Lattice-Based Cryptography: Mathematical and Computational Background

Chris Peikert
Georgia Institute of Technology

crypt@b-it 2013

Lattice-Based Cryptography

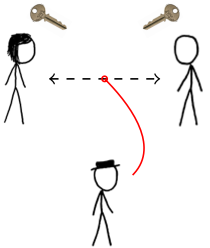
$y = g^x \bmod p$

$N = p \cdot q$

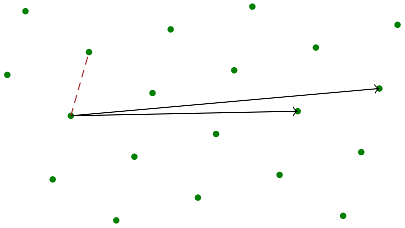
$m^e \bmod N$

$e(g^a, g^b)$

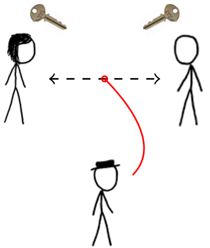
$\Longrightarrow$



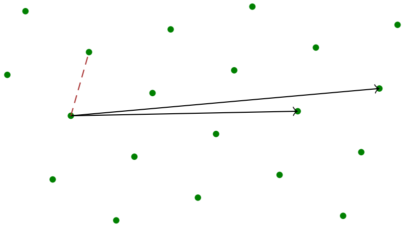
Lattice-Based Cryptography



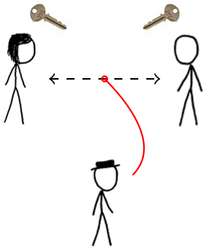
$\Longrightarrow$



Lattice-Based Cryptography



$\Longrightarrow$

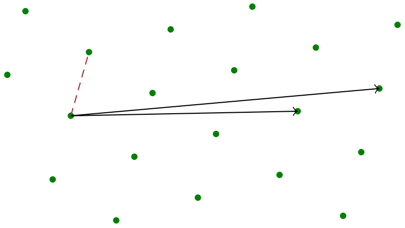


Why?

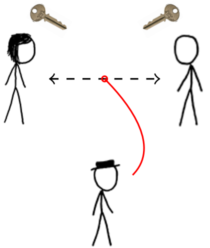
- Simple description and implementation

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

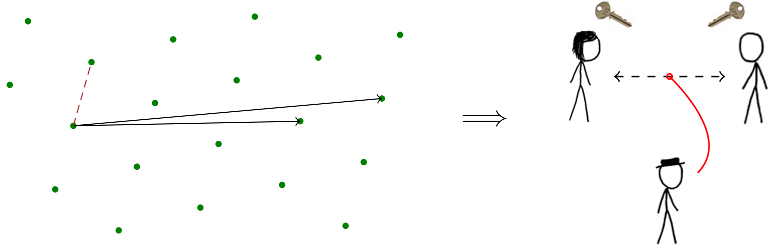


Why?

- Simple description and implementation
- Efficient: linear, highly parallel operations

(Images courtesy xkcd.org)

Lattice-Based Cryptography

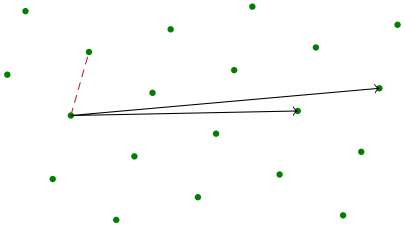


Why?

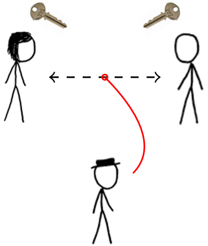
- Simple description and implementation
- Efficient: linear, highly parallel operations
- Resists quantum attacks (so far)

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$

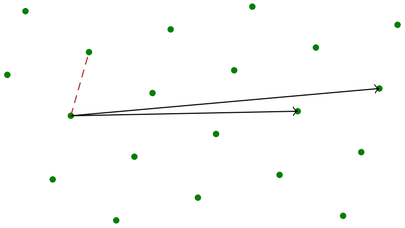


Why?

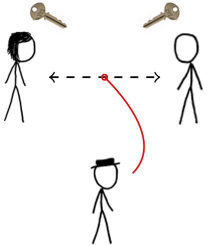
- Simple description and implementation
- Efficient: linear, highly parallel operations
- Resists quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96,...]

(Images courtesy xkcd.org)

Lattice-Based Cryptography



$\Longrightarrow$



Why?

- Simple description and implementation
- Efficient: linear, highly parallel operations
- Resists quantum attacks (so far)
- Security from worst-case assumptions [Ajtai96,...]
- Solutions to "holy grail" crypto problems [Gentry09,...]

(Images courtesy xkcd.org)

Part 1:

Mathematical Background

Coming up:

1. Definitions: lattice, basis, determinant, cosets, successive minima, ...
2. Two simple bounds on the minimum distance.

Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x} + \mathbf{y} \in \mathcal{L}$.

Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x} + \mathbf{y} \in \mathcal{L}$.

  Discrete: for all $\mathbf{x} \in \mathcal{L}$, exists $\varepsilon > 0$ s.t. $\mathcal{L} \cap \mathsf{Ball}(\mathbf{x}, \varepsilon) = \{\mathbf{x}\}$.

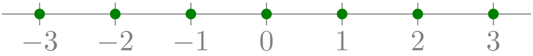
Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x} + \mathbf{y} \in \mathcal{L}$.

  Discrete: for all $\mathbf{x} \in \mathcal{L}$, exists $\varepsilon > 0$ s.t. $\mathcal{L} \cap \mathrm{Ball}(\mathbf{x}, \varepsilon) = \{\mathbf{x}\}$.

Lattices	Not lattices
$\{\mathbf{0}\}$, $\mathbb{Z} \subset \mathbb{R}$	$\mathbb{Q} \subset \mathbb{R}$
$2\mathbb{Z}$, $c\mathbb{Z}$ for any $c \in \mathbb{R}$	$2\mathbb{Z} + 1 = \{\text{odd } x \in \mathbb{Z}\}$
$\mathbb{Z}^n \subset \mathbb{R}^n$	$\mathbb{Z} + \sqrt{2}\mathbb{Z}$



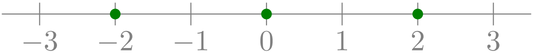
Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x} + \mathbf{y} \in \mathcal{L}$.

  Discrete: for all $\mathbf{x} \in \mathcal{L}$, exists $\varepsilon > 0$ s.t. $\mathcal{L} \cap \text{Ball}(\mathbf{x}, \varepsilon) = \{\mathbf{x}\}$.

Lattices	Not lattices
$\{\mathbf{0}\}$, $\mathbb{Z} \subset \mathbb{R}$	$\mathbb{Q} \subset \mathbb{R}$
$2\mathbb{Z}$, $c\mathbb{Z}$ for any $c \in \mathbb{R}$	$2\mathbb{Z} + 1 = \{\text{odd } x \in \mathbb{Z}\}$
$\mathbb{Z}^n \subset \mathbb{R}^n$	$\mathbb{Z} + \sqrt{2}\mathbb{Z}$



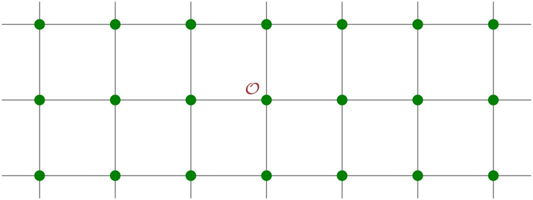
Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x}+\mathbf{y} \in \mathcal{L}$.

  Discrete: for all $\mathbf{x} \in \mathcal{L}$, exists $\varepsilon > 0$ s.t. $\mathcal{L} \cap \text{Ball}(\mathbf{x}, \varepsilon) = \{\mathbf{x}\}$.

Lattices	Not lattices
$\{\mathbf{0}\}$, $\mathbb{Z} \subset \mathbb{R}$	$\mathbb{Q} \subset \mathbb{R}$
$2\mathbb{Z}$, $c\mathbb{Z}$ for any $c \in \mathbb{R}$	$2\mathbb{Z}+1 = \{\text{odd } x \in \mathbb{Z}\}$
$\mathbb{Z}^n \subset \mathbb{R}^n$	$\mathbb{Z} + \sqrt{2}\mathbb{Z}$



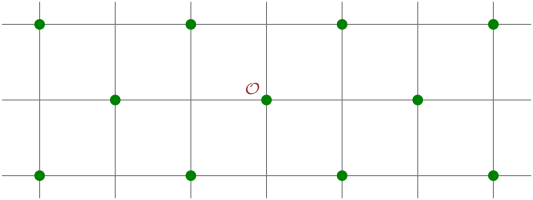
Lattices

- Lattice $\mathcal{L}$ of dimension n: a discrete additive subgroup of $\mathbb{R}^n$.

  Additive subgroup: $\mathbf{0} \in \mathcal{L}$, and $\mathbf{x}, \mathbf{y} \in \mathcal{L} \implies -\mathbf{x},\ \mathbf{x}+\mathbf{y} \in \mathcal{L}$.

  Discrete: for all $\mathbf{x} \in \mathcal{L}$, exists $\varepsilon > 0$ s.t. $\mathcal{L} \cap \mathsf{Ball}(\mathbf{x}, \varepsilon) = \{\mathbf{x}\}$.

Lattices	Not lattices
$\{\mathbf{0}\}$, $\mathbb{Z} \subset \mathbb{R}$	$\mathbb{Q} \subset \mathbb{R}$
$2\mathbb{Z}$, $c\mathbb{Z}$ for any $c \in \mathbb{R}$	$2\mathbb{Z}+1 = \{\text{odd } x \in \mathbb{Z}\}$
$\mathbb{Z}^n \subset \mathbb{R}^n$	$\mathbb{Z} + \sqrt{2}\mathbb{Z}$



This Week: Only Full-Rank Integer Lattices

- Integer lattice: $\mathcal{L} \subseteq \mathbb{Z}^n$. (Essentially equivalent to rational lattice, by scaling.)

This Week: Only Full-Rank Integer Lattices

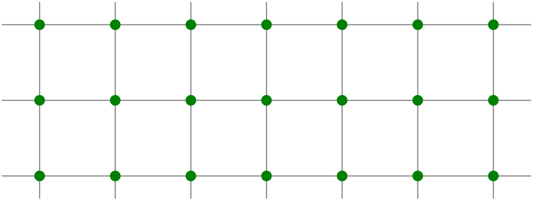
- Integer lattice: $\mathcal{L} \subseteq \mathbb{Z}^n$. (Essentially equivalent to rational lattice, by scaling.)
- Full-rank lattice: $\text{span}(\mathcal{L}) = \mathbb{R}^n$.

  Equivalently, $\mathcal{L}$ has a set of n linearly independent vectors.

This Week: Only Full-Rank Integer Lattices

- Integer lattice: $\mathcal{L} \subseteq \mathbb{Z}^n$. (Essentially equivalent to rational lattice, by scaling.)
- Full-rank lattice: $\operatorname{span}(\mathcal{L}) = \mathbb{R}^n$.
  Equivalently, $\mathcal{L}$ has a set of n linearly independent vectors.

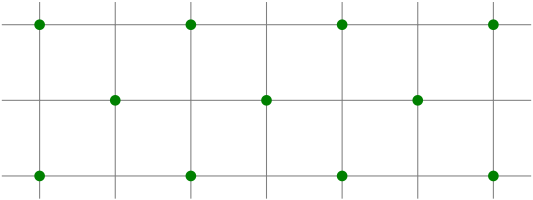
Full rank	Not full rank
$c\mathbb{Z}^n$, $c \neq 0$	$\{\mathbf{0}\}$
$(1,1) \cdot \mathbb{Z} + (-1,1) \cdot \mathbb{Z}$	$(1,1) \cdot \mathbb{Z}$



This Week: Only Full-Rank Integer Lattices

- Integer lattice: $\mathcal{L} \subseteq \mathbb{Z}^n$. (Essentially equivalent to rational lattice, by scaling.)
- Full-rank lattice: $\operatorname{span}(\mathcal{L}) = \mathbb{R}^n$.
  Equivalently, $\mathcal{L}$ has a set of n linearly independent vectors.

Full rank	Not full rank
$c\mathbb{Z}^n$, $c \neq 0$	$\{\mathbf{0}\}$
$(1,1) \cdot \mathbb{Z} + (-1,1) \cdot \mathbb{Z}$	$(1,1) \cdot \mathbb{Z}$

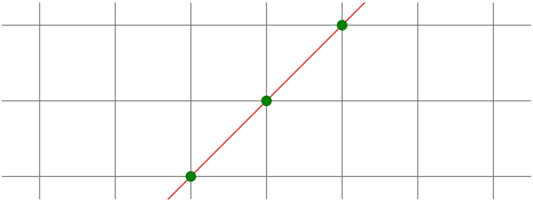


This Week: Only Full-Rank Integer Lattices

- Integer lattice: $\mathcal{L} \subseteq \mathbb{Z}^n$. (Essentially equivalent to rational lattice, by scaling.)
- Full-rank lattice: $\operatorname{span}(\mathcal{L}) = \mathbb{R}^n$.

  Equivalently, $\mathcal{L}$ has a set of n linearly independent vectors.

Full rank	Not full rank
$c\mathbb{Z}^n$, $c \neq 0$	$\{\mathbf{0}\}$
$(1,1) \cdot \mathbb{Z} + (-1,1) \cdot \mathbb{Z}$	$(1,1) \cdot \mathbb{Z}$

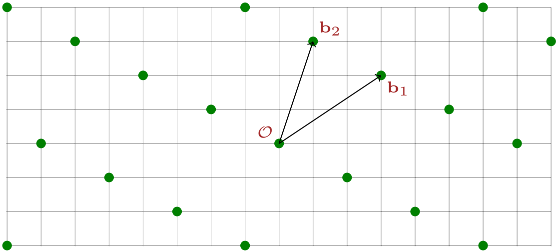


Representing Lattices: Bases

- Basis of $\mathcal{L}$: ordered set (i.e., matrix) $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s.t.

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) \stackrel{\Delta}{=} \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}.$$

  The $\mathbf{b}_i$ must be linearly ind., because $\mathrm{span}(\mathcal{L}) = \mathrm{span}(\mathbf{B}) = \mathbb{R}^n$.



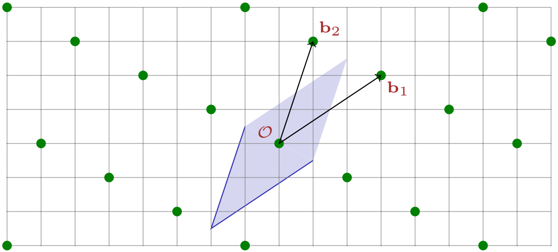
Representing Lattices: Bases

- Basis of $\mathcal{L}$: ordered set (i.e., matrix) $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s.t.

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) \stackrel{\Delta}{=} \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}.$$

  The $\mathbf{b}_i$ must be linearly ind., because $\operatorname{span}(\mathcal{L}) = \operatorname{span}(\mathbf{B}) = \mathbb{R}^n$.

- The fundamental parallelepiped of basis $\mathbf{B}$ is $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n$.



Representing Lattices: Bases

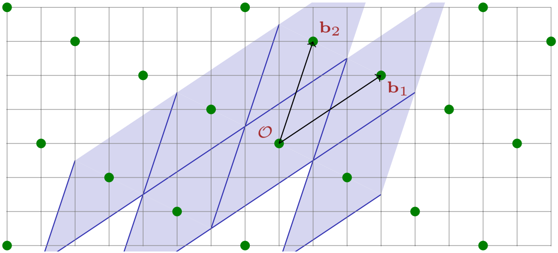
- Basis of $\mathcal{L}$: ordered set (i.e., matrix) $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s.t.

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) \stackrel{\Delta}{=} \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}.$$

  The $\mathbf{b}_i$ must be linearly ind., because $\operatorname{span}(\mathcal{L}) = \operatorname{span}(\mathbf{B}) = \mathbb{R}^n$.

- The fundamental parallelepiped of basis $\mathbf{B}$ is $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n$.

  It tiles space: $\mathbb{R}^n = \bigcup_{\mathbf{v} \in \mathcal{L}} (\mathbf{v} + \mathcal{P}(\mathbf{B}))$.



Representing Lattices: Bases

- Basis of $\mathcal{L}$: ordered set (i.e., matrix) $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ s.t.

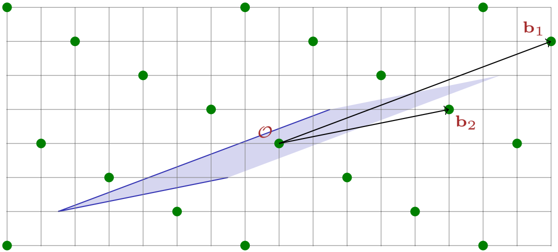
$$\mathcal{L} = \mathcal{L}(\mathbf{B}) \stackrel{\Delta}{=} \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}.$$

  The $\mathbf{b}_i$ must be linearly ind., because $\operatorname{span}(\mathcal{L}) = \operatorname{span}(\mathbf{B}) = \mathbb{R}^n$.

- The fundamental parallelepiped of basis $\mathbf{B}$ is $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot \left[-\frac{1}{2}, \frac{1}{2}\right)^n$.

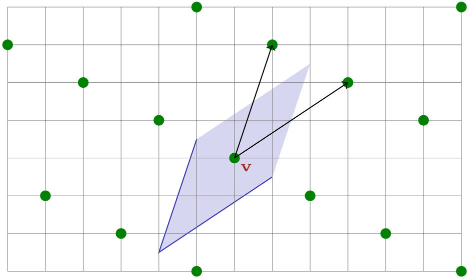
  It tiles space: $\mathbb{R}^n = \bigcup_{\mathbf{v} \in \mathcal{L}} (\mathbf{v} + \mathcal{P}(\mathbf{B}))$.

- A basis is not unique: $\mathbf{BU}$ is also a basis iff $\mathbf{U} \in \mathbb{Z}^{n \times n}, \det(\mathbf{U}) = \pm 1$.



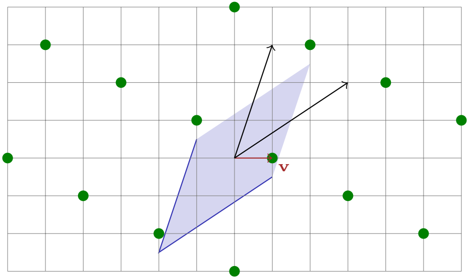
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.



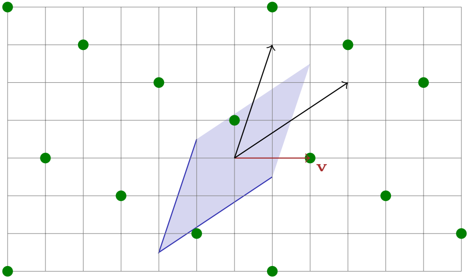
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v}+\mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1+\mathcal{L}=\mathbf{v}_2+\mathcal{L}$ iff $\mathbf{v}_1-\mathbf{v}_2\in\mathcal{L}$.



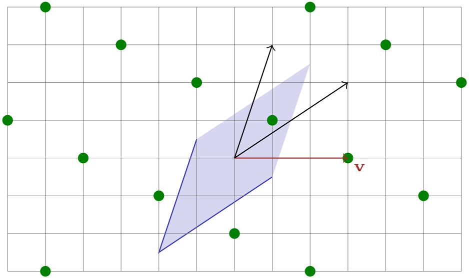
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v}+\mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1+\mathcal{L}=\mathbf{v}_2+\mathcal{L}$ iff $\mathbf{v}_1-\mathbf{v}_2\in\mathcal{L}$.



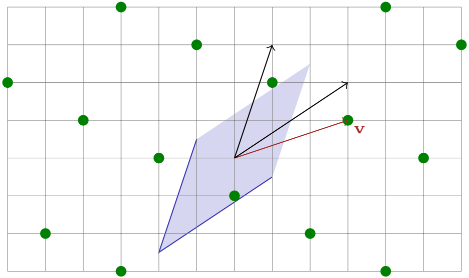
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v}+\mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1+\mathcal{L}=\mathbf{v}_2+\mathcal{L}$ iff $\mathbf{v}_1-\mathbf{v}_2\in\mathcal{L}$.



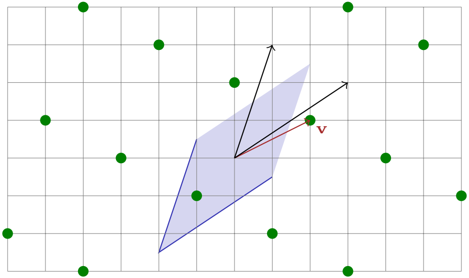
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.



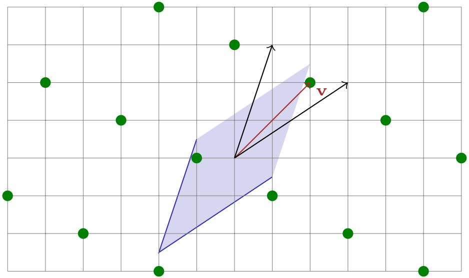
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.



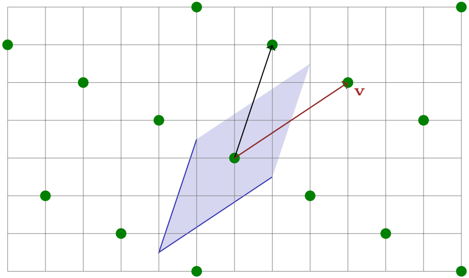
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.



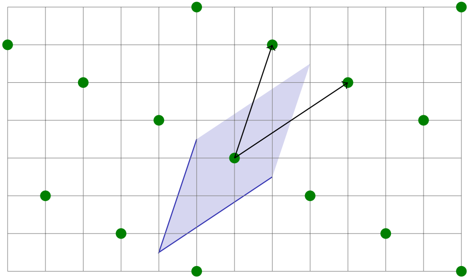
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.



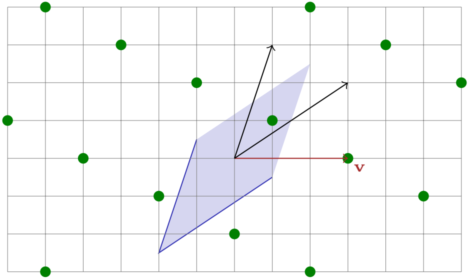
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.
- Determinant $\det(\mathcal{L}) \stackrel{\Delta}{=} |\mathbb{Z}^n/\mathcal{L}| = |\det(\mathbf{B})| = \mathrm{vol}(\mathcal{P}(\mathbf{B}))$, any basis $\mathbf{B}$.



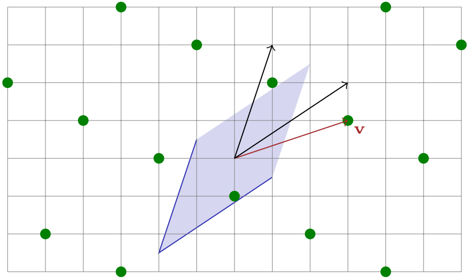
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.
- Determinant $\det(\mathcal{L}) \stackrel{\Delta}{=} |\mathbb{Z}^n/\mathcal{L}| = |\det(\mathbf{B})| = \mathrm{vol}(\mathcal{P}(\mathbf{B}))$, any basis $\mathbf{B}$.
- For any basis $\mathbf{B}$ and $\mathbf{v} \in \mathbb{R}^n$, $(\mathbf{v} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B}) = \{\bar{\mathbf{v}}\}$.
  Write $\bar{\mathbf{v}} = \mathbf{v} \bmod \mathbf{B}$, the "distinguished representative" of $\mathbf{v} + \mathcal{L}$.



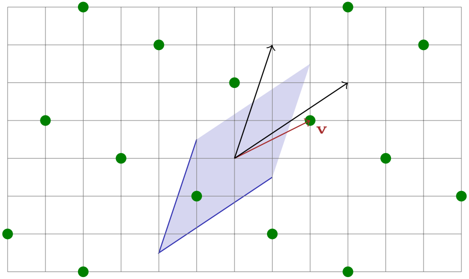
Cosets and Determinant

- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v} + \mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1 + \mathcal{L} = \mathbf{v}_2 + \mathcal{L}$ iff $\mathbf{v}_1 - \mathbf{v}_2 \in \mathcal{L}$.
- Determinant $\det(\mathcal{L}) \stackrel{\Delta}{=} |\mathbb{Z}^n/\mathcal{L}| = |\det(\mathbf{B})| = \mathrm{vol}(\mathcal{P}(\mathbf{B}))$, any basis $\mathbf{B}$.
- For any basis $\mathbf{B}$ and $\mathbf{v} \in \mathbb{R}^n$, $(\mathbf{v} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B}) = \{\bar{\mathbf{v}}\}$.
  Write $\bar{\mathbf{v}} = \mathbf{v} \bmod \mathbf{B}$, the "distinguished representative" of $\mathbf{v} + \mathcal{L}$.



Cosets and Determinant

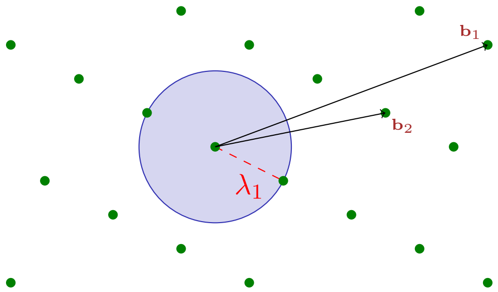
- Quotient group $\mathbb{Z}^n/\mathcal{L}$ consists of cosets $\mathbf{v}+\mathcal{L}$: "shifts" of the lattice.
  Recall: $\mathbf{v}_1+\mathcal{L}=\mathbf{v}_2+\mathcal{L}$ iff $\mathbf{v}_1-\mathbf{v}_2 \in \mathcal{L}$.
- Determinant $\det(\mathcal{L}) \stackrel{\Delta}{=} |\mathbb{Z}^n/\mathcal{L}| = |\det(\mathbf{B})| = \mathrm{vol}(\mathcal{P}(\mathbf{B}))$, any basis $\mathbf{B}$.
- For any basis $\mathbf{B}$ and $\mathbf{v} \in \mathbb{R}^n$, $(\mathbf{v}+\mathcal{L}) \cap \mathcal{P}(\mathbf{B}) = \{\bar{\mathbf{v}}\}$.
  Write $\bar{\mathbf{v}} = \mathbf{v} \bmod \mathbf{B}$, the "distinguished representative" of $\mathbf{v}+\mathcal{L}$.



Successive Minima

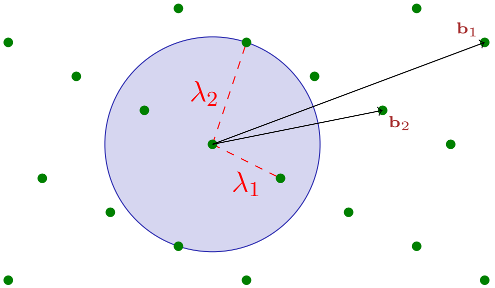
- The minimum distance of $\mathcal{L}$ is

$$\lambda_1(\mathcal{L}) \stackrel{\Delta}{=} \min_{\mathbf{0} \neq \mathbf{v} \in \mathcal{L}} \|\mathbf{v}\| = \min_{\text{distinct } \mathbf{x}, \mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|.$$



Successive Minima

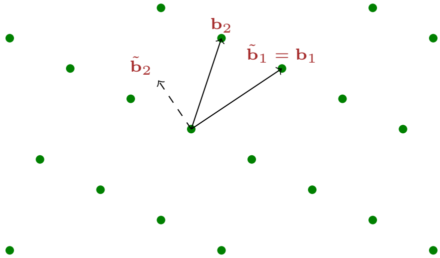
- The minimum distance of $\mathcal{L}$ is
$$\lambda_1(\mathcal{L}) \triangleq \min_{\mathbf{0} \neq \mathbf{v} \in \mathcal{L}} \|\mathbf{v}\| = \min_{\text{distinct } \mathbf{x}, \mathbf{y} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|.$$
- More generally, the ith successive minimum $(i = 1, \ldots, n)$ is
$$\begin{aligned} \lambda_i(\mathcal{L}) &\triangleq \min\{r : \mathcal{L} \text{ contains } i \text{ linearly ind. vectors of length} \leq r\} \\ &= \min\{r : \dim(\operatorname{span}(\mathcal{L} \cap \mathcal{B}(r))) \geq i\}. \end{aligned}$$



Gram-Schmidt Orthogonalization and Lower Bounding λ_1

- The GSO (or QR decomposition) of basis $\mathbf{B}$ is:

$$\mathbf{B} = \mathbf{QR} = \mathbf{Q} \cdot \begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \star & \star & \\ & \|\tilde{\mathbf{b}}_2\| & \star & \vdots \\ & & \ddots & \\ & & & \|\tilde{\mathbf{b}}_n\| \end{pmatrix}, \quad \mathbf{Q} \text{ orthonormal}$$

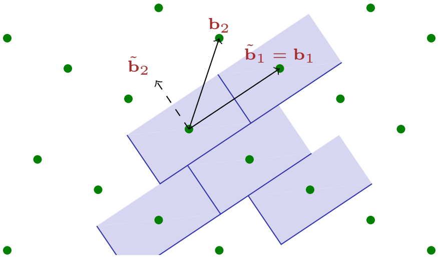


Gram-Schmidt Orthogonalization and Lower Bounding λ_1

- The GSO (or QR decomposition) of basis $\mathbf{B}$ is:

$$\mathbf{B} = \mathbf{QR} = \mathbf{Q} \cdot \begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \star & \star & \\ & \|\tilde{\mathbf{b}}_2\| & \star & \vdots \\ & & \ddots & \\ & & & \|\tilde{\mathbf{b}}_n\| \end{pmatrix}, \quad \mathbf{Q} \text{ orthonormal}$$

- Facts: $\mathcal{P}(\tilde{\mathbf{B}}) = \tilde{\mathbf{B}} \cdot [-\frac{1}{2}, \frac{1}{2})^n$ is a fund. region; $\det(\mathcal{L}) = \prod_{i=1}^{n} \|\tilde{\mathbf{b}}_i\|$.

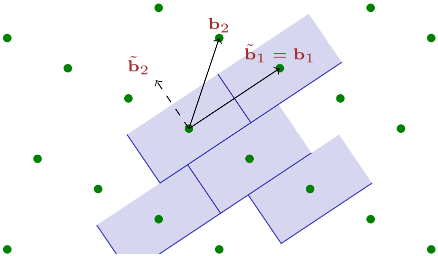


Gram-Schmidt Orthogonalization and Lower Bounding λ_1

- The GSO (or QR decomposition) of basis $\mathbf{B}$ is:

$$\mathbf{B} = \mathbf{QR} = \mathbf{Q} \cdot \begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \star & \star & \\ & \|\tilde{\mathbf{b}}_2\| & \star & \vdots \\ & & \ddots & \\ & & & \|\tilde{\mathbf{b}}_n\| \end{pmatrix}, \quad \mathbf{Q} \text{ orthonormal}$$

- Facts: $\mathcal{P}(\tilde{\mathbf{B}}) = \tilde{\mathbf{B}} \cdot [-\frac{1}{2}, \frac{1}{2})^n$ is a fund. region; $\det(\mathcal{L}) = \prod_{i=1}^{n} \|\tilde{\mathbf{b}}_i\|$.
- Fact: $\lambda_1(\mathcal{L}) \geq \min_i \|\tilde{\mathbf{b}}_i\|$.

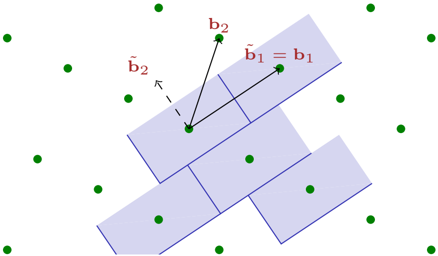


Gram-Schmidt Orthogonalization and Lower Bounding λ_1

- The GSO (or QR decomposition) of basis $\mathbf{B}$ is:

$$\mathbf{B} = \mathbf{QR} = \mathbf{Q} \cdot \begin{pmatrix} \|\tilde{\mathbf{b}}_1\| & \star & \star & \\ & \|\tilde{\mathbf{b}}_2\| & \star & \vdots \\ & & \ddots & \\ & & & \|\tilde{\mathbf{b}}_n\| \end{pmatrix}, \quad \mathbf{Q} \text{ orthonormal}$$

- Facts: $\mathcal{P}(\tilde{\mathbf{B}}) = \tilde{\mathbf{B}} \cdot [-\frac{1}{2}, \frac{1}{2})^n$ is a fund. region; $\det(\mathcal{L}) = \prod_{i=1}^{n} \|\tilde{\mathbf{b}}_i\|$.
- Fact: $\lambda_1(\mathcal{L}) \geq \min_i \|\tilde{\mathbf{b}}_i\|$. Proof: consider $\mathbf{Bc} = \mathbf{Q}(\mathbf{Rc})$ for $\mathbf{c} \in \mathbb{Z}^n$.



Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Proof of Theorem

1. Let $S' = S/2$, so $\mathrm{vol}(S') > \det(\mathcal{L})$.

Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Proof of Theorem

1. Let $S' = S/2$, so $\mathrm{vol}(S') > \det(\mathcal{L})$.
2. By pigeonhole argument, $\exists$ distinct $\mathbf{x}, \mathbf{y} \in S'$ s.t. $\mathbf{x} - \mathbf{y} \in \mathcal{L}$.

Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Proof of Theorem

1. Let $S' = S/2$, so $\mathrm{vol}(S') > \det(\mathcal{L})$.
2. By pigeonhole argument, $\exists$ distinct $\mathbf{x}, \mathbf{y} \in S'$ s.t. $\mathbf{x} - \mathbf{y} \in \mathcal{L}$.
3. Now $2\mathbf{x}, -2\mathbf{y} \in S$ by central symmetry, so $\mathbf{x} - \mathbf{y} \in S$ by convexity.

Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Proof of Theorem

1. Let $S' = S/2$, so $\mathrm{vol}(S') > \det(\mathcal{L})$.
2. By pigeonhole argument, $\exists$ distinct $\mathbf{x}, \mathbf{y} \in S'$ s.t. $\mathbf{x} - \mathbf{y} \in \mathcal{L}$.
3. Now $2\mathbf{x}, -2\mathbf{y} \in S$ by central symmetry, so $\mathbf{x} - \mathbf{y} \in S$ by convexity.

Proof of Corollary

1. Ball of radius $> \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$ is convex and centrally symmetric.

Upper Bounding λ_1: Minkowski's Theorem

Theorem

- Any convex, centrally symmetric body S of volume $> 2^n \cdot \det(\mathcal{L})$ contains a nonzero lattice point.
- Corollary: $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

Proof of Theorem

1. Let $S' = S/2$, so $\mathrm{vol}(S') > \det(\mathcal{L})$.
2. By pigeonhole argument, $\exists$ distinct $\mathbf{x}, \mathbf{y} \in S'$ s.t. $\mathbf{x} - \mathbf{y} \in \mathcal{L}$.
3. Now $2\mathbf{x}, -2\mathbf{y} \in S$ by central symmetry, so $\mathbf{x} - \mathbf{y} \in S$ by convexity.

Proof of Corollary

1. Ball of radius $> \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$ is convex and centrally symmetric.
2. It contains a cube of side length $> 2 \det(\mathcal{L})^{1/n}$, which has volume $> 2^n \cdot \det(\mathcal{L})$.

Part 2:

Computational Background

- Lattices are a source of many seemingly hard problems:
  SVP, CVP, uSVP, SIVP, BDD, CRP, DGS, . . . & decision variants.

Part 2:

Computational Background

- Lattices are a source of many seemingly hard problems:
  SVP, CVP, uSVP, SIVP, BDD, CRP, DGS, . . . & decision variants.
- We'll focus on the two most relevant to cryptography: the (approximate) Shortest Vector Problem (SVP_γ and GapSVP_γ) and Bounded-Distance Decoding (BDD) problem.

Part 2:

Computational Background

- Lattices are a source of many seemingly hard problems: SVP, CVP, uSVP, SIVP, BDD, CRP, DGS, ... & decision variants.
- We'll focus on the two most relevant to cryptography: the (approximate) Shortest Vector Problem (SVP_γ and GapSVP_γ) and Bounded-Distance Decoding (BDD) problem.
  1. They admit worst-case/average-case reductions (to SIS and LWE).

Part 2:

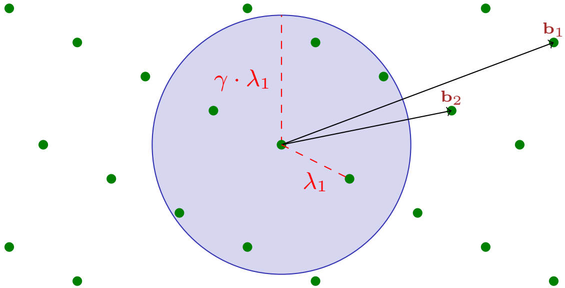
Computational Background

- Lattices are a source of many seemingly hard problems:
SVP, CVP, uSVP, SIVP, BDD, CRP, DGS, . . . & decision variants.
- We'll focus on the two most relevant to cryptography: the (approximate) Shortest Vector Problem (SVP_γ and GapSVP_γ) and Bounded-Distance Decoding (BDD) problem.
  1. They admit worst-case/average-case reductions (to SIS and LWE).
  2. Essentially all crypto schemes are based on versions of these problems.

Shortest Vector Problem: SVP_γ and GapSVP_γ

Approximation problems with factor $\gamma = \gamma(n)$:

Search: given basis $\mathbf{B}$, find nonzero $\mathbf{v} \in \mathcal{L}$ s.t. $\|\mathbf{v}\| \le \gamma \cdot \lambda_1(\mathcal{L})$.



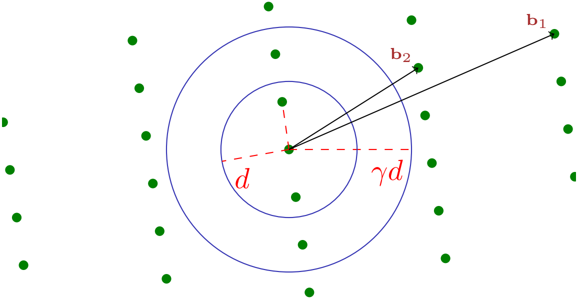
Shortest Vector Problem: SVP_γ and GapSVP_γ

Approximation problems with factor $\gamma = \gamma(n)$:

Search: given basis $\mathbf{B}$, find nonzero $\mathbf{v} \in \mathcal{L}$ s.t. $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$.

Decision: given basis $\mathbf{B}$ and real d, decide between

$$\lambda_1(\mathcal{L}) \leq d \quad \underline{\text{versus}} \quad \lambda_1(\mathcal{L}) > \gamma \cdot d.$$



Shortest Vector Problem: SVP_γ and GapSVP_γ

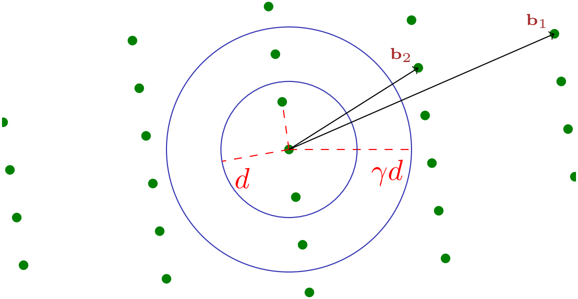
Approximation problems with factor $\gamma = \gamma(n)$:

Search: given basis $\mathbf{B}$, find nonzero $\mathbf{v} \in \mathcal{L}$ s.t. $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$.

Decision: given basis $\mathbf{B}$ and real d, decide between

$$\lambda_1(\mathcal{L}) \leq d \quad \underline{\text{versus}} \quad \lambda_1(\mathcal{L}) > \gamma \cdot d.$$

Clearly $\mathsf{GapSVP}_\gamma \leq \mathsf{SVP}_\gamma$, but the reverse direction is open!



Shortest Vector Problem: SVP_γ and GapSVP_γ

Approximation problems with factor $\gamma = \gamma(n)$:

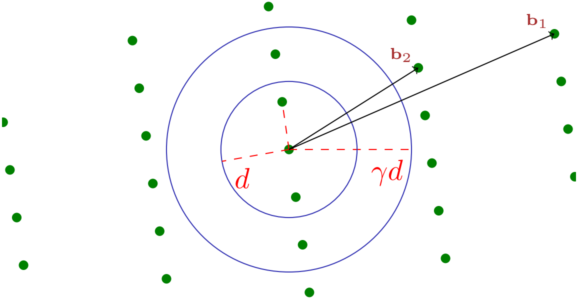
Search: given basis $\mathbf{B}$, <u>find</u> nonzero $\mathbf{v} \in \mathcal{L}$ s.t. $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$.

Decision: given basis $\mathbf{B}$ and real d, decide between

$$\lambda_1(\mathcal{L}) \leq d \quad \underline{\text{versus}} \quad \lambda_1(\mathcal{L}) > \gamma \cdot d.$$

Clearly $\mathsf{GapSVP}_\gamma \leq \mathsf{SVP}_\gamma$, but the reverse direction is open!

Recall: $\min_i \|\tilde{\mathbf{b}}_i\| \leq \lambda_1 \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$, but these are often very loose.



Complexity of GapSVP

- Clearly, (Gap)SVP$_\gamma$ can only get easier as γ increases.

Complexity of GapSVP

- Clearly, (Gap)SVP$_\gamma$ can only get easier as γ increases.

$\gamma =$	$2^{(\log n)^{1-\epsilon}}$	$\sqrt{n}$	n	$2^{\sim n}$
	NP-hard*	$\in$ NP $\cap$ coNP	crypto	SVP $\in$ P
	[Ajtai'98,...]	[GG'98,AR'05]	[Ajtai'96,...]	[LLL'82,Schnorr'87]

Complexity of GapSVP

- Clearly, (Gap)SVP$_\gamma$ can only get easier as γ increases.

$\gamma =$	$2^{(\log n)^{1-\epsilon}}$	$\sqrt{n}$	n	$2^{\sim n}$
	NP-hard*	$\in$ NP $\cap$ coNP	crypto	SVP $\in$ P
	[Ajtai'98,...]	[GG'98,AR'05]	[Ajtai'96,...]	[LLL'82,Schnorr'87]

- For $\gamma = \text{poly}(n)$, best algorithm is 2^n time & space [AKS'01,MV'10,...]

Complexity of GapSVP

- Clearly, (Gap)SVP$_\gamma$ can only get easier as γ increases.

$\gamma =$	$2^{(\log n)^{1-\epsilon}}$	$\sqrt{n}$	n	$2^{\sim n}$
	NP-hard*	$\in$ NP $\cap$ coNP	crypto	SVP $\in$ P
	[Ajtai'98,...]	[GG'98,AR'05]	[Ajtai'96,...]	[LLL'82,Schnorr'87]

- For $\gamma = \text{poly}(n)$, best algorithm is 2^n time & space [AKS'01,MV'10,...]
- For $\gamma = 2^k$, best algorithm takes $\approx 2^{n/k}$ time [Schnorr'87,...]

  E.g., $\gamma = 2^{\sqrt{n}}$ appears to be $\approx 2^{\sqrt{n}}$-hard.

An Algorithm for SVP$_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

An Algorithm for $\mathrm{SVP}_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

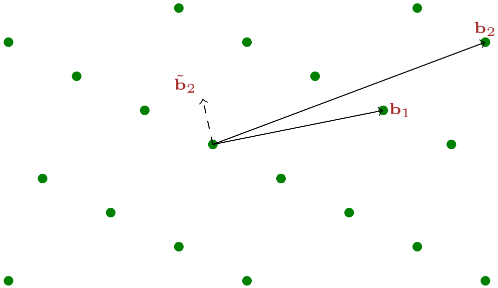
An Algorithm for SVP$_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.



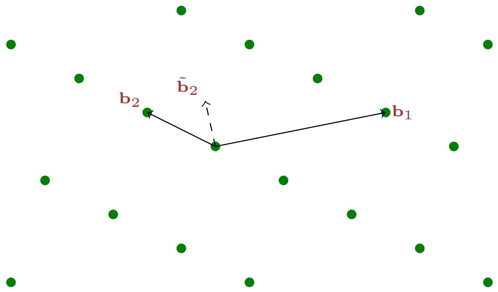
An Algorithm for SVP$_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.



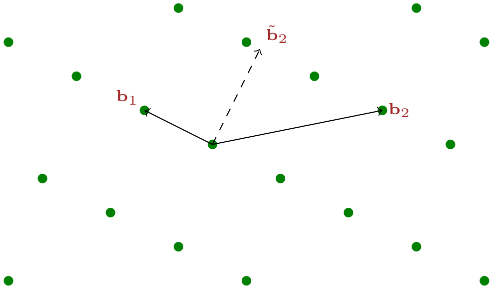
An Algorithm for SVP$_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.

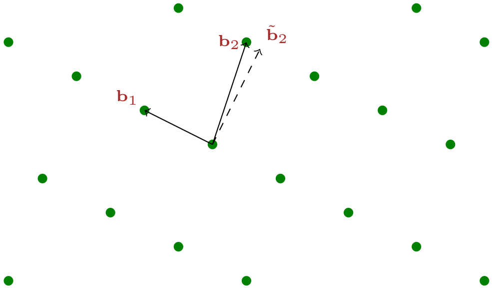


An Algorithm for $\mathrm{SVP}_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.
  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.



An Algorithm for $\mathrm{SVP}_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.

Claim 1: At end, $\|\tilde{\mathbf{b}}_2\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_1\|^2$ (as desired).

Proof: At end, $\frac{3}{4}\|\mathbf{b}_1\|^2 \leq \|\mathbf{b}_2\|^2 \leq \|\tilde{\mathbf{b}}_2\|^2 + \frac{1}{4}\|\mathbf{b}_1\|^2$.

An Algorithm for SVP$_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.

Claim 1: At end, $\|\tilde{\mathbf{b}}_2\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_1\|^2$ (as desired).

Proof: At end, $\frac{3}{4}\|\mathbf{b}_1\|^2 \leq \|\mathbf{b}_2\|^2 \leq \|\tilde{\mathbf{b}}_2\|^2 + \frac{1}{4}\|\mathbf{b}_1\|^2$.

Claim 2: Algorithm terminates after poly($|\mathbf{B}|$) many iterations.

Proof: Define $\Phi(\mathbf{B}) = \|\tilde{\mathbf{b}}_1\|^2 \cdot \|\tilde{\mathbf{b}}_2\| = \|\mathbf{b}_1\| \cdot \det(\mathcal{L})$.

When we swap, Φ decreases by $> \frac{\sqrt{3}}{2}$ factor.

It starts as $2^{\text{poly}(|\mathbf{B}|)}$ and cannot go below 1.

An Algorithm for $\mathrm{SVP}_{2^{(n-1)/2}}$ [LLL'82]

- Key idea: manipulate basis to ensure $\|\tilde{\mathbf{b}}_{i+1}\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_i\|^2$, for all i.

  This implies $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} \cdot \min_i \|\tilde{\mathbf{b}}_i\| \leq 2^{(n-1)/2} \cdot \lambda_1(\mathcal{L})$.

In two dimensions: given basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$,

1. Let $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - c \cdot \mathbf{b}_1$ for the $c \in \mathbb{Z}$ s.t. $\mathbf{b}_2 \in \tilde{\mathbf{b}}_2 + [-\frac{1}{2}, \frac{1}{2}) \cdot \mathbf{b}_1$.
2. If $\|\mathbf{b}_2\|^2 < \frac{3}{4}\|\mathbf{b}_1\|^2$, swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$ and loop. Else end.

Claim 1: At end, $\|\tilde{\mathbf{b}}_2\|^2 \geq \frac{1}{2}\|\tilde{\mathbf{b}}_1\|^2$ (as desired).

Proof: At end, $\frac{3}{4}\|\mathbf{b}_1\|^2 \leq \|\mathbf{b}_2\|^2 \leq \|\tilde{\mathbf{b}}_2\|^2 + \frac{1}{4}\|\mathbf{b}_1\|^2$.

Claim 2: Algorithm terminates after poly($|\mathbf{B}|$) many iterations.

Proof: Define $\Phi(\mathbf{B}) = \|\tilde{\mathbf{b}}_1\|^2 \cdot \|\tilde{\mathbf{b}}_2\| = \|\mathbf{b}_1\| \cdot \det(\mathcal{L})$.

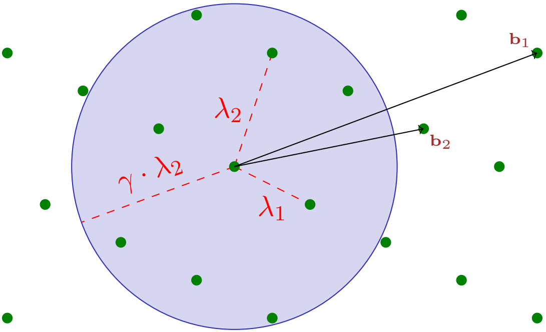
When we swap, Φ decreases by $> \frac{\sqrt{3}}{2}$ factor.

It starts as $2^{\mathrm{poly}(|\mathbf{B}|)}$ and cannot go below 1.

LLL in n dimensions: do similar loop on all adjacent pairs $\mathbf{b}_i, \mathbf{b}_{i+1}$.

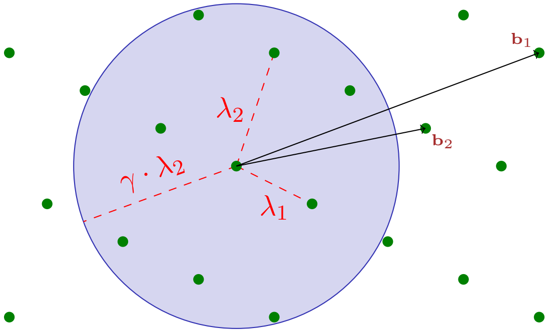
Related: Shortest Independent Vectors Problem (SIVP_γ)

- Given basis $\mathbf{B}$, <u>find</u> lin. ind. $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ s.t. $\|\mathbf{v}_i\| \le \gamma \cdot \lambda_n(\mathcal{L})$.



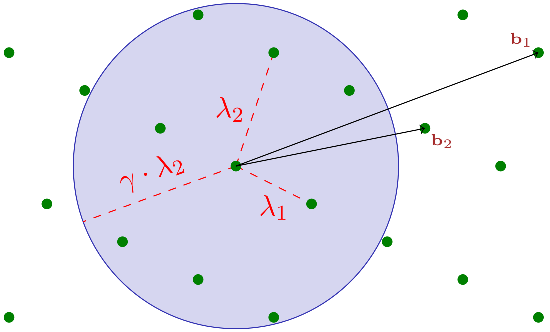
Related: Shortest Independent Vectors Problem (SIVP$_\gamma$)

- Given basis $\mathbf{B}$, find lin. ind. $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ s.t. $\|\mathbf{v}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$.
- LLL algorithm also solves SIVP$_{2^{(n-1)/2}}$.



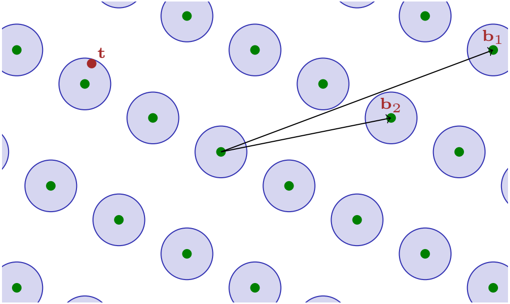
Related: Shortest Independent Vectors Problem (SIVP_γ)

- Given basis $\mathbf{B}$, find lin. ind. $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ s.t. $\|\mathbf{v}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L})$.
- LLL algorithm also solves $\mathsf{SIVP}_{2^{(n-1)/2}}$.
- We know $\mathsf{GapSVP}_\gamma \leq \mathsf{SIVP}_\gamma$, but the reverse direction is open!



Bounded-Distance Decoding (BDD)

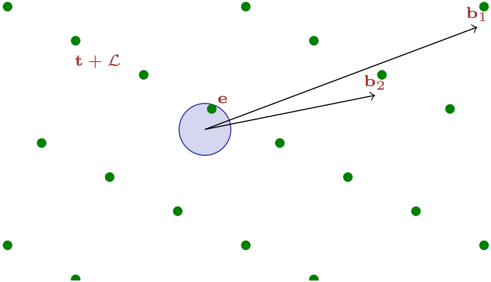
Search: given basis $\mathbf{B}$, point $\mathbf{t}$, and real $d < \lambda_1/2$ s.t. $\mathrm{dist}(\mathbf{t}, \mathcal{L}) \leq d$, find the (unique) $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$.



Bounded-Distance Decoding (BDD)

Search: given basis $\mathbf{B}$, point $\mathbf{t}$, and real $d < \lambda_1/2$ s.t. $\mathrm{dist}(\mathbf{t}, \mathcal{L}) \leq d$, find the (unique) $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$.

Equivalently, given coset $\mathbf{t} + \mathcal{L} \ni \mathbf{e}$ s.t. $\|\mathbf{e}\| \leq d$, find $\mathbf{e}$.



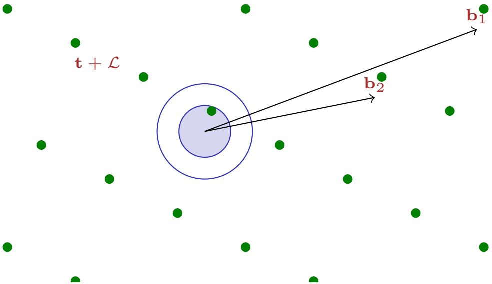
Bounded-Distance Decoding (BDD)

Search: given basis $\mathbf{B}$, point $\mathbf{t}$, and real $d < \lambda_1/2$ s.t. $\mathrm{dist}(\mathbf{t}, \mathcal{L}) \leq d$, find the (unique) $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$.

Equivalently, given coset $\mathbf{t} + \mathcal{L} \ni \mathbf{e}$ s.t. $\|\mathbf{e}\| \leq d$, find $\mathbf{e}$.

Decision: given basis $\mathbf{B}$, coset $\mathbf{t} + \mathcal{L}$, and real d, decide between

$$\mathrm{dist}(\mathbf{0}, \mathbf{t} + \mathcal{L}) \leq d \quad \underline{\text{versus}} \quad > \gamma \cdot d.$$



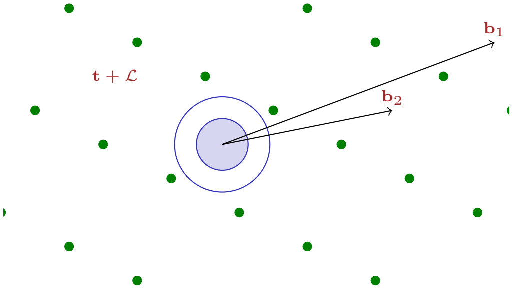
Bounded-Distance Decoding (BDD)

Search: given basis $\mathbf{B}$, point $\mathbf{t}$, and real $d < \lambda_1/2$ s.t. $\mathrm{dist}(\mathbf{t}, \mathcal{L}) \leq d$, find the (unique) $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$.

Equivalently, given coset $\mathbf{t} + \mathcal{L} \ni \mathbf{e}$ s.t. $\|\mathbf{e}\| \leq d$, find $\mathbf{e}$.

Decision: given basis $\mathbf{B}$, coset $\mathbf{t} + \mathcal{L}$, and real d, decide between

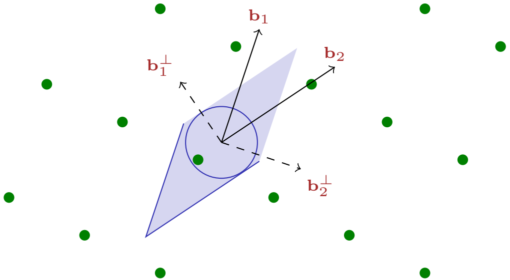
$$\mathrm{dist}(\mathbf{0}, \mathbf{t} + \mathcal{L}) \leq d \quad \underline{\text{versus}} \quad > \gamma \cdot d.$$



Algorithms for BDD [Babai'86]

"Round off:" Using a "good" basis $\mathbf{B}$, output $\mathbf{e} = \mathbf{t} \bmod \mathbf{B}$.

Works if Ball$(d) \subseteq \mathcal{P}(\mathbf{B})$: radius $d = \min_i \|\mathbf{b}_i^\perp\|/2$.



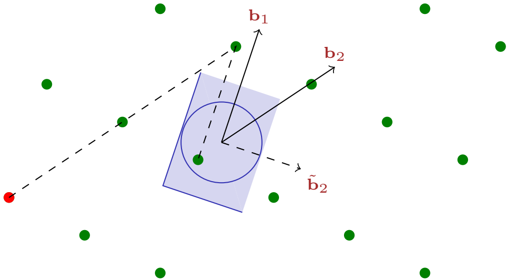
Algorithms for BDD [Babai'86]

"Round off:" Using a "good" basis $\mathbf{B}$, output $\mathbf{e} = \mathbf{t} \bmod \mathbf{B}$.

Works if $\text{Ball}(d) \subseteq \mathcal{P}(\mathbf{B})$: radius $d = \min_i \|\mathbf{b}_i^{\perp}\|/2$.

"Nearest plane:" Output $\mathbf{e} = \mathbf{t} \bmod \tilde{\mathbf{B}}$. Proceeds iteratively.

Works if $\text{Ball}(d) \subseteq \mathcal{P}(\tilde{\mathbf{B}})$: radius $d = \min_i \|\tilde{\mathbf{b}}_i\|/2$.



Wrapping Up

- Now you know (almost) everything you need to know about lattices (to do cryptography, at least).
- We've covered a lot: do the exercises to reinforce your understanding!
- Tomorrow: the cryptographic problems SIS and LWE (as SVP and BDD variants), and some basic applications.