Lattices

Mathematical background

Lattices

- $\mathbb{R}^n$: n-dimensional Euclidean space. That is,

  $\mathbb{R}^n = \{(x_1, \ldots, x_n)^{\mathrm{T}} : x_i \in \mathbb{R}, 1 \le i \le n\}$.

- If $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{T}}$, $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{T}}$, then
  - $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_i x_i y_i$ (inner product of $\mathbf{x}$ and $\mathbf{y}$)
  - $\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$ (Euclidean length or norm of $\mathbf{x}$)
  - $\|\mathbf{x} - \mathbf{y}\|$: Euclidean distance between $\mathbf{x}$ and $\mathbf{y}$.

- Definition 1: A lattice L in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$.
  - subgroup: if $\mathbf{x}, \mathbf{y} \in L$, then $\mathbf{x} - \mathbf{y} \in L$.
  - discrete: $\exists\, \varepsilon > 0$ s.t. $\|\mathbf{x} - \mathbf{y}\| \ge \varepsilon$ for all $\mathbf{x} \ne \mathbf{y} \in L$.

- Definition 2: An n-dimensional lattice of rank m is a subset $L \subseteq \mathbb{R}^n$ of the form $L = \{x_1\mathbf{b}_1 + \cdots + x_m\mathbf{b}_m : x_i \in \mathbb{Z}\}$ where $\mathbf{b}_1, \ldots, \mathbf{b}_m$ are linearly independent vectors in $\mathbb{R}^n$.
  - Every vector in L is an integer linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_m$.
  - Basis: $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is called a basis of L.
  - L has full rank if $m = n$. We will be mostly interested in full rank lattices, and call them n-dimentional lattices.

- We denote by $L(\mathbf{B})$ the lattice generated by $\mathbf{B}$. Thus, if $\mathbf{B}$ is a basis, then $L(\mathbf{B}) = \mathbf{B} \cdot \mathbb{Z}^m = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^m\}$.

- Let $\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m \in \mathbb{R}^n$ (not necessarily linearly independent).

  Let $L(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m) \triangleq \{x_1\mathbf{b}_1 + \cdots + x_m\mathbf{b}_m : x_i \in \mathbb{Z}\}$.

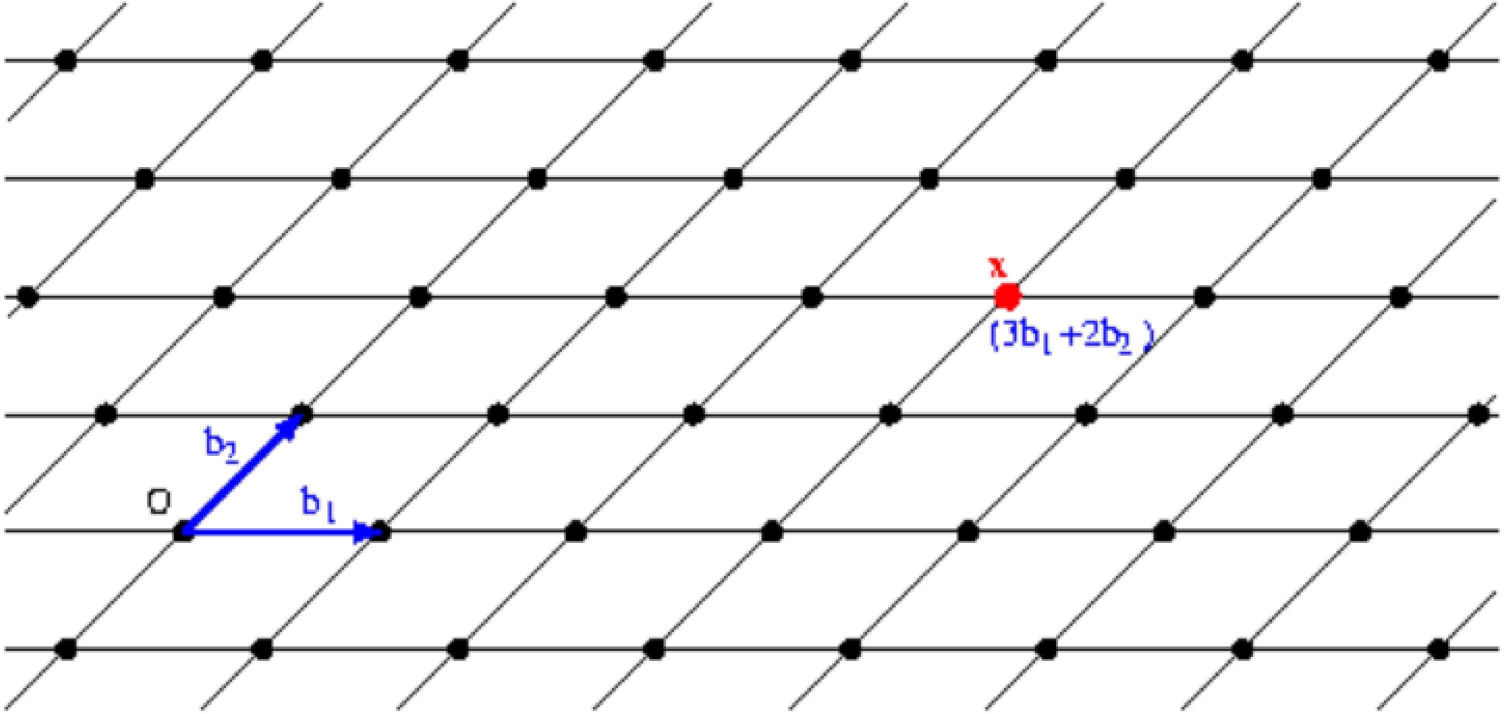
- Theorem. $L(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m)$ is a lattice
  - if $\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m \in \mathbb{Q}^n$, or
  - if $\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m$ are linearly independent.

- When $L(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m)$ is a lattice, $(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m)$ is said to be a generator. If the $\mathbf{b}_i$'s are further lineraly independent, then $(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_m)$ is a basis.

Example lattices

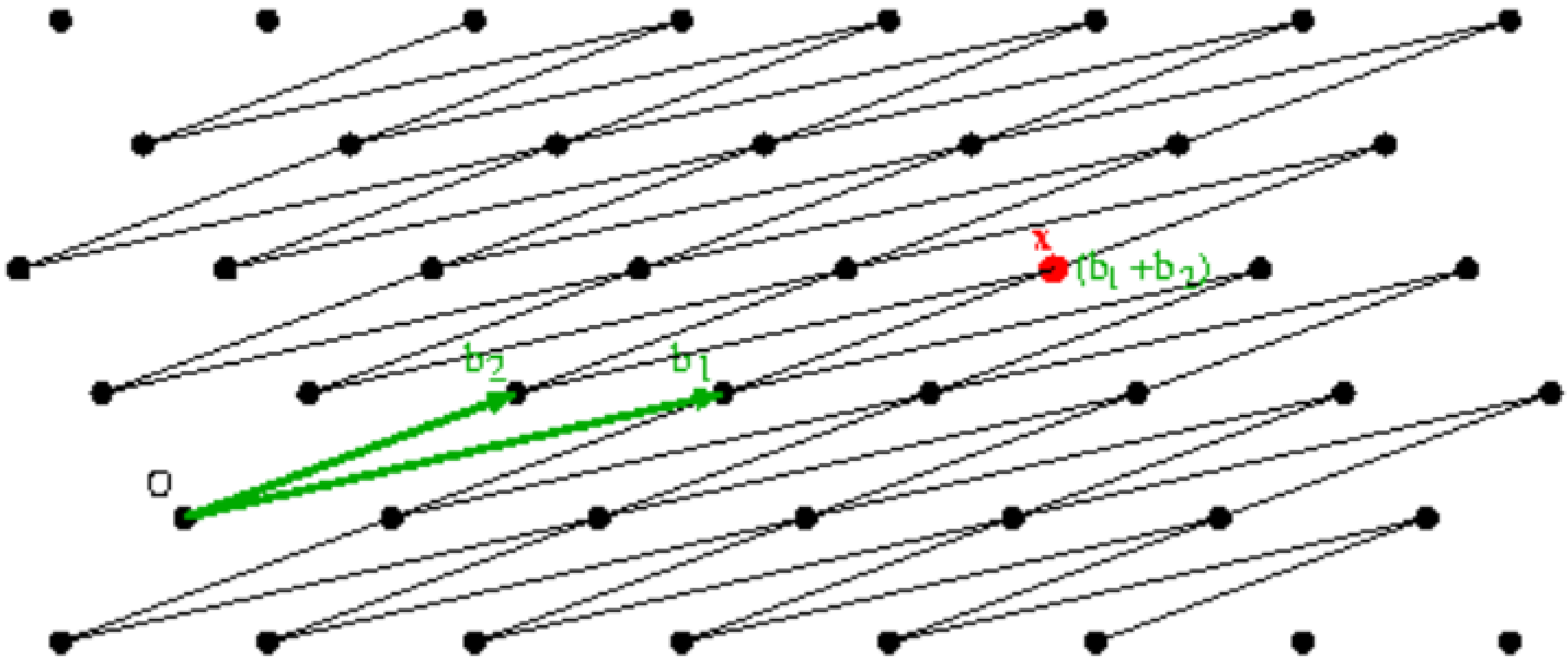
- Zero lattice: **0**.
- Lattice of integers: $\mathbb{Z}^n$.
- Integral lattices : sublattices of $\mathbb{Z}^n$.
- $\Lambda_q^{\perp}(\mathbf{A}) \triangleq \left\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{Ax} = \mathbf{0} \mod q\right\}$, where $\mathbf{A} \in \mathbb{Z}^{n\times m}$ is a matrix of dimensions $n \times m$, and q an integer.
- $L\left(1, \sqrt{2}\right) = \left\{x + \sqrt{2}y : \ x, y \in \mathbb{Z}\right\}$ is not a lattice, for there exists a sequence of rationals $\left(x_n / y_n\right)_{n\geq 1}$ s.t. $x_n / y_n \to \sqrt{2}$.

A Lattice in 2 dimensions



Source: http://cseweb.ucsd.edu/~daniele/lattice/lattice.html

A different basis for the same lattice



Source: http://cseweb.ucsd.edu/~daniele/lattice/lattice.html

Lattice Bases

- Unimodular matrix: square, having integer entries, and determinant $= \pm 1$.

- If $\mathbf{A} = \left(a_{ij}\right)$ and $\det \mathbf{A} \neq 0,$ then $\mathbf{A}^{-1} = \dfrac{1}{\det \mathbf{A}}\left(c_{ij}\right),$ where

  $c_{ij} = (-1)^{i+j} \det \mathbf{A}_{ji},$

  $\mathbf{A}_{ji} = \mathbf{A}$ with row j and column i omited.

  Furthermore, $\det \mathbf{A}^{-1} = \dfrac{1}{\det \mathbf{A}}.$

- If $\mathbf{A}$ is unimodular, then $\mathbf{A}^{-1}$ is unimodular.

Theorem: Two bases $\mathbf{B}$ and $\mathbf{C}$ generate the same lattice, i.e., $L(\mathbf{B}) = L(\mathbf{C})$, iff $\mathbf{B} = \mathbf{CU}$ for some unimodular matrix $\mathbf{U}$.

Proof: $(\Leftarrow)$ Assume $\mathbf{B} = \mathbf{CU}$, $\mathbf{U}$ unimodular. Then $\mathbf{C} = \mathbf{BU}^{-1}$,

$\mathbf{U}^{-1}$ unimodular.

$$\left.\begin{array}{l} \mathbf{B} = \mathbf{CU} \Rightarrow L(\mathbf{B}) \subseteq L(\mathbf{C}) \\ \mathbf{C} = \mathbf{BU}^{-1} \Rightarrow L(\mathbf{C}) \subseteq L(\mathbf{B}) \end{array}\right\} \Rightarrow L(\mathbf{B}) = L(\mathbf{C}).$$

$(\Rightarrow)$ Assume $L(\mathbf{B}) = L(\mathbf{C})$. Each $\mathbf{b}_i \in \mathbf{B}$ is in the lattice, hence $\mathbf{b}_i = \mathbf{C} \cdot \mathbf{v}_i$ for some $\mathbf{v}_i \in \mathbb{Z}^m$, $1 \le i \le m$, and $\mathbf{B} = \mathbf{CV}$, where $\mathbf{V} = (\mathbf{v}_i)$. Similarly, $\mathbf{C} = \mathbf{BW}$ for some square integer matrix $\mathbf{W}$.

Hence $\mathbf{B} = \mathbf{BWV} \Rightarrow \mathbf{B}\left(\mathbf{I} - \mathbf{WV}\right) = \mathbf{0} \Rightarrow \mathbf{I} - \mathbf{WV} = \mathbf{0}$ ($\mathbf{B}$ lin. indep.)

$\Rightarrow \det \mathbf{W} \cdot \det \mathbf{V} = \det \mathbf{WV} = \det \mathbf{I} = 1 \Rightarrow \det \mathbf{W} = \det \mathbf{V} = \pm 1.$

- For each $n > 1$, there is an infinite number of n-dimentional unimodular matrices.
- For example, $\begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix}$ is unimodular for any $a \in \mathbb{Z}$.
- Each lattice of rank $n > 1$ has an infinite number of bases.

Fundamental Parallelepiped

- Let $\mathbf{B} = \left(\mathbf{b}_1,\ \ldots,\ \mathbf{b}_n\right) \in \mathbb{R}^{n\times n}$ be a full rank basis.
- Fundamental parallelepiped associated to $\mathbf{B}$:

  $P(\mathbf{B}) = \left\{\mathbf{B}\cdot\mathbf{x} : \mathbf{x} = (x_1,\ \ldots,\ x_n)^{\mathrm{T}},\ 0 \le x_i < 1\right\}.$
- Centered fundamental parallelepiped:

  $C(\mathbf{B}) = \left\{\mathbf{B}\cdot\mathbf{x} : \mathbf{x} = (x_1,\ \ldots,\ x_n)^{\mathrm{T}},\ -1/2 \le x_i < 1/2\right\}.$
- $P(\mathbf{B})$ and $C(\mathbf{B})$ are half open.

- The translates $\left\{P(\mathbf{B})+\mathbf{v} : \mathbf{v} \in L(\mathbf{B})\right\}$

  form a partition of the whole space $\mathbb{R}^n$:

$$\mathbb{R}^n = \bigcup_{\mathbf{v} \in L(\mathbf{B})} \left(P(\mathbf{B})+\mathbf{v}\right)$$

- For any $\mathbf{t} \in \mathbb{R}^n$, there exists a unique point $\mathbf{r} \in P(\mathbf{B})$ s.t. $\mathbf{x} - \mathbf{r} \in L(\mathbf{B})$. This unique $\mathbf{r}$ is denoted by $\mathbf{t} \bmod \mathbf{B}$.

- $\mathbf{t} \bmod \mathbf{B}$ can be computed efficiently as:

$$\mathbf{t} \bmod \mathbf{B} = \mathbf{t} - \mathbf{B} \cdot \left\lfloor \mathbf{B}^{-1} \cdot \mathbf{t} \right\rfloor$$

where $\lfloor \mathbf{x} \rfloor$ rounds $\mathbf{x}$'s coordinates x_i to $\lfloor x_i \rfloor$.

- Similarly, the translates $\{C(\mathbf{B})+\mathbf{v} : \mathbf{v}\in L(\mathbf{B})\}$ form a partition of the whole space $\mathbb{R}^n$:

$$\mathbb{R}^n = \bigcup_{\mathbf{v}\in L(\mathbf{B})} \left(C(\mathbf{B})+\mathbf{v}\right)$$

- For any $\mathbf{t}\in\mathbb{R}^n$, there exists a unique point $\mathbf{r}\in C(\mathbf{B})$ s.t. $\mathbf{x}-\mathbf{r}\in L(\mathbf{B})$. Let's denote this unique $\mathbf{r}$ is also by $\mathbf{t} \bmod \mathbf{B}$.

- $\mathbf{t} \bmod \mathbf{B}$ can be computed efficiently as:

$$\mathbf{t} \bmod \mathbf{B} = \mathbf{t}-\mathbf{B}\cdot\lfloor \mathbf{B}^{-1}\cdot\mathbf{t}\rceil$$

where $\lfloor \mathbf{x} \rceil$ rounds $\mathbf{x}$'s coordinates to the nearest integer.

Gram-Schmidt orthogonalization

- A basis $\mathbf{B} = (\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n)$ of a vector space is orthogonal if $\langle \mathbf{b}_i, \ \mathbf{b}_j \rangle = 0$ for $i \neq j$. $\mathbf{B}$ is orthonormal if $\langle \mathbf{b}_i, \ \mathbf{b}_i \rangle = \delta_{ij}$, where δ_{ij} is Kronecker's delta.
- Any basis $\mathbf{B} = (\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n)$ can be transformed into an orthogonal basis $\mathbf{B}^* = (\mathbf{b}_1^*, \ \ldots, \ \mathbf{b}_n^*)$ using the well-known Gram-Schmidt orthogonalization process:
  - $\mathbf{b}_1^* = \mathbf{b}_1$.
  - $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*$ where $\mu_{i,j} = \dfrac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} = \dfrac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$.

Determinant

- $\mathbf{B},\ \mathbf{C} \in \mathbb{R}^{n\times n}$: full rank bases.

  $\mathbf{B}^*$: the Gram-Schmidt basis of $\mathbf{B}$.

- Theorem 1: If $\mathbf{B},\ \mathbf{C}$ are two bases of the same lattice, then

  $\det \mathbf{B} = \pm \det \mathbf{C}$. Also, $\left|\det \mathbf{B}\right| = \prod_i \left\|\mathbf{b}_i^*\right\|$.

- Definition: The determinant of a lattice $\Lambda = L(\mathbf{B})$ is

  $\det \Lambda = \det L(\mathbf{B}) = \mathrm{vol}\big(P(\mathbf{B})\big) = \prod_i \left\|\mathbf{b}_i^*\right\| = \left|\det \mathbf{B}\right|$.

- This quantity is an invariant of Λ, independent of bases.

Hermite normal form

- A square, non-singular, integer or rational matrix $\mathbf{B} = \left(b_{ij}\right)$ is in Hermite normal form (HNF) iff
  - $\mathbf{B}$ is lower triangular ($b_{ij} = 0$ for $i < j$)
  - For all $j < i$, $0 \le b_{ij} < b_{ii}$.
- Some authors prefer using upper triangular matrices.
- Examples: $\begin{pmatrix} 3 & 0 & 0 & 0 \\ 1 & 7 & 0 & 0 \\ 4 & 0 & 5 & 0 \\ 0 & 6 & 3 & 8 \end{pmatrix}$ or $\begin{pmatrix} 3 & 1 & 4 & 0 \\ 0 & 7 & 0 & 6 \\ 0 & 0 & 5 & 3 \\ 0 & 0 & 0 & 8 \end{pmatrix}$

HNF for singular or non-square matrices

- An integer or rational $n \times m$ matrix $\mathbf{B} = \left(b_{ij} \right)$ is in HNF if
  - $\exists\, 1 \le i_1 < i_2 < \cdots < i_h \le n$ s.t. $b_{ij} \ne 0 \Rightarrow \left(j \le h \right) \wedge \left(i \ge i_j \right)$.
  - For all $k < j,\ 0 \le b_{i_j,k} < b_{i_j,j}$.
- Example: $\begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 0 & 0 & 0 & 0 \\ -3 & 5 & 0 & & & \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 4 & 3 & 1 & 5 & 0 & 0 \\ -1 & 9 & 0 & -2 & 0 & 0 \end{pmatrix}$

- The first h columns are linearly independent.
- Theorem: If two matrices $\mathbf{B}$, $\mathbf{B}'$ in HNF generate the same lattice, then $\mathbf{B} = \mathbf{B}'$ (except for the number of zero-columns at the end).
- Theorem: Any lattice $L(\mathbf{B})$ has a unique basis $\mathbf{H}$ in HNF, which can be constructed from $\mathbf{B}$ in polynomial time.
- HNF is useful for solving many lattice problems.
- Basis Problem: Given a set of rational vectors $\mathbf{B}$, find a basis for the lattice $L(\mathbf{B})$.

Good bases and bad basses

- Let $\mathbf{B} = \left(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n\right)$ be a basis of lattice L.
- Roughly speaking, $\mathbf{B}$ is a good basis if
  - the vectors $\mathbf{b}_i$ are reasonably short and nearly orthogonal
  - the inequality $\prod_i \|\mathbf{b}_i\| \geq \det(L)$ comes close to equality.
- HNF(L) is a bad basis and is a good choice for the public lattice basis. It reveals no more info about L's structure than any other basis, because HNF(L) can be computed from any basis in polynomial time.

Dual Lattice

- The dual of a (full rank) lattice $\Lambda = L(\mathbf{B}) \subseteq \mathbb{R}^n$ is the set

  $$\Lambda^* = \left\{\mathbf{x} \in \mathbb{R}^n : \left\langle \mathbf{x}, \mathbf{v} \right\rangle \in \mathbb{Z} \text{ for all } \mathbf{v} \in \Lambda \right\}.$$

- Theorem: The dual of a lattice $\Lambda = L(\mathbf{B})$ is a lattice with basis $\mathbf{D} = \left(\mathbf{B}^{-1}\right)^{\mathrm{T}} = \left(\mathbf{B}^{\mathrm{T}}\right)^{-1}$. That is, $L(\mathbf{D}) = \Lambda^*$.
  - $L(\mathbf{D}) \subseteq \Lambda^* \Leftarrow \mathbf{D} \subseteq \Lambda^* \Leftarrow \mathbf{d}_i \mathbf{b}_j \in \mathbb{Z}\ \forall i, j \Leftarrow \left(\mathbf{d}_i \mathbf{b}_j\right) = \mathbf{D}^{\mathrm{T}}\mathbf{B} = \mathbf{I}.$
  - $\Lambda^* \subseteq L(\mathbf{D})$: If $\mathbf{x} \in \Lambda^*$, then $\left\langle \mathbf{x}, \mathbf{b}_j \right\rangle \in \mathbb{Z}$ for all j, which means

    $$\mathbf{B}^{\mathrm{T}}\mathbf{x} \in \mathbb{Z}^n \Rightarrow \mathbf{x} \in \left(\mathbf{B}^{\mathrm{T}}\right)^{-1}\mathbb{Z}^n = \mathbf{D}\mathbb{Z}^n = L(\mathbf{D})$$

Minimum distance and shortest vector

- Definition: The minimum distance of a lattice $\Lambda = L(\mathbf{B})$ is the smallest distance between any two lattice points:
  $\lambda(\Lambda) = \min\{\| \mathbf{x} - \mathbf{y} \| : \mathbf{x}, \mathbf{y} \in \Lambda,\ \mathbf{x} \neq \mathbf{y}\}.$
- Note that $\lambda(\Lambda)$ is equal to the length of a shortest nonzero lattice vector:
  $\lambda(\Lambda) = \lambda_1(\Lambda) = \min\{\| \mathbf{x} \| : \mathbf{x} \in \Lambda,\ \mathbf{x} \neq \mathbf{0}\}.$
- We can use min because lattices are discrete.

Successive minima

- Definition: For any lattice Λ and integer $k \le \mathrm{rank}(\Lambda)$, let $\lambda_k(\Lambda)$ be the smallest r s.t. the closed ball $\bar{B}(r)$ contains at least k linearly independent lattice vectors. That is,
  $\lambda_k(\Lambda) = \min\{\max \| \mathbf{x}_1 \|, \ldots, \| \mathbf{x}_k \| : \mathbf{x}_1, \ldots, \mathbf{x}_k \in \Lambda \text{ linearly ind.}\}$
  //length of the *k*th shortest linearly independent vector//
- Obviously, $\lambda_1(\Lambda) \le \lambda_2(\Lambda) \le \cdots \le \lambda_k(\Lambda)$.
- $\lambda_1, \ \ldots, \ \lambda_k$ are called succesive minima of Λ:
  first minimum, second minimum, and so on.

Easy Lattice Problems

- Equivalence problem: Given two bases $\mathbf{B}$ and $\mathbf{B}'$, determine if they generate the same lattice, $L(\mathbf{B}) = L(\mathbf{B}')$.

- Sum of lattices: Given bases $\mathbf{B}$ and $\mathbf{B}'$, find a basis for the smallest lattice containing both $L(\mathbf{B})$ and $L(\mathbf{B}')$, which is $L(\mathbf{B}) + L(\mathbf{B}') = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in L(\mathbf{B}),\ \mathbf{y} \in L(\mathbf{B}')\}$.

- Containment problem: Given two bases $\mathbf{B}$ and $\mathbf{B}'$, determine if $L(\mathbf{B}) \subseteq L(\mathbf{B}')$.

- Membership problem: Is $\mathbf{v} \in L(\mathbf{B})$?

- Dual lattice: Given a lattice basis $\mathbf{B}$, compute its dual.

- Intersection of lattices: Given two bases $\mathbf{B}$ and $\mathbf{B}'$, find a basis for the intersection $L(\mathbf{B}) \cap L(\mathbf{B}')$.

- Cyclic lattice:
  - Let $r(\mathbf{x})$ be the cyclic rotation of vector $\mathbf{x}$, i.e., $r(x_1, \ \dots, \ x_n) = (x_n, \ x_1, \ \dots, \ x_{n-1})$.
  - A lattice Λ is cyclic iff $\mathbf{x} \in \Lambda$ implies $r(\mathbf{x}) \in \Lambda$.
  - Problem: Given $\mathbf{B} = \left(\mathbf{b}_1, \ \dots, \ \mathbf{b}_m\right)$, find the smallest cyclic lattice containing $L(\mathbf{B})$.
  - Problem: Is a given lattice $L(\mathbf{B})$ cyclic?

Some Important Hard Lattice Problems

Shortest Vector Problems

- Exact Shortest Vector Problem (SVP):

  Given a basis for a lattice L of rank n, find a nonzero vector $\mathbf{v} \in L$ of length $\lambda_1(L)$.

- Approximate Shortest Vector Problem (SVP_γ):

  Given a basis for a lattice L of rank n, find a nonzero vector $\mathbf{v} \in L$ of length at most $\gamma \cdot \lambda_1(L)$.

  (The approximation factor γ may be a function of n.)

- SVP has been studied since the time of Gauss (1801).

Hardness of SVP_γ

- NP-hard for any constant γ.
  - There is no polynomial algorithm unless $\mathrm{P} = \mathrm{NP}$.
- Hard for $\gamma(n) = n^{c/\log\log n}$ for some $c > 0$.
  - There is no polynomial algorithm unless $\mathrm{NP} \subseteq \mathrm{RSUBEXP}$.
- Cannot be NP-hard for $\gamma(n) = \sqrt{n/\log n}$ unless $\mathrm{NP} \subseteq \mathrm{coAM}$.
- Cannot be NP-hard for $\gamma(n) = \sqrt{n}$ unless $\mathrm{NP} = \mathrm{coNP}$.

constant	$n^{c/\log\log n}$	$\sqrt{n/\log n}$	$\sqrt{n}$	$\cdots$
NP-hard	hard	unlikely NP-hard	unlikely NP-hard	$\cdots$

SVP_γ can be solved in polynomial time

- LLL algorithm (1982): for $\gamma(n) = 2^{n/2}$.
  - Deterministic algorithm.
- Schnorr (1985): for $\gamma(n) = 2^{O\left(n(\log\log n)^2/\log n\right)}$.
  - Deterministic algorithm.
- Ajtai, Kumar, and Sivakumar(2001): $\gamma(n) = 2^{O\left(n\log\log n/\log n\right)}$.
  - Ramdomized algorithm with bounded error.

$\sqrt{n}$	$\cdots$	$2^{O\left(n\log\log n/\log n\right)}$	$2^{O\left(n(\log\log n)^2/\log n\right)}$	$2^{n/2}$
unlikely NP-hard	$\cdots$	BPP	P	P

SVP_γ : open problems

It would be a breakthrough if one can:

- Solve SVP_{n^c} in polynomial time for some $c > 0$.
- Prove $\mathrm{SVP}_{n^\varepsilon}$ hard or NP-hard for some $\varepsilon > 0$.

Two other important problems: CVP and SIVP

- Closest Vector Problem (CVP_γ):

  Given a basis for a lattice (of rank n) $L \subseteq \mathbb{R}^n$ and a vector $\mathbf{t} \in \mathbb{R}^n$, find a nonzero vector $\mathbf{v} \in L$ s.t. $\|\mathbf{t} - \mathbf{v}\| \leq \gamma(n) \cdot \text{dist}(\mathbf{t}, L)$.

- Shortest Independent Vectors Problem (SIVP_γ):

  Given a basis for a lattice L of rank n, find linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ of length at most $\gamma(n) \cdot \lambda_n(n)$.

CVP_γ is at least as hard as SVP_γ

Theorem: SVP_γ can be reduced to CVP_γ : $\mathrm{SVP}_\gamma \le \mathrm{CVP}_\gamma$.

Proof (for $\gamma = 1$): Let $\mathbf{B} = \left(\mathbf{b}_1, \ldots, \mathbf{b}_n\right)$ be the input to SVP.

Wish to find a shortest vector $\mathbf{s} = \sum x_i \mathbf{b}_i \in L(\mathbf{B})$ by calling CVP. The idea is to consider a sublattice $L' \subset L(\mathbf{B})$ and a point $\mathbf{c} \in L - L'$ s.t. $\mathbf{c} + \mathbf{s} \in L',$ in which case, $\mathrm{dist}(\mathbf{c}, L') = \|\mathbf{s}\|$.

Thus, if $\mathbf{y} \leftarrow \mathrm{CVP}\left(L', \mathbf{c}\right)$ then $\mathbf{y} - \mathbf{c}$ is a a solution to $\mathrm{SVP}(L)$.

Based on this idea, for each $i,$ consider the point $\mathbf{b}_i$ and the sublattice L^i generated by $\mathbf{B}^i = \left(\mathbf{b}_1, \ldots, 2\mathbf{b}_i, \ldots, \mathbf{b}_n\right)$. We have $\mathbf{b}_i \in L - L',$ and $\mathbf{b}_i + \mathbf{s} \in L'$ if x_i is odd. Let $\mathbf{y}_i \leftarrow \mathrm{CVP}\left(\mathbf{B}^i, \mathbf{b}_i\right)$.

The shortest vector in $\left\{\mathbf{y}_i - \mathbf{b}_i\right\}_{i=1}^n$ is a shortest vector in $L(\mathbf{B})$.

Relationship among SVP_γ, CVP_γ, $SIVP_\gamma$

- $SVP_\gamma \le CVP_\gamma$.
- $SIVP_\gamma \le CVP_\gamma$.
- $SVP_1 \le SIVP_1$.
- Open problem: $SVP_\gamma \le SIVP_\gamma$?

- Bounded Distance Decoding Problem (BDDP_γ):

  Given a lattice $L \subseteq \mathbb{R}^n$ and a vector $\mathbf{t} \in \mathbb{R}^n$ satisfying $\mathrm{dist}(\mathbf{t}, L) < \lambda_1(L)\big/\big(\gamma(n)+1\big)$, find a nonzero vector $\mathbf{v} \in L$ s.t. $\|\mathbf{t}-\mathbf{v}\| \le \gamma(n)\cdot \mathrm{dist}(\mathbf{t}, L)$.

  - Same as CVP_γ except for the "bounded" condition on $\mathbf{t}$, which implies a unique solution.

  - Uniqueness: The vector $\mathbf{v} \in L$ with $\|\mathbf{t}-\mathbf{v}\| = \mathrm{dist}(\mathbf{t}, L)$) is obviously a solution, and any other $\mathbf{w} \in L$ is not a solution since $\|\mathbf{t}-\mathbf{w}\| \ge \|\mathbf{v}-\mathbf{w}\| - \|\mathbf{v}-\mathbf{t}\| \ge \lambda_1(n) - \mathrm{dist}(\mathbf{t}, L)$

    $$> \big(\gamma(n)+1\big)\cdot \mathrm{dist}(\mathbf{t}, L) - \mathrm{dist}(\mathbf{t}, L) = \gamma(n)\cdot \mathrm{dist}(\mathbf{t}, L).$$

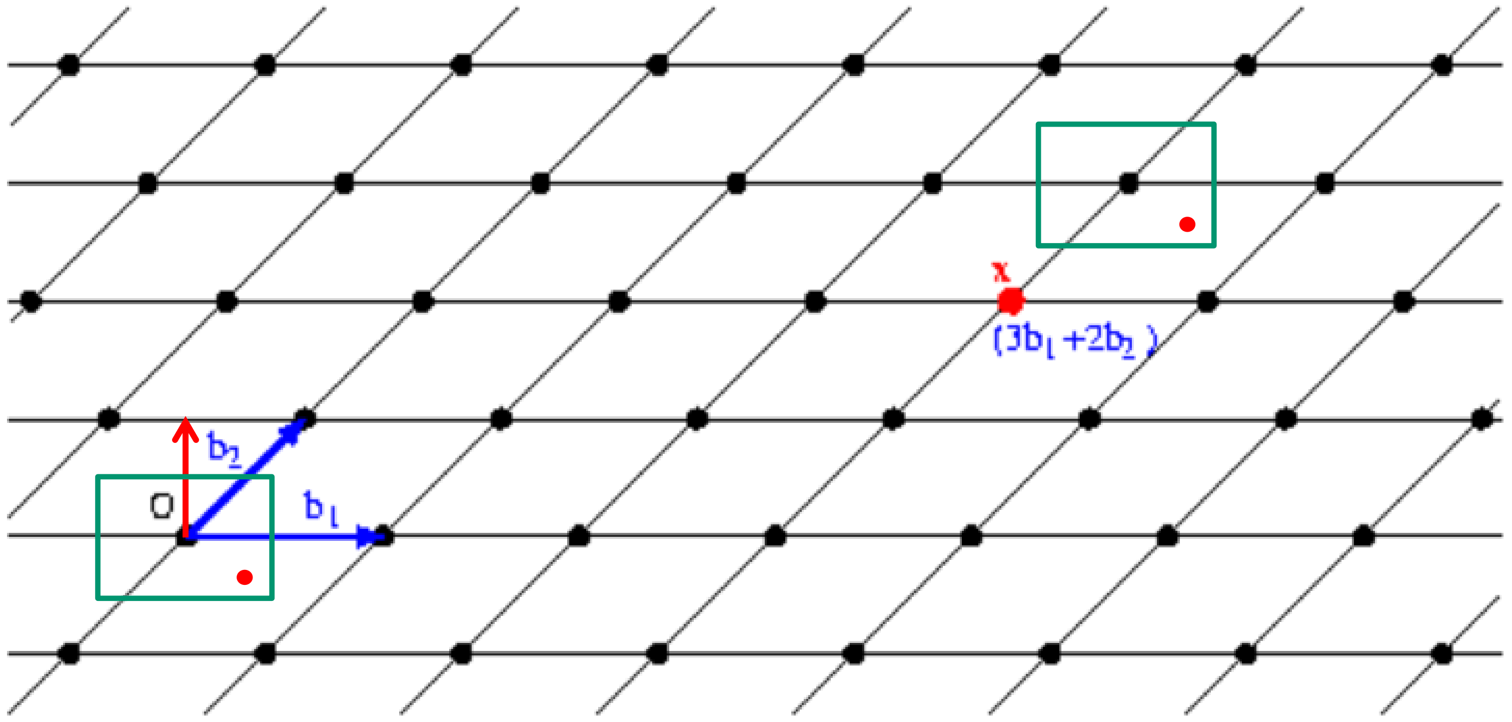
Centered Orthogonalized Parallelepiped

- Let $\mathbf{B} = \left(\mathbf{b}_1,\ \ldots,\ \mathbf{b}_n\right) \in \mathbb{R}^{m\times n}$ be a basis.
- Let $\mathbf{B}^* = \left(\mathbf{b}_1^*,\ \ldots,\ \mathbf{b}_n^*\right)$ be the Gram-Schmidt matrix of $\mathbf{B}$.
- Centered orthogonalized parallelepiped:

$$C(\mathbf{B}^*) = \left\{\mathbf{B}^* \cdot \mathbf{x} : \mathbf{x} = (x_1,\ \ldots,\ x_n)^{\mathrm{T}},\ -1/2 \le x_i < 1/2\right\}.$$

- $C(\mathbf{B}^*)$ is a fundamental region: $Span(\mathbf{B}) = \bigcup_{\mathbf{v}\in L(\mathbf{B})} \left(C(\mathbf{B}^*) + \mathbf{v}\right)$.
- Nearest plane algorithm: Given a target point $\mathbf{t} \in Span(\mathbf{B})$, find the unique cell $C(\mathbf{B}^*) + \mathbf{v}$ that contains $\mathbf{t}$.

A Lattice in 2 dimensions



Source: http://cseweb.ucsd.edu/~daniele/lattice/lattice.html

Nearest Plane Algorithm

- Given $\mathbf{B}$ and $\mathbf{t}$, find a lattice point $\mathbf{v} = c_1\mathbf{b}_1 + \cdots + c_n\mathbf{b}_n \in L(\mathbf{B})$

  s.t. $\left\langle \mathbf{t} - \mathbf{v},\ \mathbf{b}_i^* \right\rangle / \left\|\mathbf{b}_i^*\right\|^2 \in \left[-1/2,\ 1/2\right)$ for all $1 \le i \le n$.

  In particular, if $\mathbf{t} \in \mathrm{Span}(\mathbf{B})$, then $\mathbf{t} \in C(\mathbf{B}^*) + \mathbf{v}$.
- Let $L(\mathbf{B}')$ be the sublattice generated by $\mathbf{B}' = \left(\mathbf{b}_1,\ \ldots,\ \mathbf{b}_{n-1}\right)$.
- $L(\mathbf{B})$ can be decomposed into "sublattices"

$$L(\mathbf{B}) = \bigcup_{c \in \mathbb{Z}} \left(c\mathbf{b}_n + L(\mathbf{B}')\right) \subset \bigcup_{c \in \mathbb{Z}} \left(c\mathbf{b}_n^* + \mathrm{span}(\mathbf{B}')\right)$$

- The hyperplane $c\mathbf{b}_n + \mathrm{span}(\mathbf{B}')$ closest to $\mathbf{t}$ is when $c =$

  $\left\lfloor \left\langle \mathbf{t},\ \mathbf{b}_n^* \right\rangle / \left\|\mathbf{b}_n^*\right\|^2 \right\rceil$. We choose $c_n = c$.

Algorithm NearestPlane($\mathbf{B} = (\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n), \ \mathbf{t}$)

if $n = 0$ then return $\mathbf{0}$

else $\mathbf{B}^* \leftarrow \text{Gram-Schmidt}(\mathbf{B})$

$$c \leftarrow \left\lfloor \langle \mathbf{t}, \ \mathbf{b}_n^* \rangle / \|\mathbf{b}_n^*\|^2 \right\rceil$$

return $c\mathbf{b}_n + \text{NearestPlane}((\mathbf{b}_1, \ \ldots, \ \mathbf{b}_{n-1}), \ \mathbf{t} - c\mathbf{b}_n)$

Correstness Proof

- By induction. For $n = 0$, the output meets the requirement.
- Assume the algorithm returns a correct answer for ranks $< n$.
- Let $\mathbf{C} = (\mathbf{b}_1, \ \ldots, \ \mathbf{b}_{n-1})$ and $\mathbf{B} = (\mathbf{C}, \ \mathbf{b}_n)$. Then $\mathbf{B}^* = (\mathbf{C}^*, \ \mathbf{b}_n^*)$.
- By IH, the recursive call returns a lattice point $\mathbf{v}' \in L(\mathbf{C})$ s.t.

  $$\left\langle (\mathbf{t} - c\mathbf{b}_n) - \mathbf{v}', \ \mathbf{b}_i^* \right\rangle \in [-1/2, \ 1/2) \cdot \left\| \mathbf{b}_i^* \right\|^2 \text{ for all } i = 1, \ \ldots, \ n-1.$$

- The output of the algorithm is $\mathbf{v} = \mathbf{v}' + c\mathbf{b}_n$.
- Need to prove $\left\langle \mathbf{t} - \mathbf{v}, \ \mathbf{b}_i^* \right\rangle \in [-1/2, \ 1/2) \cdot \left\| \mathbf{b}_i^* \right\|^2$ for all $1 \le i \le n$.

- For $i \le n-1$, it follows from the IH since

$$\left\langle \mathbf{t}-\mathbf{v},\ \mathbf{b}_i^* \right\rangle = \left\langle \mathbf{t}-(\mathbf{v}'+c\mathbf{b}_n),\ \mathbf{b}_i^* \right\rangle = \left\langle (\mathbf{t}-c\mathbf{b}_n)-\mathbf{v}',\ \mathbf{b}_i^* \right\rangle.$$

- For $i = n$,

$$\frac{\left\langle \mathbf{t}-(\mathbf{v}'+c\mathbf{b}_n),\ \mathbf{b}_n^* \right\rangle}{\left\|\mathbf{b}_i^*\right\|^2} = \frac{\left\langle \mathbf{t},\ \mathbf{b}_n^* \right\rangle - \left\langle \mathbf{v}',\ \mathbf{b}_n^* \right\rangle - c\left\langle \mathbf{b}_n,\ \mathbf{b}_n^* \right\rangle}{\left\|\mathbf{b}_i^*\right\|^2}$$

$$= \frac{\left\langle \mathbf{t},\ \mathbf{b}_n^* \right\rangle}{\left\|\mathbf{b}_i^*\right\|^2} - c \in \left[-1/2,\ 1/2\right).$$

where we have used $\left\langle \mathbf{v}',\ \mathbf{b}_n^* \right\rangle = 0$ and $\left\langle \mathbf{b}_n,\ \mathbf{b}_n^* \right\rangle = \left\|\mathbf{b}_i^*\right\|^2$.

Nearest Plane Algorithm and Closest Vector Problem

- Fact: $\lambda_1\left(L(\mathbf{B})\right) \geq \min_i \left\|\mathbf{b}_i^*\right\|$.
- The fundamental region $C(\mathbf{B}^*)$ contains a sphere centered at $\mathbf{0}$ of radius $\rho = \min_i \left\|\mathbf{b}_i^*\right\| / 2 \leq \lambda_1\left(L(\mathbf{B})\right)/2$.
- Thus, if a point $\mathbf{t}$ is within distance ρ of a lattice point $\mathbf{v} \in L(\mathbf{B})$, then $\mathbf{v}$ is the closest lattice point to $\mathbf{t}$.

  NearestPlane$(\mathbf{B}, \mathbf{t})$ will solve the CVP.

Recall RSA Cryptosystem

- Key generation:

  (a) Randomly generate $n := pq$ for large primes $p,\ q$.

  (b) Public key: $e,$ coprime to $\varphi(n)$.

  (c) Secret key: $d := e^{-1} \bmod \varphi(n)$.

- The security of RSA requires that breaking RSA is hard for all (but a negligible portion of) instances.
  - By breaking RSA we mean finding the secret key.

- It depends on the assumption that factoring a randomly generated semiprime $n = pq$ is hard.

Ajtai's worst-case to average-case reduction

- Worst-case to worst-case reduction, say P1 $\leq$ P2:
  If there is an algorithm that solves P2 in the worst case, then there is an algorithm that slove P1 in the worst case.

- Worst-case to average-case reduction, say P1 $\leq$ P2:
  If there is an algorithm that solves a randomly generated instance of P2 with nonnegligible probability, then there is an algorithm that solves the worst case of P1 with probability ≈ 1.

- In 1996, Ajtai established such an worst-case to average-case reduction for some lattice problems.

- Let $\mathbf{A} \in \mathbb{Z}^{n \times m}$ be a matrix of dimensions $n \times m$, and q an integer, where $m = \lfloor c_1 n \log n \rfloor$ and $q = \lfloor n^{c_2} \rfloor$. Define $\Lambda_q^{\perp}(\mathbf{A}) \triangleq \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \mod q\}$.
- Ajtai showed

  worst-case n^c-unique-SVP on an n-dimentional lattice

  $\leq$ average-case SVP on $\Lambda_q^{\perp}(\mathbf{A})$ for some c_1 and c_2.
- Based on this reduction, Ajtai and Dwork in 1997 constructed a public-key cryptosystem whose security depends on the (conjectured) worst-case hardness of unique-SVP.

- Later when we study FHE schemes, it is important to note whether the security is based on worst-case or average-case hardness.

- Q: Is the security of RSA based on the worst-case hardness or the average-case hardness of semiprime factorization?