# The Mathematics of Lattices

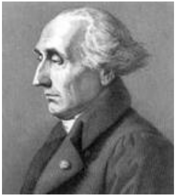
Daniele Micciancio

January 2020

# Outline

# (Point) Lattices

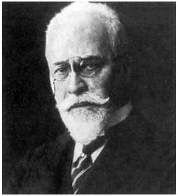
- Traditional area of mathematics



Lagrange

Gauss

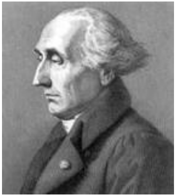
◦ ◦ ◦



Minkowski

# (Point) Lattices

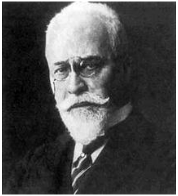
- Traditional area of mathematics



Lagrange

Gauss

∘ ∘ ∘



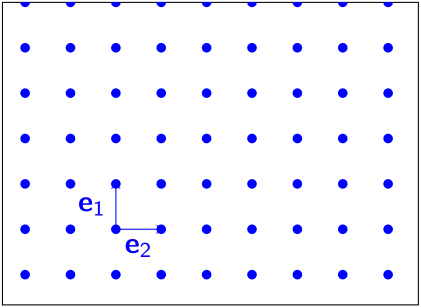
Minkowski

- 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.

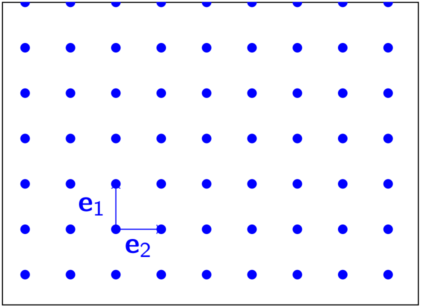
# Lattices: Definition




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

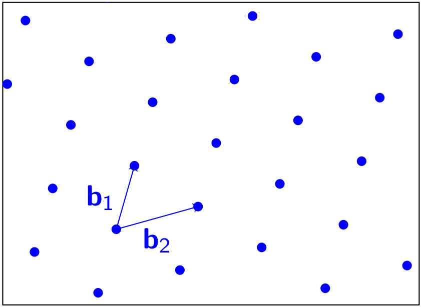
$$\Lambda = \mathbb{Z}^n$$

# Lattices: Definition




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

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



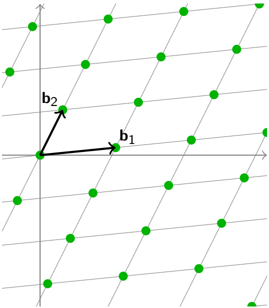

Other lattices are obtained by applying a linear transformation

$$\Lambda = \mathbf{B}\mathbb{Z}^n \qquad (\mathbf{B} \in \mathbb{R}^{d \times n})$$

# Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

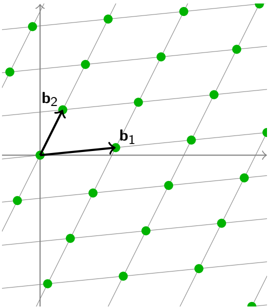
$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z}$$



# Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

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



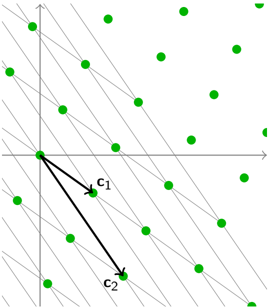
# Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has many bases

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



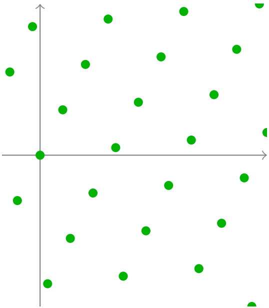
# Lattices and Bases

A lattice is the set of all integer linear combinations of (linearly independent) basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{Bx} \colon \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has many bases

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



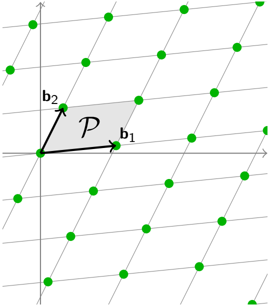
**Definition (Lattice)**

A discrete additive subgroup of $\mathbb{R}^n$

# Determinant

**Definition (Determinant)**

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

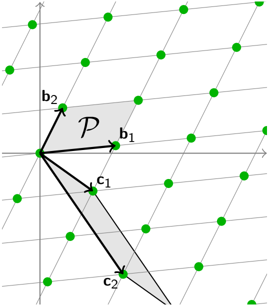


# Determinant

**Definition (Determinant)**

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

- Different bases define different fundamental regions

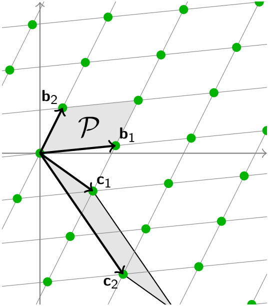


# Determinant

**Definition (Determinant)**

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

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

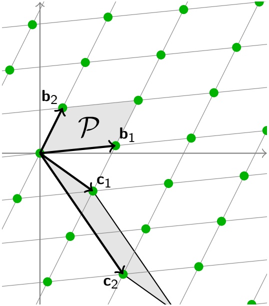


# Determinant

## Definition (Determinant)

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

- 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.



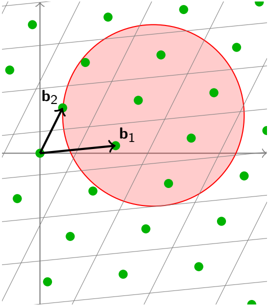
# Density estimates

**Definition (Centered Fundamental Parallelepiped)**

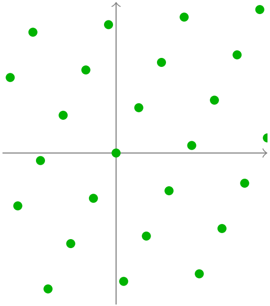
$\mathcal{P} = \sum_i \mathbf{b}_i \cdot [-1/2, 1/2)$

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

$$|S \cap \mathcal{L}| \approx \text{vol}(S) / \det(\mathcal{L})$$



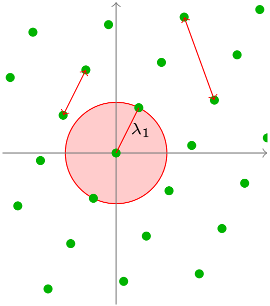
# Minimum Distance and Successive Minima



# Minimum Distance and Successive Minima

- Minimum distance

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



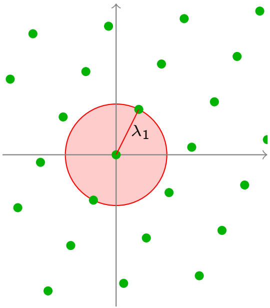
# Minimum Distance and Successive Minima

- Minimum distance

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

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

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



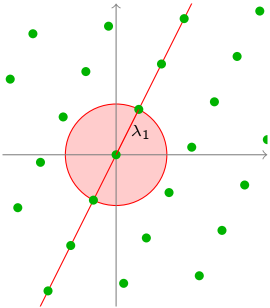
# Minimum Distance and Successive Minima

- Minimum distance

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

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

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



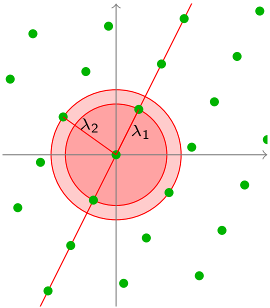
# Minimum Distance and Successive Minima

- Minimum distance

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

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

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



# Minimum Distance and Successive Minima

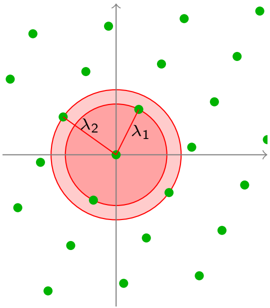
- Minimum distance

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

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

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

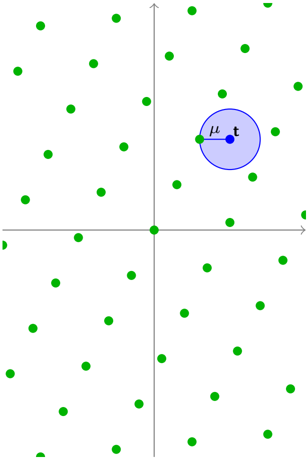
- Examples
  - $\mathbb{Z}^n$: $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1$
  - Always: $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$



# Distance Function and Covering Radius

- Distance function

$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$



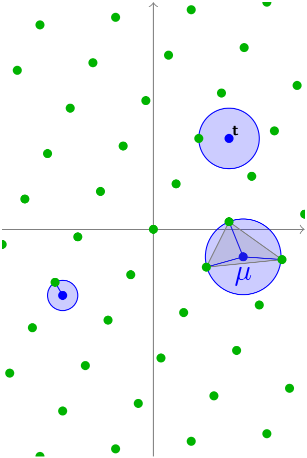
# Distance Function and Covering Radius

- Distance function

$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$

- Covering radius

$$\mu(\mathcal{L}) = \max_{\mathbf{t} \in span(\mathcal{L})} \mu(\mathbf{t}, \mathcal{L})$$



# Distance Function and Covering Radius

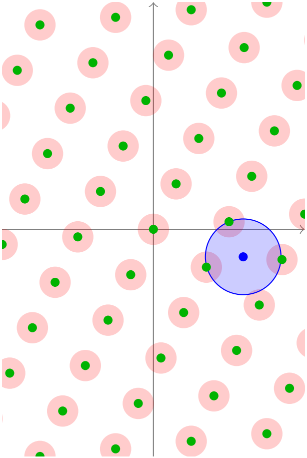
- Distance function

$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$

- Covering radius

$$\mu(\mathcal{L}) = \max_{\mathbf{t} \in span(\mathcal{L})} \mu(\mathbf{t}, \mathcal{L})$$

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



# Distance Function and Covering Radius

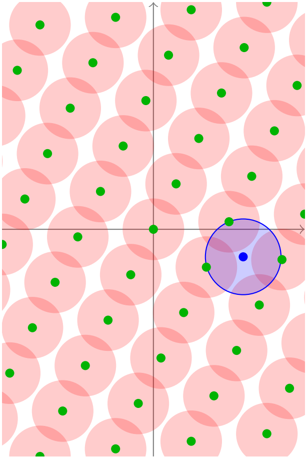
- Distance function

$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$

- Covering radius

$$\mu(\mathcal{L}) = \max_{\mathbf{t} \in span(\mathcal{L})} \mu(\mathbf{t}, \mathcal{L})$$

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



# Distance Function and Covering Radius

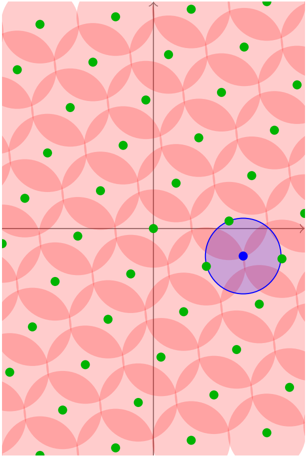
- Distance function

$$\mu(\mathbf{t}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{t} - \mathbf{x}\|$$

- Covering radius

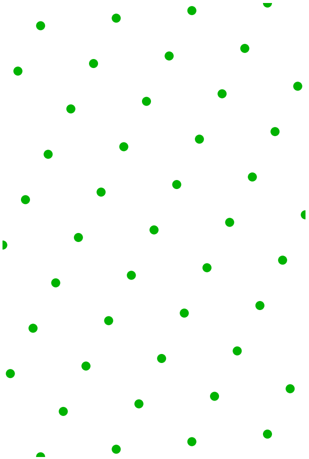
$$\mu(\mathcal{L}) = \max_{\mathbf{t} \in span(\mathcal{L})} \mu(\mathbf{t}, \mathcal{L})$$

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



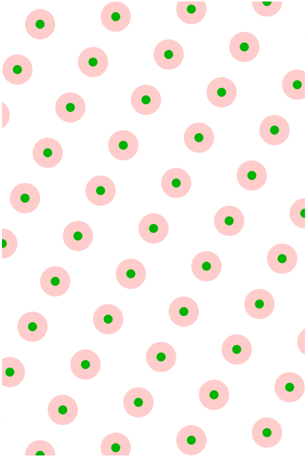
# Smoothing a lattice

Consider an arbitrary lattice, and . . .



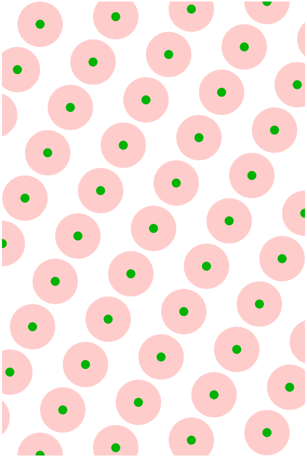
# Smoothing a lattice

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



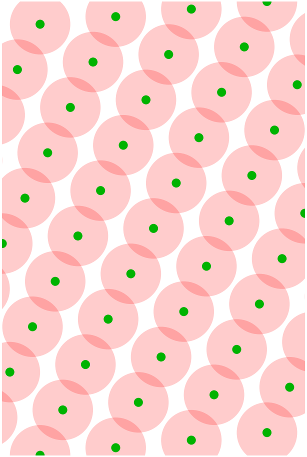
# Smoothing a lattice

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



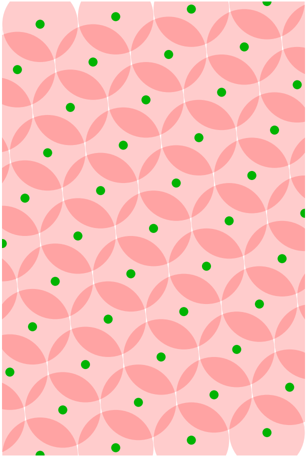
# Smoothing a lattice

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



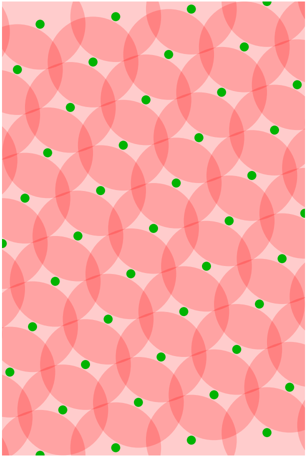
# Smoothing a lattice

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



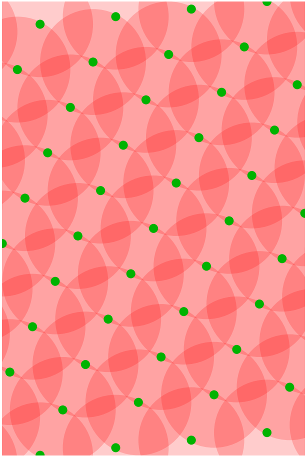
# Smoothing a lattice

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



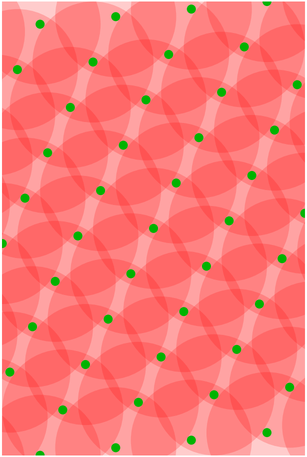
# Smoothing a lattice

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



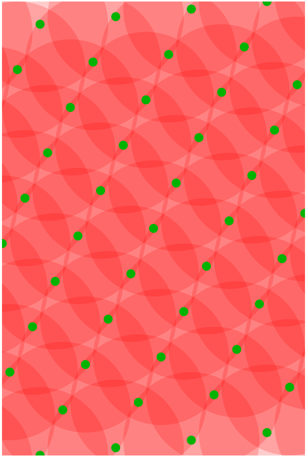
# Smoothing a lattice

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



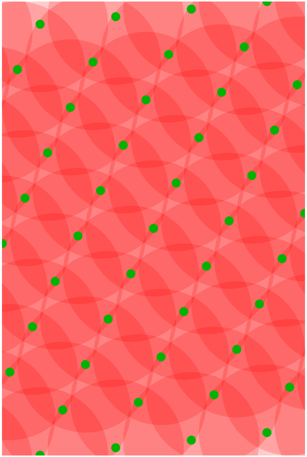
# Smoothing a lattice

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 $\|\mathbf{r}\| \leq (\log n) \cdot \sqrt{n}\lambda_n$

# 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

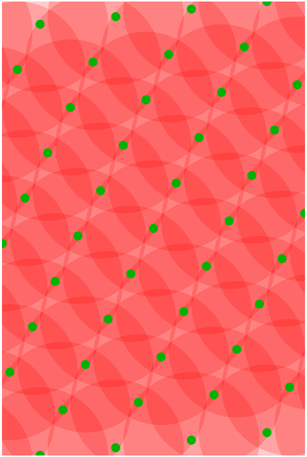
How much noise is needed?

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

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

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

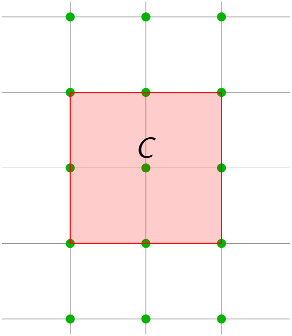
$\eta_\epsilon$: the "smoothing parameter" of a lattice [MR04].



# Minkowski's convex body theorem

**Theorem (Convex Body)**

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

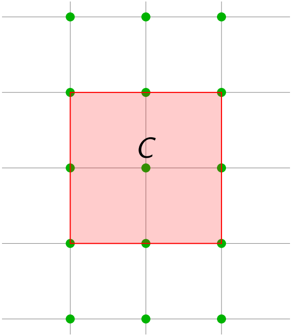


# Minkowski's convex body theorem

## Theorem (Convex Body)

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

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



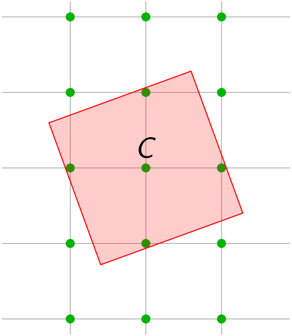
# Minkowski's convex body theorem

## Theorem (Convex Body)

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

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

- $C = \mathbf{B}^{-1}[-r, r]^n$ has volume $\det(\mathbf{B})^{-1}(2r)^n = 2^n$



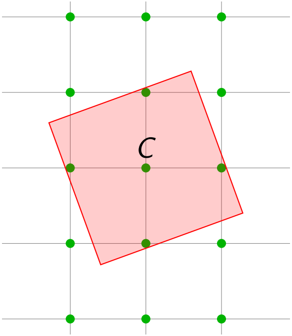
# Minkowski's convex body theorem

## Theorem (Convex Body)

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

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

- $C = \mathbf{B}^{-1}[-r, r]^n$ has volume $\det(\mathbf{B})^{-1}(2r)^n = 2^n$
- $C$ contains $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$



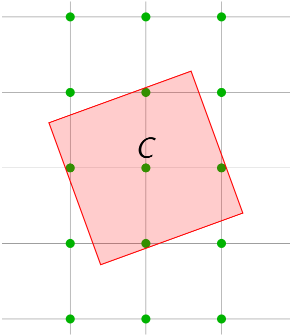
# Minkowski's convex body theorem

## Theorem (Convex Body)

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

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

- $C = \mathbf{B}^{-1}[-r, r]^n$ has volume $\det(\mathbf{B})^{-1}(2r)^n = 2^n$
- $C$ contains $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$
- $\mathbf{B}C = [-r, r]^n$ contains $\mathbf{Bx}$



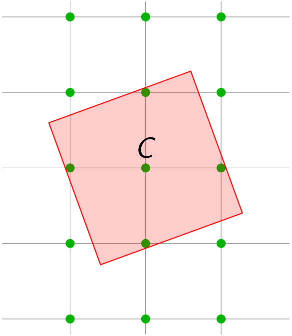
# Minkowski's convex body theorem

**Theorem (Convex Body)**

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

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

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



# Minkowski's second theorem

**Theorem (Minkowski)**

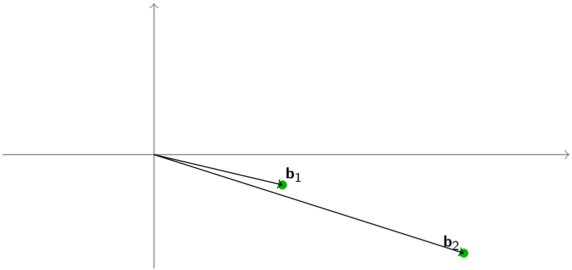
$$\lambda_1(\mathcal{L}) \leq \left(\prod_i \lambda_i(\mathcal{L})\right)^{1/n} \leq \sqrt{n}\,\det(\mathcal{L})^{1/n}$$

- 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?

# Shortest Vector Problem

**Definition (Shortest Vector Problem, SVP)**

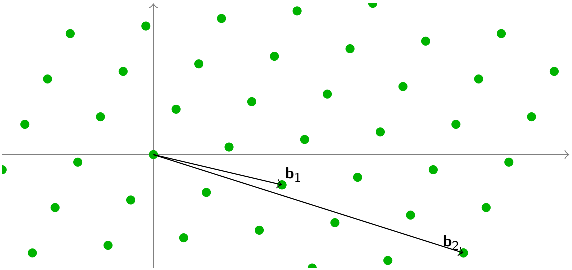
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



# Shortest Vector Problem

**Definition (Shortest Vector Problem, SVP)**

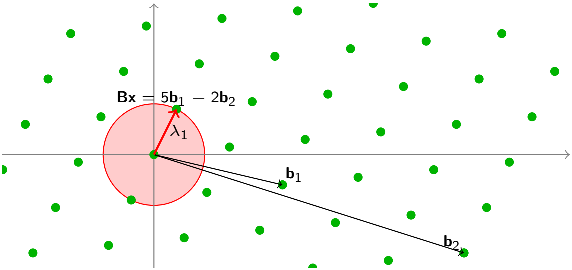
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



# Shortest Vector Problem

**Definition (Shortest Vector Problem, SVP)**

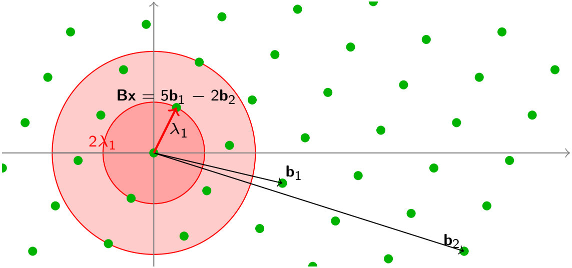
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \lambda_1$



# Shortest Vector Problem

**Definition (Shortest Vector Problem, $\mathsf{SVP}_\gamma$)**

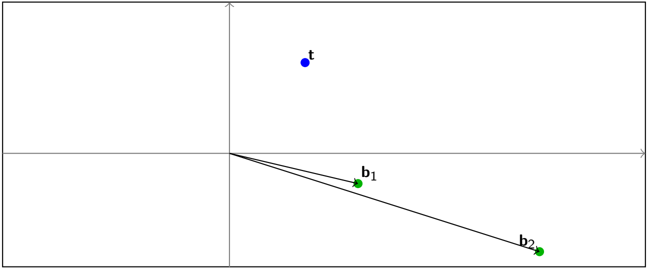
Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma\lambda_1$



# Closest Vector Problem

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

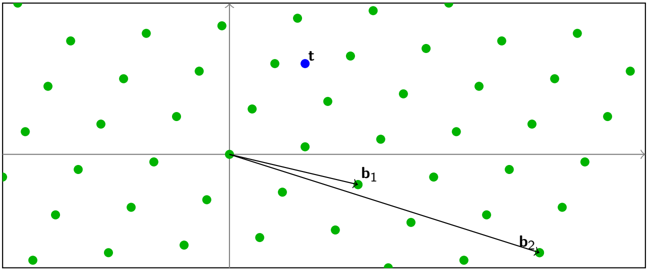
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



# Closest Vector Problem

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

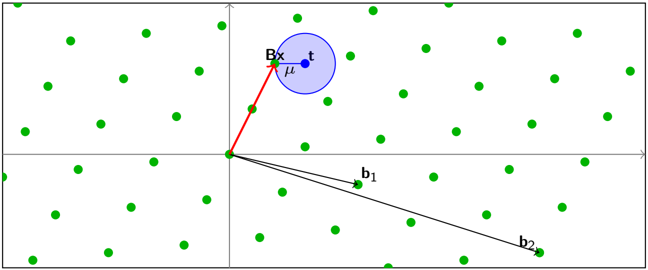
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



# Closest Vector Problem

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

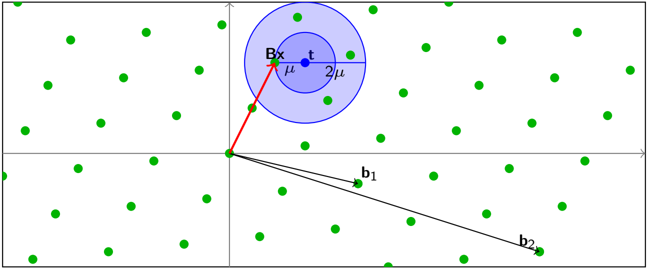
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \mu$ from the target



# Closest Vector Problem

**Definition (Closest Vector Problem, $\mathrm{CVP}_\gamma$)**

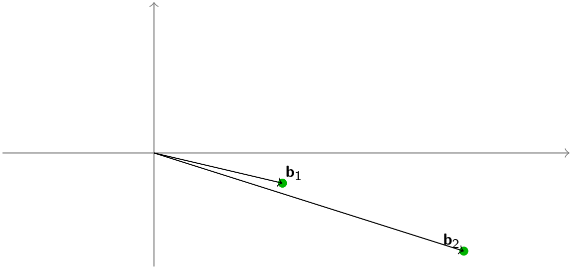
Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma\mu$ from the target



# Shortest Independent Vectors Problem

**Definition (Shortest Independent Vectors Problem, SIVP)**

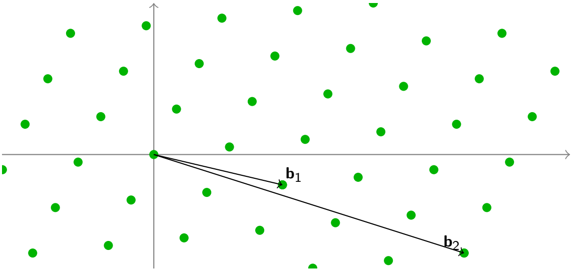
Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \lambda_n$



# Shortest Independent Vectors Problem

**Definition (Shortest Independent Vectors Problem, SIVP)**

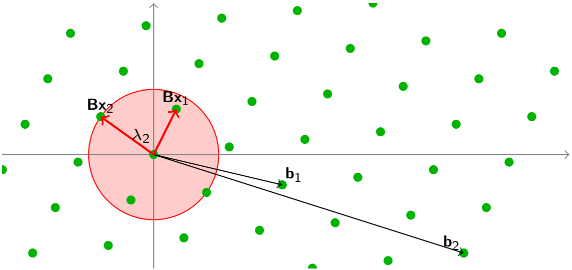
Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \lambda_n$



# Shortest Independent Vectors Problem

### Definition (Shortest Independent Vectors Problem, SIVP)

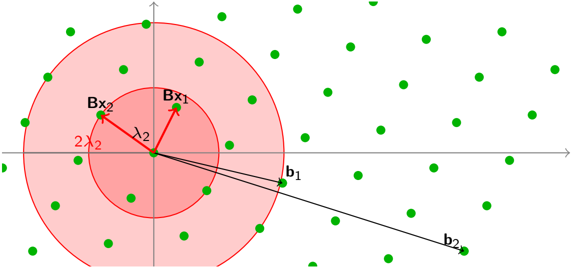
Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \lambda_n$



# Shortest Independent Vectors Problem

## Definition (Shortest Independent Vectors Problem, SIVP$_\gamma$)

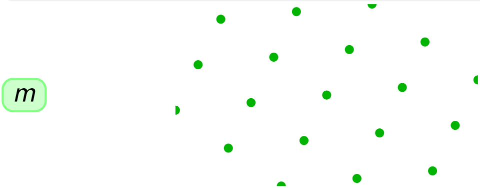
Given a lattice $\mathcal{L}(\mathbf{B})$, find $n$ linearly independent lattice vectors $\mathbf{Bx}_1, \ldots, \mathbf{Bx}_n$ of length (at most) $\max_i \|\mathbf{Bx}_i\| \leq \gamma\lambda_n$



# Coding theory

## Problem

*Reliable transmission of information over noisy channels*

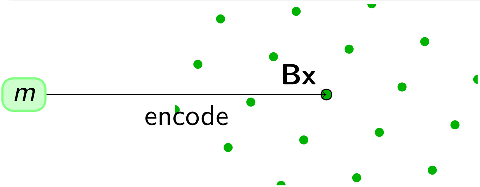



Sender wants to trasmit a message $m$

# Coding theory

## Problem

*Reliable transmission of information over noisy channels*

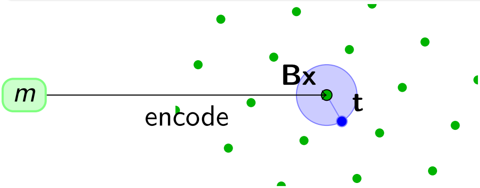



The sender encodes $m$ as a lattice point $\mathbf{Bx}$ and transmits it over a noisy channel (e.g., multiantenna system)

# Coding theory

## Problem

*Reliable transmission of information over noisy channels*

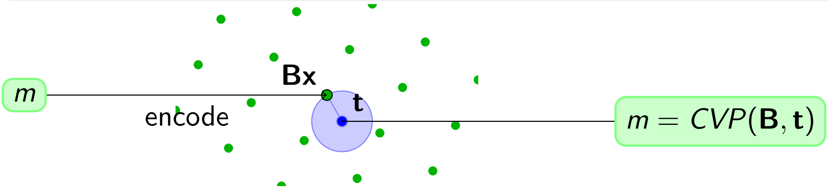



Recepient receives a perturbed lattice point $\mathbf{t} = \mathbf{Bx} + \mathbf{e}$, where $\mathbf{e}$ is a small error vector

# Coding theory

## Problem

*Reliable transmission of information over noisy channels*

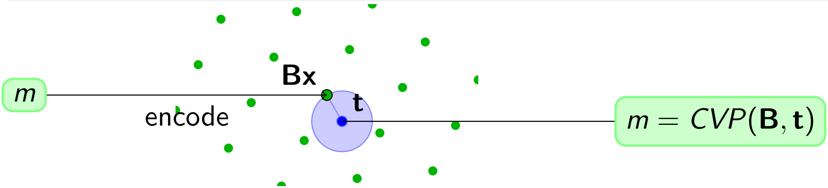



Recepient recovers the original message $m$ by finding the lattice point $\mathbf{Bx}$ closest to the target $\mathbf{t}$.

# Coding theory

## Problem

*Reliable transmission of information over noisy channels*




- CVP Decoding algorithm
- SVP Evaluating error correction radius $\lambda_1/2$
- SIVP Related to distortion in vector quantization

# Special Versions of CVP

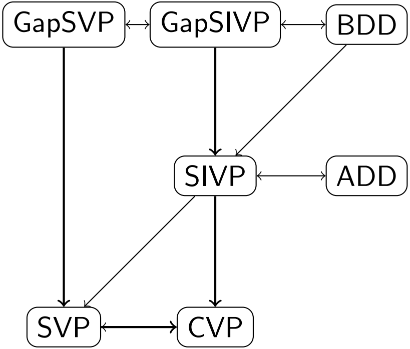
**Definition (Closest Vector Problem (CVP))**

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.

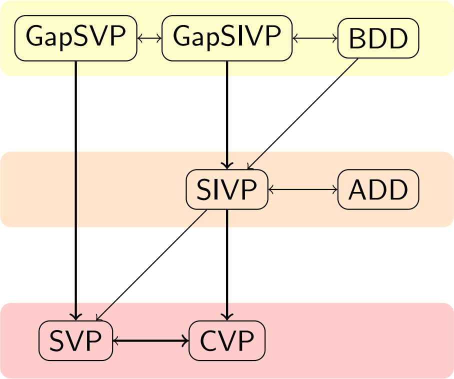
# Relations among lattice problems

- SIVP $\approx$ ADD [MG'01]
- SVP $\leq$ CVP [GMSS'99]
- SIVP $\leq$ CVP [M'08]
- BDD $\lesssim$ SIVP
- CVP $\lesssim$ SVP [L'87]
- GapSVP $\approx$ GapSIVP [LLS'91,B'93]
- GapSVP $\lesssim$ BDD [LM'09]



# Relations among lattice problems

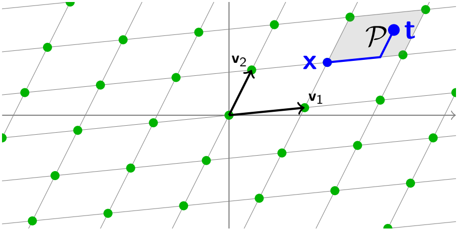
- SIVP $\approx$ ADD [MG'01]
- SVP $\leq$ CVP [GMSS'99]
- SIVP $\leq$ CVP [M'08]
- BDD $\lesssim$ SIVP
- CVP $\lesssim$ SVP [L'87]
- GapSVP $\approx$ GapSIVP [LLS'91,B'93]
- GapSVP $\lesssim$ BDD [LM'09]



# ADD reduces to SIVP

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

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



# 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

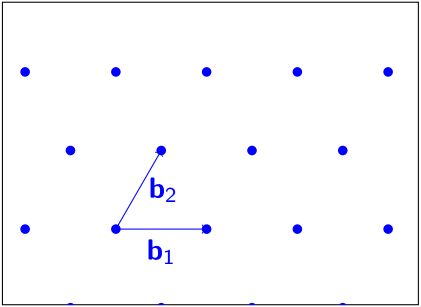
- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\text{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$

# 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 $\text{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$
- Rounding solves CVP whenever $\Lambda$ has an orthogonal basis

# Geometry of Lattices

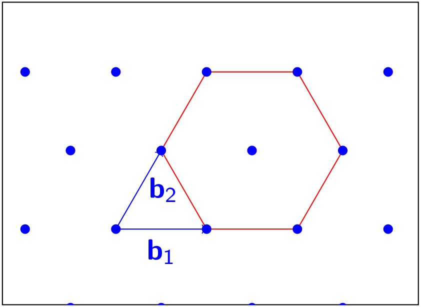
- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\mathrm{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$
- Rounding solves CVP whenever $\Lambda$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




- Not all lattices have an orthogonal basis

# Geometry of Lattices

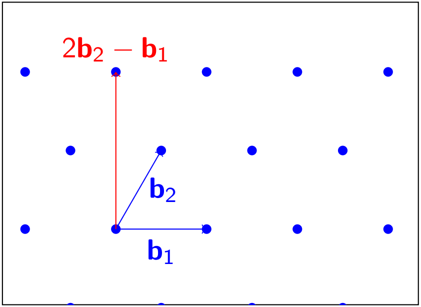
- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\mathrm{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$
- Rounding solves CVP whenever $\Lambda$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




- Not all lattices have an orthogonal basis
- E.g. "exagonal" lattice

# Geometry of Lattices

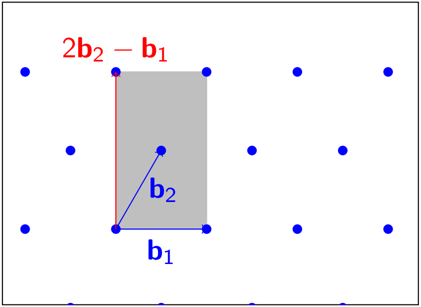
- Geometry is a powerful tool to attack combinatorial problems
  - LP/SDP relaxation + randomized rounding
  - Lattices: reduce Subset-Sum to CVP
- CVP can be easy: e.g., if $\Lambda = \mathbb{Z}^n$, then $\mathrm{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$
- Rounding solves CVP whenever $\Lambda$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




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

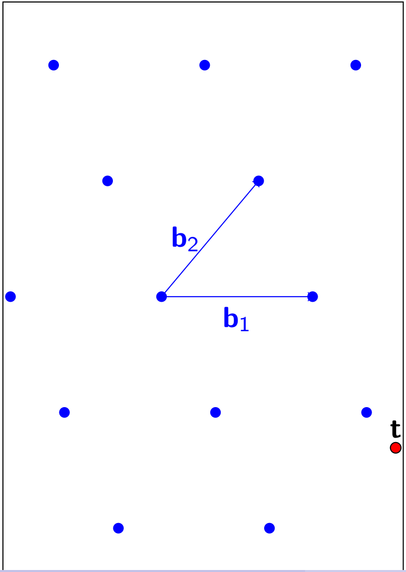
# Geometry of Lattices

- 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 $\mathrm{CVP}(\Lambda, \mathbf{t}) = \lfloor \mathbf{t} \rceil$
- Rounding solves CVP whenever $\Lambda$ has an orthogonal basis



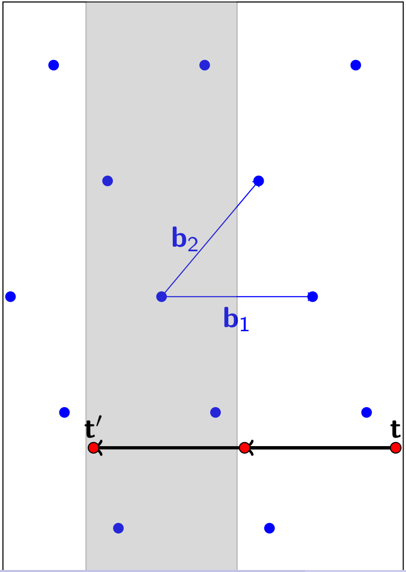

- Not all lattices have an orthogonal basis
- E.g. "exagonal" lattice
- $\mathbf{b}_1 \quad \perp \quad (2\mathbf{b}_2 - \mathbf{b}_1)$
- But they only generate a sublattice

# Size Reduction



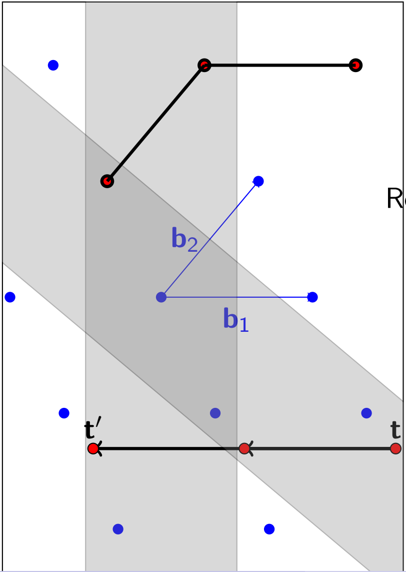

- $\mathbf{b}_1$: (short) lattice vector
- $\mathbf{t}$: arbitrary point

# 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

# 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

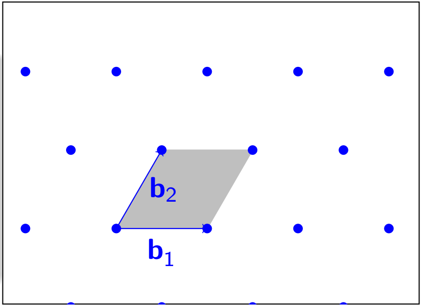
- $\mathbf{t} - \mathbf{t}' \in \Lambda$
- Key step in [LLL'82] basis reduction algorithm
- Technique is used in most other lattice algorithms

# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

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

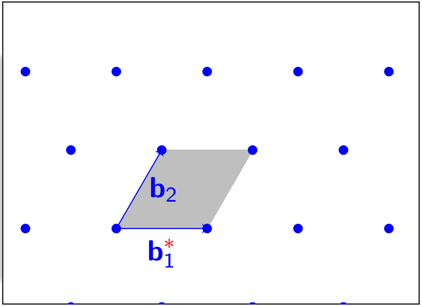


# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

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



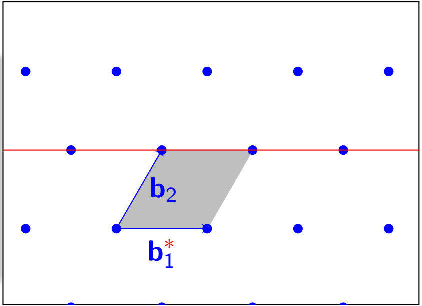
# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

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

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

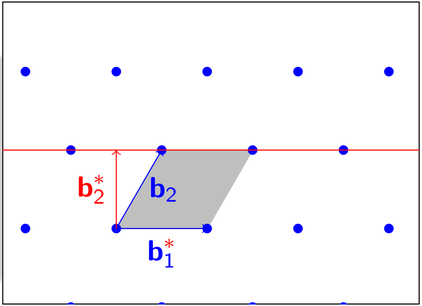


# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

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

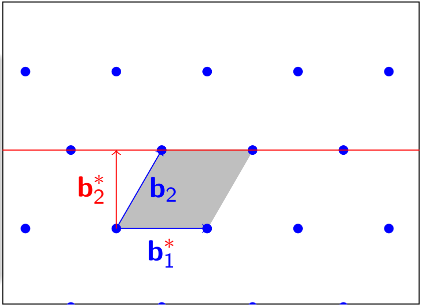


# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

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



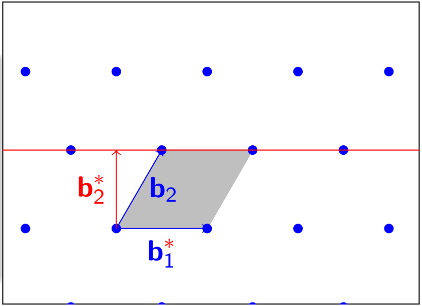

- $\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B}\mathbb{R}^n$

# Gram-Schmidt Orthogonalized Basis

**Definition (Gram-Schmidt)**

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

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



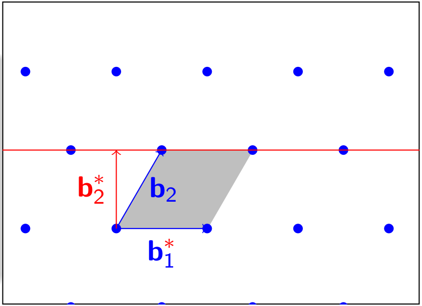

- $\mathbf{B}^*$ is an orthogonal basis for the vector space $\mathbf{B}\mathbb{R}^n$
- $\mathbf{B}^*$ is not a lattice basis for $\mathbf{B}\mathbb{Z}^n$

# Gram-Schmidt Orthogonalized Basis

## Definition (Gram-Schmidt)

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

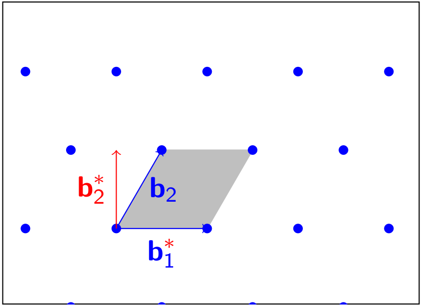
$$\mathbf{b}_i^* \in \mathbf{b}_i + [\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}]\mathbb{R}^{i-1}$$
$$\mathbf{b}_i^* \perp \mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$$




- $\mathbf{B}^*$ 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 $\mathbf{B}$

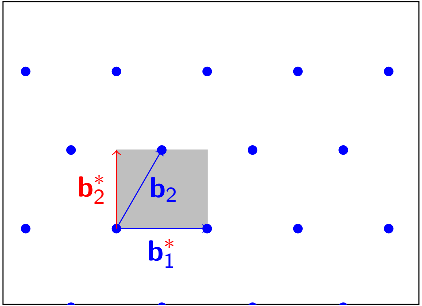
$$\det(\Lambda) = \prod_i \|\mathbf{b}_i^*\| \leq \prod_i \|\mathbf{b}_i\| \qquad (\textit{Hadamard})$$

# Lattice rounding



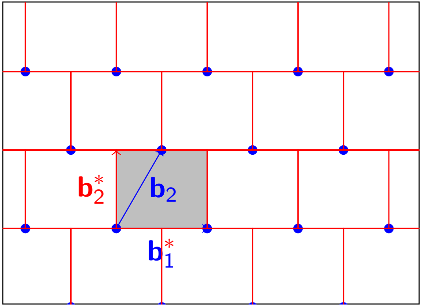
# Lattice rounding

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



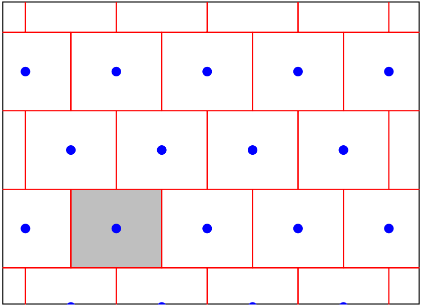
# Lattice rounding

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



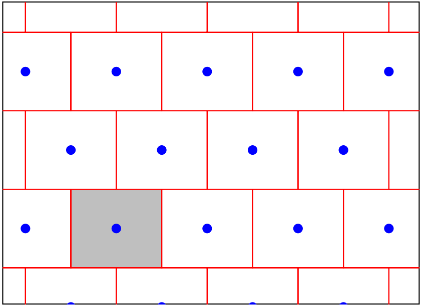
# Lattice rounding

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



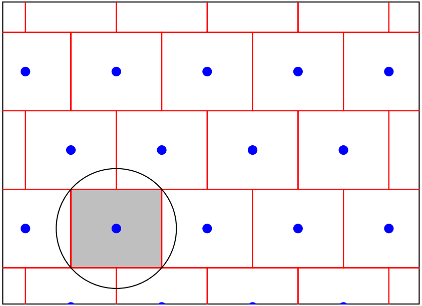
# Lattice rounding

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



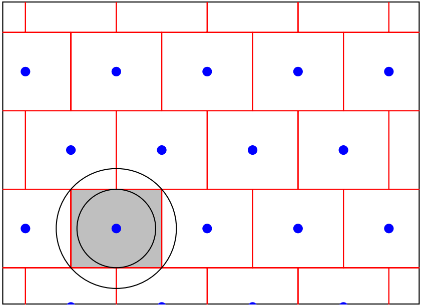
# Lattice rounding

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



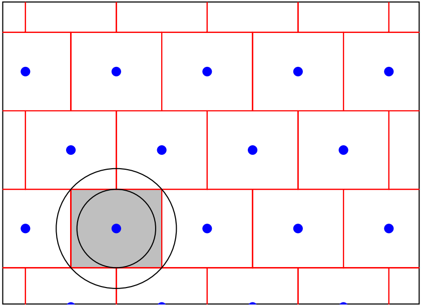
# Lattice rounding

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



# Lattice rounding

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



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

*Rounding w.r.t* $\mathbf{B}^*$ *approximates CVP within* $\sqrt{n} \cdot \frac{\max_i \|\mathbf{b}_i^*\|}{\min_i \|\mathbf{b}_i^*\|}$

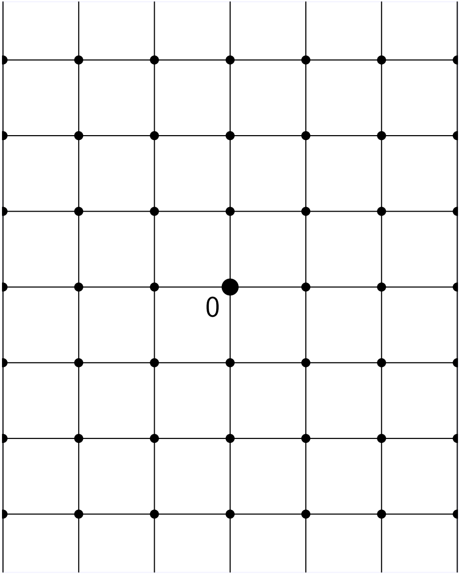
# The Dual Lattice

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

## Definition (Dual lattice)

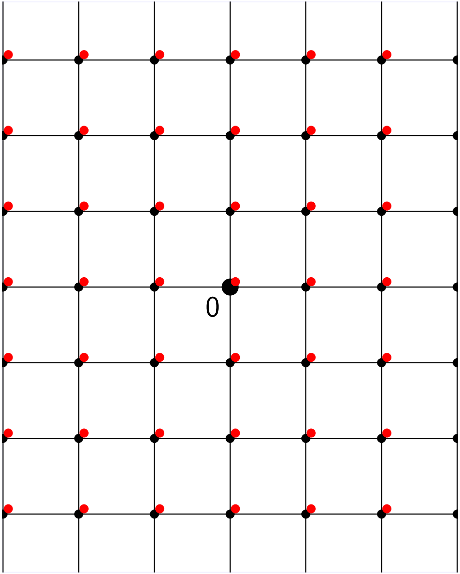
The dual of a lattice $\Lambda$ is the set of all vectors $\mathbf{x} \in span(\Lambda)$ such that $\langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}$ for all $\mathbf{v} \in \Lambda$

# Dual lattice: Examples



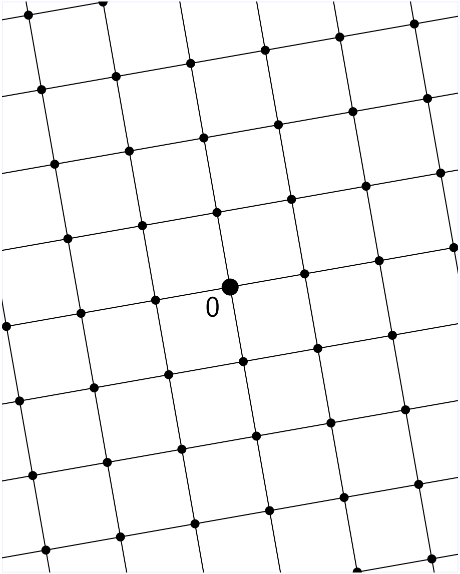

- Integer lattice $(\mathbb{Z}^n)^\vee$

# Dual lattice: Examples



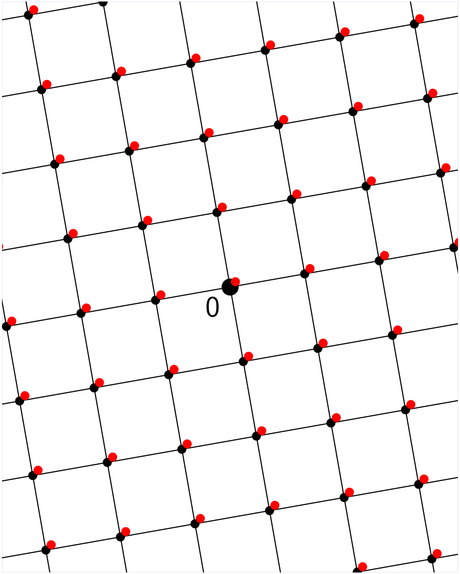

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$

# Dual lattice: Examples



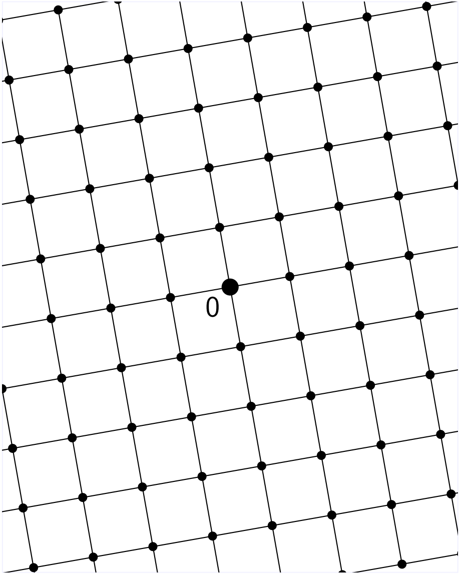

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee$

# Dual lattice: Examples



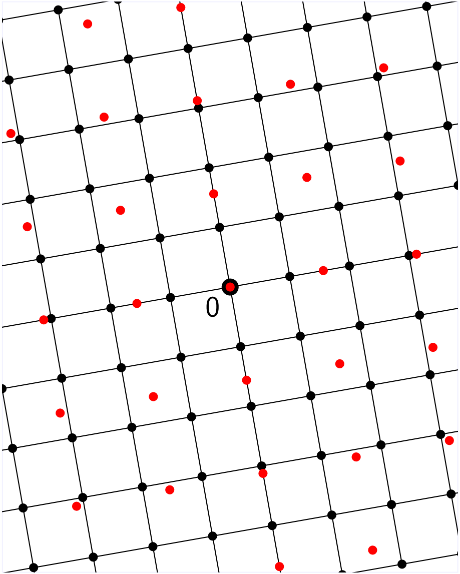

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$

# Dual lattice: Examples



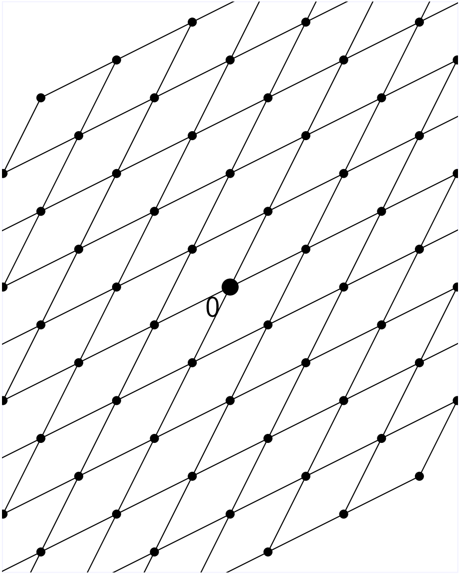

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee$

# Dual lattice: Examples



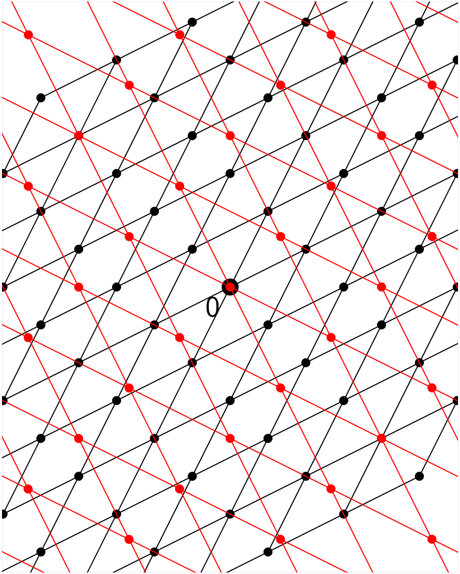

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee$
- Properties of dual:
  - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee$
  - $(\Lambda^\vee)^\vee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

# Dual lattice: Examples



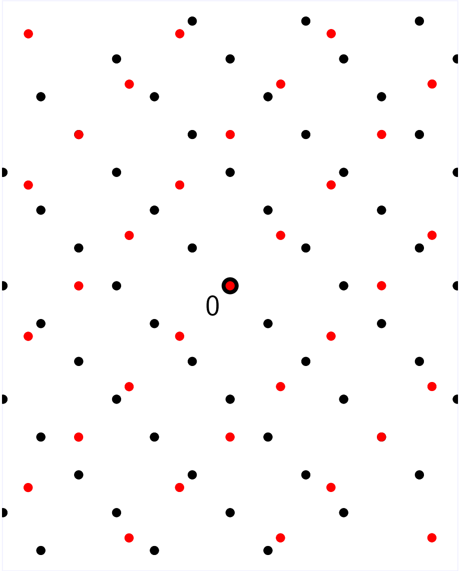

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee$
- Properties of dual:
  - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee$
  - $(\Lambda^\vee)^\vee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

# Dual lattice: Examples



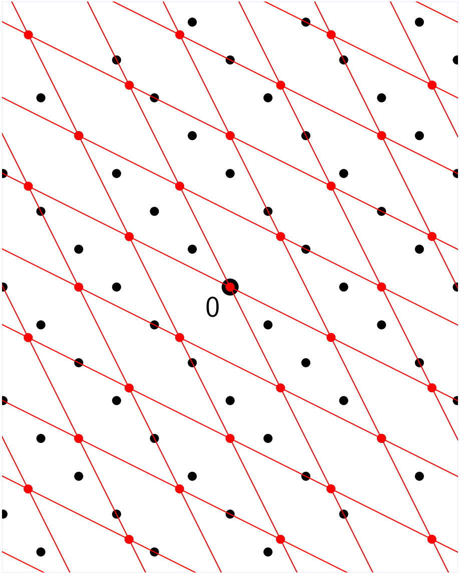

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee$
- Properties of dual:
  - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee$
  - $(\Lambda^\vee)^\vee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

# Dual lattice: Examples



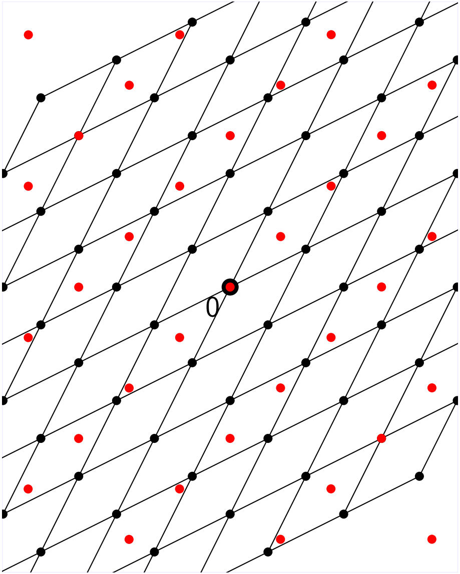

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee$
- Properties of dual:
  - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee$
  - $(\Lambda^\vee)^\vee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

# Dual lattice: Examples



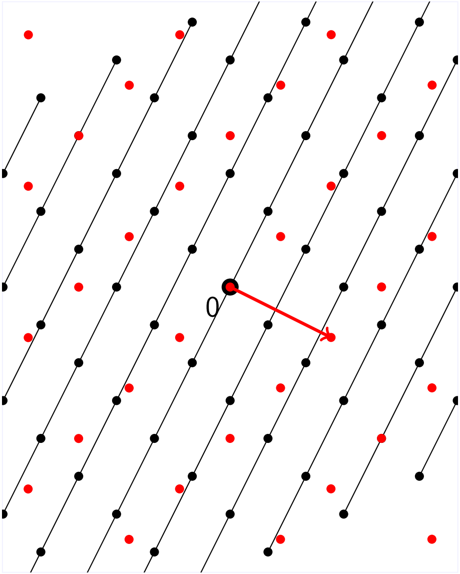

- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- Scaling $(q \cdot \Lambda)^\vee = \frac{1}{q} \cdot \Lambda^\vee$
- Properties of dual:
  - $\Lambda_1 \subseteq \Lambda_2 \iff \Lambda_1^\vee \supseteq \Lambda_2^\vee$
  - $(\Lambda^\vee)^\vee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

# Dual lattice: Examples




- Integer lattice $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
- Rotating $(\mathbf{R}\Lambda)^\vee = \mathbf{R}(\Lambda^\vee)$
- 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 $\mathbf{x} \in \Lambda$ and $\mathbf{y} \in \Lambda^\vee$:
  - $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$
  - but $\mathbf{x} + \mathbf{y}$ has no geometric meaning

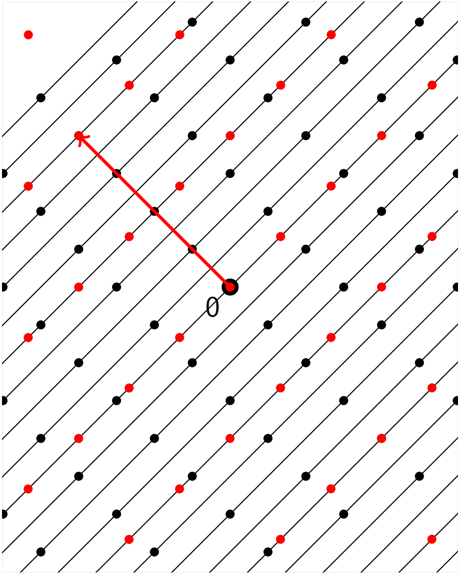
# Lattice Layers




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

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

# Lattice Layers

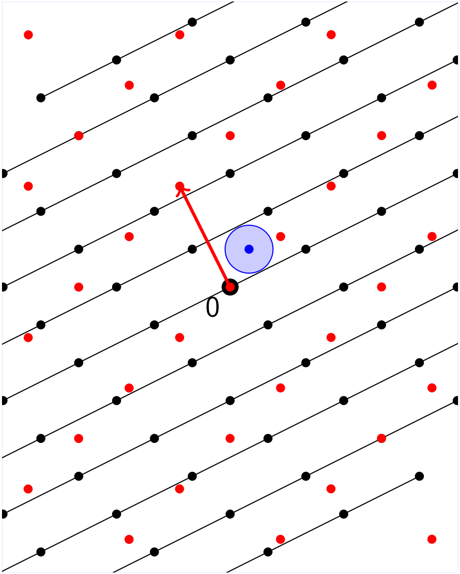



- Each dual vector $\mathbf{v} \in \mathcal{L}^\vee$, partitions the lattice $\mathcal{L}$ into layers orthogonal to $\mathbf{v}$

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

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

# Lattice Layers

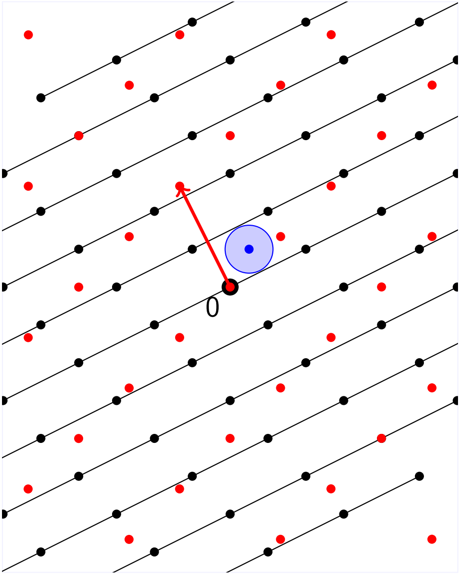



- Each dual vector $\mathbf{v} \in \mathcal{L}^\vee$, partitions the lattice $\mathcal{L}$ into layers orthogonal to $\mathbf{v}$

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

- Layers are at distance $1/\|\mathbf{v}\|$
- $\mu(\mathcal{L}) \geq \frac{1}{2\|\mathbf{v}\|}$

# 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* $\mathcal{L}$

$$1 \leq 2\lambda_1(\mathcal{L}) \cdot \mu(\mathcal{L}^\vee) \leq n.$$

**Theorem (Banaszczyk)**

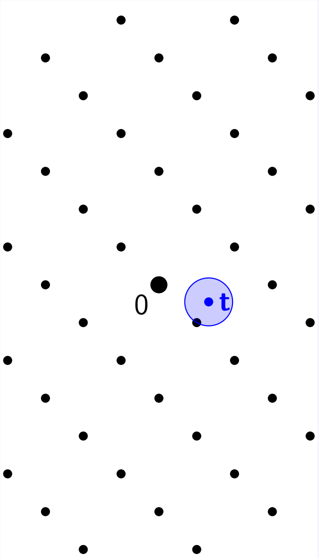
*For every* $i$,

$$1 \leq \lambda_i(\mathcal{L}) \cdot \lambda_{n-i+1}(\mathcal{L}^\vee) \leq n.$$

- 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

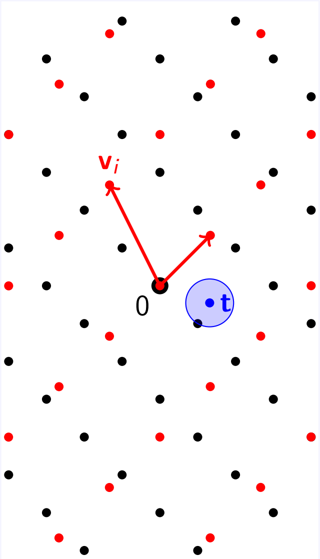
BDD input: $\mathbf{t}$ close to $\mathcal{L}$



# BDD reduces to SIVP

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

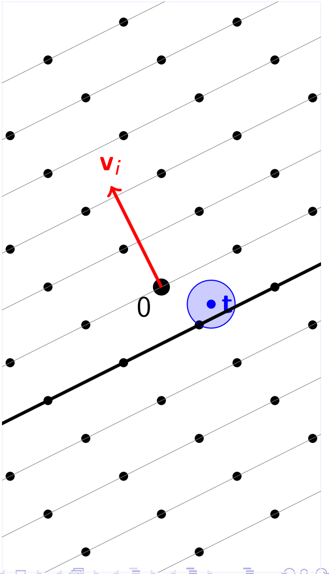
- Compute $\mathbf{V} = \text{SIVP}(\mathcal{L}^\vee)$



# BDD reduces to SIVP

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

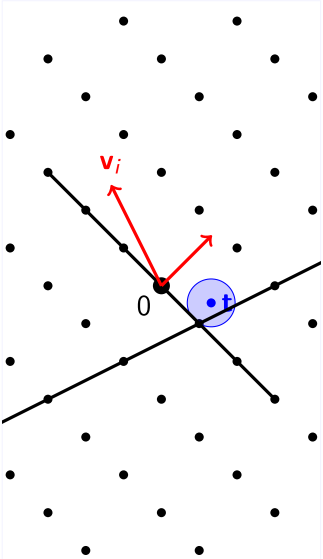
- Compute $\mathbf{V} = \mathrm{SIVP}(\mathcal{L}^\vee)$
- For each $\mathbf{v}_i \in \mathcal{L}^\vee$, find the layer $L_i = \{\mathbf{x} \mid \mathbf{x} \cdot \mathbf{v}_i = c_i\}$ closest to $\mathbf{t}$



# BDD reduces to SIVP

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

- Compute $\mathbf{V} = \mathrm{SIVP}(\mathcal{L}^\vee)$
- 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 $L_1 \cap L_2 \cap \cdots \cap L_n$

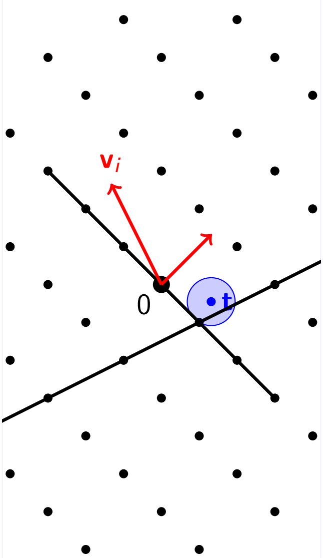


# BDD reduces to SIVP

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

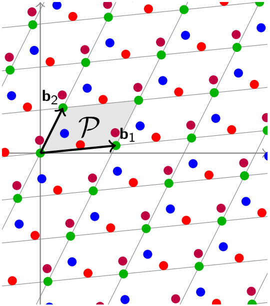
$$\mu(\mathbf{t}, \mathcal{L}) \leq \frac{\lambda_1}{2n} \leq \frac{1}{2\lambda_n^\vee} \leq \frac{1}{2\|\mathbf{v}_i\|}$$



# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

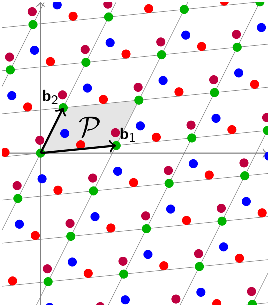


# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

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

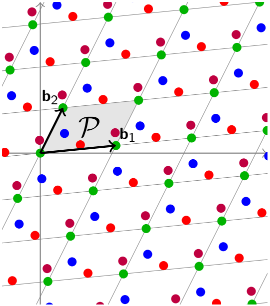


# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

- $(\mathcal{L}, +)$ is a subgroup of $(\mathbb{R}^n, +)$
- One can form the quotien group $\mathbb{R}^n/\mathcal{L}$

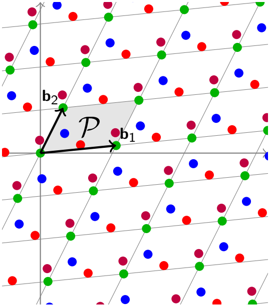


# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

- $(\mathcal{L}, +)$ is a subgroup of $(\mathbb{R}^n, +)$
- One can form the quotien group $\mathbb{R}^n/\mathcal{L}$
- Elements of $\mathbb{R}^n/\mathcal{L}$ are cosets $\mathbf{t} + \mathcal{L}$

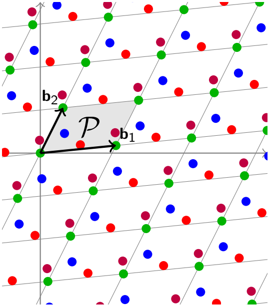


# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

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

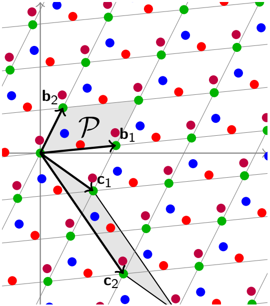


# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

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

- $(\mathcal{L}, +)$ is a subgroup of $(\mathbb{R}^n, +)$
- One can form the quotien group $\mathbb{R}^n/\mathcal{L}$
- Elements of $\mathbb{R}^n/\mathcal{L}$ are cosets $\mathbf{t} + \mathcal{L}$
- Any fundamental region $P$ gives a set of standard representatives
- $\mathcal{P} = \sum_i \mathbf{b}_i \cdot [0, 1) \equiv \mathbb{R}^n/\mathcal{L}$



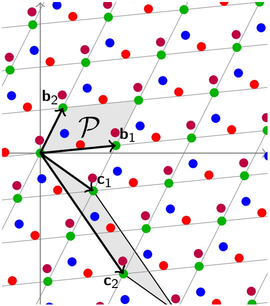
# Working modulo a lattice

**Definition (Fundamental Region of a lattice)**

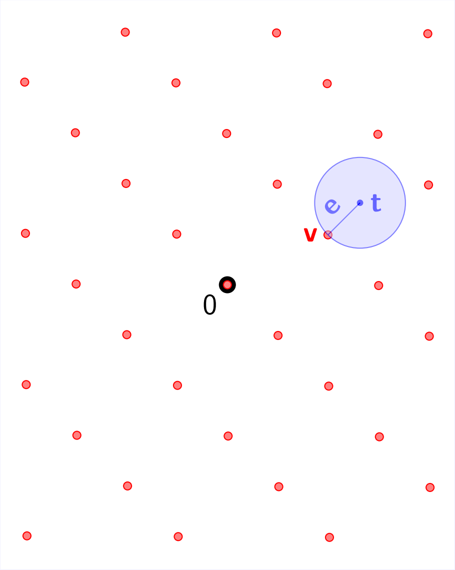
$P \subset \mathbb{R}^n$: $\{P + \mathbf{x} \mid \mathbf{x} \in \mathcal{L}\}$ is a partition of $\mathbb{R}^n$.

- $(\mathcal{L}, +)$ is a subgroup of $(\mathbb{R}^n, +)$
- One can form the quotien group $\mathbb{R}^n/\mathcal{L}$
- Elements of $\mathbb{R}^n/\mathcal{L}$ are cosets $\mathbf{t} + \mathcal{L}$
- Any fundamental region $P$ gives a set of standard representatives
- $\mathcal{P} = \sum_i \mathbf{b}_i \cdot [0,1) \equiv \mathbb{R}^n/\mathcal{L}$
- $\mathbf{t} + \mathcal{L}$ is uniquely identified by

$$(\mathbf{B}^\vee)\mathbf{t} \pmod 1$$



# CVP and lattice cosets

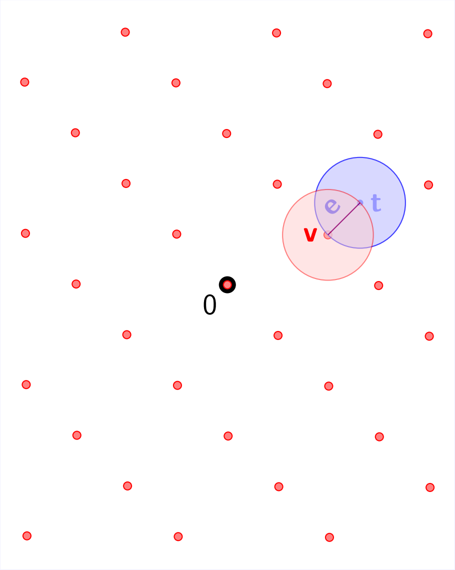



- Lattice $\Lambda$, target $\mathbf{t}$

**Definition**

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

# CVP and lattice cosets

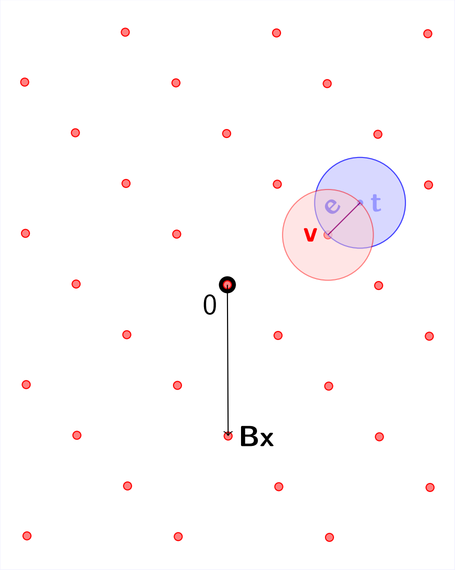



- Lattice $\Lambda$, target $\mathbf{t}$
- CVP: Find $\mathbf{v}$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible

**Definition**

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

# CVP and lattice cosets

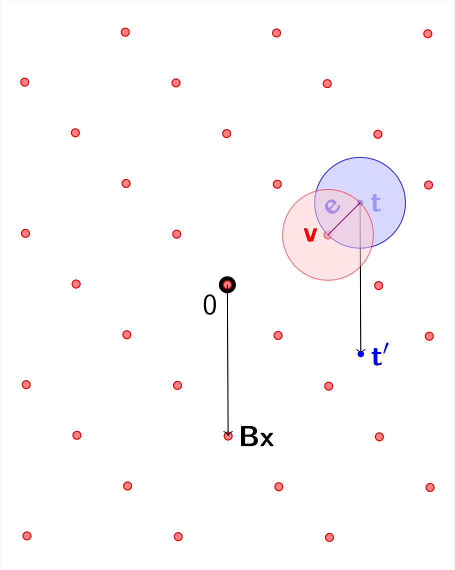



- Lattice $\Lambda$, target $\mathbf{t}$
- CVP: Find $\mathbf{v}$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible

## Definition

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

# CVP and lattice cosets

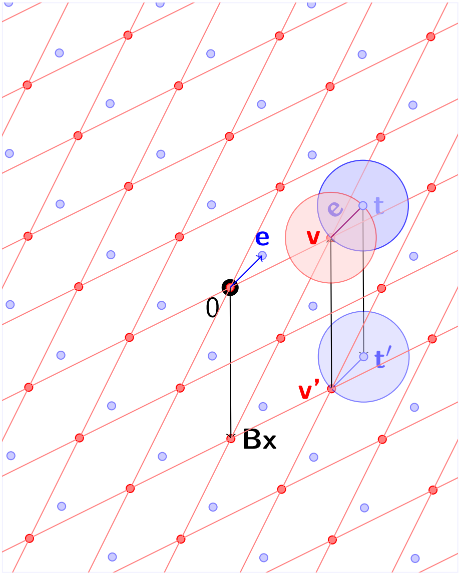



- Lattice $\Lambda$, target $\mathbf{t}$
- CVP: Find $\mathbf{v}$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible
- $\mathbf{t}' = \mathbf{t} + \mathbf{Bx}$

## Definition

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

# CVP and lattice cosets

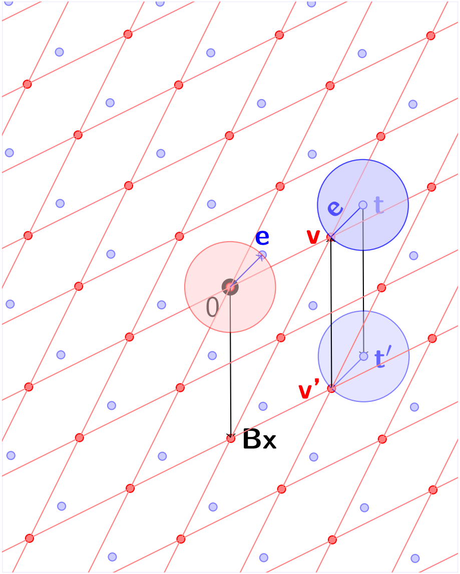



- Lattice $\Lambda$, target $\mathbf{t}$
- CVP: Find $\mathbf{v}$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible
- $\mathbf{t}' = \mathbf{t} + \mathbf{Bx}$
- $\mathbf{v} = \mathbf{v}' - \mathbf{Bx}$

### Definition

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

# CVP and lattice cosets

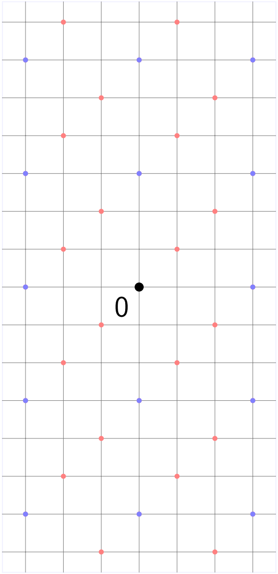



- Lattice $\Lambda$, target $\mathbf{t}$
- CVP: Find $\mathbf{v}$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v}$ is shortest possible
- $\mathbf{t}' = \mathbf{t} + \mathbf{Bx}$
- $\mathbf{v} = \mathbf{v}' - \mathbf{Bx}$

## Definition

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

# 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 $\mathbf{A} \in \mathbb{Z}_q^{n \times d}$)

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

# Examples of $q$-ary lattices

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

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

**Theorem**

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

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

For any fixed $\mathbf{A}$, the lattices $\Lambda_q(\mathbf{A})$ and $\Lambda_q^\perp(\mathbf{A})$ are different

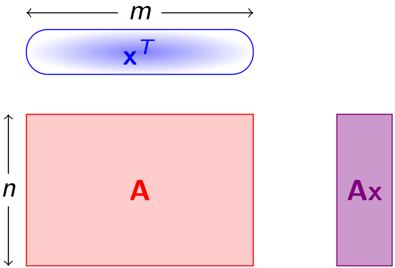
# Duality of $q$-ary lattices

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

$$\begin{aligned} \Lambda_q(\mathbf{A})^\vee &= \frac{1}{q}\Lambda_q^\perp(\mathbf{A}) \\ \Lambda_q^\perp(\mathbf{A})^\vee &= \frac{1}{q}\Lambda_q(\mathbf{A}) \end{aligned}$$

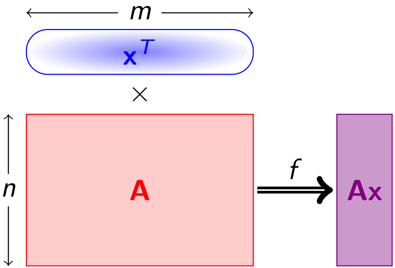
# Ajtai's one-way function (SIS)

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



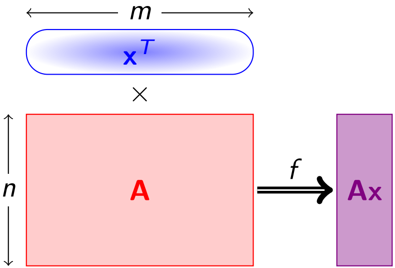
# Ajtai's one-way function (SIS)

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



# Ajtai's one-way function (SIS)

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




### Theorem (A'96)

*For $m > n \lg q$, if lattice problems (SIVP) are hard to approximate in the worst-case, then $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$ 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

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short

# Ajtai's function and $q$-ary lattices

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short
- The $q$-ary lattice $\Lambda_q^{\perp}(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$

# Ajtai's function and $q$-ary lattices

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short
- The $q$-ary lattice $\Lambda_q^\perp(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$
- Finding collisions $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{y})$ is equivalent to finding short vectors $\mathbf{x} - \mathbf{y} \in \Lambda_q^\perp(\mathbf{A})$

# Ajtai's function and $q$-ary lattices

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short
- The $q$-ary lattice $\Lambda_q^\perp(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$
- Finding collisions $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{y})$ is equivalent to finding short vectors $\mathbf{x} - \mathbf{y} \in \Lambda_q^\perp(\mathbf{A})$
- The output of $f_{\mathbf{A}}(\mathbf{x})$ is the syndrome of $\mathbf{x}$

# Ajtai's function and $q$-ary lattices

- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short
- The $q$-ary lattice $\Lambda_q^{\perp}(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$
- Finding collisions $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{y})$ is equivalent to finding short vectors $\mathbf{x} - \mathbf{y} \in \Lambda_q^{\perp}(\mathbf{A})$
- The output of $f_{\mathbf{A}}(\mathbf{x})$ is the syndrome of $\mathbf{x}$
- Inverting $f_{\mathbf{A}}(\mathbf{x})$ is the same as CVP in its syndrome decoding formulation with lattice $\Lambda_q^{\perp}(\mathbf{A})$ and target $\mathbf{t} \in \mathbf{x} + \Lambda_q^{\perp}(\mathbf{A})$

# Ajtai's function and $q$-ary lattices

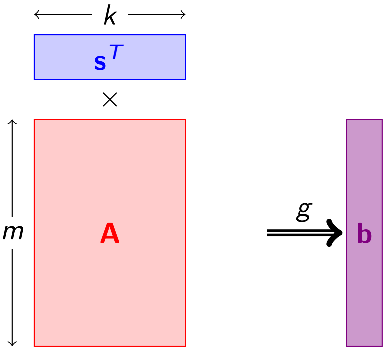
- $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \bmod q$, where $\mathbf{x}$ is short
- The $q$-ary lattice $\Lambda_q^{\perp}(\mathbf{A})$ is the kernel of $f_{\mathbf{A}}$
- Finding collisions $f_{\mathbf{A}}(\mathbf{x}) = f_{\mathbf{A}}(\mathbf{y})$ is equivalent to finding short vectors $\mathbf{x}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

**Remark**

*SIS $\equiv$ Approximate ADD (Absolute Distance Decoding)*

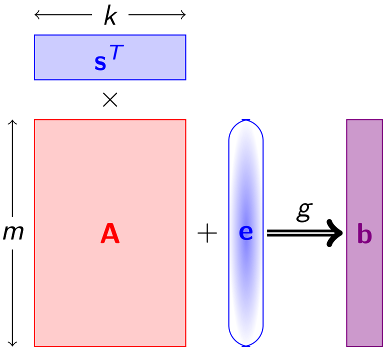
# Regev's Learning With Errors (LWE)

- $\mathbf{A} \in \mathbb{Z}_q^{m \times k}$, $\mathbf{s} \in \mathbb{Z}_q^k$, $\mathbf{e} \in \mathcal{E}^m$.
- $g_{\mathbf{A}}(\mathbf{s} \quad) = \mathbf{As} \qquad \bmod q$



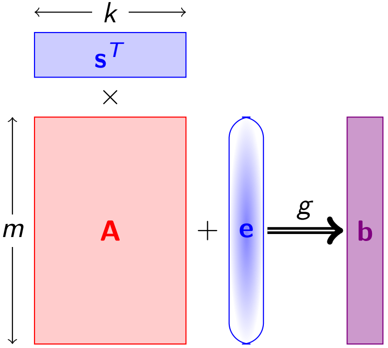
# Regev's Learning With Errors (LWE)

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



# Regev's Learning With Errors (LWE)

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




**Theorem (R'05)**

*The function $g_{\mathbf{A}}(\mathbf{s}, \mathbf{e})$ 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: $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{As}+\mathbf{e}$, where $\mathbf{e}$ is small and $\mathbf{s}$ is arbitrary
  - Output: $\mathbf{s}, \mathbf{e}$

# LWE and $q$-ary lattices

- Learning with errors:
  - Input: $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{As}+\mathbf{e}$, where $\mathbf{e}$ is small and $\mathbf{s}$ is arbitrary
  - Output: $\mathbf{s}, \mathbf{e}$
- If $\mathbf{e} = \mathbf{0}$, then $\mathbf{As}+\mathbf{e} = \mathbf{As} \in \Lambda(\mathbf{A}^t)$

# LWE and $q$-ary lattices

- Learning with errors:
  - Input: $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{As}+\mathbf{e}$, where $\mathbf{e}$ is small and $\mathbf{s}$ is arbitrary
  - Output: $\mathbf{s}, \mathbf{e}$
- If $\mathbf{e} = \mathbf{0}$, then $\mathbf{As}+\mathbf{e} = \mathbf{As} \in \Lambda(\mathbf{A}^t)$
- Same as CVP in random $q$-ary lattice $\Lambda(\mathbf{A}^t)$ with random target $\mathbf{t} = \mathbf{As}+\mathbf{e}$

# LWE and $q$-ary lattices

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

# LWE and $q$-ary lattices

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