Immanuel Kant Baltic Federal University

Eindhoven University of Technology

Lower bounds on lattice sieving and information set decoding

Elena Kirshanova, Thijs Laarhoven

mail@thijs.com
https://www.thijs.com/

Crypto 2021, virtual
(August 17, 2021)

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of “long” vectors.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.

- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of "long" vectors.
  - Combine "nearby" vectors to obtain shorter vectors.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.

- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of “long” vectors.
  - Combine “nearby” vectors to obtain shorter vectors.
  - Repeat until sufficiently “short” vectors are found.

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\Longrightarrow$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of “long” vectors.
  - Combine “nearby” vectors to obtain shorter vectors.
  - Repeat until sufficiently “short” vectors are found.
- **Closest pairs problem**: Key subroutine for efficiently combining vectors.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.

- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of "long" vectors.
  - Combine "nearby" vectors to obtain shorter vectors.
  - Repeat until sufficiently "short" vectors are found.

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of "long" vectors.
  - Combine "nearby" vectors to obtain shorter vectors.
  - Repeat until sufficiently "short" vectors are found.
- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\Longrightarrow$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of "long" vectors.
  - Combine "nearby" vectors to obtain shorter vectors.
  - Repeat until sufficiently "short" vectors are found.
- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.

TU/e

Abstract

- **Post-quantum cryptography**: Lattice-based, code-based cryptography.
  - NIST standardization: Dominated by lattices and codes.
  - Security relies on hardness of lattice problems, decoding problems.
  - Long-term security $\implies$ Conservative bounds.
- **State-of-the-art cryptanalysis**: Lattice sieving, information set decoding.
  - Sample large database of “long” vectors.
  - Combine “nearby” vectors to obtain shorter vectors.
  - Repeat until sufficiently “short” vectors are found.
- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\Longrightarrow$ Improvements still possible?

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.

TU/e

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.
  - Tight lower bound for lattice sieving $\implies$ [BDGL16] optimal.

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.
  - Tight lower bound for lattice sieving $\implies$ [BDGL16] optimal.
  - Non-tight lower bound for ISD $\implies$ [MO15] possibly suboptimal?

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\implies$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.
  - Tight lower bound for lattice sieving $\implies$ [BDGL16] optimal.
  - Non-tight lower bound for ISD $\implies$ [MO15] possibly suboptimal?
- **Cryptographic implications**: Better understanding of hardness.

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\Longrightarrow$ Improvements still possible?

- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.
  - Tight lower bound for lattice sieving $\Longrightarrow$ [BDGL16] optimal.
  - Non-tight lower bound for ISD $\Longrightarrow$ [MO15] possibly suboptimal?

- **Cryptographic implications**: Better understanding of hardness.
  - Cryptanalysis: Search for improvements elsewhere [Duc18, A+19].

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\Longrightarrow$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to “hash-based” model.
  - Tight lower bound for lattice sieving $\Longrightarrow$ [BDGL16] optimal.
  - Non-tight lower bound for ISD $\Longrightarrow$ [MO15] possibly suboptimal?
- **Cryptographic implications**: Better understanding of hardness.
  - Cryptanalysis: Search for improvements elsewhere [Duc18, A+19].
  - Motivates focus on best lattice sieve [AGPS20, DSvW21].

TU/e

Abstract

- **Closest pairs problem**: Key subroutine for efficiently combining vectors.
  - Subroutine dominates overall algorithm complexities.
  - Naive approach: Quadratic for pairs of vectors.
  - Hash-based approaches: Subquadratic time complexity.
  - No matching lower bounds $\Longrightarrow$ Improvements still possible?
- **Contributions**: Lower bounds for corresponding nearest neighbor problems.
  - Conditional: Applies to "hash-based" model.
  - Tight lower bound for lattice sieving $\Longrightarrow$ [BDGL16] optimal.
  - Non-tight lower bound for ISD $\Longrightarrow$ [MO15] possibly suboptimal?
- **Cryptographic implications**: Better understanding of hardness.
  - Cryptanalysis: Search for improvements elsewhere [Duc18, A+19].
  - Motivates focus on best lattice sieve [AGPS20, DSvW21].
  - Parameter selection: Conditional security guarantees.

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find “almost all” pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find "almost all" pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.
- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})].$$

TU/e

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find "almost all" pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.
- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})].$$

- **Locality-sensitive hashing**: Build and populate hash tables using "nice" hash functions, and combine pairs of vectors within hash buckets.

TU/e

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find "almost all" pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.
- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})].$$

- **Locality-sensitive hashing**: Build and populate hash tables using "nice" hash functions, and combine pairs of vectors within hash buckets.
  - **Lattice sieving**: $M = \mathcal{S}^{d-1}$, $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_2$, $|L| = 2^{\Theta(d)}$.

TU/e

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find "almost all" pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.
- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})].$$

- **Locality-sensitive hashing**: Build and populate hash tables using "nice" hash functions, and combine pairs of vectors within hash buckets.
  - **Lattice sieving**: $M = \mathcal{S}^{d-1}$, $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_2$, $|L| = 2^{\Theta(d)}$.
  - **ISD setting**: $M = \{0, 1\}^d$, $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_1$, $|L| = 2^{\Theta(d)}$.

Hash-based model

- **Closest pairs problem**:
  Let (M, d) be a bounded metric space, and let $r \geq 0$ be a given target distance.
  Let $L \subset M$ be a subset of M, with elements drawn uniformly at random from M.
  Find "almost all" pairs $\mathbf{x}, \mathbf{y} \in L$ satisfying $d(\mathbf{x}, \mathbf{y}) \leq r$.
- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})].$$

- **Locality-sensitive hashing**: Build and populate hash tables using "nice" hash functions, and combine pairs of vectors within hash buckets.
  - **Lattice sieving**: $M = \mathcal{S}^{d-1}$, $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_2$, $|L| = 2^{\Theta(d)}$.
  - **ISD setting**: $M = \{0, 1\}^d$, $d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_1$, $|L| = 2^{\Theta(d)}$.
  - **Nearest neighbor literature**: Various (M, d), focus on $|L| = 2^{o(d)}$.

Hash-based model

- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim M \\ d(\mathbf{x},\mathbf{y}) \leq r}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim M} [h(\mathbf{x}) = h(\mathbf{y})] .$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y}\sim M \\ d(\mathbf{x},\mathbf{y})\leq r}}[h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y}\sim M}[h(\mathbf{x}) = h(\mathbf{y})].$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [h(\mathbf{x}) = h(\mathbf{y})] \gg \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} [h(\mathbf{x}) = h(\mathbf{y})] .$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\sum_n \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [h(\mathbf{x}) = h(\mathbf{y}) = n] \gg \sum_n \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} [h(\mathbf{x}) = h(\mathbf{y}) = n].$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\sum_n \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(n)\right] \gg \sum_n \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(n)\right].$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\sum_n \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(n)\right] \gg \sum_n \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(n)\right].$$

- Usually $h^{-1}(n)$ has similar shapes for all n.

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$n \cdot \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(0)\right] \gg n \cdot \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(0)\right].$$

- Usually $h^{-1}(n)$ has similar shapes for all n.

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(0)\right] \gg \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} \left[\mathbf{x}, \mathbf{y} \in h^{-1}(0)\right].$$

- Usually $h^{-1}(n)$ has similar shapes for all n.

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \Pr_{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1}} [\mathbf{x}, \mathbf{y} \in A].$$

- Usually $h^{-1}(n)$ has similar shapes for all n.

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions:** Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \sigma(A)^2.$$

- Usually $h^{-1}(n)$ has similar shapes for all n.

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \sigma(A)^2.$$

- Usually $h^{-1}(n)$ has similar shapes for all n.
- **Problem**: For fixed $\sigma(A)$, find $A \subset \mathcal{S}^{d-1}$ which maximizes:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A].$$

TU/e

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ *be arbitrary Lebesgue-integrable functions. Let* $h : [-1, 1] \to \mathbb{R}$ *be non-decreasing, bounded, and measurable. Let* $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ *be the symmetric non-decreasing rearrangements of* f, g*. Then:*

$$\iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f(\mathbf{x}) g(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}) \leq \iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f^*(\mathbf{x}) g^*(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}).$$

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1, 1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f(\mathbf{x}) g(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}) \leq \iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f^*(\mathbf{x}) g^*(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}).$$

$$f(\mathbf{x}) = \mathbb{1}\{\mathbf{x} \in A\}$$

$$g(\mathbf{y}) = \mathbb{1}\{\mathbf{y} \in A\}$$

$$h(\mathbf{x} \cdot \mathbf{y}) = \mathbb{1}\{\mathbf{x} \cdot \mathbf{y} \geq \gamma\}$$

TU/e

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1, 1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f(\mathbf{x}) g(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}) \leq \iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} f^*(\mathbf{x}) g^*(\mathbf{y}) h(\mathbf{x} \cdot \mathbf{y}) \, \mathrm{d}\sigma(\mathbf{x}) \, \mathrm{d}\sigma(\mathbf{y}).$$

$$\begin{aligned} f(\mathbf{x}) &= \mathbb{1}\{\mathbf{x} \in A\} & \to \quad & f^*(\mathbf{x}) = \mathbb{1}\{\mathbf{x} \in \mathcal{C}_A\} \\ g(\mathbf{y}) &= \mathbb{1}\{\mathbf{y} \in A\} & \to \quad & g^*(\mathbf{y}) = \mathbb{1}\{\mathbf{y} \in \mathcal{C}_A\} \\ h(\mathbf{x} \cdot \mathbf{y}) &= \mathbb{1}\{\mathbf{x} \cdot \mathbf{y} \geq \gamma\} & & (\sigma(A) = \sigma(\mathcal{C}_A)) \end{aligned}$$

TU/e

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1,1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\iint_{\mathcal{S}^{d-1}\times\mathcal{S}^{d-1}} \mathbb{1}\{\mathbf{x} \in A\}\mathbb{1}\{\mathbf{y} \in A\}\mathbb{1}\{\mathbf{x}\cdot\mathbf{y} \geq \gamma\}\,\mathrm{d}\sigma^2 \leq \iint_{\mathcal{S}^{d-1}\times\mathcal{S}^{d-1}} \mathbb{1}\{\mathbf{x} \in \mathcal{C}_A\}\mathbb{1}\{\mathbf{y} \in \mathcal{C}_A\}\mathbb{1}\{\mathbf{x}\cdot\mathbf{y} \geq \gamma\}\,\mathrm{d}\sigma^2.$$

$$f(\mathbf{x}) = \mathbb{1}\{\mathbf{x} \in A\} \quad \to \quad f^*(\mathbf{x}) = \mathbb{1}\{\mathbf{x} \in \mathcal{C}_A\}$$

$$g(\mathbf{y}) = \mathbb{1}\{\mathbf{y} \in A\} \quad \to \quad g^*(\mathbf{y}) = \mathbb{1}\{\mathbf{y} \in \mathcal{C}_A\}$$

$$h(\mathbf{x}\cdot\mathbf{y}) = \mathbb{1}\{\mathbf{x}\cdot\mathbf{y} \geq \gamma\} \qquad (\sigma(A) = \sigma(\mathcal{C}_A))$$

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ *be arbitrary Lebesgue-integrable functions. Let* $h : [-1, 1] \to \mathbb{R}$ *be non-decreasing, bounded, and measurable. Let* $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ *be the symmetric non-decreasing rearrangements of* f, g*. Then:*

$$\iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} \mathbb{1}\{\mathbf{x} \in A\} \mathbb{1}\{\mathbf{y} \in A\} \mathbb{1}\{\mathbf{x} \cdot \mathbf{y} \geq \gamma\} \, \mathrm{d}\sigma^2 \leq \iint_{\mathcal{S}^{d-1} \times \mathcal{S}^{d-1}} \mathbb{1}\{\mathbf{x} \in \mathcal{C}_A\} \mathbb{1}\{\mathbf{y} \in \mathcal{C}_A\} \mathbb{1}\{\mathbf{x} \cdot \mathbf{y} \geq \gamma\} \, \mathrm{d}\sigma^2.$$

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1, 1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\Pr_{\mathbf{x},\mathbf{y}\sim\mathcal{S}^{d-1}}[\mathbf{x}, \mathbf{y} \in A, \mathbf{x} \cdot \mathbf{y} \geq \gamma] \leq \Pr_{\mathbf{x},\mathbf{y}\sim\mathcal{S}^{d-1}}[\mathbf{x}, \mathbf{y} \in \mathcal{C}_A, \mathbf{x} \cdot \mathbf{y} \geq \gamma].$$

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1,1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\Pr_{\substack{\mathbf{x},\mathbf{y}\sim\mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y}\geq\gamma}} [\mathbf{x}, \mathbf{y} \in A] \leq \Pr_{\substack{\mathbf{x},\mathbf{y}\sim\mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y}\geq\gamma}} [\mathbf{x}, \mathbf{y} \in \mathcal{C}_A].$$

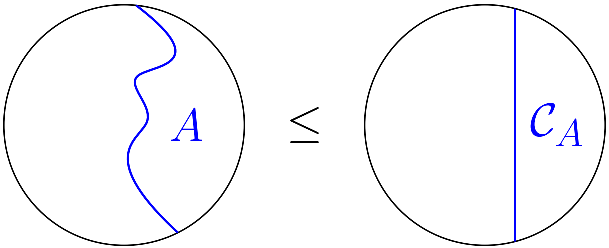
TU/e

Lower bounds (Euclidean sphere)

Lemma (Baernstein–Taylor inequality for $\mathcal{S}^{d-1}$ [BT76])

Let $f, g : \mathcal{S}^{d-1} \to \mathbb{R}$ be arbitrary Lebesgue-integrable functions. Let $h : [-1,1] \to \mathbb{R}$ be non-decreasing, bounded, and measurable. Let $f^*, g^* : \mathcal{S}^{d-1} \to \mathbb{R}$ be the symmetric non-decreasing rearrangements of f, g. Then:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \leq \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in \mathcal{C}_A].$$



Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \sigma(A)^2.$$

- Usually $h^{-1}(n)$ has similar shapes for all n.
- **Problem**: For fixed $\sigma(A)$, find $A \subset \mathcal{S}^{d-1}$ which maximizes:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x} \cdot \mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A]$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \sigma(A)^2.$$

- Usually $h^{-1}(n)$ has similar shapes for all n.
- **Problem**: For fixed $\sigma(A)$, find $A \subset \mathcal{S}^{d-1}$ which maximizes:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \leq \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in \mathcal{C}_A].$$

Lower bounds (Euclidean sphere)

- **Locality-sensitive hash functions**: Functions h satisfying:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \gg \sigma(A)^2.$$

- Usually $h^{-1}(n)$ has similar shapes for all n.
- **Problem**: For fixed $\sigma(A)$, find $A \subset \mathcal{S}^{d-1}$ which maximizes:

$$\Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in A] \leq \Pr_{\substack{\mathbf{x},\mathbf{y} \sim \mathcal{S}^{d-1} \\ \mathbf{x}\cdot\mathbf{y} \geq \gamma}} [\mathbf{x}, \mathbf{y} \in \mathcal{C}_A].$$

- **Solution**: Performance maximized for spherical caps!

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.
- **Classical sieving**: $2^{0.292d+o(d)}$ [BDGL16] is conditionally optimal.

TU/e

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.
- **Classical sieving**: $2^{0.292d+o(d)}$ [BDGL16] is conditionally optimal.
- **Sieving + Grover**: $2^{0.265d+o(d)}$ [Laa16] is conditionally optimal.

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.
- **Classical sieving**: $2^{0.292d+o(d)}$ [BDGL16] is conditionally optimal.
- **Sieving + Grover**: $2^{0.265d+o(d)}$ [Laa16] is conditionally optimal.
  - **Sieving + QRW**: $2^{0.257d+o(d)}$ [CL21] improves quantum part.

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.
- **Classical sieving**: $2^{0.292d+o(d)}$ [BDGL16] is conditionally optimal.
- **Sieving + Grover**: $2^{0.265d+o(d)}$ [Laa16] is conditionally optimal.
  - **Sieving + QRW**: $2^{0.257d+o(d)}$ [CL21] improves quantum part.
  - Does not violate lower bound.

Lower bounds (lattice sieving)

- Conditional, asymptotic bounds: Lattice sieving with hash-based searching.
- **Classical sieving**: $2^{0.292d+o(d)}$ [BDGL16] is conditionally optimal.
- **Sieving + Grover**: $2^{0.265d+o(d)}$ [Laa16] is conditionally optimal.
  - **Sieving + QRW**: $2^{0.257d+o(d)}$ [CL21] improves quantum part.
  - Does not violate lower bound.
- **Tuple sieving**: results from [HKL18] are conditionally optimal.

Open problems

- Conditional on hash-based approach $\rightarrow$ Other closest pair techniques?

Open problems

- Conditional on hash-based approach → Other closest pair techniques?
- Only affects closest pairs subroutine → Improve other parts?

TU/e

Open problems

- Conditional on hash-based approach → Other closest pair techniques?
- Only affects closest pairs subroutine → Improve other parts?
- Asymptotics about leading constant → Decrease subexponential overhead?

Open problems

- Conditional on hash-based approach → Other closest pair techniques?
- Only affects closest pairs subroutine → Improve other parts?
- Asymptotics about leading constant → Decrease subexponential overhead?
- Bound for ISD not tight → Better techniques/bounds?

Open problems

- Conditional on hash-based approach → Other closest pair techniques?
- Only affects closest pairs subroutine → Improve other parts?
- Asymptotics about leading constant → Decrease subexponential overhead?
- Bound for ISD not tight → Better techniques/bounds?

Thank you for watching!