The Mathematics of Lattices

Daniele Micciancio

January 2020
Outline

1. Point Lattices and Lattice Parameters

2. Computational Problems
   - Coding Theory

3. The Dual Lattice

4. $Q$-ary Lattices and Cryptography
1. Point Lattices and Lattice Parameters

2. Computational Problems
   - Coding Theory

3. The Dual Lattice

4. Q-ary Lattices and Cryptography
(Point) Lattices

- Traditional area of mathematics

Lagrange  Gauss  Minkowski
(Point) Lattices

- Traditional area of mathematics

- Key to many algorithmic applications
  - Cryptanalysis (e.g., breaking low-exponent RSA)
  - Coding Theory (e.g., wireless communications)
  - Optimization (e.g., Integer Programming with fixed number of variables)
  - Cryptography (e.g., Cryptographic functions from worst-case complexity assumptions, Fully Homomorphic Encryption)
Lattice Cryptography: a Timeline

- **1982**: LLL basis reduction algorithm
  - Traditional use of lattice algorithms as a cryptanalytic tool
- **1996**: Ajtai’s connection
  - Relates average-case and worst-case complexity of lattice problems
  - Application to one-way functions and collision resistant hashing
- **2002**: Average-case/worst-case connection for structured lattices.
  Key to efficient lattice cryptography.
- **2005**: (Quantum) Hardness of Learning With Errors (Regev)
  - Similar to Ajtai’s connection, but for injective functions
  - Wide cryptographic applicability: PKE, IBE, ABE, FHE.
Lattices: Definition

The simplest lattice in $n$-dimensional space is the integer lattice

$$\Lambda = \mathbb{Z}^n$$
Lattices: Definition

The simplest lattice in $n$-dimensional space is the integer lattice

$$\Lambda = \mathbb{Z}^n$$

Other lattices are obtained by applying a linear transformation

$$\Lambda = B\mathbb{Z}^n \quad (B \in \mathbb{R}^{d \times n})$$
A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $B = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n$:

$$\mathcal{L} = \sum_{i=1}^{n} b_i \cdot \mathbb{Z}$$
A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $B = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n$:

$$L = \sum_{i=1}^{n} b_i \cdot \mathbb{Z} = \{Bx : x \in \mathbb{Z}^n\}$$
Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors \( B = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n:\n
\[ \mathcal{L} = \sum_{i=1}^{n} b_i \cdot \mathbb{Z} = \{Bx : x \in \mathbb{Z}^n\} \]

The same lattice has many bases

\[ \mathcal{L} = \sum_{i=1}^{n} c_i \cdot \mathbb{Z} \]
A lattice is the set of all integer linear combinations of (linearly independent) basis vectors \( \mathbf{B} = \{ \mathbf{b}_1, \ldots, \mathbf{b}_n \} \subset \mathbb{R}^n \):

\[
\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{ \mathbf{B} \mathbf{x} : \mathbf{x} \in \mathbb{Z}^n \}
\]

The same lattice has many bases

\[
\mathcal{L} = \sum_{i=1}^{n} \mathbf{c}_i \cdot \mathbb{Z}
\]

Definition (Lattice)

A discrete additive subgroup of \( \mathbb{R}^n \)
Definition (Determinant)

\[ \det(L) = \text{volume of the fundamental region } P = \sum_i b_i \cdot [0, 1) \]
**Determinant**

**Definition (Determinant)**

$$\det(\mathcal{L}) = \text{volume of the fundamental region } \mathcal{P} = \sum_i b_i \cdot [0, 1)$$

- Different bases define different fundamental regions
**Definition (Determinant)**

\[ \text{det}(\mathcal{L}) = \text{volume of the fundamental region } \mathcal{P} = \sum_i b_i \cdot [0, 1) \]

- Different bases define different fundamental regions
- All fundamental regions have the same volume
# Determinant

**Definition (Determinant)**

\[
\det(L) = \text{volume of the fundamental region } P = \sum_i b_i \cdot [0, 1)
\]

- Different bases define different fundamental regions
- All fundamental regions have the same volume
- The determinant of a lattice can be efficiently computed from any basis.
Density estimates

**Definition (Centered Fundamental Parallelepiped)**

\[ \mathcal{P} = \sum_i b_i \cdot [-1/2, 1/2) \]

- \( \text{vol}(\mathcal{P}(B)) = \det(\mathcal{L}) \)
- \( \{x + \mathcal{P}(B) \mid x \in \mathcal{L}\} \) partitions \( \mathbb{R}^n \)
- For all sufficiently large \( S \subseteq \mathbb{R}^n \)

\[ |S \cap \mathcal{L}| \approx \frac{\text{vol}(S)}{\det(\mathcal{L})} \]
Minimum Distance and Successive Minima

Minimum distance

$$\lambda_1 = \min_{x, y \in L, x \neq y} \|x - y\|$$

Successive minima ($i = 1, \ldots, n$)

$$\lambda_i = \min \{ r : \dim \text{span}(B(r)) \cap L \geq i \}$$

Examples

$$Z_n: \lambda_1 = \lambda_2 = \ldots = \lambda_n = 1$$

Always:

$$\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$$
Minimum Distance and Successive Minima

- **Minimum distance**

\[ \lambda_1 = \min_{x, y \in \mathcal{L}, x \neq y} \|x - y\| \]

\[ = \min_{x \in \mathcal{L}, x \neq 0} \|x\| \]
Minimum Distance and Successive Minima

- **Minimum distance**

\[
\lambda_1 = \min_{x, y \in \mathcal{L}, x \neq y} \|x - y\|
\]

\[
= \min_{x \in \mathcal{L}, x \neq 0} \|x\|
\]

- **Successive minima (\(i = 1, \ldots, n\))**

\[
\lambda_i = \min\{r : \dim \text{span}(B(r) \cap \mathcal{L}) \geq i\}
\]
Minimum Distance and Successive Minima

- **Minimum distance**

\[
\lambda_1 = \min_{x, y \in \mathcal{L}, x \neq y} \|x - y\| \\
= \min_{x \in \mathcal{L}, x \neq 0} \|x\|
\]

- **Successive minima** \((i = 1, \ldots, n)\)

\[
\lambda_i = \min \{r : \dim \text{span}(B(r) \cap \mathcal{L}) \geq i\}
\]
Minimum Distance and Successive Minima

- **Minimum distance**

\[
\lambda_1 = \min_{x, y \in \mathcal{L}, x \neq y} \|x - y\| = \min_{x \in \mathcal{L}, x \neq 0} \|x\|
\]

- **Successive minima \((i = 1, \ldots, n)\)**

\[
\lambda_i = \min\{r : \dim \text{span}(B(r) \cap \mathcal{L}) \geq i\}
\]
Minimum Distance and Successive Minima

- **Minimum distance**

  \[ \lambda_1 = \min_{x, y \in \mathcal{L}, x \neq y} \|x - y\| \]

  \[ = \min_{x \in \mathcal{L}, x \neq 0} \|x\| \]

- **Successive minima** \((i = 1, \ldots, n)\)

  \[ \lambda_i = \min\{r : \dim \text{span}(B(r) \cap \mathcal{L}) \geq i\} \]

- **Examples**
  - \(\mathbb{Z}^n\): \(\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1\)
  - **Always**: \(\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n\)
Distance Function and Covering Radius

- **Distance function**

\[ \mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \| t - x \| \]
Distance Function and Covering Radius

- **Distance function**
  \[ \mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \| t - x \| \]

- **Covering radius**
  \[ \mu(\mathcal{L}) = \max_{t \in \text{span}(\mathcal{L})} \mu(t, \mathcal{L}) \]
Distance Function and Covering Radius

- **Distance function**
  \[ \mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \|t - x\| \]

- **Covering radius**
  \[ \mu(\mathcal{L}) = \max_{t \in \text{span}(\mathcal{L})} \mu(t, \mathcal{L}) \]

- Spheres of radius \( \mu(\mathcal{L}) \) centered around all lattice points cover the whole space.
Distance Function and Covering Radius

- **Distance function**
  \[ \mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \| t - x \| \]

- **Covering radius**
  \[ \mu(\mathcal{L}) = \max_{t \in \text{span}(\mathcal{L})} \mu(t, \mathcal{L}) \]

- Spheres of radius \( \mu(\mathcal{L}) \) centered around all lattice points cover the whole space.
Distance Function and Covering Radius

- Distance function
  \[ \mu(t, \mathcal{L}) = \min_{x \in \mathcal{L}} \|t - x\| \]

- Covering radius
  \[ \mu(\mathcal{L}) = \max_{t \in \text{span}(\mathcal{L})} \mu(t, \mathcal{L}) \]

- Spheres of radius \( \mu(\mathcal{L}) \) centered around all lattice points cover the whole space
Smoothing a lattice

Consider an arbitrary lattice, and ...
Smoothing a lattice

Consider an arbitrary lattice, and ... add noise to each lattice point
Smoothing a lattice

Consider an arbitrary lattice, and ... add noise to each lattice point ... more noise, and more and more, until

\[ \| r \| \leq (\log n) \cdot \sqrt{n} \lambda_n \]

\( \eta \epsilon \leq (\log n) \lambda_n \).

\( \eta \epsilon \): the "smoothing parameter" of a lattice [MR04].
Smoothing a lattice

Consider an arbitrary lattice, and ... add noise to each lattice point ... more noise, and more and more, until

\[ \|r\| \leq (\log n) \cdot \sqrt{n} \lambda n \]

\( \eta \epsilon \leq (\log n) \lambda n \).

\( \eta \epsilon \): the "smoothing parameter" of a lattice [MR04].
Smoothing a lattice

Consider an arbitrary lattice, and . . . add noise to each lattice point . . . more noise, and more and more, until

\[ \| r \| \leq (\log n) \cdot \sqrt{n} \lambda_n \]

\( \eta \epsilon \leq (\log n) \lambda_n \).

\( \eta \epsilon \): the "smoothing parameter" of a lattice [MR04].
Smoothing a lattice

Consider an arbitrary lattice, and ... add noise to each lattice point ... more noise, and more and more, until ... we reach an almost uniform distribution
Smoothing a lattice

Consider an arbitrary lattice, and . . . add noise to each lattice point . . . more noise, and more and more, until . . . we reach an almost uniform distribution.
Smoothing a lattice

Consider an arbitrary lattice, and . . . add noise to each lattice point . . . more noise, and more and more, until . . . we reach an almost uniform distribution.
Smoothing a lattice

Consider an arbitrary lattice, and . . . add noise to each lattice point . . . more noise, and more and more, until . . . we reach an almost uniform distribution.
Smoothing a lattice

Consider an arbitrary lattice, and add noise to each lattice point, more noise, and more and more, until we reach an almost uniform distribution.

**How much noise is needed?**

At most $\|r\| \leq (\log n) \cdot \sqrt{n} \lambda_n$
Smoothing a lattice

Consider an arbitrary lattice, and . . . add noise to each lattice point . . . more noise, and more and more, until . . . we reach an almost uniform distribution

**How much noise is needed?**
At most $\|\mathbf{r}\| \leq (\log n) \cdot \sqrt{n}\lambda_n$

Best done using **Gaussian** noise $\mathbf{r}$ of width

$$|r_i| \approx \eta_\epsilon \leq (\log n)\lambda_n.$$  

$\eta_\epsilon$: the “smoothing parameter” of a lattice [MR04].
Minkowski’s convex body theorem

Theorem (Convex Body)

Let $C \subset \mathbb{R}^n$ be a symmetric convex body. If $\text{vol}(C) > 2^n$, then $C$ contains a nonzero integer vector.
Minkowski’s convex body theorem

**Theorem (Convex Body)**

Let \( C \subset \mathbb{R}^n \) be a symmetric convex body. If \( \text{vol}(C) > 2^n \), then \( C \) contains a nonzero integer vector.

Let \( \mathcal{L} = B\mathbb{Z}^n \) and \( r = \det(\mathcal{L})^{1/n} \). Then,

\[
\text{vol}(C) = \det(B)^{-1/n} (2r)^n = 2^n
\]
Theorem (Convex Body)

Let $C \subset \mathbb{R}^n$ be a symmetric convex body. If $\text{vol}(C) > 2^n$, then $C$ contains a nonzero integer vector $x \in \mathbb{Z}^n \setminus \{0\}$.

Let $\mathcal{L} = B\mathbb{Z}^n$ and $r = \det(\mathcal{L})^{1/n}$. Then,

- $C = B^{-1}[-r, r]^n$ has volume $\det(B)^{-1}(2r)^n = 2^n$
Minkowski’s convex body theorem

**Theorem (Convex Body)**

Let $C \subset \mathbb{R}^n$ be a symmetric convex body. If $\text{vol}(C) > 2^n$, then $C$ contains a nonzero integer vector.

Let $\mathcal{L} = B\mathbb{Z}^n$ and $r = \text{det}(\mathcal{L})^{1/n}$. Then,

- $C = B^{-1}[-r, r]^n$ has volume $\text{det}(B)^{-1}(2r)^n = 2^n$
- $C$ contains $x \in \mathbb{Z}^n \setminus \{0\}$
Minkowski’s convex body theorem

**Theorem (Convex Body)**

Let $C \subset \mathbb{R}^n$ be a symmetric convex body. If $\text{vol}(C) > 2^n$, then $C$ contains a nonzero integer vector.

Let $\mathcal{L} = B\mathbb{Z}^n$ and $r = \det(\mathcal{L})^{1/n}$. Then,
- $C = B^{-1}[-r, r]^n$ has volume $\det(B)^{-1}(2r)^n = 2^n$
- $C$ contains $x \in \mathbb{Z}^n \setminus \{0\}$
- $BC = [-r, r]^n$ contains $Bx$
Minkowski’s convex body theorem

**Theorem (Convex Body)**

Let $C \subset \mathbb{R}^n$ be a symmetric convex body. If $\text{vol}(C) > 2^n$, then $C$ contains a nonzero integer vector.

Let $\mathcal{L} = B \mathbb{Z}^n$ and $r = \det(\mathcal{L})^{1/n}$. Then,

- $C = B^{-1}[-r, r]^n$ has volume $\det(B)^{-1}(2r)^n = 2^n$
- $C$ contains $x \in \mathbb{Z}^n \setminus \{0\}$
- $BC = [-r, r]^n$ contains $Bx$
- $\lambda_1(\mathcal{L}) \leq \sqrt{n}r = \sqrt{n} \det(\mathcal{L})^{1/n}$
Minkowski’s second theorem

Theorem (Minkowski)

\[ \lambda_1(\mathcal{L}) \leq \left( \prod_i \lambda_i(\mathcal{L}) \right)^{1/n} \leq \sqrt{n} \det(\mathcal{L})^{1/n} \]

- For \( \mathbb{Z}^n \), \( \lambda_1 = (\prod_i \lambda_i)^{1/n} = 1 \) is smaller than Minkowski’s bound by \( \sqrt{n} \)
- \( \lambda_1(\mathcal{L}) \) can be arbitrarily smaller than Minkowski’s bound
- \( (\prod_i \lambda_i(\mathcal{L}))^{1/n} \) is never smaller than Minkowski’s bound by more than \( \sqrt{n} \)
- Can you find lattices with \( (\prod_i \lambda_i(\mathcal{L}))^{1/n} \geq \Omega(\sqrt{n}) \det(\mathcal{L})^{1/n} \) within a constant from Minkowski’s bound?
1. Point Lattices and Lattice Parameters

2. Computational Problems
   - Coding Theory

3. The Dual Lattice

4. Q-ary Lattices and Cryptography
Definition (Shortest Vector Problem, SVP)

Given a lattice $\mathcal{L}(B)$, find a (nonzero) lattice vector $Bx$ (with $x \in \mathbb{Z}^k$) of length (at most) $\|Bx\| \leq \lambda_1$
Definition (Shortest Vector Problem, SVP)

Given a lattice $\mathcal{L}(B)$, find a (nonzero) lattice vector $Bx$ (with $x \in \mathbb{Z}^k$) of length (at most) $\|Bx\| \leq \lambda_1$
Shortest Vector Problem

Definition (Shortest Vector Problem, SVP)

Given a lattice $\mathcal{L}(B)$, find a (nonzero) lattice vector $Bx$ (with $x \in \mathbb{Z}^k$) of length (at most) $\|Bx\| \leq \lambda_1$
Computational Problems

Shortest Vector Problem

Definition (Shortest Vector Problem, SVP$_\gamma$)

Given a lattice $\mathcal{L}(B)$, find a (nonzero) lattice vector $Bx$ (with $x \in \mathbb{Z}^k$) of length (at most) $\|Bx\| \leq \gamma \lambda_1$
Closest Vector Problem

Definition (Closest Vector Problem, CVP)

Given a lattice $\mathcal{L}(B)$ and a target point $t$, find a lattice vector $Bx$ within distance $\|Bx - t\| \leq \mu$ from the target.
**Definition (Closest Vector Problem, CVP)**

Given a lattice $\mathcal{L}(B)$ and a target point $t$, find a lattice vector $Bx$ within distance $\|Bx - t\| \leq \mu$ from the target.
Closest Vector Problem

Definition (Closest Vector Problem, CVP)

Given a lattice $\mathcal{L}(B)$ and a target point $t$, find a lattice vector $Bx$ within distance $\|Bx - t\| \leq \mu$ from the target.
Closest Vector Problem

Definition (Closest Vector Problem, CVP\(\gamma\))

Given a lattice \(\mathcal{L}(B)\) and a target point \(t\), find a lattice vector \(Bx\) within distance \(\|Bx - t\| \leq \gamma \mu\) from the target.
Shortest Independent Vectors Problem

Definition (Shortest Independent Vectors Problem, SIVP)

Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{B}x_1, \ldots, \mathbf{B}x_n$ of length (at most) $\max_i \|\mathbf{B}x_i\| \leq \lambda_n$
Definition (Shortest Independent Vectors Problem, SIVP)

Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{B}x_1, \ldots, \mathbf{B}x_n$ of length (at most) $\max_i \|\mathbf{B}x_i\| \leq \lambda_n$
Definition (Shortest Independent Vectors Problem, SIVP)

Given a lattice $\mathcal{L}(B)$, find $n$ linearly independent lattice vectors $Bx_1, \ldots, Bx_n$ of length (at most) $\max_i \|Bx_i\| \leq \lambda_n$
Definition (Shortest Independent Vectors Problem, SIVP_γ)

Given a lattice \( \mathcal{L}(B) \), find \( n \) linearly independent lattice vectors \( Bx_1, \ldots, Bx_n \) of length (at most) \( \max_i \|Bx_i\| \leq \gamma \lambda_n \)
Coding theory

Problem

*Reliable transmission of information over noisy channels*

Sender wants to transmit a message $m$
Problem

Reliable transmission of information over noisy channels

The sender encodes $m$ as a lattice point $Bx$ and transmits it over a noisy channel (e.g., multiantenna system)
Coding theory

Problem

*Reliable transmission of information over noisy channels*

Recipient receives a perturbed lattice point $\mathbf{t} = \mathbf{Bx} + \mathbf{e}$, where $\mathbf{e}$ is a small error vector.
Coding theory

Problem

*Reliable transmission of information over noisy channels*

Received message $m$ by finding the lattice point $Bx$ closest to the target $t$.
Coding theory

Problem

Reliable transmission of information over noisy channels

\[ m = \text{CVP}(B, t) \]

- **CVP**: Decoding algorithm
- **SVP**: Evaluating error correction radius \( \lambda_1/2 \)
- **SIVP**: Related to distortion in vector quantization
Special Versions of CVP

**Definition (Closest Vector Problem (CVP))**

Given \((\mathcal{L}, \mathbf{t}, d)\), with \(\mu(\mathbf{t}, \mathcal{L}) \leq d\), find a lattice point within distance \(d\) from \(\mathbf{t}\).

- If \(d\) is arbitrary, then one can find the closest lattice vector by binary search on \(d\).
- **Bounded Distance Decoding (BDD):** If \(d < \lambda_1(\mathcal{L})/2\), then there is at most one solution. Solution is the closest lattice vector.
- **Absolute Distance Decoding (ADD):** If \(d \geq \mu(\mathcal{L})\), then there is always at least one solution. Solution may not be closest lattice vector.
Relations among lattice problems

- \( \text{SIVP} \approx \text{ADD} \) [MG’01]
- \( \text{SVP} \leq \text{CVP} \) [GMSS’99]
- \( \text{SIVP} \leq \text{CVP} \) [M’08]
- \( \text{BDD} \lesssim \text{SIVP} \)
- \( \text{CVP} \lesssim \text{SVP} \) [L’87]
- \( \text{GapSVP} \approx \text{GapSIVP} \) [LLS’91, B’93]
- \( \text{GapSVP} \lesssim \text{BDD} \) [LM’09]
Relations among lattice problems

- $\text{SIVP} \approx \text{ADD}$ [MG’01]
- $\text{SVP} \leq \text{CVP}$ [GMSS’99]
- $\text{SIVP} \leq \text{CVP}$ [M’08]
- $\text{BDD} \preceq \text{SIVP}$
- $\text{CVP} \preceq \text{SVP}$ [L’87]
- $\text{GapSVP} \approx \text{GapSIVP}$ [LLS’91, B’93]
- $\text{GapSVP} \preceq \text{BDD}$ [LM’09]
ADD reduces to SIVP

ADD input: $\mathcal{L}$ and arbitrary $t$

- Compute short vectors $V = SIVP(\mathcal{L})$
- Use $V$ to find a lattice vector within distance $\sum_i \frac{1}{2} \|v_i\| \leq (n/2)\lambda_n \leq n\mu$ from $t$
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\text{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rfloor$
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\text{CVP}(\Lambda, t) = \lceil t \rceil$
- Rounding solves CVP whenever $\Lambda$ has an orthogonal basis
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\text{CVP}(\Lambda, t) = \lfloor t \rfloor$
- Rounding solves CVP whenever $\Lambda$ has an orthogonal basis

- Not all lattices have an orthogonal basis

![Diagram of a lattice with basis vectors $b_1$ and $b_2$.]
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if \( \Lambda = \mathbb{Z}^n \), then \( \text{CVP}(\Lambda, t) = \lceil t \rceil \)
- Rounding solves CVP whenever \( \Lambda \) has an orthogonal basis

- Not all lattices have an orthogonal basis
- E.g. “exagonal” lattice
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if \( \Lambda = \mathbb{Z}^n \), then \( \text{CVP}(\Lambda, t) = \lceil t \rceil \)
- Rounding solves CVP whenever \( \Lambda \) has an orthogonal basis

Not all lattices have an orthogonal basis
- E.g. “exagonal” lattice
- \( \mathbf{b}_1 \perp (2\mathbf{b}_2 - \mathbf{b}_1) \)
Geometry of Lattices

- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\text{CVP}(\Lambda, t) = \lceil t \rceil$
- Rounding solves CVP whenever $\Lambda$ has an orthogonal basis

- Not all lattices have an orthogonal basis
  - E.g. “exagonal” lattice
  - $b_1 \perp (2b_2 - b_1)$
  - But they only generate a sublattice
Size Reduction

- $b_1$: (short) lattice vector
- $t$: arbitrary point

Can make $t$ shorter by adding $\pm b_1$

Repeat until $t$ is shortest

Remarks

$t - t' \in \Lambda$

Key step in [LLL'82] basis reduction algorithm

Technique is used in most other lattice algorithms
Size Reduction

- \( \mathbf{b}_1 \): (short) lattice vector
- \( \mathbf{t} \): arbitrary point
- Can make \( \mathbf{t} \) shorter by adding \( \pm \mathbf{b}_1 \)
- Repeat until \( \mathbf{t} \) is shortest

Remarks

\( \mathbf{t} - \mathbf{t}' \in \Lambda \)

Key step in \[LLL'82\] basis reduction algorithm

Technique is used in most other lattice algorithms
Size Reduction

- $b_1$: (short) lattice vector
- $t$: arbitrary point
- Can make $t$ shorter by adding $\pm b_1$
- Repeat until $t$ is shortest

Remarks

- $t - t' \in \Lambda$
- Key step in [LLL’82] basis reduction algorithm
- Technique is used in most other lattice algorithms
**Definition (Gram-Schmidt)**

Basis $\mathcal{B} = [b_1, \ldots, b_n]$

- $b_i^* \in b_i + [b_1, \ldots, b_{i-1}]\mathbb{R}^{i-1}$
- $b_i^* \perp b_1, \ldots, b_{i-1}$

$\mathcal{B}^*$ is an orthogonal basis for the vector space $\mathcal{B}$.

$\mathcal{B}^*$ is not a lattice basis for $\mathcal{B}$.

Still, $\mathcal{B}^*$ is useful to evaluate the quality of lattice basis.

$\det(\Lambda) = \prod_i ||b^*_i|| \leq \prod_i ||b_i||$ (Hadamard)
Gram-Schmidt Orthogonalized Basis

**Definition (Gram-Schmidt)**

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

\[
\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]\mathbb{R}^{i-1}
\]

\[
\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}
\]
**Definition (Gram-Schmidt)**

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

\[
\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]\mathbb{R}^{i-1}
\]

\[
\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}
\]

$\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B}$.

$\mathbf{B}^*$ is not a lattice basis for $\mathbb{Z}^n$.

Still, $\mathbf{B}^*$ is useful to evaluate the quality of lattice basis $\Lambda$:

\[
\det(\Lambda) = \prod \| \mathbf{b}_i^* \| \leq \prod \| \mathbf{b}_i \| \quad \text{(Hadamard)}
\]
Gram-Schmidt Orthogonalized Basis

Definition (Gram-Schmidt)

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

$\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]\mathbb{R}^{i-1}$

$\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$

$\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbb{R}^n$

$\mathbf{B}^*$ is not a lattice basis for $\mathbb{Z}^n$

Still, $\mathbf{B}^*$ is useful to evaluate the quality of lattice basis

$\det(\Lambda) = \prod_i \|\mathbf{b}_i\| \leq \prod_i \|\mathbf{b}_i^*\| \leq \prod_i \|\mathbf{b}_i\|$ (Hadamard)
Gram-Schmidt Orthogonalized Basis

Definition (Gram-Schmidt)

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

- $\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}] \mathbb{R}^{i-1}$
- $\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$

$\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B} \mathbb{R}^n$
Gram-Schmidt Orthogonalized Basis

**Definition (Gram-Schmidt)**

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

- $\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]\mathbb{R}^{i-1}$
- $\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$

- $\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B}\mathbb{R}^n$
- $\mathbf{B}^*$ is **not** a lattice basis for $\mathbf{B}\mathbb{Z}^n$
Gram-Schmidt Orthogonalized Basis

**Definition (Gram-Schmidt)**

Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$

\[ \mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}] \mathbb{R}^{i-1} \]

\[ \mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1} \]

- $\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B} \mathbb{R}^n$
- $\mathbf{B}^*$ is **not** a lattice basis for $\mathbf{B} \mathbb{Z}^n$
- Still, $\mathbf{B}^*$ is useful to evaluate the quality of lattice basis $\mathbf{B}$

\[ \det(\Lambda) = \prod_i \| \mathbf{b}_i^* \| \leq \prod_i \| \mathbf{b}_i \| \quad (\text{Hadamard}) \]
Lattice rounding

\[ \mathbf{b}^* \cdot [0, 1] \] is also a fundamental region for \( \Lambda \).

Any \( t \) can be efficiently rounded to \( v \in \Lambda \) with \( \| t - v \| \leq \frac{1}{2} \sqrt{\sum_i \| \mathbf{b}^*_i \|^2} \).

\( v \) solves CVP when \( \| t - v \| \leq \min_i \| \mathbf{b}^*_i \| / 2 \).

**Lemma (Nearest Plane Algorithm [Babai 1986])**

Rounding w.r.t \( \mathbf{B}^* \) approximates CVP within \( \sqrt{n} \cdot \max_i \| \mathbf{b}^*_i \| / \min_i \| \mathbf{b}^*_i \| \).
Lattice rounding

- $\mathbf{B}^* [0, 1]^n$ is also a fundamental region for $\Lambda$
Lattice rounding

- $B^* [0, 1]^n$ is also a fundamental region for $\Lambda$

Diagram: A lattice grid with vectors $b_1^*$ and $b_2^*$, and a shaded fundamental parallelogram.
Lattice rounding

- $\mathbf{B}^*[0, 1]^n$ is also a fundamental region for $\Lambda$

![Diagram showing lattice points and fundamental region]
Lattice rounding

- $B^* [0, 1]^n$ is also a fundamental region for $\Lambda$
- Any $t$ can be efficiently rounded to $v \in \Lambda$

\[ \|t - v\| \leq \frac{1}{2} \sqrt{\sum_i \|b^* i\|^2} \]

Lemma (Nearest Plane Algorithm [Babai 1986])

Rounding w.r.t $B^*$ approximates CVP within $\sqrt{n} \cdot \max_i \|b^* i\| / \min_i \|b^* i\|$
Lattice rounding

- $B^*[0,1]^n$ is also a fundamental region for $\Lambda$
- Any $t$ can be efficiently rounded to $v \in \Lambda$
- $\|t - v\| \leq \frac{1}{2} \sqrt{\sum_i \|b_i^*\|^2}$
Lattice rounding

- $B^*[0, 1]^n$ is also a fundamental region for $\Lambda$
- Any $t$ can be efficiently rounded to $v \in \Lambda$
- $\|t - v\| \leq \frac{1}{2} \sqrt{\sum_i \|b_i^*\|^2}$
- $v$ solves CVP when $\|t - v\| \leq \min \|b_i^*\|/2$
Lattice rounding

- $B^*[0, 1]^n$ is also a fundamental region for $\Lambda$
- Any $t$ can be efficiently rounded to $v \in \Lambda$
- $\|t - v\| \leq \frac{1}{2} \sqrt{\sum_{i} \|b_i^*\|^2}$
- $v$ solves CVP when $\|t - v\| \leq \min_i \|b_i^*\|/2$

Lemma (Nearest Plane Algorithm [Babai 1986])

*Rounding w.r.t $B^*$ approximates CVP within* $\sqrt{n} \cdot \frac{\max_i \|b_i^*\|}{\min_i \|b_i^*\|}$
1. Point Lattices and Lattice Parameters

2. Computational Problems
   - Coding Theory

3. The Dual Lattice

4. Q-ary Lattices and Cryptography
The Dual Lattice

- A vector space over $\mathbb{R}$ is a set of vectors $V$ with
  - a vector addition operation $x + y \in V$
  - a scalar multiplication $a \cdot x \in V$
- The dual of a vector space $V$ is the set $V^\vee = \text{Hom}(V, \mathbb{R})$ of linear functions $\phi : V \to \mathbb{R}$, typically represented as vectors $x \in V$, where $\phi_x(y) = \langle x, y \rangle$
- The dual of a lattice $\Lambda$ is defined similarly as the set of linear functions $\phi_x : \Lambda \to \mathbb{Z}$ represented as vectors $x \in \text{span}(\Lambda)$.

**Definition (Dual lattice)**

The dual of a lattice $\Lambda$ is the set of all vectors $x \in \text{span}(\Lambda)$ such that $\langle x, v \rangle \in \mathbb{Z}$ for all $v \in \Lambda$. 
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)\n\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((R\Lambda)^\vee\)
Dual lattice: Examples

- Integer lattice $(\mathbb{Z}^n) \lor = \mathbb{Z}^n$
- Rotating $(\mathbb{R} \Lambda) \lor = \mathbb{R}(\Lambda \lor)$
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((\mathbb{R}\Lambda)^\vee = \mathbb{R}(\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee\)
Dual lattice: Examples

- Integer lattice: \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating: \((R\Lambda)^\vee = R(\Lambda^\vee)\)
- Scaling: \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)
- Properties of dual:
  - \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
  - \((\Lambda^\vee)^\vee = \Lambda\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((\mathbb{R} \Lambda)^\vee = \mathbb{R} (\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)
- Properties of dual:
  - \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
  - \((\Lambda^\vee)^\vee = \Lambda\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((R\Lambda)^\vee = R(\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)
- Properties of dual:
  - \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
  - \((\Lambda^\vee)^\vee = \Lambda\)
- Operations on \(x \in \Lambda\) and \(y \in \Lambda^\vee\):
  - \(\langle x, y \rangle \in \mathbb{Z}\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((R\Lambda)^\vee = R(\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)

Properties of dual:
- \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
- \((\Lambda^\vee)^\vee = \Lambda\)

Operations on \(x \in \Lambda\) and \(y \in \Lambda^\vee\):
- \(\langle x, y \rangle \in \mathbb{Z}\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((R\Lambda)^\vee = R(\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)
- Properties of dual:
  - \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
  - \((\Lambda^\vee)^\vee = \Lambda\)
- Operations on \(x \in \Lambda\) and \(y \in \Lambda^\vee\):
  - \(\langle x, y \rangle \in \mathbb{Z}\)
Dual lattice: Examples

- Integer lattice \((\mathbb{Z}^n)^\vee = \mathbb{Z}^n\)
- Rotating \((R\Lambda)^\vee = R(\Lambda^\vee)\)
- Scaling \((q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee\)
- Properties of dual:
  - \(\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee\)
  - \((\Lambda^\vee)^\vee = \Lambda\)
- Operations on \(x \in \Lambda\) and \(y \in \Lambda^\vee\):
  - \(\langle x, y \rangle \in \mathbb{Z}\)
  - but \(x + y\) has no geometric meaning
Lattice Layers

Each dual vector $\mathbf{v} \in \mathcal{L}^\vee$, partitions the lattice $\mathcal{L}$ into layers orthogonal to $\mathbf{v}$

$$L_i = \{ \mathbf{x} \in \mathcal{L} \mid \mathbf{x} \cdot \mathbf{v} = i \}$$
Each dual vector $\mathbf{v} \in \mathcal{L}^\vee$, partitions the lattice $\mathcal{L}$ into layers orthogonal to $\mathbf{v}$

$$L_i = \{ \mathbf{x} \in \mathcal{L} \mid \mathbf{x} \cdot \mathbf{v} = i \}$$

Layers are at distance $1/\|\mathbf{v}\|$
Each dual vector \( \mathbf{v} \in \mathcal{L}^\vee \), partitions the lattice \( \mathcal{L} \) into layers orthogonal to \( \mathbf{v} \):

\[
L_i = \{ \mathbf{x} \in \mathcal{L} \mid \mathbf{x} \cdot \mathbf{v} = i \}
\]

Layers are at distance \( 1/\|\mathbf{v}\| \):

\[
\mu(\mathcal{L}) \geq \frac{1}{2\|\mathbf{v}\|}
\]
Lattice Layers

- Each dual vector $\mathbf{v} \in \mathcal{L}^\vee$, partitions the lattice $\mathcal{L}$ into layers orthogonal to $\mathbf{v}$

$$L_i = \{ \mathbf{x} \in \mathcal{L} \mid \mathbf{x} \cdot \mathbf{v} = i \}$$

- Layers are at distance $1/\|\mathbf{v}\|$.

- $\mu(\mathcal{L}) \geq \frac{1}{2\|\mathbf{v}\|}$

- If $\lambda_1(\mathcal{L}^\vee)$ is small, then $\mu(\mathcal{L})$ is large.
Transference Theorems

Theorem (Banaszczyk)
For any lattice $\mathcal{L}$
\[
1 \leq 2\lambda_1(\mathcal{L}) \cdot \mu(\mathcal{L}^\lor) \leq n.
\]

Theorem (Banaszczyk)
For every $i$,
\[
1 \leq \lambda_i(\mathcal{L}) \cdot \lambda_{n-i+1}(\mathcal{L}^\lor) \leq n.
\]

- Approximating $\lambda_1(\mathcal{L})$ within a factor $n$ is in $NP \cap coNP$
- Same is true for $\lambda_i, \ldots, \lambda_n$ and $\mu$. 

**BDD reduces to SIVP**

**BDD input:** $t$ close to $L$

BDD reduces to SIVP

Compute $V = SIVP(L \vee L)$

For each $v_i \in L \vee L$, find the layer $L_i = \{ x | x \cdot v_i = c_i \}$ closest to $t$

Output $L_1 \cap L_2 \cap \cdots \cap L_n$

Output is correct as long as

$$\mu(t, L) \leq \frac{1}{2} \|v_i\|_0$$
BDD reduces to SIVP

BDD input: \( t \) close to \( \mathcal{L} \)

- Compute \( \mathbf{V} = \text{SIVP}(\mathcal{L}^\vee) \)
BDD reduces to SIVP

BDD input: \( \mathbf{t} \) close to \( \mathcal{L} \)

- Compute \( \mathbf{V} = \text{SIVP}(\mathcal{L}^\vee) \)
- For each \( \mathbf{v}_i \in \mathcal{L}^\vee \), find the layer \( L_i = \{ \mathbf{x} | \mathbf{x} \cdot \mathbf{v}_i = c_i \} \) closest to \( \mathbf{t} \)
BDD reduces to SIVP

BDD input: \( \mathbf{t} \) close to \( \mathcal{L} \)
- Compute \( \mathbf{V} = \text{SIVP}(\mathcal{L}^\vee) \)
- For each \( \mathbf{v}_i \in \mathcal{L}^\vee \), find the layer \( L_i = \{ \mathbf{x} \mid \mathbf{x} \cdot \mathbf{v}_i = c_i \} \) closest to \( \mathbf{t} \)
- Output \( L_1 \cap L_2 \cap \cdots \cap L_n \)
BDD reduces to SIVP

BDD input: $\mathbf{t}$ close to $\mathcal{L}$
- Compute $\mathbf{V} = \text{SIVP}(\mathcal{L}^\vee)$
- For each $\mathbf{v}_i \in \mathcal{L}^\vee$, find the layer $L_i = \{ \mathbf{x} \mid \mathbf{x} \cdot \mathbf{v}_i = c_i \}$ closest to $\mathbf{t}$
- Output $L_1 \cap L_2 \cap \cdots \cap L_n$
- Output is correct as long as

$$\mu(\mathbf{t}, \mathcal{L}) \leq \frac{\lambda_1}{2n} \leq \frac{1}{2\lambda_n^\vee} \leq \frac{1}{2\|\mathbf{v}_i\|}$$
Working modulo a lattice

Definition (Fundamental Region of a lattice)

\( P \subset \mathbb{R}^n: \{ P + x \mid x \in \mathcal{L} \} \) is a partition of \( \mathbb{R}^n \).
Working modulo a lattice

Definition (Fundamental Region of a lattice)

\[ P \subset \mathbb{R}^n: \{ P + x \mid x \in \mathcal{L} \} \text{ is a partition of } \mathbb{R}^n. \]

- \((\mathcal{L}, +)\) is a subgroup of \((\mathbb{R}^n, +)\)
Working modulo a lattice

Definition (Fundamental Region of a lattice)

\( \mathcal{P} \subset \mathbb{R}^n: \{ \mathcal{P} + \mathbf{x} \mid \mathbf{x} \in \mathcal{L} \} \) is a partition of \( \mathbb{R}^n \).

- \((\mathcal{L}, +)\) is a subgroup of \((\mathbb{R}^n, +)\)
- One can form the quotient group \( \mathbb{R}^n/\mathcal{L} \)
Definition (Fundamental Region of a lattice)

\[ P \subset \mathbb{R}^n: \{ P + x \mid x \in \mathcal{L} \} \text{ is a partition of } \mathbb{R}^n. \]

- \((\mathcal{L}, +)\) is a subgroup of \((\mathbb{R}^n, +)\)
- One can form the quotient group \(\mathbb{R}^n / \mathcal{L}\)
- Elements of \(\mathbb{R}^n / \mathcal{L}\) are cosets \(t + \mathcal{L}\)
Definition (Fundamental Region of a lattice)

$P \subset \mathbb{R}^n$: $\{P + x \mid x \in \mathcal{L}\}$ is a partition of $\mathbb{R}^n$.

- $(\mathcal{L}, +)$ is a subgroup of $(\mathbb{R}^n, +)$
- One can form the quotient group $\mathbb{R}^n/\mathcal{L}$
- Elements of $\mathbb{R}^n/\mathcal{L}$ are cosets $t + \mathcal{L}$
- Any fundamental region $P$ gives a set of standard representatives
Definition (Fundamental Region of a lattice)

\[ P \subset \mathbb{R}^n: \{ P + x \mid x \in \mathcal{L} \} \text{ is a partition of } \mathbb{R}^n. \]

- \((\mathcal{L}, +)\) is a subgroup of \((\mathbb{R}^n, +)\)
- One can form the quotient group \(\mathbb{R}^n/\mathcal{L}\)
- Elements of \(\mathbb{R}^n/\mathcal{L}\) are cosets \(t + \mathcal{L}\)
- Any fundamental region \(P\) gives a set of standard representatives
- \(P = \sum_i b_i \cdot [0, 1) \equiv \mathbb{R}^n/\mathcal{L}\)
Definition (Fundamental Region of a lattice)

\[ P \subset \mathbb{R}^n: \{ P + x \mid x \in \mathcal{L} \} \text{ is a partition of } \mathbb{R}^n. \]

- \((\mathcal{L}, +)\) is a subgroup of \((\mathbb{R}^n, +)\)
- One can form the quotient group \(\mathbb{R}^n/\mathcal{L}\)
- Elements of \(\mathbb{R}^n/\mathcal{L}\) are cosets \(t + \mathcal{L}\)
- Any fundamental region \(P\) gives a set of standard representatives
- \(P = \sum_i b_i \cdot [0, 1) \equiv \mathbb{R}^n/\mathcal{L}\)
- \(t + \mathcal{L}\) is uniquely identified by \((B^\top)t \pmod{1}\)
CVP and lattice cosets

Definition

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$.
CVP and lattice cosets

- Lattice $\Lambda$, target $t$
- CVP: Find $v$ such that $e = t - v$ is shortest possible

**Definition**

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$. 
CVP and lattice cosets

- Lattice $\Lambda$, target $t$
- CVP: Find $v$ such that $e = t - v$ is shortest possible

**Definition**

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$. 

Daniele Micciancio (UCSD)
CVP and lattice cosets

- Lattice $\Lambda$, target $t$
- CVP: Find $v$ such that $e = t - v$ is shortest possible
- $t' = t + Bx$

**Definition**

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$. 
CVP and lattice cosets

- Lattice $\Lambda$, target $t$
- CVP: Find $v$ such that $e = t - v$ is shortest possible
- $t' = t + Bx$
- $v = v' - Bx$

Definition

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$.
CVP and lattice cosets

- Lattice $\Lambda$, target $t$
- CVP: Find $v$ such that $e = t - v$ is shortest possible
- $t' = t + Bx$
- $v = v' - Bx$

**Definition**

CVP (coset formulation) Given a lattice coset $t + \mathcal{L}$, find the (approximately) shortest element of $t + \mathcal{L}$. 
1. Point Lattices and Lattice Parameters

2. Computational Problems
   - Coding Theory

3. The Dual Lattice

4. Q-ary Lattices and Cryptography
Random lattices in Cryptography

- Cryptography typically uses (random) lattices $\Lambda$ such that
  - $\Lambda \subseteq \mathbb{Z}^d$ is an integer lattice
  - $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer $q$.
- Cryptographic functions based on $q$-ary lattices involve only arithmetic modulo $q$.

**Definition ($q$-ary lattice)**

$\Lambda$ is a $q$-ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$
Examples of $q$-ary lattices

Examples (for any $A \in \mathbb{Z}_q^{n \times d}$)

- $\Lambda_q(A) = \{x \mid x \mod q \in A^T \mathbb{Z}_q^n\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^\perp(A) = \{x \mid Ax = 0 \mod q\} \subseteq \mathbb{Z}^d$
Examples of $q$-ary lattices

Examples (for any $A \in \mathbb{Z}_q^{n \times d}$)

- $\Lambda_q(A) = \{ x \mid x \mod q \in A^T \mathbb{Z}_q^n \} \subseteq \mathbb{Z}^d$
- $\Lambda_q^\perp(A) = \{ x \mid Ax = 0 \mod q \} \subseteq \mathbb{Z}^d$

Theorem

For any lattice $\Lambda$ the following conditions are equivalent:

- $q\mathbb{Z}^d \subseteq \Lambda \subseteq \mathbb{Z}^d$
- $\Lambda = \Lambda_q(A)$ for some $A$
- $\Lambda = \Lambda_q^\perp(A)$ for some $A$

For any fixed $A$, the lattices $\Lambda_q(A)$ and $\Lambda_q^\perp(A)$ are different
Duality of $q$-ary lattices

- For any fixed $A$, the lattices $\Lambda_q(A)$ and $\Lambda_q^\perp(A)$ are different.
- For any $A \in \mathbb{Z}^{n \times d}_q$ there is a $A' \in \mathbb{Z}^{k \times d}_q$ such that $\Lambda_q(A) = \Lambda_q^\perp(A')$.
- For any $A' \in \mathbb{Z}^{k \times d}_q$ there is a $A \in \mathbb{Z}^{n \times d}_q$ such that $\Lambda_q(A) = \Lambda_q^\perp(A')$.
- The $q$-ary lattices associated to $A$ are dual (up to scaling)

\[
\Lambda_q(A)^\vee = \frac{1}{q} \Lambda_q^\perp(A)
\]
\[
\Lambda_q^\perp(A)^\vee = \frac{1}{q} \Lambda_q(A)
\]
Ajtai’s one-way function (SIS)

- Parameters: \( m, n, q \in \mathbb{Z} \)
- Key: \( A \in \mathbb{Z}^{n \times m}_q \)
- Input: \( x \in \{0, 1\}^m \)

\[
\text{Output: } f_A(x) = Ax \mod q
\]

Theorem (A'96)

For \( m > n \log q \), if lattice problems (SIVP) are hard to approximate in the worst-case, then \( f_A(x) = Ax \mod q \) is a one-way function.

Applications: OWF [A’96], Hashing [GGH’97], Commit [KTX’08], IDs schemes [L’08], Signatures [LM’08, GPV’08, …, DDLL’13] …
Ajtai’s one-way function (SIS)

- Parameters: $m, n, q \in \mathbb{Z}$
- Key: $A \in \mathbb{Z}_q^{n \times m}$
- Input: $x \in \{0, 1\}^m$
- Output: $f_A(x) = Ax \mod q$

Theorem (A'96)

For $m > n \log q$, if lattice problems (SIVP) are hard to approximate in the worst-case, then $f_A(x) = Ax \mod q$ is a one-way function.

Applications: OWF [A'96], Hashing [GGH'97], Commit [KTX'08], IDs schemes [L'08], Signatures [LM'08, GPV'08, ... , DDLL'13]...
Ajtai’s one-way function (SIS)

- **Parameters:** $m, n, q \in \mathbb{Z}$
- **Key:** $A \in \mathbb{Z}_q^{n \times m}$
- **Input:** $x \in \{0, 1\}^m$
- **Output:** $f_A(x) = Ax \mod q$

**Theorem (A’96)**

*For $m > n \log q$, if lattice problems (SIVP) are hard to approximate in the worst-case, then $f_A(x) = Ax \mod q$ is a one-way function.*

Applications: OWF [A’96], Hashing [GGH’97], Commit [KTX’08], ID schemes [L’08], Signatures [LM’08, GPV’08, . . ., DDLL’13] . . .
Ajtai’s function and $q$-ary lattices

- $f_A(x) = Ax \mod q$, where $x$ is short
Ajtai’s function and $q$-ary lattices

- $f_A(x) = Ax \mod q$, where $x$ is short
- The $q$-ary lattice $\Lambda_q^\perp(A)$ is the kernel of $f_A$
Ajtai’s function and $q$-ary lattices

- $f_A(x) = Ax \mod q$, where $x$ is short
- The $q$-ary lattice $\Lambda_q^\perp(A)$ is the kernel of $f_A$
- Finding collisions $f_A(x) = f_A(y)$ is equivalent to finding short vectors $x - y \in \Lambda_q^\perp(A)$
Ajtai’s function and $q$-ary lattices

- $f_A(x) = Ax \mod q$, where $x$ is short
- The $q$-ary lattice $\Lambda_q^\perp(A)$ is the kernel of $f_A$
- Finding collisions $f_A(x) = f_A(y)$ is equivalent to finding short vectors $x - y \in \Lambda_q^\perp(A)$
- The output of $f_A(x)$ is the syndrome of $x$
**Ajtai’s function and \( q \)-ary lattices**

- \( f_A(x) = Ax \mod q \), where \( x \) is short
- The \( q \)-ary lattice \( \Lambda_q(A) \) is the kernel of \( f_A \)
- Finding collisions \( f_A(x) = f_A(y) \) is equivalent to finding short vectors \( x - y \in \Lambda_q(A) \)
- The output of \( f_A(x) \) is the syndrome of \( x \)
- Inverting \( f_A(x) \) is the same as CVP in its syndrome decoding formulation with lattice \( \Lambda_q(A) \) and target \( t \in x + \Lambda_q(A) \)
Ajtai’s function and $q$-ary lattices

- $f_A(x) = Ax \mod q$, where $x$ is short
- The $q$-ary lattice $\Lambda_q^\perp(A)$ is the kernel of $f_A$
- Finding collisions $f_A(x) = f_A(y)$ is equivalent to finding short vectors $x - y \in \Lambda_q^\perp(A)$
- The output of $f_A(x)$ is the syndrome of $x$
- Inverting $f_A(x)$ is the same as CVP in its syndrome decoding formulation with lattice $\Lambda_q^\perp(A)$ and target $t \in x + \Lambda_q^\perp(A)$
- For $f_A$ to be a compression function, $x$ is longer than $\frac{1}{2} \lambda_1(\Lambda_q^\perp(A))$

Remark

SIS $\equiv$ Approximate ADD (Absolute Distance Decoding)
Regev’s Learning With Errors (LWE)

- \( A \in \mathbb{Z}_q^{m \times k}, \ s \in \mathbb{Z}_q^k, \ e \in \mathcal{E}^m. \)
- \( g_A(s, e) = As \mod q \)
Regev’s Learning With Errors (LWE)

- \( A \in \mathbb{Z}_q^{m \times k}, \ s \in \mathbb{Z}_q^k, \ e \in \mathcal{E}^m. \)
- \( g_A(s; e) = As + e \mod q \)
- Learning with Errors: Given \( A \) and \( g_A(s, e) \), recover \( s \).
Regev’s Learning With Errors (LWE)

- \( A \in \mathbb{Z}_q^{m \times k}, \ s \in \mathbb{Z}_q^k, \ e \in \mathcal{E}^m. \)
- \( g_A(s; e) = As + e \text{ mod } q \)
- Learning with Errors: Given \( A \) and \( g_A(s, e) \), recover \( s \).

**Theorem (R’05)**

The function \( g_A(s, e) \) is hard to invert on the average, assuming SIVP is hard to approximate in the worst-case.

Applications: CPA PKE [R’05], CCA PKE [PW’08], (H)IBE [GPV’08,CHKP’10,ABB’10], FHE [. . . ,B’12,AP’13,GSW’13], . . .
LWE and $q$-ary lattices

- **Learning with errors:**
  - **Input:** $A \in \mathbb{Z}_q^{m \times n}$ and $As + e$, where $e$ is small and $s$ is arbitrary
  - **Output:** $s, e$

If $e = 0$, then $As + e = As \in \Lambda(A_t)$

Same as CVP in random $q$-ary lattice $\Lambda(A_t)$ with random target $t = As + e$

Usually $e$ is shorter than $\frac{1}{2}\lambda_1(\Lambda(A_t))$, and $e$ is uniquely determined

**Remark**

$LWE \equiv$ Approximate BDD (Bounded Distance Decoding)
LWE and $q$-ary lattices

- Learning with errors:
  - Input: $\mathbf{A} \in \mathbb{Z}_{q}^{m \times n}$ and $\mathbf{A}s + \mathbf{e}$, where $\mathbf{e}$ is small and $s$ is arbitrary
  - Output: $s, \mathbf{e}$

- If $\mathbf{e} = \mathbf{0}$, then $\mathbf{A}s + \mathbf{e} = \mathbf{A}s \in \Lambda(\mathbf{A}^t)$
LWE and $q$-ary lattices

- Learning with errors:
  - Input: $A \in \mathbb{Z}_q^{m \times n}$ and $As + e$, where $e$ is small and $s$ is arbitrary
  - Output: $s, e$

- If $e = 0$, then $As + e = As \in \Lambda(A^t)$

- Same as CVP in random $q$-ary lattice $\Lambda(A^t)$ with random target $t = As + e$
LWE and $q$-ary lattices

- Learning with errors:
  - Input: $A \in \mathbb{Z}_q^{m \times n}$ and $As + e$, where $e$ is small and $s$ is arbitrary
  - Output: $s, e$

- If $e = 0$, then $As + e = As \in \Lambda(A^t)$

- Same as CVP in random $q$-ary lattice $\Lambda(A^t)$ with random target $t = As + e$

- Usually $e$ is shorter than $\frac{1}{2} \lambda_1(\Lambda(A^T))$, and $e$ is uniquely determined
LWE and $q$-ary lattices

- **Learning with errors:**
  - Input: $A \in \mathbb{Z}_q^{m \times n}$ and $As+e$, where $e$ is small and $s$ is arbitrary
  - Output: $s, e$
- If $e = 0$, then $As+e = As \in \Lambda(A^t)$
- Same as CVP in random $q$-ary lattice $\Lambda(A^t)$ with random target $t = As+e$
- Usually $e$ is shorter than $\frac{1}{2} \lambda_1(\Lambda(A^T))$, and $e$ is uniquely determined

**Remark**

$LWE \equiv$ Approximate BDD (Bounded Distance Decoding)
Much more ...

Not covered in this introduction:

- Gaussian measures and harmonic analysis
- Lattices from Algebraic Number Theory
- Other norms
- Sphere packings
- Average-case to Worst-case connection