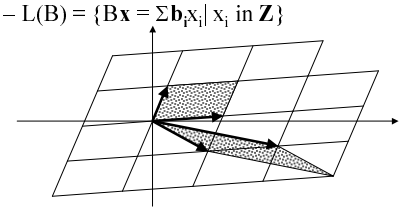
Lattices and Their Applications

Lecturer: Moni Naor

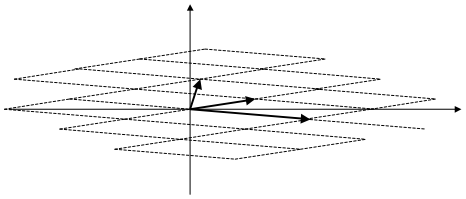
Lattices

- Represented by a basis B = $\mathbf{b_1},\ldots,\mathbf{b_n}$ in $\mathbf{R}^m$
  - $\mathbf{b_1},\ldots,\mathbf{b_n}$ linearly independent
- Lattice generated by B:
  - $L(B) = \{B\mathbf{x} = \Sigma \mathbf{b_i} x_i \mid x_i \text{ in } \mathbf{Z}\}$



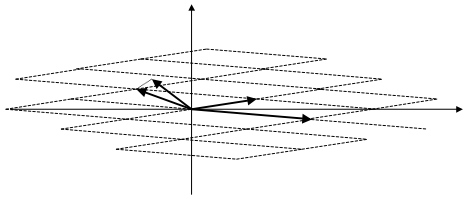
Shortest Vector Problem

- Given a lattice L = $\{\mathbf{b_1},\ldots,\mathbf{b_n}\}$, find a non-zero integer vector **x** such that ||Bx|| is minimum.



Closest Vector Problem

- Given a lattice L = $\{\mathbf{b_1},\ldots,\mathbf{b_n}\}$, and a target vector **y**, find an integer vector **x** such that $\|B\mathbf{x} - \mathbf{y}\|$ is minimum.



Computational Problems

	Shortest Vector Problem Given a lattice B	Closest Vector Problem Given B and target vector **y**
search	• Find **x** in $\mathbf{Z}^n \setminus \{\mathbf{0}\}$ s.t. min $\|B\mathbf{x}\|$	• Find **x** in $\mathbf{Z}^n$ s.t. min $\|B\mathbf{x} - \mathbf{y}\|$
value	• Find min $\|B\mathbf{x}\|$	• Find min $\|B\mathbf{x} - \mathbf{y}\|$
approx	• Find d in the range [min $\|B\mathbf{x}\|$, g min $\|B\mathbf{x}\|$]	• Find d in the range [min$\|B\mathbf{x}-\mathbf{y}\|$, g min$\|B\mathbf{x}-\mathbf{y}\|$]

Known Results

CVP	SVP
• [vEB 81] NP-hard in L_p norm $\|\mathbf{x}\|_p = (\Sigma x_i^p)^{1/p}$	• [Dir. 1842] Formulation of the problem
• [ABSS 93] NP-hard to approx. within any constant	• [vEB 81] NP-hard in L_∞ norm $\|\mathbf{x}\|_\infty = \max \|x_i\|$
• [DKS 98] NP-hard to approx. within $\exp(\lg^{1-\varepsilon} n)$	• [Ajtai 97] NP-hard in $\|\mathbf{x}\|_2$ (for randomized reductions)
• [Babai] Approx. 2^n in P	• [LLL 82] Approx. $2^{n/2}$ in P
• [LLS 86] Approx. $n^{1.5}$ in coNP	• [S 87] Approx. $2^{\varepsilon n}$ in P
• [H 88, B 88] Approx. n in coNP	• [LLS 86] Approx. n in coNP
• [GG 98] Approx. $n^{1/2}$ in coAM	• [GG 98] Approx. $n^{1/2}$ in coAM

Equivalent bases

- $L(\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_{n-1}}, \mathbf{b_n})$
  $= L(\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_{n-1}}, \mathbf{b_n} - \sum_{i=1}^{n-1} \lambda_i \cdot \mathbf{b_i})$

In general:

B and **B'** are *equivalent* iff there exists a unimodular matrix **U** s.t.

$$\mathbf{B'} = \mathbf{B}\,\mathbf{U}$$

Volume

- The determinant of a lattice $L(\mathbf{B})$ is the volume of the fundamental paralleliped

Claim: det. Is a lattice *invariant* (does not depend on the particular basis) and is equal to $\sqrt{\det(\mathbf{B}^t\,\mathbf{B})}$

Gram Schmidt Orthogonalization

- For $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$ The *GSO* is $\mathbf{b_1}^*, \mathbf{b_2}^* \ldots, \mathbf{b_n}^*$ where

$$\mathbf{b_i}^* = \mathbf{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \cdot \mathbf{b_j}^*$$

where $\mu_{ij} = \langle \mathbf{b_i}, \mathbf{b_j}^* \rangle / \langle \mathbf{b_j}^*, \mathbf{b_j}^* \rangle$

We also have have: $\mathbf{b_i} = \mathbf{b_i}^* + \sum_{j=1}^{i-1} \mu_{ij} \cdot \mathbf{b_j}^*$

Claim: $\det(\mathbf{B}^{*t}\mathbf{B}^*) = \det(\mathbf{B}^t\mathbf{B}) = \|\mathbf{b_1}^*\|^2 \|\mathbf{b_2}^*\|^2 \ldots \|\mathbf{b_n}^*\|^2$

GSO and Short Vectors

Claim:
For basis $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$ and *GSO* $\mathbf{b_1}^*, \mathbf{b_2}^* \ldots, \mathbf{b_n}^*$ we have

$$\|\mathbf{v}\| \geq \min\{\|\mathbf{b_1}^*\|, \|\mathbf{b_2}^*\|, \ldots, \|\mathbf{b_n}^*\|\}$$

for all $\mathbf{v} \in L(\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_{n-1}}, \mathbf{b_n}) / \{\mathbf{0}\}$

Proof:
let $\mathbf{v} = \sum_{i=1}^{k} \lambda_i \mathbf{b_i}$
where k is largest index with non-zero λ_i …

Length Reduced Basis

- An ordered basis $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$ is called *length reduced* if $|\mu_{ij}| \leq ½$
- Algorithm
  - Input: $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$
  - For i = 2,3, … , n
    - For j = i-1,i-2, …1

$$\mathbf{b_i} \leftarrow \mathbf{b_i} - \lceil \mu_{ij} \rfloor \cdot \mathbf{b_j}$$

  - Output: length reduced $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$

Where $\lceil \delta \rfloor = \lfloor \delta + ½ \rfloor$

…length reduced basis

- The step $\mathbf{b_i} \leftarrow \mathbf{b_i} - \lceil \mu_{ij} \rfloor \cdot \mathbf{b_j}$ makes

$$\mu_{ij}^{new} \leftarrow \mu_{ij}^{old} - 1 \cdot \lceil \mu_{ij} \rfloor$$

Hence $|\mu_{ij}^{new}| \leq ½$

Reduced Basis

Definition: Let $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$ be a basis and $\mathbf{b_1}^*, \mathbf{b_2}^*, \ldots, \mathbf{b_n}^*$ its GSO. We say that the basis is *reduced* if

$$\|\mathbf{b_i}^*\|^2 \leq 2\,\|\mathbf{b_{i+1}}^*\|^2 \text{ for } 1 \leq i \leq n$$

Short Vectors and Reduced Basis

Theorem: if $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$ is a *reduced* basis then

$$2^{(n-1)/2}\,\|\mathbf{v}\| \geq \|\mathbf{b_1}\|$$

for all $\mathbf{v} \in L(\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_{n-1}}, \mathbf{b_n}) \setminus \{\mathbf{0}\}$

Proof:

$$\|\mathbf{b_1}\|^2 = \|\mathbf{b_1}^*\|^2 \leq 2\,\|\mathbf{b_2}^*\|^2 \leq 2 \cdot 2\,\|\mathbf{b_3}^*\|^2 \ldots \leq 2^{n-1}\,\|\mathbf{b_n}^*\|^2$$

Hence: $\|\mathbf{v}\| \geq \min\{\|\mathbf{b_1}^*\|, \|\mathbf{b_2}^*\|, \ldots, \|\mathbf{b_n}^*\|\}$

$$\geq \min\{\|\mathbf{b_1}\|, \|\mathbf{b_1}\|/2, \ldots, \|\mathbf{b_1}\|/2^{(n-1)/2}\}$$

$$= \|\mathbf{b_1}\|/2^{(n-1)/2}$$

$\therefore$ In a reduced basis $\|\mathbf{b_1}\|$ is a $2^{(n-1)/2}$ approximation to the SVP.

Finding Reduced Basis (LLL)

Input: $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$

- Compute GSO of $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$
- While $i \leq n$
  - For $j = i\text{-}1, i\text{-}2, \ldots 1$ — Replacement step
    $\mathbf{b_i} \leftarrow \mathbf{b_i} - \lceil \mu_{ij} \rfloor \cdot \mathbf{b_j}$
  - If $i > 1$ and $\|\mathbf{b_{i-1}}^*\|^2 > 2\,\|\mathbf{b_i}^*\|^2$ — Exchange step
    exchange $\mathbf{b_{i-1}}$ and $\mathbf{b_i}$ and update GSO. $i \leftarrow i\text{-}1$
  - Else $i \leftarrow i+1$

Output: reduced $\mathbf{b_1}, \mathbf{b_2} \ldots, \mathbf{b_n}$

Run time analysis of algorithm

- Approach: find a quantity that decreases with some operations

let $d_k = \Pi_{i=1}^{k} \|\mathbf{b_i}^*\|^2$

Let $D = \Pi_{i=1}^{n} d_k$

Claim: at a replacement step, for all k d_k is unchanged

Claim: at an exchange step, for all $k \neq i\text{-}1$ d_k is unchanged and $d_{i-1}^{new} \leq \frac{3}{4}\, d_{i-1}^{old}$

$\therefore$ D is reduced by $\frac{3}{4}$ at every exchange step

Applications

- Subset sum or breaking knapsack cryptosystems
- Predicting a linear congruential pseudo-random generator
- Small exponent RSA/Rabin
- Small private exponent
- Factoring polynomials over the integers and rationals
- Simultaneous Diophantine Approximation/rounding
- IP in fixed dimension
- Closest vector problem
- Lattice based cryptosystems

Simultaneous Diophantine Approximation

Given $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{R}$ want good rational approximation with same denominator.

I. e. find $q, p_1, p_2, \ldots, p_n \in \mathbf{Z}$ s.t.

- $|\alpha_i - p_i/q|$ is small
- q is not too large

- Decimal expansion - error ~ $1/q$
- For n=1 continued fraction error ~ $1/q^2$

Simultaneous Diophantine Approximation and SVP

Dirichlet: possible to get $|\alpha_i - p_i/q| \leq 1/q^{1+1/n}$

Find $\beta_1, \beta_2, \ldots, \beta_n$ s.t. $\alpha_i \approx \beta_i = u_i/v_i$

For ε fix $Q = 1/\varepsilon^n$ and $w = 1/(\varepsilon^n 2^{n(n+1)/4})$

$$\mathbf{C} = \begin{matrix} w & 0 & 0 & \ldots & 0 \\ \beta_1 & -1 & 0 & \ldots & 0 \\ \beta_2 & 0 & -1 & \ldots & 0 \\ \ldots & & & & \\ \beta_n & 0 & 0 & \ldots & -1 \\ \mathbf{c_0} & \mathbf{c_1} & \mathbf{c_2} & \ldots & \mathbf{c_n} \end{matrix}$$

Simultaneous Diophantine Approximation and SVP

Find reduced basis $\mathbf{b_0}, \mathbf{b_1}, \ldots, \mathbf{b_n}$ for $L(\mathbf{C})$

We know

$$\|\mathbf{b_0}\|^{2(n+1)} \leq \|\mathbf{b_0}\|^2 \cdot 2\|\mathbf{b_1}^*\|^2 \cdot \ldots \cdot 2^n \|\mathbf{b_n}^*\|^2$$
$$= 2^{n(n+1)/2} \|\mathbf{b_0}^*\|^2 \cdot \|\mathbf{b_1}^*\|^2 \cdot \ldots \cdot \|\mathbf{b_n}^*\|^2$$

Since $\mathbf{b_1}^*, \mathbf{b_2}^*, \ldots, \mathbf{b_n}^*$ are orthogonal,

$\|\mathbf{b_0}^*\| \|\mathbf{b_1}^*\| \ldots \|\mathbf{b_n}^*\| = \det(\mathbf{B}^*) = \det(\mathbf{B}) = w$

Hence $\|\mathbf{b_0}\| \leq 2^{n/4} w = \varepsilon$.

Since $\mathbf{b_0} \in L(\mathbf{C})$ we have

$\mathbf{b_0} = q\mathbf{c_0} + \sum_{i=1}^n p_i \mathbf{c_i} = (qw, q\beta_1 - p_1, \ldots, q\beta_n - p_n)$.

Lattice Based Cryptosystems

- Ajtai'96: SVP (approximation) admits a reduction from the *worst* to the average case
- Ajtai-Dwork: a public-key cryptosystem whose security is based on a worst case problem
  - GGH: another cryptosystem (no proof of equivalence)
- Ajtai: SVP is NP-Hard under randomized reductions
  - Hard to approximate within $\sqrt{2}$, [Micciancio]

References

- L. Lovàsz, *An Algorithmic Theory of Numbers, Graphs, and Convexity*
- J. von zur Gathen and and J. Gerhard, *Modern Computer Algebra*
- D. Micciancio,
- Implementation: NTL free library http://www.shoup.net/ntl/