Lecture 19

CS522: Advanced Algorithms

December 6, 2004
Lecturer: Kamal Jain
Notes: Ethan Phelps-Goodman

19.1 Introduction

Today's lecture covers the lattice basis reduction algorithm of Lenstra, Lenstra, and Lovasz (LLL). We prove bounds on the size of the basis vectors, and polynomial runtime. This leads immediately to an approximation algorithm for the Shortest Vector Problem (SVP).

19.2 The LLL Algorithm

The LLL algorithm generalizes the two dimensional Gram-Schmidt Orthogonalization we saw last lecture. Recall that we can assume the lattice L is given to us as a set of basis vectors $\overrightarrow{v_1} \dots \overrightarrow{v_n}$, with $\overrightarrow{v_i} \in \mathbb{Q}^n$ and all $\overrightarrow{v_i}$ linearly independent. We consider the problem of finding the "smallest" set of basis vectors for the same lattice.

19.2.1 Gram-Schmidt Orthogonalization

We work with the n basis vectors as rows in an $n \times n$ matrix. We begin by computing the Gram-Schmidt Orthogonalization of the vectors. This is a rotated basis that has all zeros in the upper diagonal:

$$\begin{bmatrix} v_{11} & & & \\ v_{21} & v_{22} & & \\ \vdots & & \ddots & \\ v_{n1} & & \dots & v_{nn} \end{bmatrix}$$

We use the notation $\overrightarrow{v_{ij}}$ to mean the vector with v_{ij} in the jth position and all other entries 0. To construct a Gram-Schmidt basis we first rotate the basis so that $\overrightarrow{v_1}$ is zero in all but the first coordinate. Then rotate the space so that $\overrightarrow{v_2}$ is zero in all but the first two coordinates, and so on. The entries of the resulting matrix are given by:

$$\begin{aligned} \overrightarrow{v_{11}} &= \overrightarrow{v_1} \\ \overrightarrow{v_{ki}} &= \frac{\overrightarrow{v_k} \cdot \overrightarrow{v_{ii}}}{\|\overrightarrow{v_{ii}}\|^2} \overrightarrow{v_{ii}}, \qquad \forall k > i \\ \overrightarrow{v_{kk}} &= \overrightarrow{v_k} - \sum_{i=1}^{k-1} \overrightarrow{v_{ki}} \end{aligned}$$

We change notation slightly so that the off diagonal entries are written in terms the diagonal entry above them. We write the i, jth entry as $\mu_{ij} v_{jj}$, where $\mu_{ij} = \frac{v_{ij}}{v_{jj}}$. The completed Gram-Schmidt basis has the form:

$$\begin{bmatrix} v_{11} & & & & \\ \mu_{21}v_{11} & v_{22} & & & \\ \mu_{31}v_{11} & \mu_{32}v_{22} & v_{33} & & \\ \vdots & & & \ddots & \\ \mu_{n1}v_{11} & & \dots & & v_{nn} \end{bmatrix}$$

Since this transformation can be done in polynomial time, we will assume from now on that our basis is in this form.

19.2.2 Reduced Bases

The Gram-Schmidt Orthogonalization is then modified to put it in reduced form. These definitions are generalizations of the definitions from last lecture.

Definition 1. *A basis is* weakly reduced *if*

$$|\mu_{ij}| \leq \frac{1}{2} \qquad \forall \quad 1 \leq j < i \leq n.$$

Definition 2. *A basis is* LLL *reduced if it is weakly reduced, and*

$$\|\overrightarrow{v_{ii}}\| \leq \frac{2}{3}\|\mu_{i+1,i}\overrightarrow{v_{i+1,i}} + \overrightarrow{v_{i+1,i+1}}\|$$

Before showing how such a basis can be found in polynomial time we prove some theorems regarding the relationship between the basis vectors and the shortest vector in the lattice.

Lemma 1.

$$\|\textit{shortest vector}\| \geq \min_i(\|\overrightarrow{v_{ii}}\|)$$

Proof. In fact, we will show that any vector in the lattice satisfies this inequality. Consider some vector $b \in L$. We can write

$$\vec{b} = \sum_{i=1}^{k} m_i \overrightarrow{v_i}$$

where k is the index of the largest non-zero term when $\vec{b}$ is written as an integer combination of $\overrightarrow{v_1} \dots \overrightarrow{v_n}$. Then we have

$$\begin{aligned} \|b\| &= \|\sum_{i=1}^{k} m_i \overrightarrow{v_i}\| \\ &= \|\sum_{i=1}^{k-1} m_i \overrightarrow{v_i} + m_k \overrightarrow{v_k}\| \\ &= \|\sum_{i=1}^{k-1} m_i \overrightarrow{v_i} + m_k \sum_{j=1}^{k-1} \overrightarrow{v_{kj}} + m_k \overrightarrow{v_{kk}}\| \\ &\geq \|m_k \overrightarrow{v_{kk}}\|. \end{aligned}$$

The last inequality holds because $\overrightarrow{v_{kk}}$ is perpendicular to the rest of the vectors. The lemma follows, since $m_k \in \mathbb{Z}$ and $m_k \neq 0$ by assumption. □

The following two lemmas will help us to prove later theorems.

Lemma 2.

$$\|\overrightarrow{v_{ii}}\| \leq \sqrt{2}\|\overrightarrow{v_{i+1,i+1}}\|$$

Proof. This is a simple generalization of the proof from last lecture that $\|\overrightarrow{v_{11}}\| \leq \sqrt{2}\|\overrightarrow{v_{22}}\|$. □

Lemma 3.

$$\|\overrightarrow{v_{11}}\| \leq 2^{\frac{k-1}{2}}\|\overrightarrow{v_{kk}}\|$$

Proof. This follows from induction on i using the previous lemma. □

Lemma 1 gave lower bounds for the shortest vector. We can give better bounds in terms of the first vector in the reduced basis.

Theorem 1.

$$\|\overrightarrow{v_1}\| \leq 2^{\frac{n-1}{2}}\|\textit{shortest vector}\|$$

Proof.

$$\begin{aligned}
\|\overrightarrow{v_1}\| &\leq 2^{\frac{k-1}{2}}\|\overrightarrow{v_{kk}}\| \\
&\leq 2^{\frac{n-1}{2}}\|\overrightarrow{v_{kk}}\| \\
&\leq 2^{\frac{n-1}{2}}\min_i \overrightarrow{v_{ii}} \\
&\leq 2^{\frac{n-1}{2}}\|\text{shortest vector}\|
\end{aligned}$$

□

Theorem 2.

$$\|\overrightarrow{v_{11}}\| \leq 2^{\frac{n-1}{4}}\sqrt[n]{\det(L)}$$

Proof. From lemma 3, for $1 \leq k \leq n$ we can write:

$$\begin{aligned}
\|\overrightarrow{v_1}\| &\leq 2^0\|\overrightarrow{v_{11}}\| \\
\|\overrightarrow{v_1}\| &\leq 2^{\frac{1}{2}}\|\overrightarrow{v_{22}}\| \\
&\vdots \\
\|\overrightarrow{v_1}\| &\leq 2^{\frac{n-1}{2}}\|\overrightarrow{v_{nn}}\|
\end{aligned}$$

Multiplying these n equations together, we get

$$\begin{aligned}
\|\overrightarrow{v_1}\|^n &\leq 2^0 2^{\frac{1}{2}} \cdots 2^{\frac{n-1}{2}}\|\overrightarrow{v_{11}}\|\|\overrightarrow{v_{22}}\| \cdots \|\overrightarrow{v_{nn}}\| \\
&= 2^{\frac{n(n-1)}{4}}\det(L)
\end{aligned}$$

Taking the nth root gives the desired inequality. □

Theorem 2 actually implies theorem 1, but we did not have time to cover this in class. A consequence of this implication is that if you have

$$\|\overrightarrow{v_1}\| \leq f\sqrt[n]{\det(L)}$$

for some f, then you automatically have

$$\|\overrightarrow{v_1}\| \leq f^2\|\text{shortest vector}\|.$$

19.2.3 Proving Polynomial Runtime

Theorem 3. *Given a lattice L, an LLL reduced basis for L can be found in polynomial time.*

Proof. First we show that a weakly reduced basis can be found quickly. Recall that a basis is not weakly reduced if $|\mu_{ij}| > \frac{1}{2}$ for some i, j. To correct this entry we can simply subtract off $\overrightarrow{v_j}$ from $\overrightarrow{v_i}$ until $\mu_{ij} \leq \frac{1}{2}$. This is accomplished by

$$\overrightarrow{v_i} \longleftarrow \overrightarrow{v_i} - [\mu_{ij}]\overrightarrow{v_j}$$

where $[\mu_{ij}]$ is the closest integer to μ_{ij}. This leaves all entries of $\overrightarrow{v_i}$ to the right of j unchanged, but it will change the entries to the left. By repeated application from right to left, and top to bottom, we can get a weakly reduced basis in polynomial time.

This shows how to find a weakly reduced basis. The second constraint is that $\|\overrightarrow{v_{ii}}\| \leq \frac{2}{3}\|\mu_{i+1,i}\overrightarrow{v_{i+1,i}} + \overrightarrow{v_{i+1,i+1}}\|$. If this constraint is broken at some i, we simply swap rows i and $i+1$. The complete algorithm is just an alternating sequence of swapping rows and computing the weakly reduced basis. The process stops when no constraints are violated.

To prove that this process terminates in polynomial time, we introduce a potential function ϕ. Let

$$\phi = \prod_{i=1}^{n} |v_{ii}|^{n-i}.$$

We consider the change in ϕ after rows are swapped, which we denote $\frac{\phi^{new}}{\phi^{old}}$. Note that only rows i and $i+1$ change after the swap, so all other rows cancel out, leaving only

$$\begin{aligned} \frac{\phi^{new}}{\phi^{old}} &= \frac{|v_{ii}^{new}|^{n-1}|v_{i+1,i+1}^{new}|^{n-(i+1)}}{|v_{ii}^{old}|^{n-1}|v_{i+1,i+1}^{old}|^{n-(i+1)}} \\ &= \frac{\overrightarrow{v_{ii}}^{new}}{\overrightarrow{v_{ii}}^{old}} \end{aligned}$$

Since the vectors differed by a factor of $\frac{2}{\sqrt{3}}$ before the swap, so get

$$\frac{\phi^{new}}{\phi^{old}} \leq \frac{\sqrt{3}}{2}.$$

Thus ϕ decreases exponentially in the number of swaps. To prove a polynomial runtime we need to show that the separation between our starting ϕ and our terminating ϕ is at most exponential.

We assume without loss of generality that our original basis is integral. Then

$$\begin{aligned} \phi &= \prod_{i=1}^{n} |v_{ii}|^{n-i} \\ &\leq \prod_{i=1}^{n} \|\overrightarrow{v_i}\|^{n-i} \\ &\leq \prod_{i=1}^{n} \|\vec{v}\|_{max}^{n-i} \\ &= \|\vec{v}\|_{max}^{\frac{n(n-1)}{2}} \end{aligned}$$

This gives an exponential upper bound on ϕ. All that remains is to show that ϕ does not get too small and we'll have a polynomial runtime. First, note that we can write ϕ in terms of the determinate. Let V_k be the first k rows and columns of our basis matrix. Then

$$\begin{aligned}\phi &= \prod_{i=1}^{n} |v_{ii}|^{n-i} \\ &= (|v_{11}|)(|v_{11}||v_{22}|)\cdots(|v_{11}|\ldots|v_{nn}|) \\ &= \det(V_1)\det(V_2)\ldots\det(V_n) \\ &= \prod_{i=1}^{n} \det(V_i)\end{aligned}$$

Since determinates are invariant under change of basis, and our original basis was integeral, ϕ must be integral, and in particular, $\phi \geq 1$. Thus in a polynomial number of steps ϕ will hit its lower bound and the algorithm will terminate.

□

19.2.4 Tight bounds

The following example shows that the exponential bound on the shortest vector approximation is tight.

Let $\rho = \frac{\sqrt{3}}{2}$. Consider the basis

$$\begin{bmatrix} 1 & & & & & \\ \frac{1}{2} & \rho & & & & \\ \frac{1}{2} & \frac{\rho}{2} & \rho^2 & & & \\ \vdots & & & \ddots & & \\ \frac{1}{2} & \frac{\rho}{2} & \frac{\rho^2}{2} & \cdots & \frac{\rho^{n-1}}{2} & \rho^n \end{bmatrix}$$

This basis satisfies both conditions of an LLL basis. The LLL algorithm therefore outputs 1 as the length of the shortest vector. However, the vector

$$\overrightarrow{v_n} - \overrightarrow{v_{n-1}} = (0, \ldots, -\frac{\rho^{n-1}}{2}, \rho^n)$$

has length exponentially smaller than 1.