

Notes for Lecture 11

Lattice Basis Reduction:

Recall that for an input basis (b_1, b_2, \dots, b_n) , the Gram-Schmidt process produces an orthogonal basis $(b_1^*, b_2^*, \dots, b_n^*)$ such that for all $i > j$:

$$\begin{aligned} b_i^* &= b_i - \sum_{j < i} \mu_{i,j} b_j^* \\ \mu_{i,j} &= \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)} \\ \text{span}(b_1, b_2, \dots, b_i) &= \text{span}(b_1^*, b_2^*, \dots, b_i^*) \end{aligned}$$

Here (x, y) is the inner product of the vectors x and y .

A basis is *reduced* if the following holds for all $i > j$:

$$|\mu_{i,j}| \leq \frac{1}{2} \tag{1}$$

$$|b_{i-1}^*| \leq \frac{4}{3} |b_j^* + \mu_{i,i-1} b_{j-1}^*|^2 \tag{2}$$

- (1) Implies that the basis vectors are not too far from being orthogonal.
- (2) Implies $|b_{i-1}^*|^2 \leq 2|b_i^*|^2$, which says that vectors do not get too much shorter as we progress.

Lenstra-Lenstra-Lovász Algorithm

First we define a subroutine PIVOT(i, j) which modifies b_i such that:

$$\begin{aligned} b_i &= b_i - t b_j^* \\ t &= \lfloor (b_i, b_j^*) / (b_j^*, b_j^*) + 0.5 \rfloor \end{aligned}$$

```

LLL-ALG ( $b_1, b_2, \dots, b_n$ )
 $b_1^* = b_1$ 
 $k = 2$ 

(*) invariant assertion, for  $i \leq k - 1, j < i$ :

$$\begin{cases} \mu_{i,j} \leq \frac{1}{2} \\ |b_{i-1}^*|^2 \leq \frac{4}{3}|b_i^*|^2 + \mu_{i,i-1}|b_{i-1}^*|^2 \\ b_1^*, \dots, b_{k-1}^* \text{ are known} \end{cases}$$


PIVOT( $k, k - 1$ )
COMPUTE  $b_k^*$ 
if  $|b_{k-1}^*|^2 > \frac{4}{3}|b_k^*|^2 + \mu_{k,k-1}|b_{k-1}^*|^2$  then
    SWAP( $b_k, b_{k-1}$ )
     $k = k - 1$ 
    go to (*)
else
    for  $l = k - 2$  to  $1$  do
        PIVOT( $k, l$ )
        COMPUTE  $b_k^*$ 
    if  $k < n$  then
         $k = k + 1$ 
        go to (*)
return ( $b_1, \dots, b_n$ )

```

Notice throughout the algorithm the value of k may increase or decrease, so we need to show a proof of termination.

Proof of Termination:

First we define a potential function:

$$\begin{aligned} \Phi(b_1, \dots, b_n) &= |b_1^*|^{2n} |b_2^*|^{2(n-1)} \dots |b_n^*|^2 \\ &\leq |b_1|^{2n} |b_2|^{2(n-1)} \dots |b_n|^2 \end{aligned}$$

Now, we note that with every swap we decrease the potential by a factor of $3/4$ and otherwise the potential does not change. The final potential has a value of at least 1, so the maximum number of interchanges is:

$$2n \log_{4/3}(|b_1| |b_2| \dots |b_n|)$$

The running time of the algorithm (in bit operations) is $O(n^6 (\log \beta)^3)$, where $\beta = \max_j |b_j|^2$.

Feasibility of Integer Programs

Theorem 1 (Lenstra) *For fixed n , integer programming feasibility in \mathbb{R}^n is in \mathbf{P} .*

For some polyhedron $K = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ we want to know if $K \cap \mathbb{Z}^n \neq \emptyset$. Or in other words, is there a feasible integer solution.

We make the following assumptions:

- K is bounded and has positive volume.
- There exists a linear transformation $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that $\exists p, r, R$ which satisfy:

$$B(P, r) \subseteq T(K) \subseteq B(P, R), \text{ and } \frac{R}{r} \leq c_1$$

Where $B(c, \rho)$ is the ball centered at c with radius ρ .

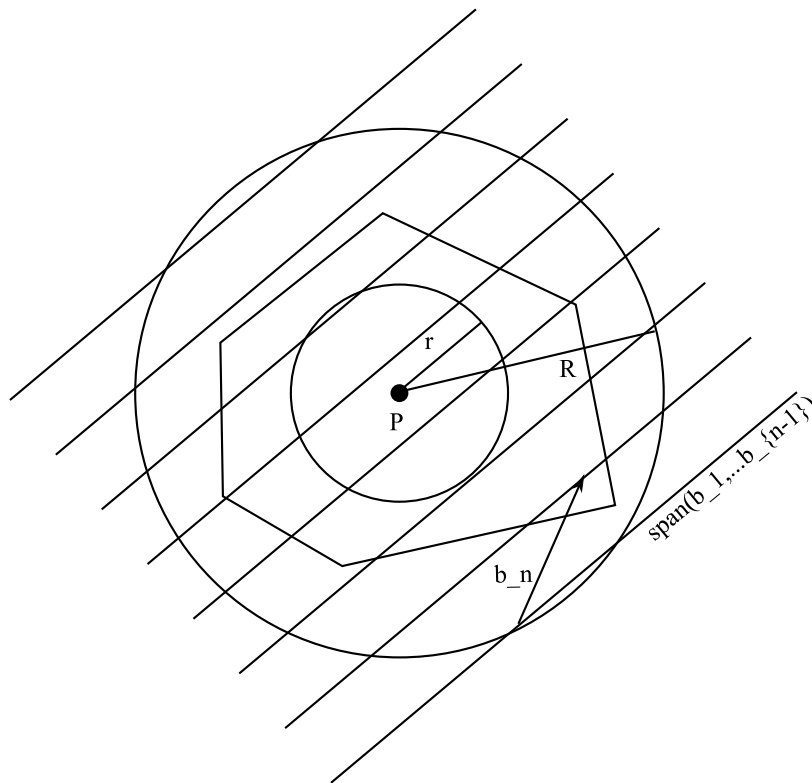
Under the transformation T the image of \mathbb{Z}^n is a lattice L with basis $\{T(e_1), T(e_2), \dots, T(e_n)\}$, where e_i is the i th unit vector. The question we are now asking is whether or not $T(K) \cap L \neq \emptyset$.

First we construct a reduced basis $\{b_1, \dots, b_n\}$ which we recall satisfies the inequality:

$$|b_1| |b_2| \dots |b_n| \leq c_2 \det(L)$$

Previously c_2 was a function exponential in n , however we are now holding n constant.

We can picture the reformulated problem as:



Here L is a set of parallel $(n - 1)$ -dimensional hyperplanes.

In this new space we will show that either:

Case 1 We can trivially find a feasible solution.

Case 2 The number of parallel hyperplanes intersection $B(P, R)$ is bound by a constant, and we can test for feasibility within each of those $(n - 1)$ dimensional hyperplanes.

First we need a lemma:

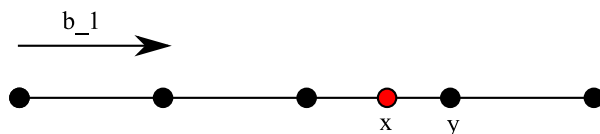
Lemma 2 For any point $x \in \mathbb{R}^n$ we can find a point $y \in L$ such that

$$|x - y|^2 \leq \frac{1}{4}(|b_1|^2 + |b_2|^2 + \dots + |b_n|^2)$$

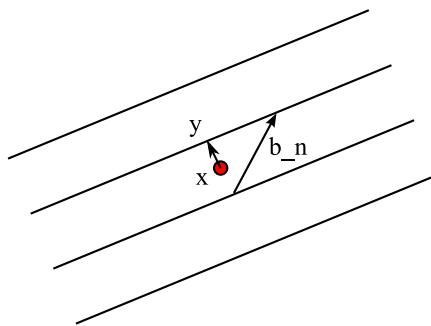
PROOF: We will use induction on n .

Base case, $n = 1$. We take y as the lattice point nearest to x . So clearly,

$$|x - y| \leq \frac{1}{2}|b_1|$$



Induction step, assume true for $n - 1$. In the n dimensional case project y onto the closest $n - 1$ hyperplane, which will be closer than $\frac{1}{2}|b_n|$.



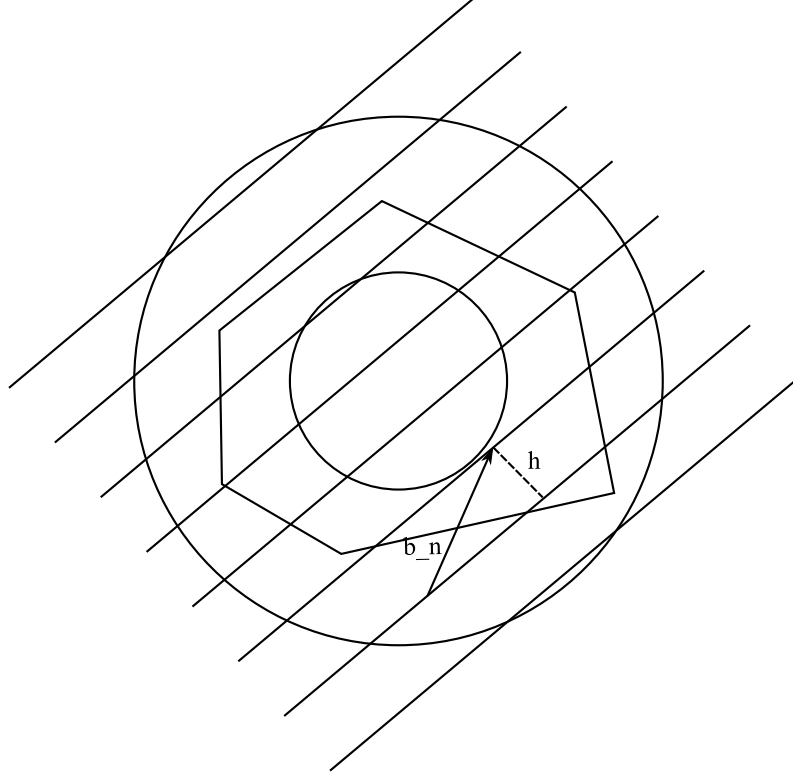
□

We now apply this construction to P , the center of the balls. Assume $|b_n| = \max_i |b_i|$.

$$\begin{aligned} |P - y|^2 &\leq \frac{1}{4}(|b_1|^2 + \dots + |b_n|^2) \\ &\leq \frac{1}{4}n|b_n|^2 \\ |P - y| &\leq \sqrt{n}|b_n| \end{aligned}$$

Case 1 $\frac{1}{2}\sqrt{2}|b_n| \leq r$, which implies a feasible solution exists inside the smaller ball.

Case 2 $\frac{1}{2}\sqrt{2}|b_n| > r$, in this case we wish to show a bound on the number of hyperplanes that intersect the ball of radius R . We will then recursively solve an integer programming feasibility problem on each of these hyperplanes.



Let t equal the number of hyperplanes intersecting the ball. So we have:

$$t - 1 \leq \frac{2R}{h}$$

Using the facts that $\frac{R}{r} \leq c_1$ and $r < \frac{1}{2}\sqrt{n}|b_n|$ we get:

$$2R \leq c_1\sqrt{n}|b_n|$$

Now for a lower bound on h we use the fact that (b_1, \dots, b_n) is a reduced basis and define L' as the basis spanned by (b_1, \dots, b_{n-1}) .

$$\begin{aligned} |b_1||b_2| \dots |b_n| &\leq c_2 \det(L) \\ &= c_2 h \det(L') \\ &\leq c_2 h |b_1| \dots |b_{n-1}| \end{aligned}$$

Which finally implies

$$h \geq \frac{|b_n|}{c_2}$$

Substituting into the expression for t we get the bound:

$$\begin{aligned} \frac{2R}{h} &\leq \frac{c_1 \sqrt{n} |b_n|}{|b_n|/c_2} \\ &= c_1 c_2 \sqrt{n} \end{aligned}$$

This is constant for fixed n .

By induction, our recursive algorithm for integer programming runs in polynomial time in any fixed number of dimensions.