless of the norm used i.e. are there reductions which go from the ℓ_p norm to the ℓ_2 and can we extend these reductions to other norms?
- What other lattice problems seem to be most easy in the ℓ_2 norm?

Working in other norms

Can we relate other norms to the ℓ_p norms?

An approach

Bourgain's metric embedding theorem provides a way to convert from any norm to the ℓ_2 norm.
This seems harder to use however, because it seems many results rely on the linearity of the embedding to limit the amount of points to "check" under embedding, and because the approximation factor picked up from the embedding can be pretty large. Furthermore, the proof of Bourgain's metric embedding theorem requires that we work over a finite set of points.

References

[FLM77] T. Figiel, J. Lindenstrauss, and V. D. Milman. "The dimension of almost spherical sections of convex bodies". In: *Acta Mathematica* 139.none (1977), pp. 53–94. DOI: 10.1007/BF02392234. URL: https://doi.org/10.1007/BF02392234.

[Ind03] Piotr Indyk. "Better Algorithms for High-Dimensional Proximity Problems via Asymmetric Embeddings". In: *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '03. Baltimore, Maryland: Society for Industrial and Applied Mathematics, 2003, pp. 539–545. ISBN: 0898715385.

[RR06] Oded Regev and Ricky Rosen. "Lattice Problems and Norm Embeddings". In: *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '06. Seattle, WA, USA: Association for Computing Machinery, 2006, pp. 447–456. ISBN: 1595931341. DOI: 10.1145/1132516.1132581. URL: https://doi.org/10.1145/1132516.1132581.