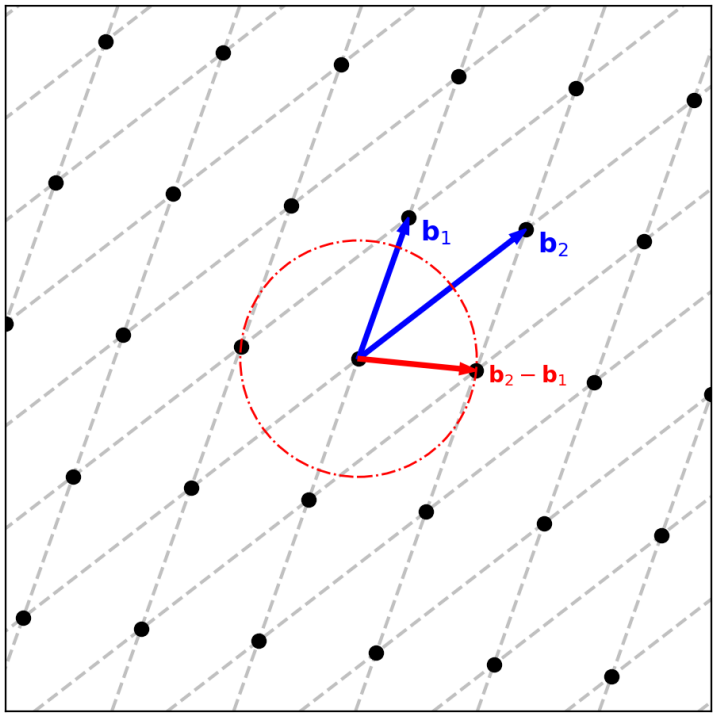
Improved Hardness of BDD and SVP under Gap-(S)ETH

Yi Tang
Joint work with Huck Bennett and Chris Peikert

September 16, 2021
(last updated on January 31, 2022)

Preliminaries: Lattices

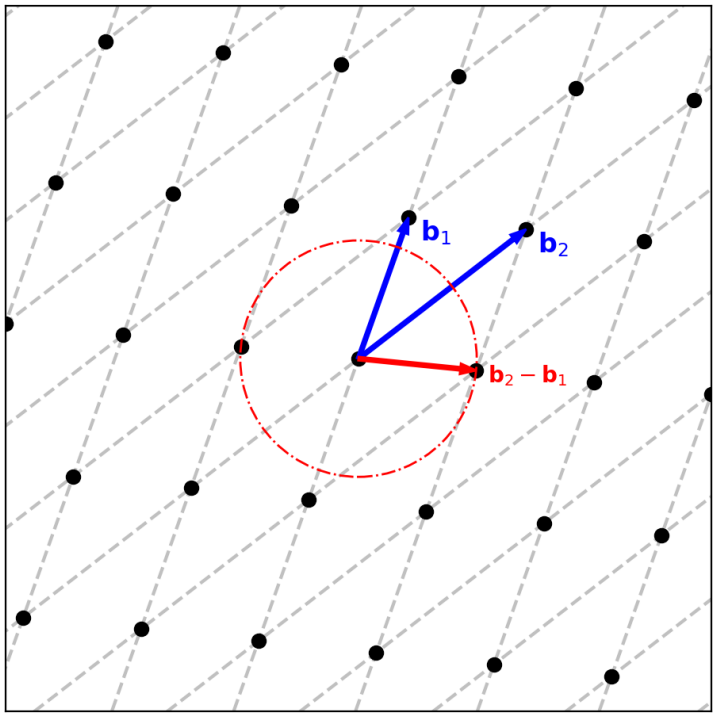
Lattice $\mathcal{L} \subset \mathbb{R}^d$: set of all integer linear combinations of a basis.
Basis $B \in \mathbb{R}^{d \times n}$: rank n, dimension d, $\mathcal{L} = B \cdot \mathbb{Z}^n$.



Minimum distance (in ℓ_p) $\lambda_1^{(p)}(\mathcal{L})$: smallest ℓ_p norm in $\mathcal{L} \setminus \{0\}$.

Preliminaries: Lattices

Lattice $\mathcal{L} \subset \mathbb{R}^d$: set of all integer linear combinations of a basis.
Basis $B \in \mathbb{R}^{d \times n}$: rank n, dimension d, $\mathcal{L} = B \cdot \mathbb{Z}^n$.



Minimum distance (in ℓ_p) $\lambda_1^{(p)}(\mathcal{L})$: smallest ℓ_p norm in $\mathcal{L} \setminus \{0\}$.

Preliminaries: Lattice Problems

Lattice Problems and post-quantum cryptography:

- Cryptography based on number theory would be broken by attacks with quantum.
- People believe lattice problems have no quantum solution, and thus lattice-based cryptosystems are quantum-secure.

Desired hardness of lattice problems:

- Good news: *worst-case* hardness of lattice problems leads to *average-case* security of the cryptosystems.
- Need precise fine-grained hardness of lattice problems for setting parameters of the cryptosystems confidently.
- Cryptosystems are based on problems unlikely to be NP-hard, while state-of-the-art attacks reduce to problems where we can show NP-hardness / fine-grained hardness.

Preliminaries: Lattice Problems

Lattice Problems and post-quantum cryptography:

- Cryptography based on number theory would be broken by attacks with quantum.
- People believe lattice problems have no quantum solution, and thus lattice-based cryptosystems are quantum-secure.

Desired hardness of lattice problems:

- Good news: *worst-case* hardness of lattice problems leads to *average-case* security of the cryptosystems.
- Need precise fine-grained hardness of lattice problems for setting parameters of the cryptosystems confidently.
- Cryptosystems are based on problems unlikely to be NP-hard, while state-of-the-art attacks reduce to problems where we can show NP-hardness / fine-grained hardness.

Preliminaries: Lattice Problems

Lattice Problems and post-quantum cryptography:

- Cryptography based on number theory would be broken by attacks with quantum.
- People believe lattice problems have no quantum solution, and thus lattice-based cryptosystems are quantum-secure.

Desired hardness of lattice problems:

- Good news: *worst-case* hardness of lattice problems leads to *average-case* security of the cryptosystems.
- Need precise fine-grained hardness of lattice problems for setting parameters of the cryptosystems confidently.
- Cryptosystems are based on problems unlikely to be NP-hard, while state-of-the-art attacks reduce to problems where we can show NP-hardness / fine-grained hardness.

Preliminaries: Lattice Problems

Lattice Problems and post-quantum cryptography:

- Cryptography based on number theory would be broken by attacks with quantum.
- People believe lattice problems have no quantum solution, and thus lattice-based cryptosystems are quantum-secure.

Desired hardness of lattice problems:

- Good news: *worst-case* hardness of lattice problems leads to *average-case* security of the cryptosystems.
- Need precise fine-grained hardness of lattice problems for setting parameters of the cryptosystems confidently.
- Cryptosystems are based on problems unlikely to be NP-hard, while state-of-the-art attacks reduce to problems where we can show NP-hardness / fine-grained hardness.

Preliminaries: Lattice Problems

γ-approximate Shortest Vector Problem in ℓ_p ($\mathrm{SVP}_{p,\gamma}$)

Instance: lattice $\mathcal{L}$.
Goal: decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$.

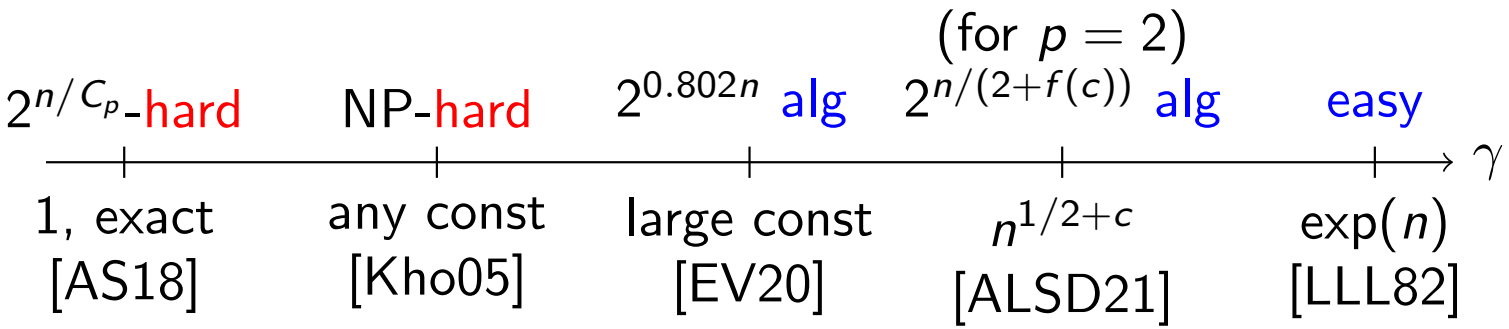
Hardness results and algorithms for $\mathrm{SVP}_{p,\gamma}$ (in previous works):

Preliminaries: Lattice Problems

γ-approximate Shortest Vector Problem in ℓ_p ($\mathrm{SVP}_{p,\gamma}$)

Instance: lattice $\mathcal{L}$.
Goal: decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$.

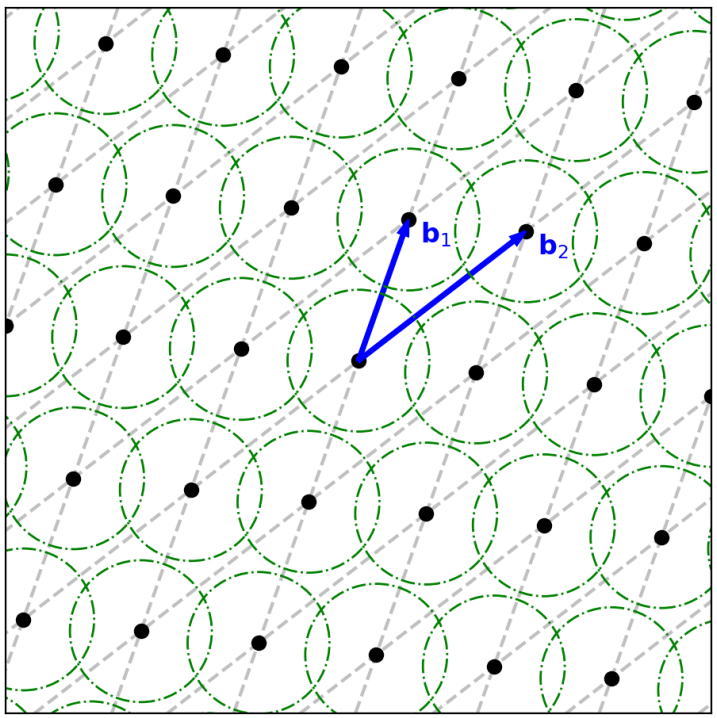
Hardness results and algorithms for $\mathrm{SVP}_{p,\gamma}$ (in previous works):



Preliminaries: Lattice Problems

Bounded Distance Decoding in ℓ_p with relative distance α ($\mathrm{BDD}_{p,\alpha}$)

Instance: lattice $\mathcal{L} \subset \mathbb{R}^d$ and target $t \in \mathbb{R}^d$
satisfying $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.
Goal: find closest lattice vector to t in $\mathcal{L}$.



($p = 2$, $\alpha = 0.6$)

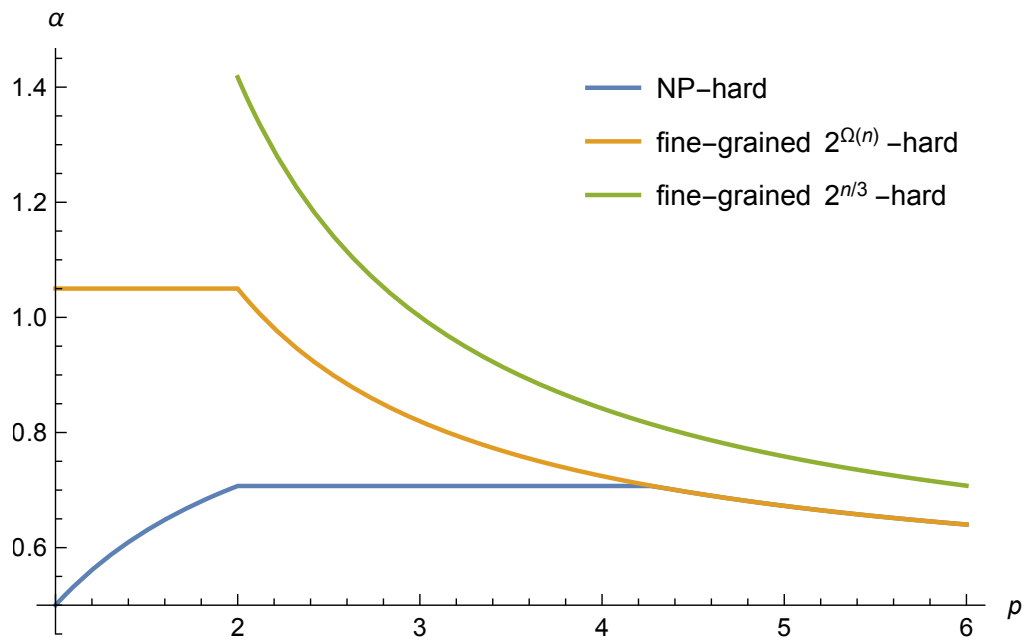
Preliminaries: Lattice Problems

$\mathrm{BDD}_{p,\alpha}$

Instance: $\mathcal{L}, t$ satisfying $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.
Goal: find closest lattice vector to t in $\mathcal{L}$.

Smaller α corresponds to stronger promise and easier problem.

Hardness results for $\mathrm{BDD}_{p,\alpha}$ (in previous works [LLM06, BP20]):



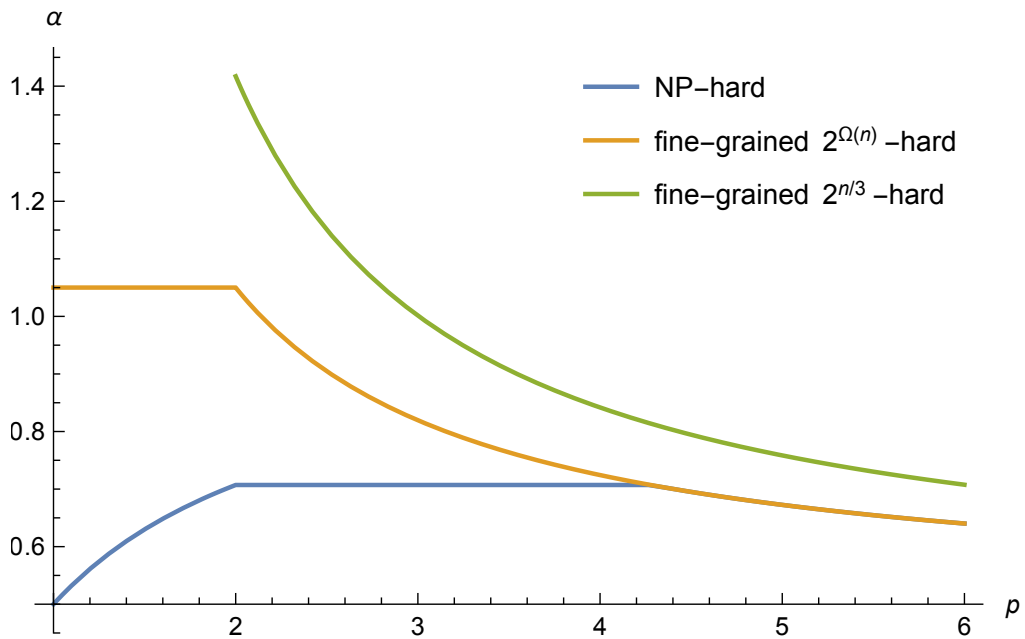
Preliminaries: Lattice Problems

$\mathrm{BDD}_{p,\alpha}$

Instance: $\mathcal{L}, t$ satisfying $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.
Goal: find closest lattice vector to t in $\mathcal{L}$.

Smaller α corresponds to stronger promise and easier problem.

Hardness results for $\mathrm{BDD}_{p,\alpha}$ (in previous works [LLM06, BP20]):



Preliminaries: Exponential Time Hypothesis

Standard approach to fine-grained hardness: Exponential Time Hypothesis (ETH).

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): k-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-ETH & Gap-SETH: Gap-3-$\mathrm{SAT}_{1-\delta,1}$ & Gap-k-$\mathrm{SAT}_{1-\delta,1}$.
- Randomized/non-uniform variants: rand/non-unif time.

Assumption strength:

- plain $\leq$ gap;
- plain $\leq$ randomized $\leq$ non-uniform.

Preliminaries: Exponential Time Hypothesis

Standard approach to fine-grained hardness: Exponential Time Hypothesis (ETH).

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): k-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-ETH & Gap-SETH: Gap-3-$\mathrm{SAT}_{1-\delta,1}$ & Gap-k-$\mathrm{SAT}_{1-\delta,1}$.
- Randomized/non-uniform variants: rand/non-unif time.

Assumption strength:

- plain $\leq$ gap;
- plain $\leq$ randomized $\leq$ non-uniform.

Preliminaries: Exponential Time Hypothesis

Standard approach to fine-grained hardness: Exponential Time Hypothesis (ETH).

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): k-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-ETH & Gap-SETH: Gap-3-$\mathrm{SAT}_{1-\delta,1}$ & Gap-k-$\mathrm{SAT}_{1-\delta,1}$.
- Randomized/non-uniform variants: rand/non-unif time.

Assumption strength:

- plain $\leq$ gap;
- plain $\leq$ randomized $\leq$ non-uniform.

Preliminaries: Exponential Time Hypothesis

Standard approach to fine-grained hardness: Exponential Time Hypothesis (ETH).

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): k-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-ETH & Gap-SETH: Gap-3-$\mathrm{SAT}_{1-\delta,1}$ & Gap-k-$\mathrm{SAT}_{1-\delta,1}$.
- Randomized/non-uniform variants: rand/non-unif time.

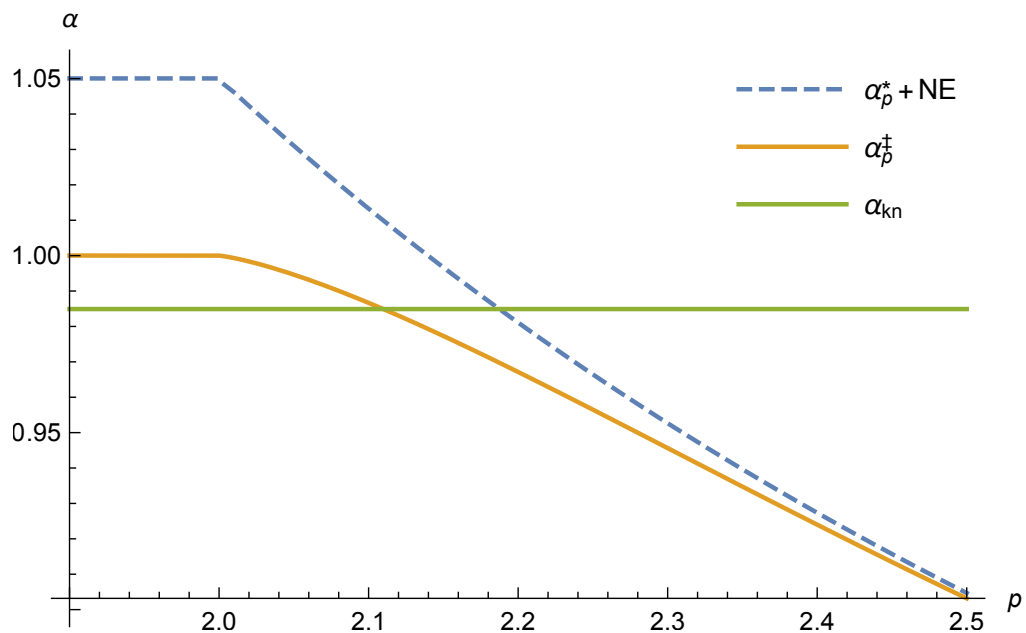
Assumption strength:

- plain $\leq$ gap;
- plain $\leq$ randomized $\leq$ non-uniform.

Our Results: ETH-Type Hardness of BDD

1. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{\mathsf{kn}} \approx 0.98491$, under non-unif Gap-ETH.
2. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_p^{\ddagger}$, under rand Gap-ETH.

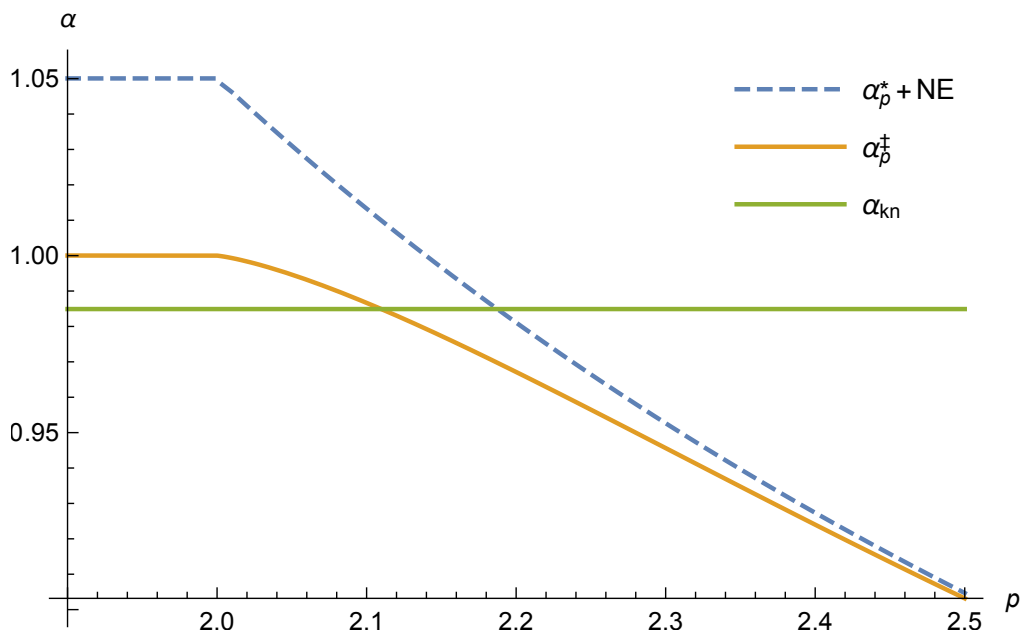
- Previous bound [BP20]: α_p^* (with norm embed), under rand ETH.



Our Results: ETH-Type Hardness of BDD

1. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{\mathsf{kn}} \approx 0.98491$, under non-unif Gap-ETH.
2. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_p^{\ddagger}$, under rand Gap-ETH.

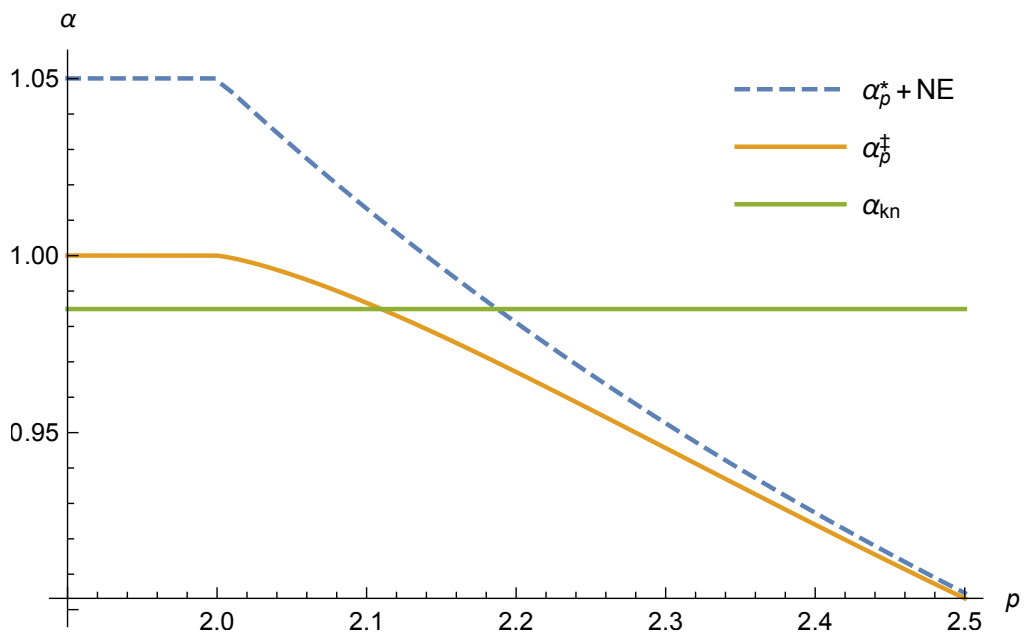
- Previous bound [BP20]: α_p^* (with norm embed), under rand ETH.



Our Results: ETH-Type Hardness of BDD

1. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{\mathsf{kn}} \approx 0.98491$, under non-unif Gap-ETH.
2. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_p^{\ddagger}$, under rand Gap-ETH.

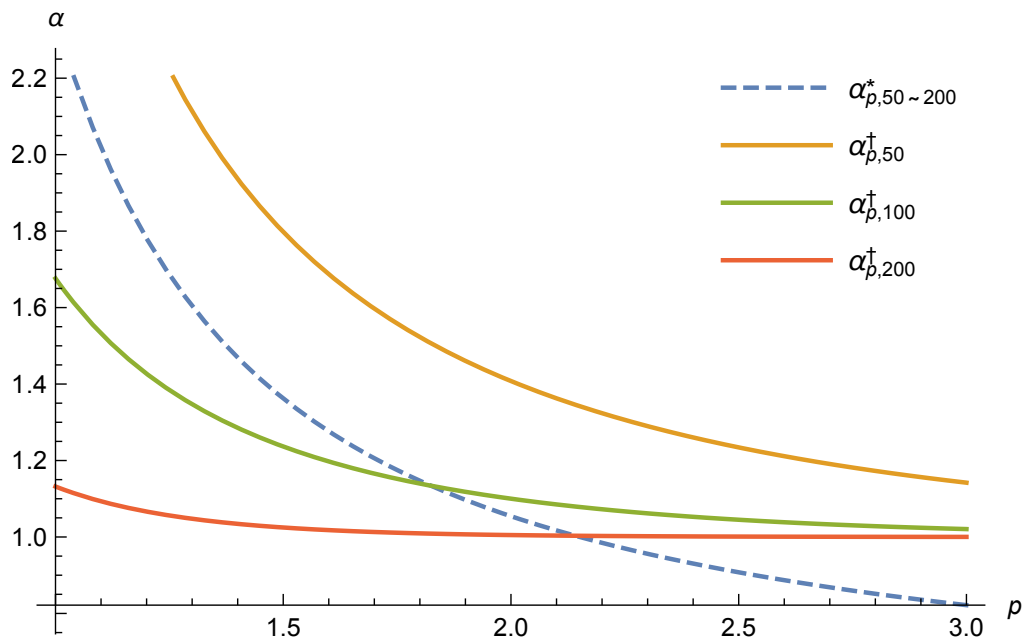
- Previous bound [BP20]: α_p^* (with norm embed), under rand ETH.



Our Results: SETH-Type Hardness of BDD

3. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for any $p \in [1,\infty)$, $p \notin 2\mathbb{Z}$, $C > 1$, and $\alpha > \alpha^{\dagger}_{p,C}$, under non-unif Gap-SETH.

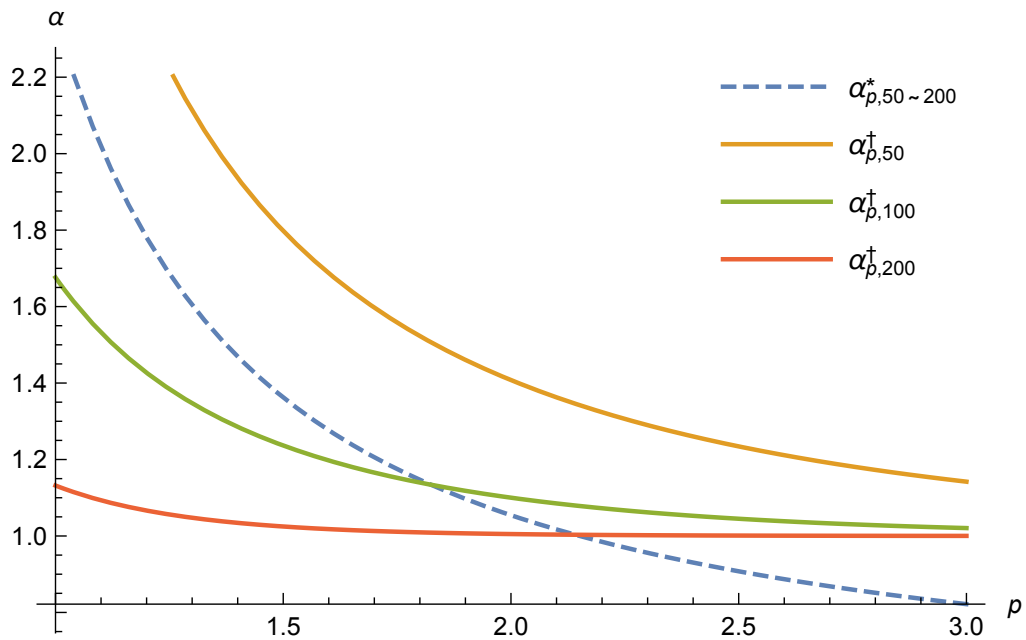
- Previous bound [BP20]: $\alpha^{*}_{p,C}$, under rand SETH.



Our Results: SETH-Type Hardness of BDD

3. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for any $p \in [1,\infty)$, $p \notin 2\mathbb{Z}$, $C > 1$, and $\alpha > \alpha^{\dagger}_{p,C}$, under non-unif Gap-SETH.

- Previous bound [BP20]: $\alpha^{*}_{p,C}$, under rand SETH.



Our Results: SETH-Type Hardness of SVP

4. For any $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$ and $C > C_p$, $\mathrm{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for some constant $\gamma > 1$, under randomized Gap-SETH.

- Previous result [AS18]: $\gamma = 1$, under rand SETH.

Our Results: SETH-Type Hardness of SVP

4. For any $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$ and $C > C_p$, $\mathrm{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for some constant $\gamma > 1$, under randomized Gap-SETH.

- Previous result [AS18]: $\gamma = 1$, under rand SETH.

Proof Starting Point: Gap-(S)ETH-Hardness of CVP'

γ-approximate Closest Vector Problem in ℓ_p ($\mathrm{CVP}_{p,\gamma}$)

Instance: lattice $\mathcal{L} \subset \mathbb{R}^d$ with basis B and target $t \in \mathbb{R}^d$.
Goal: decide whether $\mathrm{dist}_p(t, \mathcal{L}) \leq 1$ or $\mathrm{dist}_p(t, \mathcal{L}) > \gamma$.

Restriction $\mathrm{CVP}'_{p,\gamma}$: further require $\mathrm{dist}_p(t, B \cdot \{0,1\}^n) \leq 1$ for the case $\mathrm{dist}_p(t, \mathcal{L}) \leq 1$.

Proof Starting Point: Gap-(S)ETH-Hardness of CVP'

γ-approximate Closest Vector Problem in ℓ_p ($\mathrm{CVP}_{p,\gamma}$)

Instance: lattice $\mathcal{L} \subset \mathbb{R}^d$ with basis B and target $t \in \mathbb{R}^d$.
Goal: decide whether $\mathrm{dist}_p(t, \mathcal{L}) \leq 1$ or $\mathrm{dist}_p(t, \mathcal{L}) > \gamma$.

Restriction $\mathrm{CVP}'_{p,\gamma}$: further require $\mathrm{dist}_p(t, B \cdot \{0,1\}^n) \leq 1$ for the case $\mathrm{dist}_p(t, \mathcal{L}) \leq 1$.

Proof Starting Point: Gap-(S)ETH-Hardness of CVP'

Hardness results for $\mathrm{CVP}'_{p,\gamma}$:

- [BGS17] Under rand Gap-ETH, $\mathrm{CVP}'_{p,\gamma(p)}$ cannot be solved in $2^{o(n)}$ time.
- [ABGS21] Under rand Gap-SETH, ($p \notin 2\mathbb{Z}$,) $\mathrm{CVP}'_{p,\gamma(p,\varepsilon)}$ cannot be solved in $2^{(1-\varepsilon)n}$ time.

Goal: reduce $\mathrm{CVP}'_{p,\gamma}$ in rank n' to $\mathrm{BDD}/\mathrm{SVP}$ in rank $n = Cn'$.

- If C depends on γ then we get hardness for $2^{o(n)}$ time.
- If $C > 1$ is free then we get hardness for $2^{n/C}$ time.

Proof Starting Point: Gap-(S)ETH-Hardness of CVP'

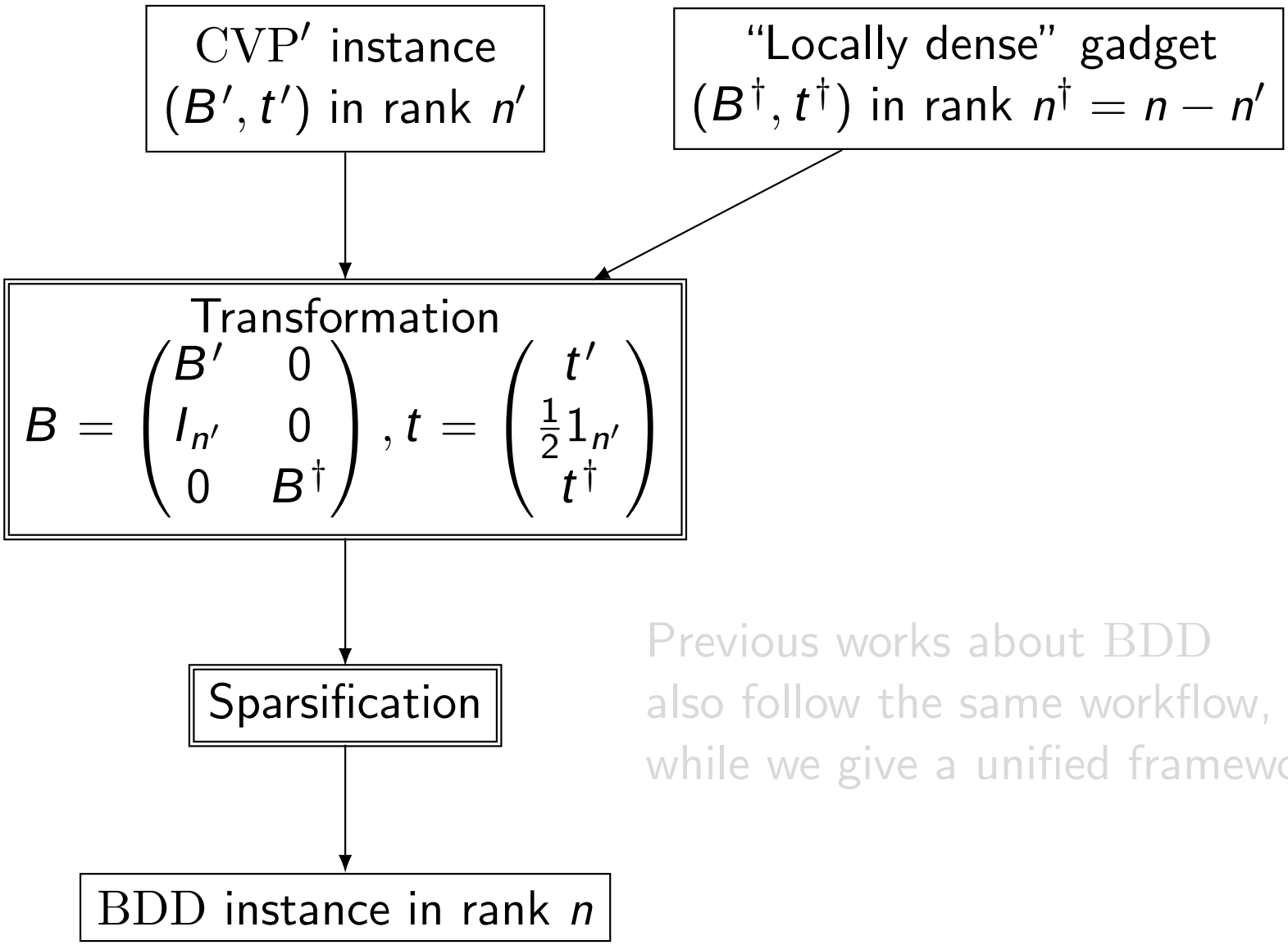
Hardness results for $\mathrm{CVP}'_{p,\gamma}$:

- [BGS17] Under rand Gap-ETH, $\mathrm{CVP}'_{p,\gamma(p)}$ cannot be solved in $2^{o(n)}$ time.
- [ABGS21] Under rand Gap-SETH, ($p \notin 2\mathbb{Z}$,) $\mathrm{CVP}'_{p,\gamma(p,\varepsilon)}$ cannot be solved in $2^{(1-\varepsilon)n}$ time.

Goal: reduce $\mathrm{CVP}'_{p,\gamma}$ in rank n' to $\mathrm{BDD}/\mathrm{SVP}$ in rank $n = Cn'$.

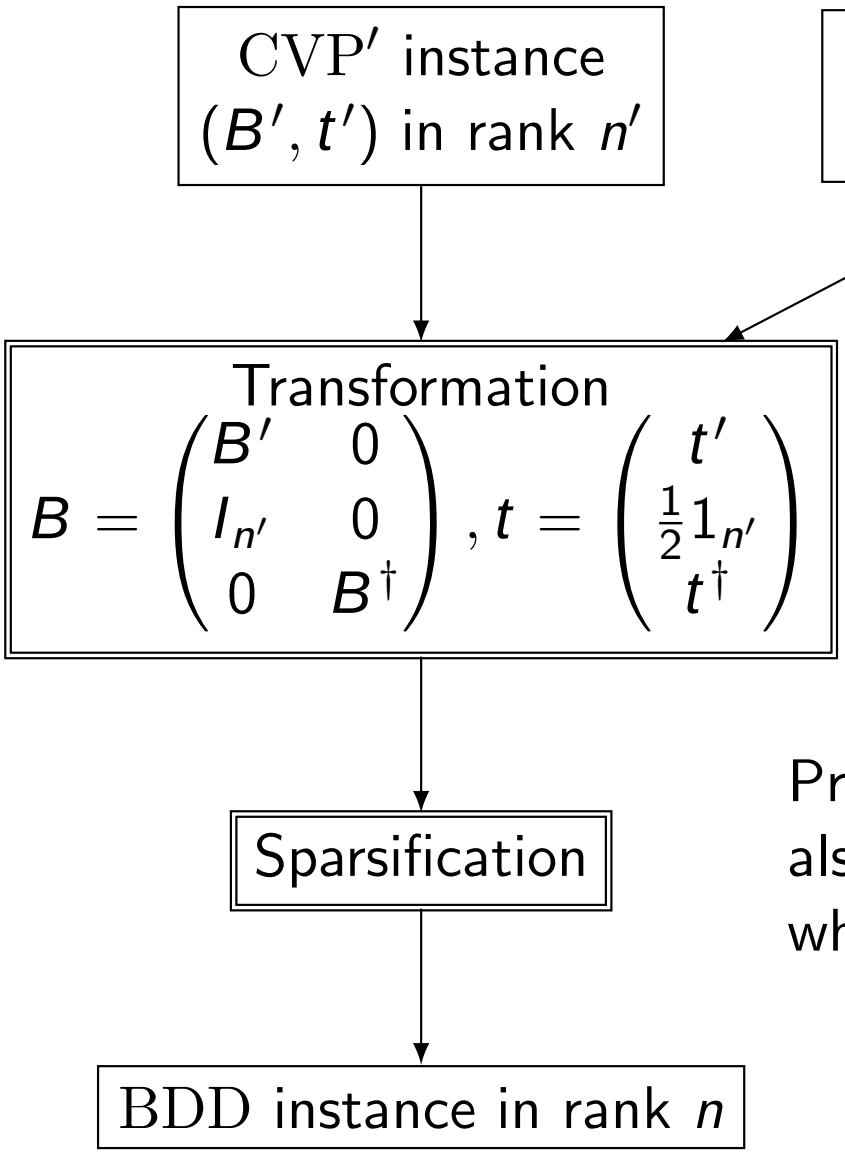
- If C depends on γ then we get hardness for $2^{o(n)}$ time.
- If $C > 1$ is free then we get hardness for $2^{n/C}$ time.

Reduction to BDD



Previous works about BDD also follow the same workflow, while we give a unified framework.

Reduction to BDD



Previous works about BDD also follow the same workflow, while we give a unified framework.

Rephrasing BDD with Point-Counting

Recall (search) $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ with $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, find closest lattice vector to t in $\mathcal{L}$.

Decisional $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ and distance r, decide whether

- $\mathrm{dist}_p(t, \mathcal{L}) \leq r$ and $\lambda_1^{(p)}(\mathcal{L}) \geq r/\alpha$, or
- $\mathrm{dist}_p(t, \mathcal{L}) > r$.

In terms of point-counting: decide whether

- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq 1$ and $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathcal{L} \setminus \{0\})| = 0$, or
- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| = 0$.

Relaxation (A, G)-$\mathrm{BDD}_{p,\alpha}$: decide whether

- "(good) close" count $\geq G$ and "short" count $\leq A$, or
- "annoying close" count $\leq A$.

(Decisional BDD is just $(0, 1)$-BDD.)

Rephrasing BDD with Point-Counting

Recall (search) $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ with $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, find closest lattice vector to t in $\mathcal{L}$.

Decisional $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ and distance r, decide whether

- $\mathrm{dist}_p(t, \mathcal{L}) \leq r$ and $\lambda_1^{(p)}(\mathcal{L}) \geq r/\alpha$, or
- $\mathrm{dist}_p(t, \mathcal{L}) > r$.

In terms of point-counting: decide whether

- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq 1$ and $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathcal{L} \setminus \{0\})| = 0$, or
- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| = 0$.

Relaxation (A, G)-$\mathrm{BDD}_{p,\alpha}$: decide whether

- "(good) close" count $\geq G$ and "short" count $\leq A$, or
- "annoying close" count $\leq A$.

(Decisional BDD is just $(0, 1)$-BDD.)

Rephrasing BDD with Point-Counting

Recall (search) $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ with $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, find closest lattice vector to t in $\mathcal{L}$.

Decisional $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ and distance r, decide whether

- $\mathrm{dist}_p(t, \mathcal{L}) \leq r$ and $\lambda_1^{(p)}(\mathcal{L}) \geq r/\alpha$, or
- $\mathrm{dist}_p(t, \mathcal{L}) > r$.

In terms of point-counting: decide whether

- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq 1$ and $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathcal{L} \setminus \{0\})| = 0$, or
- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| = 0$.

Relaxation (A, G)-$\mathrm{BDD}_{p,\alpha}$: decide whether

- "(good) close" count $\geq G$ and "short" count $\leq A$, or
- "annoying close" count $\leq A$.

(Decisional BDD is just $(0, 1)$-BDD.)

Rephrasing BDD with Point-Counting

Recall (search) $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ with $\mathrm{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, find closest lattice vector to t in $\mathcal{L}$.

Decisional $\mathrm{BDD}_{p,\alpha}$: given $\mathcal{L}, t$ and distance r, decide whether

- $\mathrm{dist}_p(t, \mathcal{L}) \leq r$ and $\lambda_1^{(p)}(\mathcal{L}) \geq r/\alpha$, or
- $\mathrm{dist}_p(t, \mathcal{L}) > r$.

In terms of point-counting: decide whether

- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq 1$ and $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathcal{L} \setminus \{0\})| = 0$, or
- $|\mathcal{B}_p(r; t) \cap \mathcal{L}| = 0$.

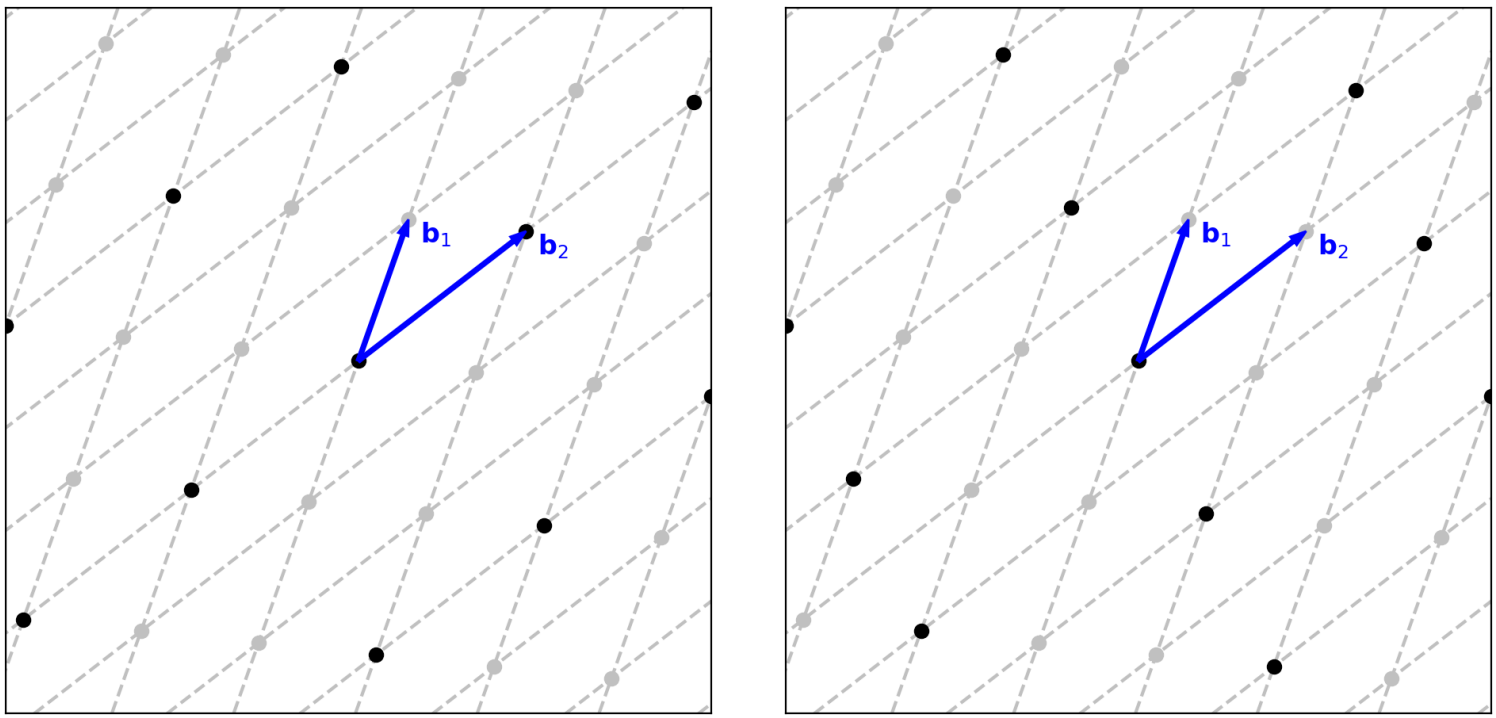
Relaxation (A, G)-$\mathrm{BDD}_{p,\alpha}$: decide whether

- "(good) close" count $\geq G$ and "short" count $\leq A$, or
- "annoying close" count $\leq A$.

(Decisional BDD is just $(0, 1)$-BDD.)

Lattice Sparsification

Sparsification algorithm: given lattice $\mathcal{L}$ and prime index q, sample sublattice $\mathcal{L}' \subset \mathcal{L}$ such that for any[1] finite set $S \subset \mathcal{L}$, $|S \cap \mathcal{L}'|$ concentrates around $|S|/q$.



$(q = 3)$

[1] S needs to satisfy certain technical conditions.

Lattice Sparsification

Sparsification algorithm: sample sublattice $\mathcal{L}' \subset \mathcal{L}$ such that $|S \cap \mathcal{L}'|$ concentrates around $|S|/q$.

If $G \gg A$, say $G \geq 400A$, then (A, G)-$\mathrm{BDD}_{p,\alpha}$ reduces to decisional $\mathrm{BDD}_{p,\alpha}$ by sparsification with index $q \approx 20A$.

New goal: reduce CVP' to (A, G)-BDD with $G \gg A$.

Lattice Sparsification

Sparsification algorithm: sample sublattice $\mathcal{L}' \subset \mathcal{L}$ such that $|S \cap \mathcal{L}'|$ concentrates around $|S|/q$.

If $G \gg A$, say $G \geq 400A$, then (A, G)-$\mathrm{BDD}_{p,\alpha}$ reduces to decisional $\mathrm{BDD}_{p,\alpha}$ by sparsification with index $q \approx 20A$.

New goal: reduce CVP' to (A, G)-BDD with $G \gg A$.

Transforming CVP' Instances

The transformation takes as input $\mathrm{CVP}'_{p,\gamma}$ instance (B', t') and parameters $B^\dagger, t^\dagger, r, s$, and outputs (A, G)-$\mathrm{BDD}_{p,\alpha}$ instance:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix}, \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}, \qquad r .$$

For CVP' YES instance:

- Promise: $\mathrm{dist}_p(t', B'x) \leq 1$ for some $x \in \{0,1\}^{n'}$.
- "Short" count: $|\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.
- "Close" count: $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq |\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger|$.[2]

[2] The arithmetic of the distances here is showcased for ℓ_1, and should be $(r^p - s^p - n'/2^p)^{1/p}$ for general ℓ_p. We will continue to simplify this way in the remaining slides.

Transforming CVP' Instances

The transformation takes as input $\mathrm{CVP}'_{p,\gamma}$ instance (B', t') and parameters $B^\dagger, t^\dagger, r, s$, and outputs (A, G)-$\mathrm{BDD}_{p,\alpha}$ instance:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix}, \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}, \qquad r\ .$$

For CVP' YES instance:

- Promise: $\mathrm{dist}_p(t', B'x) \leq 1$ for some $x \in \{0,1\}^{n'}$.
- "Short" count: $|\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.
- "Close" count: $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq |\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger|$.[2]

[2] The arithmetic of the distances here is showcased for ℓ_1, and should be $(r^p - s^p - n'/2^p)^{1/p}$ for general ℓ_p. We will continue to simplify this way in the remaining slides.

Transforming CVP' Instances

The transformation takes as input $\mathrm{CVP}'_{p,\gamma}$ instance (B', t') and parameters $B^\dagger, t^\dagger, r, s$, and outputs (A, G)-$\mathrm{BDD}_{p,\alpha}$ instance:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix}, \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}, \qquad r .$$

For CVP' YES instance:

- Promise: $\mathrm{dist}_p(t', B'x) \leq 1$ for some $x \in \{0,1\}^{n'}$.
- "Short" count: $|\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.
- "Close" count: $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq |\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger|$.[2]

[2] The arithmetic of the distances here is showcased for ℓ_1, and should be $(r^p - s^p - n'/2^p)^{1/p}$ for general ℓ_p. We will continue to simplify this way in the remaining slides.

Transforming CVP' Instances

The transformation takes as input $\mathrm{CVP}'_{p,\gamma}$ instance (B', t') and parameters $B^\dagger, t^\dagger, r, s$, and outputs (A, G)-$\mathrm{BDD}_{p,\alpha}$ instance:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix}, \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}, \qquad r\ .$$

For CVP' YES instance:

- Promise: $\mathrm{dist}_p(t', B'x) \leq 1$ for some $x \in \{0,1\}^{n'}$.
- "Short" count: $|\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.
- "Close" count: $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \geq |\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger|$.[2]

[2] The arithmetic of the distances here is showcased for ℓ_1, and should be $(r^p - s^p - n'/2^p)^{1/p}$ for general ℓ_p. We will continue to simplify this way in the remaining slides.

Transforming CVP' Instances

The transformation outputs:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix} , \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix} , \qquad r .$$

For CVP' NO instance:

- Promise: $\mathrm{dist}_p(t', \mathcal{L}') > \gamma$.
- "Annoying close" count:

$$|\mathcal{B}_p(r; t) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|.$$

Putting together, for $G \gg A$, we want:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg \max\{|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|, |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|\} .$$

Transforming CVP' Instances

The transformation outputs:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix} , \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix} , \qquad r .$$

For CVP' NO instance:

- Promise: $\mathrm{dist}_p(t', \mathcal{L}') > \gamma$.
- "Annoying close" count:
  $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.

Putting together, for $G \gg A$, we want:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg \max\{|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|, |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|\} .$$

Transforming CVP' Instances

The transformation outputs:

$$B = \begin{pmatrix} sB' & 0 \\ I_{n'} & 0 \\ 0 & B^\dagger \end{pmatrix} , \qquad t = \begin{pmatrix} st' \\ \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix} , \qquad r .$$

For CVP' NO instance:

- Promise: $\mathrm{dist}_p(t', \mathcal{L}') > \gamma$.
- "Annoying close" count:
  $|\mathcal{B}_p(r; t) \cap \mathcal{L}| \leq |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.

Putting together, for $G \gg A$, we want:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg \max\{|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|, \\ |\mathcal{B}_p^\circ(r - \gamma s; \begin{pmatrix} \frac{1}{2}1_{n'} \\ t^\dagger \end{pmatrix}) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|\} .$$

Locally Dense Gadgets

Desired property (first consider the "short" term):

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \ .$$

Observations:

- $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger|$.
- $|\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^{n'}|$ is exponential in n' (for sufficiently large ρ).

Hence we want the gadget to be *locally dense*, i.e., to have exponentially more "close" than "short" lattice vectors:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger| \ .$$

(Similarly, we also want the locally dense gadget to have exponentially more "close" than "annoying close" lattice vectors.)

Locally Dense Gadgets

Desired property (first consider the "short" term):

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \ .$$

Observations:

- $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger|$.
- $|\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^{n'}|$ is exponential in n' (for sufficiently large ρ).

Hence we want the gadget to be *locally dense*, i.e., to have exponentially more "close" than "short" lattice vectors:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger| \ .$$

(Similarly, we also want the locally dense gadget to have exponentially more "close" than "annoying close" lattice vectors.)

Locally Dense Gadgets

Desired property (first consider the "short" term):

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \ .$$

Observations:

- $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger|$.
- $|\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^{n'}|$ is exponential in n' (for sufficiently large ρ).

Hence we want the gadget to be *locally dense*, i.e., to have exponentially more "close" than "short" lattice vectors:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger| \ .$$

(Similarly, we also want the locally dense gadget to have exponentially more "close" than "annoying close" lattice vectors.)

Locally Dense Gadgets

Desired property (first consider the "short" term):

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \gg |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \ .$$

Observations:

- $|\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger|$.
- $|\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^{n'}|$ is exponential in n' (for sufficiently large ρ).

Hence we want the gadget to be *locally dense*, i.e., to have exponentially more "close" than "short" lattice vectors:

$$|\mathcal{B}_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger| \ .$$

(Similarly, we also want the locally dense gadget to have exponentially more "close" than "annoying close" lattice vectors.)

Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets $(B^\dagger, t^\dagger)$ satisfying[3]

$$|\mathcal{B}_p(\alpha_G; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(1) \cap \mathcal{L}^\dagger| \ ,$$

then for $\mathrm{BDD}_{p,\alpha}$:
under Gap-ETH,[4] it cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_G$;
under Gap-SETH, it cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_G + \frac{1}{f_p(\nu^{C-1})} \ .$$

(Here $f_p(\cdot)$ is increasing and has $\lim_{x\to 1} f_p(x) = 0$, $\lim_{x\to\infty} f_p(x) = \infty$.)

[3] The locally dense gadget needs to satisfy another similar property involving "annoying close" count, which contains similar parameters α_A, ν' and they also (substantially) affect the bounds on α.

[4] Whether we need rand/non-unif Gap-(S)ETH depends on whether the gadgets can be efficiently constructed.

Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets $(B^\dagger, t^\dagger)$ satisfying[3]

$$|\mathcal{B}_p(\alpha_G; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(1) \cap \mathcal{L}^\dagger| \ ,$$

then for $\mathrm{BDD}_{p,\alpha}$:
under Gap-ETH,[4] it cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_G$;
under Gap-SETH, it cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_G + \frac{1}{f_p(\nu^{C-1})} \ .$$

(Here $f_p(\cdot)$ is increasing and has $\lim_{x\to 1} f_p(x) = 0$, $\lim_{x\to\infty} f_p(x) = \infty$.)

[3] The locally dense gadget needs to satisfy another similar property involving "annoying close" count, which contains similar parameters α_A, ν' and they also (substantially) affect the bounds on α.

[4] Whether we need rand/non-unif Gap-(S)ETH depends on whether the gadgets can be efficiently constructed.

Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets $(B^\dagger, t^\dagger)$ satisfying[3]

$$|\mathcal{B}_p(\alpha_G; t^\dagger) \cap \mathcal{L}^\dagger| \geq \nu^{n^\dagger} |\mathcal{B}_p^\circ(1) \cap \mathcal{L}^\dagger| \ ,$$

then for $\mathrm{BDD}_{p,\alpha}$:
under Gap-ETH,[4] it cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_G$;
under Gap-SETH, it cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_G + \frac{1}{f_p(\nu^{C-1})} \ .$$

(Here $f_p(\cdot)$ is increasing and has $\lim_{x\to 1} f_p(x) = 0$, $\lim_{x\to\infty} f_p(x) = \infty$.)

[3] The locally dense gadget needs to satisfy another similar property involving "annoying close" count, which contains similar parameters α_A, ν' and they also (substantially) affect the bounds on α.

[4] Whether we need rand/non-unif Gap-(S)ETH depends on whether the gadgets can be efficiently constructed.

Instantiating the Main Theorem: Result 3

Lattice *kissing number* τ_n^{L}: $\max_{\mathcal{L}} |\mathcal{B}_p(1) \cap (\mathcal{L} \setminus \{0\})|$ for rank-n lattice $\mathcal{L}$ with $\lambda_1^{(p)}(\mathcal{L}) = 1$.

[Vlă19]: for $p = 2$, $\tau_n^{\mathsf{L}} \geq 2^{c_{\mathsf{kn}} n - o(n)}$, where $c_{\mathsf{kn}} \geq 0.02194$.

Gadgets (in ℓ_2): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$. Parameters: $\alpha_G = 1$, $\nu = 2^{c_{\mathsf{kn}}}$.

Using norm embeddings, we also get gadgets in all ℓ_p in cost of slightly larger $\alpha_G = 1 + o(1)$. Then we have our Result 3: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_{p,C}^\dagger := 1 + \frac{1}{f_p(2^{c_{\mathsf{kn}}(C-1)})} .$$

Instantiating the Main Theorem: Result 3

Lattice *kissing number* τ_n^{L}: $\max_{\mathcal{L}} |\mathcal{B}_p(1) \cap (\mathcal{L} \setminus \{0\})|$ for rank-n lattice $\mathcal{L}$ with $\lambda_1^{(p)}(\mathcal{L}) = 1$.

[Vlă19]: for $p = 2$, $\tau_n^{\mathsf{L}} \geq 2^{c_{\mathsf{kn}} n - o(n)}$, where $c_{\mathsf{kn}} \geq 0.02194$.

Gadgets (in ℓ_2): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$. Parameters: $\alpha_G = 1$, $\nu = 2^{c_{\mathsf{kn}}}$.

Using norm embeddings, we also get gadgets in all ℓ_p in cost of slightly larger $\alpha_G = 1 + o(1)$. Then we have our Result 3: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_{p,C}^\dagger := 1 + \frac{1}{f_p(2^{c_{\mathsf{kn}}(C-1)})} .$$

Instantiating the Main Theorem: Result 3

Lattice *kissing number* τ_n^{L}: $\max_{\mathcal{L}} |\mathcal{B}_p(1) \cap (\mathcal{L} \setminus \{0\})|$ for rank-n lattice $\mathcal{L}$ with $\lambda_1^{(p)}(\mathcal{L}) = 1$.

[Vlă19]: for $p = 2$, $\tau_n^{\mathsf{L}} \geq 2^{c_{\mathsf{kn}} n - o(n)}$, where $c_{\mathsf{kn}} \geq 0.02194$.

Gadgets (in ℓ_2): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$.
Parameters: $\alpha_G = 1$, $\nu = 2^{c_{\mathsf{kn}}}$.

Using norm embeddings, we also get gadgets in all ℓ_p in cost of slightly larger $\alpha_G = 1 + o(1)$. Then we have our Result 3: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_{p,C}^\dagger := 1 + \frac{1}{f_p(2^{c_{\mathsf{kn}}(C-1)})} .$$

Instantiating the Main Theorem: Result 3

Lattice *kissing number* τ_n^{L}: $\max_{\mathcal{L}} |\mathcal{B}_p(1) \cap (\mathcal{L} \setminus \{0\})|$ for rank-n lattice $\mathcal{L}$ with $\lambda_1^{(p)}(\mathcal{L}) = 1$.

[Vlă19]: for $p = 2$, $\tau_n^{\mathsf{L}} \geq 2^{c_{\mathsf{kn}} n - o(n)}$, where $c_{\mathsf{kn}} \geq 0.02194$.

Gadgets (in ℓ_2): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$. Parameters: $\alpha_G = 1$, $\nu = 2^{c_{\mathsf{kn}}}$.

Using norm embeddings, we also get gadgets in all ℓ_p in cost of slightly larger $\alpha_G = 1 + o(1)$. Then we have our Result 3: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_{p,C}^\dagger := 1 + \frac{1}{f_p(2^{c_{\mathsf{kn}}(C-1)})} \ .$$

Instantiating the Main Theorem: Result 1

To decrease α_G for the exponential kissing number gadgets:

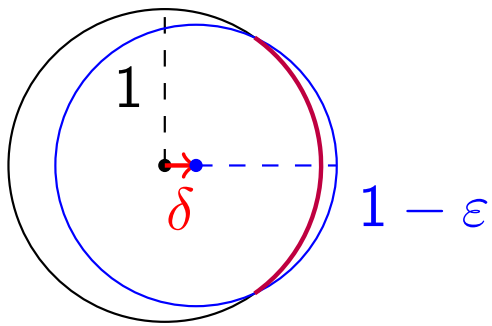
- Move $t^\dagger$ away from 0 by δ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the "close" count as well, by an expected factor of $\text{area}(S^{n-1} \cap \mathcal{B}_p(1-\varepsilon; t^\dagger))/\,\text{area}(S^{n-1})$, where S^{n-1} is the unit sphere.
- ([AS18] also uses this idea while we have tighter loss factor.)

Taking care of the tradeoff between the "close" count and δ, ε, we manage to get α_G approaching $2^{-c_{\text{kn}}}$, which gives our Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\text{kn}} := 2^{-c_{\text{kn}}}$.

Instantiating the Main Theorem: Result 1

To decrease α_G for the exponential kissing number gadgets:

- Move $t^\dagger$ away from 0 by δ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the "close" count as well, by an expected factor of $\text{area}(S^{n-1} \cap \mathcal{B}_p(1-\varepsilon; t^\dagger))/\,\text{area}(S^{n-1})$, where S^{n-1} is the unit sphere.
- ([AS18] also uses this idea while we have tighter loss factor.)

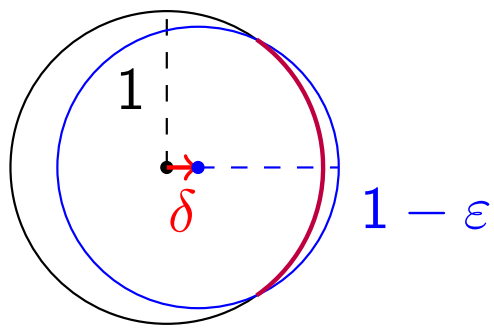


Taking care of the tradeoff between the "close" count and δ, ε, we manage to get α_G approaching $2^{-c_{\text{kn}}}$, which gives our Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\text{kn}} := 2^{-c_{\text{kn}}}$.

Instantiating the Main Theorem: Result 1

To decrease α_G for the exponential kissing number gadgets:

- Move $t^\dagger$ away from 0 by δ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the "close" count as well, by an expected factor of $\text{area}(S^{n-1} \cap \mathcal{B}_p(1-\varepsilon; t^\dagger))/\,\text{area}(S^{n-1})$, where S^{n-1} is the unit sphere.
- ([AS18] also uses this idea while we have tighter loss factor.)



Taking care of the tradeoff between the "close" count and δ, ε, we manage to get α_G approaching $2^{-c_{\mathsf{kn}}}$, which gives our Result 1: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\mathsf{kn}} := 2^{-c_{\mathsf{kn}}}$.

Instantiating the Main Theorem: Result 2

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n/\rho$, $t^\dagger = (t/\rho) \cdot 1_n$.
Minimize α_G over ρ, t subject to

$$|\mathcal{B}_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^n| \ .$$

Suppose $\alpha_p^\ddagger$ is the optimum. Then we have our Result 2: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\ddagger$.

- $|\mathcal{B}_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ can be approximated by a numerical function $\beta_{p,t}(a)^n$ to within a $2^{o(n)}$ factor.
- We find that empirically the optimizer for t is always $1/2$.
- [BP20] does no optimization and fix $t = 1/2$, $\rho = n/(2\alpha_G)$. As a result, our Result 2 is always no weaker than [BP20].

Instantiating the Main Theorem: Result 2

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n/\rho$, $t^\dagger = (t/\rho) \cdot 1_n$.
Minimize α_G over ρ, t subject to

$$|\mathcal{B}_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^n| \ .$$

Suppose $\alpha_p^\ddagger$ is the optimum. Then we have our Result 2: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\ddagger$.

- $|\mathcal{B}_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ can be approximated by a numerical function $\beta_{p,t}(a)^n$ to within a $2^{o(n)}$ factor.
- We find that empirically the optimizer for t is always $1/2$.
- [BP20] does no optimization and fix $t = 1/2$, $\rho = n/(2\alpha_G)$. As a result, our Result 2 is always no weaker than [BP20].

Instantiating the Main Theorem: Result 2

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n/\rho$, $t^\dagger = (t/\rho)\cdot 1_n$.
Minimize α_G over ρ, t subject to

$$|\mathcal{B}_p(\alpha_G \rho; t\cdot 1_n) \cap \mathbb{Z}^n| > |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^n| \ .$$

Suppose $\alpha_p^\ddagger$ is the optimum. Then we have our Result 2: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\ddagger$.

- $|\mathcal{B}_p(a\cdot n; t\cdot 1_n) \cap \mathbb{Z}^n|$ can be approximated by a numerical function $\beta_{p,t}(a)^n$ to within a $2^{o(n)}$ factor.
- We find that empirically the optimizer for t is always $1/2$.
- [BP20] does no optimization and fix $t = 1/2$, $\rho = n/(2\alpha_G)$. As a result, our Result 2 is always no weaker than [BP20].

Instantiating the Main Theorem: Result 2

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n/\rho$, $t^\dagger = (t/\rho)\cdot 1_n$.
Minimize α_G over ρ, t subject to

$$|\mathcal{B}_p(\alpha_G \rho; t\cdot 1_n) \cap \mathbb{Z}^n| > |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^n| \ .$$

Suppose $\alpha_p^\ddagger$ is the optimum. Then we have our Result 2: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\ddagger$.

- $|\mathcal{B}_p(a\cdot n; t\cdot 1_n) \cap \mathbb{Z}^n|$ can be approximated by a numerical function $\beta_{p,t}(a)^n$ to within a $2^{o(n)}$ factor.
- We find that empirically the optimizer for t is always $1/2$.
- [BP20] does no optimization and fix $t = 1/2$, $\rho = n/(2\alpha_G)$. As a result, our Result 2 is always no weaker than [BP20].

Instantiating the Main Theorem: Result 2

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n/\rho$, $t^\dagger = (t/\rho) \cdot 1_n$.
Minimize α_G over ρ, t subject to

$$|\mathcal{B}_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^n| \ .$$

Suppose $\alpha_p^\ddagger$ is the optimum. Then we have our Result 2: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\ddagger$.

- $|\mathcal{B}_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ can be approximated by a numerical function $\beta_{p,t}(a)^n$ to within a $2^{o(n)}$ factor.
- We find that empirically the optimizer for t is always $1/2$.
- [BP20] does no optimization and fix $t = 1/2$, $\rho = n/(2\alpha_G)$. As a result, our Result 2 is always no weaker than [BP20].

Reduction to SVP

Overview:

- Similar to the case of BDD, the reduction consists of the (same!) transformation and the sparsification, as well as a standard technique, Kannan's embedding, at the end.
- The transformation maps $\mathrm{CVP}'_{p,\gamma}$ instances to instances of a similar intermediate problem $(A, G)\text{-}\mathrm{CVP}_{p,\gamma'}$.
- [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for $\mathrm{CVP}'_{p,\gamma}$ other than $\mathrm{CVP}'_{p,1}$.
- The same gadgets from integer lattices as Result 2 are used.

Reduction to SVP

Overview:

- Similar to the case of BDD, the reduction consists of the (same!) transformation and the sparsification, as well as a standard technique, Kannan's embedding, at the end.
- The transformation maps $\mathrm{CVP}'_{p,\gamma}$ instances to instances of a similar intermediate problem (A, G)-$\mathrm{CVP}_{p,\gamma'}$.
- [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for $\mathrm{CVP}'_{p,\gamma}$ other than $\mathrm{CVP}'_{p,1}$.
- The same gadgets from integer lattices as Result 2 are used.

Reduction to SVP

Overview:

- Similar to the case of BDD, the reduction consists of the (same!) transformation and the sparsification, as well as a standard technique, Kannan's embedding, at the end.
- The transformation maps $\mathrm{CVP}'_{p,\gamma}$ instances to instances of a similar intermediate problem (A, G)-$\mathrm{CVP}_{p,\gamma'}$.
- [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for $\mathrm{CVP}'_{p,\gamma}$ other than $\mathrm{CVP}'_{p,1}$.
- The same gadgets from integer lattices as Result 2 are used.

Reduction to SVP

Overview:

- Similar to the case of BDD, the reduction consists of the (same!) transformation and the sparsification, as well as a standard technique, Kannan's embedding, at the end.
- The transformation maps $\mathrm{CVP}'_{p,\gamma}$ instances to instances of a similar intermediate problem (A, G)-$\mathrm{CVP}_{p,\gamma'}$.
- [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for $\mathrm{CVP}'_{p,\gamma}$ other than $\mathrm{CVP}'_{p,1}$.
- The same gadgets from integer lattices as Result 2 are used.

References

Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz.
Fine-grained hardness of CVP(P)—everything that we can prove (and nothing else).
In *SODA*, pages 1816–1835, 2021.

Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz.
A $2^{n/2}$-time algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an improved time-approximation tradeoff for (H)SVP.
In *EUROCRYPT*, pages 467–497. 2021.

Divesh Aggarwal and Noah Stephens-Davidowitz.
(Gap/S)ETH hardness of SVP.
In *STOC*, pages 228–238, 2018.

Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz.
On the quantitative hardness of CVP.
In *FOCS*, pages 13–24. 2017.

Huck Bennett and Chris Peikert.
Hardness of bounded distance decoding on lattices in ℓ_p norms.
In *CCC*, pages Art. 36, 21. 2020.

Friedrich Eisenbrand and Moritz Venzin.
Approximate CVP_p in time $2^{0.802n}$.
In *ESA*, pages Art. No. 43, 15. 2020.

Subhash Khot.
Hardness of approximating the shortest vector problem in lattices.
J. ACM, 52(5):789–808, 2005.

A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász.
Factoring polynomials with rational coefficients.
Math. Ann., 261(4):515–534, 1982.

Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio.
On bounded distance decoding for general lattices.
In *Approximation, randomization and combinatorial optimization*, volume 4110 of *Lecture Notes in Comput. Sci.*, pages 450–461. Springer, Berlin, 2006.

Serge Vlăduț.
Lattices with exponentially large kissing numbers.
Mosc. J. Comb. Number Theory, 8(2):163–177, 2019.