CSE 206A: Lattice Algorithms and Applications Spring 2007

Lecture 8 : The dual lattice and reducing SVP to MVP

Lecturer: Daniele Micciancio *Scribe: Scott Yilek*

1 Overview

In the last lecture we explored the reductions between the closest vector and shortest vector problems (both the search and optimization versions). Today, we show that SVP can actually be reduced to a related problem called the *Minkowski's Vector Problem* (or MVP for short). Specifically, we will show that

$$\text{SVP}_{\gamma'} \Rightarrow \text{MVP}_{\gamma}$$

(notice the approximation factor is different).

The MVP_γ problem is as follows. Given a basis $\mathbf{B}$ for some lattice, find a lattice point $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{v}\| \leq \gamma \cdot \sqrt{n} \cdot \det(\mathbf{B})^{1/n}$.

2 The Dual Lattice

To show that $\text{SVP}_{\gamma'}$ reduces to MVP_γ, we will make use of something called the *Dual Lattice*. The dual of a lattice will have many interesting applications.

2.1 Definition

The dual of a lattice is the set of linear functions from lattice points to integers. More formally, for any lattice L, the dual lattice $L^* = \{f : L \to \mathbb{Z} \mid f \text{ is linear}\}$. When we say that "$f$ is linear" we mean that $f(a\mathbf{x} + b\mathbf{y}) = af(\mathbf{x}) + bf(\mathbf{y})$.

This gives rise to a different definition of the dual lattice:

$$L^* = \{\mathbf{v} \in \text{span}(\mathbf{B}) \ : \ \langle \mathbf{v}, \mathbf{x} \rangle \in \mathbb{Z} \ \forall \mathbf{x} \in L\} \tag{1}$$

since every linear f can be written as $f_{\mathbf{v}}(\mathbf{x}) = \langle \mathbf{v}, \mathbf{x} \rangle$. This can be seen easily as follows:

$$\begin{aligned} f(\mathbf{Bx}) &= \sum x_i \cdot f(\mathbf{b}_i) \\ &= \langle \mathbf{x}, [f(\mathbf{b}_1), \ldots, f(\mathbf{b}_n)] \rangle \\ &= \langle \mathbf{Bx}, \mathbf{B} \cdot (\mathbf{B}^\mathsf{T}\mathbf{B})^{-1} f(\mathbf{B}) \rangle \\ &= (\mathbf{Bx})^\mathsf{T} \cdot \underbrace{(\mathbf{B} \cdot (\mathbf{B}^\mathsf{T}\mathbf{B})^{-1} \cdot f(\mathbf{B}))}_{\text{in the linear span}} \end{aligned}$$

We can simplify the definition one step further by only considering basis vectors instead of arbitrary $\mathbf{x} \in L$:

$$L^* = \{\mathbf{v} \in \text{span}(\mathbf{B}) \ : \ \langle \mathbf{v}, \mathbf{b}_i \rangle \in \mathbb{Z}\} \tag{2}$$

To see that the definitions are equivalent, one direction is trivial, since each $\mathbf{b}_i \in L$. Thus this definition is clearly weaker than the other. To see the other direction, consider the product of an arbitrary lattice vector with $\mathbf{v}$:

$$\langle \sum \mathbf{b}_i \cdot a_i \rangle = \sum a_i \cdot \langle \mathbf{b}_i, \mathbf{v} \rangle$$

Since each $a_i \in \mathbb{Z}$, then if $\langle \mathbf{b}_i, \mathbf{v} \rangle \in \mathbb{Z}$, every lattice vector $\mathbf{x}$ will be such that $\langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}$.

2.2 Some Examples

To aid in understanding the dual of a lattice, we will give some simple examples.
Example 1:
Let $L = \mathbb{Z}^n$ (each lattice point is a vector of n integers). Then, the dual lattice is simply $L^* = \mathbb{Z}^n = L$.
Example 2:
Consider the lattice $L = 2 \cdot \mathbb{Z}^n$. The dual of this lattice is $L^* = \frac{1}{2}\mathbb{Z}^n$. This is easy to see if we think of the lattice $\mathbb{Z}^n$ as having basis $I = [e_1, \ldots, e_n]$ (where e_i is the corresponding column in the identity matrix). Then, any $x \in L^*$ must be such that $\langle x, 2e_i \rangle \in \mathbb{Z}$.
Example 3:
$L = \{x \in \mathbb{Z}^n \ : \ \sum x_i \text{ is even}\}$. It can be easily checked that the dual lattice is $\mathbb{Z}^n + (\frac{1}{2}, \ldots, \frac{1}{2})^T$, i.e., the union of two copies of the integer lattice shifted by the all $\frac{1}{2}$ vector.

The lattice in the last example is called the 'checkerboard lattice' for its look in 2 dimensions. In dimension 2, the checkerboard lattice is just a rotated and scaled copy of $\mathbb{Z}^2$. (Recall that a rotation matrix is such that $Q^\mathsf{T}Q = I$.) This gives a very simple way to compute the dual of the 2-dimensional checkerboard lattice.

Our examples give us a couple of simple, yet useful, theorems about the dual of a lattice

Theorem 1 *For a scalar c and lattice L, $(cL)^* = 1/cL^*$.*

Theorem 2 *For rotation matrix Q and lattice L, $(QL)^* = QL^*$.*

3 Properties of the dual

We will prove some important properties of the dual of a lattice. The first will give us a general formula to compute a basis for the dual given a basis for the original lattice.

Claim 1 *For any lattice L generated by basis $\mathbf{B}$, the dual L^* has basis $\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1}$. As a special case, when the lattice is full rank, the dual basis can be computed more simply as the inverse transpose of $\mathbf{B}$.*

This claim says that $\mathcal{L}(\mathbf{B})^* = \mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})$. To prove the claim we will first show that lattice points $\mathbf{v} \in \mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})$ are such that $\langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}$ for $\mathbf{x} \in \mathcal{L}(\mathbf{B})$. Consider $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^k$. Then,

$$\begin{aligned} \langle \mathbf{B}\mathbf{y}, \mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1}\mathbf{x} \rangle &= \mathbf{y}^\mathsf{T}\mathbf{B}^\mathsf{T}\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1}\mathbf{x} \\ &= \mathbf{y}^\mathsf{T}\mathbf{x} \in \mathbb{Z} \end{aligned}$$

For the other direction, we will consider some $\mathbf{x}' \in \mathbb{R}^n$, and show that if $\mathbf{Bx}'$ is in $\mathcal{L}(\mathbf{B})^*$, then it is also in $\mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})$

$$\mathbf{Bx} \in \mathcal{L}(\mathbf{B})^* \Rightarrow \mathbf{Bx} = \mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1} \underbrace{(\mathbf{B}^\mathsf{T}\mathbf{B})\mathbf{x}}_{\in \mathbb{Z}^k} \in \mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})$$

where $(\mathbf{B}^\mathsf{T}\mathbf{B})\mathbf{x} \in \mathbb{Z}^k$ since $\mathbf{Bx}$ is in the dual lattice and thus $(\mathbf{B}^\mathsf{T}\mathbf{B})\mathbf{x} = \langle \mathbf{B}, \mathbf{v} \in \mathcal{L}(\mathbf{B})^* \rangle \in \mathbb{Z}$.

Claim 2 *For any lattice $L = \mathcal{L}(\mathbf{B})$ the dual of the dual lattice is the oribinal lattice, i.e., $L^{**} = L$. Also, the determinant of the dual lattice is* $\det(L)^* = (\det(L))^{-1}$

Both properties easily follow from the formula for the dual basis. For the first claim, if we apply the formula twice we get

$$\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}((\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1})^T(\mathbf{B}(\mathbf{B}^T\mathbf{B})^{-1}))^{-1} = \mathbf{B}.$$

To prove the second claim, consider the determinant of the dual lattice $\mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})$:

$$\begin{aligned}
\det(\mathcal{L}(\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})) &= \sqrt{\det((\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})^\mathsf{T}\mathbf{B}(\mathbf{B}^\mathsf{T}\mathbf{B})^{-1})} \\
&= \sqrt{\det((\mathbf{B}^\mathsf{T}\mathbf{B})^{-\mathsf{T}})} \\
&= (\sqrt{\det((\mathbf{B}^\mathsf{T}\mathbf{B})^\mathsf{T})})^{-1} \\
&= (\sqrt{\det(\mathbf{B}^\mathsf{T}\mathbf{B})})^{-1} \\
&= \det(\mathcal{L}(\mathbf{B}))^{-1}
\end{aligned}$$

4 Reducing SVP to MVP

Now that we've seen some examples of the dual of a lattice and some of its properties, we will use it to find an approximate shortest vector. Before we get to the reduction, consider any lattice L, its dual L^*, and a vector $\mathbf{v} \in L^*$. We can represent L as a union of sets:

$$L = \bigcup L_i$$

where $i \in \mathbb{Z}$ and $L_i = \{\mathbf{x} \in L \ : \ \langle \mathbf{x}, \mathbf{v} \rangle = i\} \subseteq \{\mathbf{x} \in \text{span}(L) \ : \ \langle \mathbf{x}, \mathbf{v} \rangle = i\}$. When $\mathbf{v}$ is a primitive vector in L^*, each L_i is equal to a shifted copy $L_0 + c_i \cdot \mathbf{v}/\|\mathbf{v}\|^2$ of the lattice L_0. (If $\mathbf{v}$ is not a primitive vector, i.e., $\mathbf{v} = c\mathbf{v}'$ is a multiple of some other lattice vector $\mathbf{v}' \in L^*$, then $\langle \mathbf{x}, \mathbf{v} \rangle = c\langle \mathbf{x}, \mathbf{v}' \rangle \in c\mathbb{Z}$, and L_i is nonempty only when i is a multiple of c.)

This means that the hyperplanes are distance $1/\|\mathbf{v}\|$ apart. A depiction can be seen in Figure 1.

Now we wish to reduce the Shortest Vector Problem to the Minkowski Vector Problem. Say that we have an algorithm M for the Minkowski Vector Problem (with approximation factor γ). Given a lattice $L = \mathcal{L}(\mathbf{B})$, we get

$$\begin{aligned}
M(\mathcal{L}(\mathbf{B})) &= \mathbf{x} \text{ such that } \|\mathbf{x}\| \leq \gamma\sqrt{n}\det(\mathcal{L}(\mathbf{B}))^{1/n} \\
M(\mathcal{L}(\mathbf{B})^*) &= \mathbf{y} \text{ such that } \|\mathbf{y}\| \leq \gamma\sqrt{n}\det(\mathcal{L}(\mathbf{B})^*)^{1/n}
\end{aligned}$$

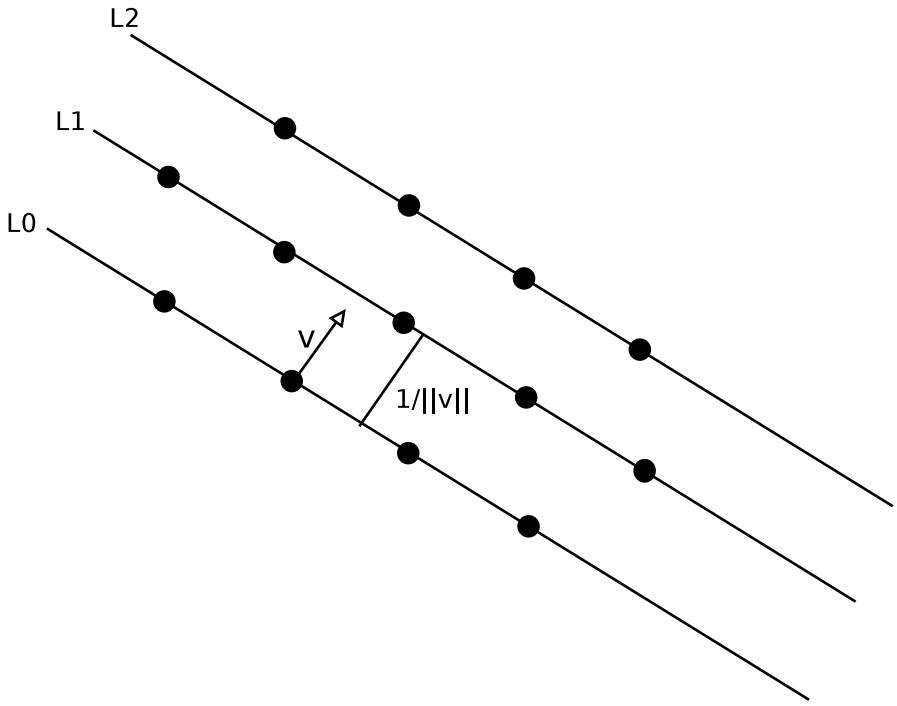

Figure 1: Each L_i represents a hyperplane in the lattice, each $1/\|\mathbf{v}\|$ apart.

From the previous section we know the determinant of the dual is the inverse of the determinant of the original lattice, so

$$M(\mathcal{L}(\mathbf{B})^*) = \mathbf{y} \leq \gamma\sqrt{n}\det(\mathbf{B})^{-1/n}$$

and thus

$$\|\mathbf{x}\|\|\mathbf{y}\| \leq n\gamma^2. \tag{3}$$

Rearranging the equation gives us $1/\|\mathbf{y}\| \geq \|\mathbf{x}\|/n\gamma^2$. From this we can see that if $\|\mathbf{x}\|$ is small, then we have a short vector. On the other hand, if $\|\mathbf{x}\|$ is large, then the hyperplanes are far apart (i.e. $1/\|\mathbf{y}\|$ is large).

4.1 The Algorithm

Our algorithm for SVP is recursive and is as follows. Given as input $\mathbf{B}$, let $\mathbf{x} = M(\mathbf{B})$ and $\mathbf{y} = M(\mathbf{B}^*)$. Then let $\mathcal{L}(\mathbf{B}') = \{\mathbf{v} \in \mathcal{L}(\mathbf{B}) : \langle \mathbf{v}, \mathbf{y} \rangle = 0\}$. This lattice consists of points along a single hyperplane (L_0 from our picture above). Now, we let $\mathbf{x}' = \text{SVP}(\mathbf{B}')$, the result of a recursive call to our algorithm (note that $\mathbf{B}'$ has decreased dimension by 1). The algorithm outputs the shorter of $\mathbf{x}$ and $\mathbf{x}'$.

To prove the correctness of our algorithm, consider 2 cases.

Case 1: $\lambda_1(\mathbf{B}) = \lambda_1(\mathbf{B}')$
In this case the shortest vector lies on the hyperplane and we make a recursive call to get

$\mathbf{x}'$. It follows that

$$\begin{aligned} \|\mathbf{x}'\| &\leq \gamma^2(n-1)\lambda_1(\mathbf{B}') \\ &\leq \gamma^2(n-1)\lambda_1(\mathbf{B}) \\ &\leq \gamma^2 n\lambda_1(\mathbf{B}) \end{aligned}$$

Case 2: $\lambda_1(\mathbf{B}) \geq 1/\|\mathbf{y}\|$
From this (combined with (3)) we get

$$\|\mathbf{x}\| \leq \frac{n\gamma^2}{\|\mathbf{y}\|} \leq n\gamma^2\lambda_1(\mathbf{B})$$

5 Conclusion

We have seen how to approximate SVP given an algorithm for approximating MVP. This technique makes use of the dual lattice, an object which will be useful in other contexts (like the homework) as well. A similar technique to the one in this lecture can be used to reduce CVP to SVP, as we will see in the next lecture.