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

![Diagram of lattice points and basis vectors](image)
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 $\ell_p$) $\lambda_1^{(p)}(\mathcal{L})$: smallest $\ell_p$ 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.
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 \( \ell_p \) (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 SVP\(_{p,\gamma}\) (in previous works):**

<table>
<thead>
<tr>
<th>( 2^{n/C_p} )-hard</th>
<th>NP-hard</th>
<th>( 2^{0.802n} ) alg</th>
<th>( 2^{n/(2+f(c))} ) alg</th>
<th>easy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, exact [AS18]</td>
<td>any const large const [Kho05] [EV20]</td>
<td>[ALSD21] [LLL82]</td>
<td>exp(( n ))</td>
<td></td>
</tr>
</tbody>
</table>
### Preliminaries: Lattice Problems

**γ-approximate Shortest Vector Problem in ℓₚ (SVPₚ,γ)**

**Instance:** lattice \( L \).
**Goal:** decide whether \( \lambda₁^{(p)}(L) \leq 1 \) or \( \lambda₁^{(p)}(L) > γ \).

<table>
<thead>
<tr>
<th>Hardness results and algorithms for SVPₚ,γ (in previous works):</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2^{n/C_p} )-hard</td>
</tr>
<tr>
<td>1, exact ([AS18])</td>
</tr>
</tbody>
</table>
Preliminaries: Lattice Problems

**Bounded Distance Decoding in $\ell_p$**

with relative distance $\alpha$ ($\text{BDD}_{p,\alpha}$)

Instance: lattice $\mathcal{L} \subseteq \mathbb{R}^d$ and target $t \in \mathbb{R}^d$ satisfying $\text{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.

Goal: find closest lattice vector to $t$ in $\mathcal{L}$.

($p = 2, \alpha = 0.6$)
Preliminaries: Lattice Problems

**BDD}_{p, \alpha}**

Instance: \( \mathcal{L}, t \) satisfying \( \text{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda^{(p)}_1(\mathcal{L}) \).

Goal: find closest lattice vector to \( t \) in \( \mathcal{L} \).

Smaller \( \alpha \) corresponds to stronger promise and easier problem.

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

![Graph showing hardness results for BDD_{p, \alpha}](image)
Preliminaries: Lattice Problems

**BDD}_{p,\alpha}\)**

Instance: $\mathcal{L}, \mathbf{t}$ satisfying $\text{dist}_p(\mathbf{t}, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.

Goal: find closest lattice vector to $\mathbf{t}$ in $\mathcal{L}$.

Smaller $\alpha$ corresponds to stronger promise and easier problem.

Hardness results for $\text{BDD}_{p,\alpha}$ (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-SAT$_{1-\delta,1}$ & Gap-k-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-SAT$_{1-\delta,1}$ & Gap-$k$-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: $\text{Gap-3-SAT}_{1-\delta,1}$ & $\text{Gap-k-SAT}_{1-\delta,1}$.
▶ 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-SAT$_{1-\delta,1}$ & Gap-$k$-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. BDD_{p,\alpha} cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{kn} \approx 0.98491$, under non-unif Gap-ETH.

2. BDD_{p,\alpha} cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_p^{\dagger}$, under rand Gap-ETH.

Previous bound [BP20]: $\alpha_p^*$ (with norm embed), under rand ETH.
Our Results: ETH-Type Hardness of BDD

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

► Previous bound [BP20]: $\alpha_{p}^{*}$ (with norm embed), under rand ETH.
Our Results: ETH-Type Hardness of BDD

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

2. $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_p^{\dagger}$, under rand Gap-ETH.

Previous bound [BP20]: $\alpha_p^*$ (with norm embed), under rand ETH.
Our Results: SETH-Type Hardness of BDD

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

Previous bound [BP20]: $\alpha_{p,C}^*$, under rand SETH.
Our Results: SETH-Type Hardness of BDD

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

- Previous bound [BP20]: $\alpha_{p,C}^\ast$, under rand SETH.
4. For any $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$ and $C > C_p$, $\text{SVP}_{p,\gamma}$ 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 $C > C_p$, 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 $CVP'$

$\gamma$-approximate Closest Vector Problem in $\ell_p$ ($CVP_{p,\gamma}$)

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

Restriction $CVP'_{p,\gamma}$: further require $\text{dist}_p(t, B \cdot \{0,1\}^n) \leq 1$ for the case $\text{dist}_p(t, \mathcal{L}) \leq 1$. 
Proof Starting Point: Gap-(S)ETH-Hardness of CVP′

$\gamma$-approximate Closest Vector Problem in $\ell_p$ ($\text{CVP}_{p,\gamma}$)

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

Restriction $\text{CVP'}_{p,\gamma}$: further require $\text{dist}_p(t, B \cdot \{0,1\}^n) \leq 1$ for the case $\text{dist}_p(t, \mathcal{L}) \leq 1$. 
Proof Starting Point: Gap-(S)ETH-Hardness of CVP′

Hardness results for $\text{CVP}′_{p,\gamma}$:

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

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

- If $C$ depends on $\gamma$ then we get hardness for $2^{o(n)}$ time.
- If $C > 1$ is free then we get hardness for $2^{n/C}$ time.
Hardness results for $\text{CVP}'_{p,\gamma}$:

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

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

- If $C$ depends on $\gamma$ 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

CVP' instance \((B', t')\) in rank \(n'\)

"Locally dense" gadget \((B^\dagger, t^\dagger)\) in rank \(n^\dagger = n - n'\)

Transformation

\[
B = \begin{pmatrix}
B' & 0 \\
I_{n'} & 0 \\
0 & B^\dagger
\end{pmatrix},
\quad t = \begin{pmatrix}
t' \\
\frac{1}{2} 1_{n'} \\
t^\dagger
\end{pmatrix}
\]

Sparsification

BDD instance in rank \(n\)

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

CVP' instance \((B', t')\) in rank \(n'\)

“Locally dense” gadget \((B^\dagger, t^\dagger)\) in rank \(n^\dagger = n - n'\)

Transformation

\[
B = \begin{pmatrix}
B' & 0 \\
I_{n'} & 0 \\
0 & B^\dagger
\end{pmatrix},
\quad t = \begin{pmatrix}
t' \\
\frac{1}{2}1_{n'} \\
t^\dagger
\end{pmatrix}
\]

Sparsification

BDD instance in rank \(n\)

Previous works about BDD also follow the same workflow, while we give a unified framework.
Rephrasing BDD with Point-Counting

Recall (search) $\text{BDD}_{p,\alpha}$: given $\mathcal{L}, \mathbf{t}$ with $\text{dist}_p(\mathbf{t}, \mathcal{L}) \leq \alpha \cdot \lambda^{(p)}_1(\mathcal{L})$, find closest lattice vector to $\mathbf{t}$ in $\mathcal{L}$.

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

- $\text{dist}_p(\mathbf{t}, \mathcal{L}) \leq r$ and $\lambda^{(p)}_1(\mathcal{L}) \geq r/\alpha$, or
- $\text{dist}_p(\mathbf{t}, \mathcal{L}) > r$.

In terms of point-counting: decide whether

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

Relaxation $(A, G)$-$\text{BDD}_{p,\alpha}$: 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) $\text{BDD}_{p,\alpha}$: given $\mathcal{L}$, $t$ with $\text{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$, find closest lattice vector to $t$ in $\mathcal{L}$.

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

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

In terms of point-counting: decide whether

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

Relaxation $(A, G)$-$\text{BDD}_{p,\alpha}$: 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) $BDD_{p,α}$: given $L, t$ with $dist_p(t, L) ≤ α \cdot \lambda_1^{(p)}(L)$, find closest lattice vector to $t$ in $L$.

Decisional $BDD_{p,α}$: given $L, t$ and distance $r$, decide whether

- $dist_p(t, L) ≤ r$ and $\lambda_1^{(p)}(L) ≥ r/α$, or
- $dist_p(t, L) > r$.

In terms of point-counting: decide whether

- $|B_p(r; t) \cap L| ≥ 1$ and $|B_p^o(r/α) \cap (L \setminus \{0\})| = 0$, or
- $|B_p(r; t) \cap L| = 0$.

Relaxation $(A, G)$-$BDD_{p,α}$: decide whether

- “(good) close” count $≥ G$ and “short” count $≤ A$, or
- “annoying close” count $≤ A$.

(Decisional BDD is just $(0, 1)$-BDD.)
Rephrasing BDD with Point-Counting

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

Decisional \( \text{BDD}_{p, \alpha} \): given \( \mathcal{L}, \mathbf{t} \) and distance \( r \), decide whether

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

In terms of point-counting: decide whether

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

Relaxation \((A, G)\)-\( \text{BDD}_{p, \alpha} \): 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 finite set $S \subset \mathcal{L}$, $|S \cap \mathcal{L}'|$ concentrates around $|S|/q$.

$(q = 3)$

$^1S$ 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 $(A, G)$-BDD$_{\rho,\alpha}$ reduces to decisional BDD$_{\rho,\alpha}$ 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 $(A, G)$-BDD$_{p,\alpha}$ reduces to decisional 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 CVP’\(_p,\gamma\) instance (\(B', t'\)) and parameters \(B^{\dagger}, t^{\dagger}, r, s\), and outputs (\(A, G\))-BDD\(_p,\alpha\) instance:

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

For CVP’ YES instance:

- Promise: \(\text{dist}_p(t', B'x) \leq 1\) for some \(x \in \{0, 1\}^{n'}\).
- “Short” count: \(|B^o_p(r/\alpha) \cap L| \leq |B^o_p(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus L^{\dagger})|\).
- “Close” count: \(|B_p(r; t) \cap L| \geq |B_p(r - s - n'/2; t^{\dagger}) \cap L^{\dagger}|\). \(^2\)

\(^2\)The arithmetic of the distances here is showcased for \(\ell_1\), and should be \((r^p - s^p - n'/2^p)^{1/p}\) for general \(\ell_p\). We will continue to simplify this way in the remaining slides.
Transforming CVP′ Instances

The transformation takes as input CVP′$_{p,\gamma}$ instance $(B′, t′)$ and parameters $B^\dagger$, $t^\dagger$, $r$, $s$, and outputs $(A, G)$-BDD$_{p,\alpha}$ instance:

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

For CVP′ YES instance:

- Promise: $\text{dist}_p(t′, B′x) \leq 1$ for some $x \in \{0, 1\}^{n'}$.
- “Short” count: $|B^o_p(r/\alpha) \cap \mathcal{L}| \leq |B^o_p(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)|$.
- “Close” count: $|B_p(r; t) \cap \mathcal{L}| \geq |B_p(r - s - n'/2; t^\dagger) \cap \mathcal{L}^\dagger|$.$^2$

---

$^2$The arithmetic of the distances here is showcased for $\ell_1$, and should be $(r^p - s^p - n'/2^p)^{1/p}$ for general $\ell_p$. We will continue to simplify this way in the remaining slides.
Transforming CVP′ Instances

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

\[
B = \begin{pmatrix}
    sB' & 0 \\
    l_{n'} & 0 \\
    0 & B^\dagger
\end{pmatrix}, \quad t = \begin{pmatrix}
    st' \\
    \frac{1}{2}1_{n'} \\
    t^\dagger
\end{pmatrix}, \quad r.
\]

For CVP′ YES instance:

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

\(^2\)The arithmetic of the distances here is showcased for \(\ell_1\), and should be \((r^p - s^p - n'/2^p)^{1/p}\) for general \(\ell_p\). We will continue to simplify this way in the remaining slides.
Transforming CVP′ Instances

The transformation takes as input CVP′_{p,γ} instance \((B', t')\) and parameters \(B^\dagger, t^\dagger, r, s\), and outputs \((A, G)\)-BDD_{p,α} instance:

\[
B = \begin{pmatrix}
    sB' & 0 \\
    l_n' & 0 \\
    0 & B^\dagger
\end{pmatrix}, \quad t = \begin{pmatrix}
    st' \\
    \frac{1}{2}1_{n'} \\
    t^\dagger
\end{pmatrix}, \quad r.
\]

For CVP′ YES instance:

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

\(^2\)The arithmetic of the distances here is showcased for \(\ell_1\), and should be \((r^p - s^p - n'/2^p)^{1/p}\) for general \(\ell_p\). We will continue to simplify this way in the remaining slides.
Transforming \( CVP' \) Instances

The transformation outputs:

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

For \( CVP' \) NO instance:

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

\[
|B_p(r; t) \cap L| \leq |B_p^\circ(r - \gamma s; \left(\frac{1}{2}1_{n'}\right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|.
\]

Putting together, for \( G \gg A \), we want:

\[
|B_p(r - s - n'/2; t^\dagger) \cap L^\dagger| \gg \max\{|B_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|, \\
|B_p^\circ(r - \gamma s; \left(\frac{1}{2}1_{n'}\right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|\}.
\]
Transforming CVP' Instances

The transformation outputs:

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

For CVP' NO instance:

- **Promise:** \( \text{dist}_p(t', L') > \gamma. \)
- **“Annoying close” count:**

\[
|B_p(r; t) \cap L| \leq |B^\circ_p(r - \gamma s; \left(\frac{1}{2}1_{n'}\right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|.
\]

Putting together, for \( G \gg A \), we want:

\[
|B_p(r - s - n'/2; t^\dagger) \cap L^\dagger| \gg \max\{|B^\circ_p(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|, \\
|B^\circ_p(r - \gamma s; \left(\frac{1}{2}1_{n'}\right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|\}.
\]
Transforming CVP′ Instances

The transformation outputs:

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

For CVP′ NO instance:

- Promise: \( \text{dist}_p(t', L') > \gamma \).
- “Annoying close” count:
  \[ |B_p(r; t) \cap L| \leq |B^\circ_p(r - \gamma s; \left( \frac{1}{2}1_{n'} \right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|. \]

Putting together, for \( G \gg A \), we want:

\[ |B_p(r - s - n'/2; t^\dagger) \cap L^\dagger| \gg \max\{|B^\circ_p(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|, \\
|B^\circ_p(r - \gamma s; \left( \frac{1}{2}1_{n'} \right)) \cap (\mathbb{Z}^{n'} \oplus L^\dagger)|\}. \]
Locally Dense Gadgets

Desired property (first consider the “short” term):

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

Observations:

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

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

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

(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:

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

Hence we want the gadget to be \textit{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):

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

Observations:

\[ |\mathcal{B}_p^\circ(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^\circ(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^\circ(r/\alpha) \cap \mathcal{L}^\dagger|. \]

\[ |\mathcal{B}_p^\circ(\rho) \cap \mathbb{Z}^{n'}| \text{ is exponential in } n' \text{ (for sufficiently large } \rho). \]

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.)
Desired property (first consider the “short” term):

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

Observations:

- $$|\mathcal{B}_p^o(r/\alpha) \cap (\mathbb{Z}^{n'} \oplus \mathcal{L}^\dagger)| \leq |\mathcal{B}_p^o(r/\alpha) \cap \mathbb{Z}^{n'}| \cdot |\mathcal{B}_p^o(r/\alpha) \cap \mathcal{L}^\dagger|.$$ 

- $$|\mathcal{B}_p^o(\rho) \cap \mathbb{Z}^{n'}|$$ is exponential in $$n'$$ (for sufficiently large $$\rho$$).

Hence we want the gadget to be \textit{locally dense}, i.e., to have exponentially more “close” than “short” lattice vectors:

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

(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

\[
|B_p(\alpha_G; t^\dagger) \cap L^\dagger| \geq \nu^{n^\dagger}|B^\circ_p(1) \cap L^\dagger|,
\]

then for \(BDD_{p,\alpha}\):

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 \(\alpha_A, \nu'\) and they also (substantially) affect the bounds on \(\alpha\).

\(^4\)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\(^3\)

\[
|B_p(\alpha_G; t^\dagger) \cap L^\dagger| \geq \nu^n |B_p(1) \cap L^\dagger|, \]

then for 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 \(\alpha_A, \nu'\) and they also (substantially) affect the bounds on \(\alpha\).

\(^4\)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 \((B^†, t^†)\) satisfying

\[ |B_p(\alpha_G; t^†) \cap L^†| \geq \nu^{n^†} |B_p^0(1) \cap L^†| , \]

then for \(BDD_p, \alpha\):

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 \(\alpha_A, \nu'\) and they also (substantially) affect the bounds on \(\alpha\).

\(^4\)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 $\tau_n^L$: $\max_{\mathcal{L}} |B_p(1) \cap (\mathcal{L} \setminus \{0\})|$ for rank-$n$ lattice $\mathcal{L}$ with $\lambda_1^{(p)}(\mathcal{L}) = 1$.

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

Gadgets (in $l_2$): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$.

Parameters: $\alpha_G = 1$, $\nu = 2^{c_{kn}}$.

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: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all

$$\alpha > \alpha_{p,c}^\dagger := 1 + \frac{1}{f_p(2^{c_{kn}(c-1)})}.$$
Instantiating the Main Theorem: Result 3

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

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

Gadgets (in $\ell_2$): exponential kissing number lattice $\mathcal{L}^\dagger$, $t^\dagger = 0$. Parameters: $\alpha_G = 1$, $\nu = 2^{c_{kn}}$.

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

$$\alpha > \alpha_{p,c}^\dagger := 1 + \frac{1}{f_p(2^{c_{kn}(c-1)})}.$$
Instantiating the Main Theorem: Result 3

Lattice \textit{kissing number} \( \tau^L_n \): \( \max_{\mathcal{L}} |B_p(1) \cap (\mathcal{L} \setminus \{0\})| \) for rank-\( n \) lattice \( \mathcal{L} \) with \( \lambda^{(p)}_1(\mathcal{L}) = 1 \).

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

Gadgets (in \( \ell_2 \)): exponential kissing number lattice \( \mathcal{L}^\dagger \), \( t^\dagger = 0 \).

Parameters: \( \alpha_G = 1 \), \( \nu = 2^{c_{kn}} \).

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

\[
\alpha > \alpha^\dagger_{p,C} := 1 + \frac{1}{f_p(2^{c_{kn}(C-1)})} .
\]
Instantiating the Main Theorem: Result 3

Lattice \textit{kissing number} \( \tau_{n}^{L} \): \( \max_{\mathcal{L}} |B_{p}(1) \cap (\mathcal{L} \setminus \{0\})| \) for rank-\( n \) lattice \( \mathcal{L} \) with \( \lambda_{1}^{(p)}(\mathcal{L}) = 1 \).

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

Gadgets (in \( \ell_{2} \)): exponential kissing number lattice \( \mathcal{L}^{\dagger} \), \( t^{\dagger} = 0 \).
Parameters: \( \alpha_{G} = 1 \), \( \nu = 2^{c_{kn}} \).

Using norm embeddings, we also get gadgets in all \( \ell_{p} \) in cost of slightly larger \( \alpha_{G} = 1 + o(1) \). Then we have our Result 3: \( \text{BDD}_{p,\alpha} \) cannot be solved in \( 2^{n/C} \) time for all \( \alpha > \alpha_{p,C}^{\dagger} := 1 + \frac{1}{f_{p}(2^{c_{kn}(C-1)})} \).
Instantiating the Main Theorem: Result 1

To decrease $\alpha_G$ for the exponential kissing number gadgets:

- Move $t^\dagger$ away from 0 by $\delta$ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the “close” count as well, by an expected factor of $\frac{\text{area}(S^{n-1} \cap \mathcal{B}_p(1 - \varepsilon; t^\dagger))}{\text{area}(S^{n-1})}$, 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 $\delta, \varepsilon$, we manage to get $\alpha_G$ approaching $2^{-c_{kn}}$, which gives our Result 1:

$\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn} := 2^{-c_{kn}}$. 
Instantiating the Main Theorem: Result 1

To decrease $\alpha_G$ for the exponential kissing number gadgets:

- Move $t^\dagger$ away from 0 by $\delta$ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the “close” count as well, by an expected factor of $\frac{\text{area}(S^{n-1} \cap B_p(1 - \varepsilon; t^\dagger))}{\text{area}(S^{n-1})}$, 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 $\delta, \varepsilon$, we manage to get $\alpha_G$ approaching $2^{-\alpha_{kn}}$, which gives our Result 1:

$\text{BDD}_{\rho, \alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn} := 2^{-\alpha_{kn}}$. 
Instantiating the Main Theorem: Result 1

To decrease $\alpha_G$ for the exponential kissing number gadgets:

- Move $t^\dagger$ away from 0 by $\delta$ in random direction.
- Set $\alpha_G = 1 - \varepsilon$ for $\varepsilon < \delta$.
- Nevertheless this decreases the “close” count as well, by an expected factor of $\text{area}(S^{n-1} \cap B_p(1 - \varepsilon; t^\dagger))/\text{area}(S^{n-1})$, 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 $\delta, \varepsilon$, we manage to get $\alpha_G$ approaching $2^{-c_{kn}}$, which gives our Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn} := 2^{-c_{kn}}$. 
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 $\alpha_G$ over $\rho$, $t$ subject to

$$|B_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |B_p^o(\rho) \cap \mathbb{Z}^n|.$$

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

- $|B_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ 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 \( \alpha_G \) over \( \rho, t \) subject to

\[
|B_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |B^\circ_p(\rho) \cap \mathbb{Z}^n|.
\]

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

- \( |B_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n| \) 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 \( \alpha_G \) over \( \rho, t \) subject to

\[
|B_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |B_p(\rho) \cap \mathbb{Z}^n|.
\]

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

\[\blacktriangleright\] \( |B_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n| \) can be approximated by a numerical function \( \beta_{p,t}(a)^n \) to within a \( 2^{o(n)} \) factor.

\[\blacktriangleright\] We find that empirically the optimizer for \( t \) is always 1/2.

\[\blacktriangleright\] [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 $\alpha_G$ over $\rho, t$ subject to

$$|B_p(\alpha_G \rho; t \cdot 1_n) \cap \mathbb{Z}^n| > |B_\circ_p(\rho) \cap \mathbb{Z}^n|.$$ 

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

- $|B_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ 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 $\alpha_G$ over $\rho$, $t$ subject to

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

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

▶ $|\mathcal{B}_p(a \cdot n; t \cdot 1_n) \cap \mathbb{Z}^n|$ 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 \( \text{CVP}_{p,\gamma} \) instances to instances of a similar intermediate problem \((A, G)-\text{CVP}_{p,\gamma'}\).

- [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for \( \text{CVP}_{p,\gamma} \) other than \( \text{CVP}_{p,1} \).

- 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 \( \text{CVP}^\prime_{p,\gamma} \) instances to instances of a similar intermediate problem \((A, G)-\text{CVP}_{p,\gamma'}\).

▶ \([AS18]\) has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for \( \text{CVP}^\prime_{p,\gamma} \) other than \( \text{CVP}^\prime_{p,1} \).

▶ 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 $\text{CVP}_{p,\gamma}^\prime$ instances to instances of a similar intermediate problem $(A, G)$-$\text{CVP}_{p,\gamma}^\prime$.

▶ [AS18] has the same workflow, while we have a more general transformation with a larger parameter space, and we can set parameters working for $\text{CVP}_{p,\gamma}^\prime$ other than $\text{CVP}_{p,1}^\prime$.

▶ The same gadgets from integer lattices as Result 2 are used.
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 \( \text{CVP}_{p,\gamma} \) instances to instances of a similar intermediate problem \((A, G)\)-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 \( \text{CVP}_{p,\gamma} \) other than \( \text{CVP}'_{p,1} \).
- 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).

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.

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.

Huck Bennett and Chris Peikert.
Hardness of bounded distance decoding on lattices in $\ell_p$ norms.

Friedrich Eisenbrand and Moritz Venzin.
Approximate CVP$_p$ in time $2^{0.802n}$.

Subhash Khot.
Hardness of approximating the shortest vector problem in lattices.

Factoring polynomials with rational coefficients.

Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio.
On bounded distance decoding for general lattices.

Serge Vlăduţ.
Lattices with exponentially large kissing numbers.