LLL Overview
Lenstra-Lenstra-Lovász lattice basis reduction

Curtis Bright

July 31, 2008
Lattices

• Let $b_1, b_2, \ldots, b_n$ be linearly independent vectors in $\mathbb{R}^n$.

• The lattice $L \subset \mathbb{R}^n$ generated by $b_1, b_2, \ldots, b_n$ is:

$$L = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\}$$

• $b_1, b_2, \ldots, b_n$ is a basis of $L$. When $n > 1$, infinitely many bases exist.
Lattice Volume

- The basis vectors form an $n$-dimensional parallelootope:

$$P = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in [0, 1) \right\}$$

- Define $\text{vol}(L)$ to be the volume of $P$:

$$\text{vol}(L) = |\det(b_1 \ b_2 \cdots \ b_n)|$$

- This is independent of the choice of basis of $L$. 
**Theorem** (Hadamard’s Inequality). Let $b_1, \ldots, b_n$ be a basis of $L$. Then

$$\text{vol}(L) \leq \prod_{i=1}^{n} \|b_i\|$$

with equality if and only if the basis vectors are orthogonal.

- Intuitively, the amount of nonorthogonality of a basis is measured by $\prod_{i=1}^{n} \|b_i\|$. 
Hermite’s Constant(s)

Theorem (Hermite). There exists a constant \( \gamma_n \) such that all lattices of dimension \( n \) have some basis \( b_1, \ldots, b_n \) which satisfies

\[
\prod_{i=1}^{n} \|b_i\| \leq \sqrt{\gamma_n^n \text{vol}(L)}.
\]

- Langrange had previously given an algorithm to find a basis \( b_1, b_2 \) of any lattice \( L \subset \mathbb{R}^2 \) such that

\[
\|b_1\| \cdot \|b_2\| \leq \sqrt{4/3 \text{vol}(L)}.
\]

Thus, \( \gamma_2 \leq \sqrt{4/3} \).
Langrage’s Algorithm

Input: A basis $b_1, b_2 \in \mathbb{R}^2$ for lattice $L$ with $\|b_1\| \leq \|b_2\|$

Output: A basis of $L$ with $\|b_1\| \leq \|b_2\|$ and $|b_1 \cdot b_2| \leq \|b_1\|^2 / 2$

REPEAT:

Add multiples of $b_1$ to $b_2$ to minimize the projection of $b_2$ on $b_1$

IF $\|b_1\| \leq \|b_2\|$ THEN RETURN $b_1, b_2$
• We have $\|b_1\| \cdot \|b_2\| = \sqrt{4/3 \text{vol}(L)}$ for the basis we just found, and by inspection we see $\|b_1\| \cdot \|b_2\|$ cannot be decreased: therefore $\gamma_2 = \sqrt{4/3}$.

• Hermite generalized this algorithm to find bases $b_1, \ldots, b_n$ of any lattice $L \subset \mathbb{R}^n$ such that

$$\prod_{i=1}^{n} \|b_i\| \leq \sqrt{\gamma_2^{n-1} \text{vol}(L)}.$$ 

Thus, $\gamma_n \leq \gamma_2^{n-1}$.

• In fact, $\gamma_n \in \Theta(n)$: for large $n$, $\frac{n}{2\pi e} < \gamma_n < \frac{n}{\pi e}$. 
Basis Reduction

- Bases with short vectors are easier to work with.

- The best possible basis would have $b_1$ as the shortest nonzero vector in the lattice and in general $b_i$ as the shortest nonzero vector such that $b_1, \ldots, b_i$ is linearly independent.

- Unfortunately, in general finding the shortest nonzero vector of a lattice is an NP-hard problem.

- And it is unknown if the running time of Hermite’s generalized algorithm is polynomial in $n$.

- However, relaxing some of the requirements on the basis will enable us to give an algorithm which is polynomial time in $n$. 
Relaxed Basis Conditions

- Reducing the vector lengths $\|b_i\|$ will also reduce $\prod_{i=1}^{n} \|b_i\|$: good bases tend to be approximately orthogonal.

- We will therefore try to minimize shortness and nonorthogonality.
  - Minimize the projection of $b_i$ on span($b_1, \ldots, b_{i-1}$).
  - Roughly speaking, enforce a condition $\|b_i\| \geq \frac{1}{2} \|b_{i-1}\|$. 
The Gram-Schmidt Process

- Given a basis $b_1, \ldots, b_n$ for $\mathbb{R}^n$, the Gram-Schmidt process finds an orthogonal basis $b_1^*, \ldots, b_n^*$ for $\mathbb{R}^n$ [not $L$].

- Define $\text{proj}_u v = \frac{v \cdot u}{u \cdot u} u$. 
• The orthogonal basis of $\mathbb{R}^n$ is computed as follows:

\[
\begin{align*}
    b_1^* &= b_1 \\
b_2^* &= b_2 - \text{proj}_{b_1^*} b_2 \\
b_3^* &= b_3 - \text{proj}_{b_1^*} b_3 - \text{proj}_{b_2^*} b_3 \\
b_4^* &= b_4 - \text{proj}_{b_1^*} b_4 - \text{proj}_{b_2^*} b_4 - \text{proj}_{b_3^*} b_4 \\
    &\vdots \\
b_i^* &= b_i - \sum_{j=1}^{i-1} \text{proj}_{b_j^*} b_i
\end{align*}
\]

• Intuitively, $b_i^* = \text{proj}_{\text{span}(b_1, \ldots, b_{i-1})^\perp} b_i$.

• Let $\mu_{i,j}$ be the coefficient used in $\text{proj}_{b_j^*} b_i$, i.e., $\mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.

• It is likely $\mu_{i,j} \notin \mathbb{Z}$, so likely $b_i^* \notin L$ for $i > 1$. 
Vector Size Reduction

• We can’t use $b_1^*, \ldots, b_n^*$ as a basis for $L$, but we can modify the Gram-Schmidt process so that all coefficients used will be integers:

\[
\begin{align*}
    b_1 & := b_1 \\
    b_2 & := b_2 - \left\lceil \mu_{2,1} \right\rceil b_1 \\
    b_3 & := b_3 - \left\lceil \mu_{3,1} \right\rceil b_1 - \left\lceil \mu_{3,2} \right\rceil b_2 \\
    b_4 & := b_4 - \left\lceil \mu_{4,1} \right\rceil b_1 - \left\lceil \mu_{4,2} \right\rceil b_2 - \left\lceil \mu_{4,3} \right\rceil b_3 \\
    \vdots \\
    b_i & := b_i - \sum_{j=i-1}^{1} \left\lceil \mu_{i,j} \right\rceil b_j
\end{align*}
\]

• Then the new values of $b_1, \ldots, b_n$ will be a basis for $L$ with $|\mu_{i,j}| \leq \frac{1}{2}$ for all $i > j$. Such a basis is called size-reduced.
Lovász Condition

• It is preferable to have \(\|b_n^*\| \geq \|b_{n-1}^*\| \geq \cdots \geq \|b_1^*\|\).

• Hermite showed every lattice has a size-reduced basis such that \(\|b_i^*\| \geq \frac{1}{\gamma_2} \|b_{i-1}^*\| \) for \(2 \leq i \leq n\). (But without an efficient way to find such a basis...)

• Instead, LLL uses a relaxed version known as the Lovász Condition:

\[
\|b_i^* + \text{proj}_{b_{i-1}^*} b_i \| \geq \frac{1}{\gamma_2} \|b_{i-1}^*\|
\]
LLL Algorithm

Input: A basis \( b_1, \ldots, b_n \in \mathbb{R}^n \) for lattice \( L \)

Output: A basis of \( L \) which is size-reduced and satisfies the Lovász Condition

Initialization: \( k := 2; \) Compute GSO (\( b_i^* \) and \( \mu_{i,j} \))

\[
\text{WHILE } k \leq n \text{ DO }
\]
\[
\text{FOR } i \text{ FROM } k - 1 \text{ TO } 1 \text{ DO }
\]
\[
b_i := b_i - \left\lceil \mu_{k,i} \right\rceil b_i
\]
\[
\mu_{k,j} := \mu_{k,j} - \left\lceil \mu_{k,i} \right\rceil \mu_{i,j} \text{ for } j \leq i
\]
\[
\text{IF Lovász Condition is satisfied (or } k = 1 \text{) THEN }
\]
\[
k := k + 1
\]
\[
\text{ELSE }
\]
\[
\text{Swap } b_k \text{ and } b_{k-1} \text{ and update GSO }
\]
\[
k := k - 1
\]
\[
\text{RETURN } b_1, \ldots, b_n
\]
LLL-reduced Basis Properties

\[ \prod_{i=1}^{n} \|b_i\| \leq \sqrt{2^{n-1}} \sqrt[n]{\text{vol}(L)} \]

- Thus \( \gamma_n \leq 1.41^{n-1} \) (Hermite’s Algorithm gave \( \gamma_n \leq 1.15^{n-1} \)).

- Also, some \( b_i \) will satisfy

  \[ \|b_i\| \leq \sqrt{2^{n-2}} \lambda_1(L) \]

  where \( \lambda_1(L) \) is the shortest nonzero vector of \( L \).