Discrete Math, Tenth Problem Set (July 11)

REU 2003

Instructor: Laszlo Babai
Scribe: D. Jeremy Copeland

1 Orthogonality defect

Exercise 1.1 (Hadamard inequality). Show that if $\{\mathbf{b}_1, \cdots \mathbf{b}_n\}$ is a basis of $\mathbb{R}^n$, then

$$|\det(\mathbf{b}_1 \cdots \mathbf{b}_n)| \leq \prod_{i=1}^{n} \|\mathbf{b}_i\|$$

Exercise 1.2. Show that in the previous exercise, there is equality if and only if the basis is orthogonal.

Definition 1.3. The **orthogonality defect** of a basis $\{\mathbf{b}_1, \cdots \mathbf{b}_n\}$ is defined as the quantity:

$$\frac{\prod_{i=1}^{n} \|\mathbf{b}_i\|}{|\det(\mathbf{b}_1 \cdots \mathbf{b}_n)|}$$

The following theorem is left as a challenge to the reader.

Theorem 1.4. *Every lattice has a basis with orthogonality defect less than n^n.*

2 Short vectors

We would like to talk about finding a short vector in a lattice. Thus we need a notion of shortness.

Definition 2.1. The **infinity norm** of a vector, x, with coordinates x_i is:

$$\|x\|_\infty := \max(|x_i|).$$

Definition 2.2. The $\mathbf{L}_2$ **norm** of a vector, x, with coordinates x_i is:

$$\|x\|_{\mathrm{L}_2} = \|x\|_2 := (\sum x_i^2)^{1/2}.$$

Whenever we write $\|x\|$, we implicitly mean $\|x\|_2$. In order to move between these notions, we need the following:

Exercise 2.3.

$$\|x\|_\infty \leq \|x\|_2 \leq n^{1/2}\|x\|_\infty.$$

Definition 2.4. Let $\omega_\mathbf{n}$ denote the volume of the unit ball in $\mathbb{R}^n$.

Exercise$^+$ 2.5.

$$\omega_n = \frac{\pi^{n/2}}{(n/2)!},$$

where for odd $n = 2k+1$, the value of $(n/2)!$ is interpreted as

$$\left(k + \frac{1}{2}\right)! = \frac{\sqrt{\pi}}{4^k} \cdot \frac{(2k+1)!}{k!}.$$

Exercise 2.6. Prove that Stirling's formula extends to the factorials of half-integers:

$$\left(\frac{n}{2}\right)! \sim \left(\frac{n}{2\mathrm{e}}\right)^{n/2} \sqrt{\pi n}.$$

Exercise 2.7. Prove: $\omega_n^{1/n} \sim \sqrt{2\pi \mathrm{e}/n}.$

The factorial function is extended to all complex numbers except the negative integers by the Gamma function defined by

$$\Gamma(z) = \int_0^\infty t^{z-1}\mathrm{e}^{-t}dt.$$

This function is related to factorials (including the factorial of half-integers as defined above) by the identity $x! = \Gamma(x+1)$. Stirling's formula holds for positive real values $x \to \infty$:

$$\Gamma(x+1) \sim (x/\mathrm{e})^x\sqrt{2\pi x}.$$

The Gamma function satisfies the identity $\Gamma(z+1) = z\Gamma(z)$ and $\Gamma(3/2) = (1/2)! = \sqrt{\pi}/2$.

Exercise 2.8. From the value given for $\Gamma(3/2)$ and the identity $\Gamma(z+1) = z\Gamma(z)$, deduce the value given above for the factorials of half-integers.

Check out "Eric Weisstein's world of mathematics" about the amazing world of the Gamma function at `http://mathworld.wolfram.com/GammaFunction.html`.

Applying Minkowski's theorem to spheres and cubes centered around the origin gives the following two theorems:

Theorem 2.9. *Let L be a lattice, and let $\Delta = |\det(L)|$ be the volume of a fundamental parallelepiped. Then there exists a nonzero element $x \in L$ such that*

$$\|x\| \leq \frac{2}{\omega_n^{1/n}} \Delta^{1/n}.$$

Note that the right-hand side is asymptotically $c\sqrt{n}\Delta^{1/n}$, where $c = \sqrt{2/\pi \mathrm{e}}$.

Theorem 2.10. *With the notation as in the previous theorem, there exists a nonzero element $x \in L$ such that $\|x\|_\infty \leq \Delta^{1/n}$.*

Theorem 2.11. *If $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is a Lovasz-reduced basis, then*

- *(a)* $\|\mathbf{b}_1\| \leq 2^{(n-1)/2} min(L)$
- *(b)* $\|\mathbf{b}_1\| \leq 2^{n(n-1)/4} \Delta^{1/n}$
- *(c)* $\|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\| \leq 2^{n(n-1)/4} \Delta$.

This theorem follows from the following lemma and the defining properties of Lovasz reduced bases.

Lemma 2.12. *If $(\mathbf{b}_1, \cdots \mathbf{b}_n)$ is a Lovasz reduced basis, then $\|\mathbf{b}_i\| \leq 2^{(i-1)/2} \|\mathbf{b}_i^*\|$.*

Exercise 2.13. Prove the Lemma and the Theorem. *Hint.* Simple claculation using the defining properties of a Lovasz-reduced basis.

Remark 2.14. Δ can be defined for a lattice not of full rank, since the fundamental parallelpiped has an n-dimensional volume even if it resides in $\mathbb{R}^m$ for some $m \geq n$. Recall that $\Delta = \sqrt{\det G(\mathbf{b}_1, \ldots, \mathbf{b}_n)}$, where G is the Gram matrix (see handout, section on Euclidean spaces).

3 Application: polynomial time algorithm for Simultaneous Diophantine Approximation

Throughout this section, let $\alpha = (\alpha_1, \cdots \alpha_n)$ be a vector in $\mathbb{Q}^n$, and let $\epsilon > 0$ be a real number. We would like to find integers $q > 0, p_1, \ldots, p_n$ such that

$$|q\alpha_i - p_i| < \epsilon$$

for all i, and q is relatively small, say $q \leq Q$ for a given value Q.

The question is, for what Q can we

- guarantee that there exists a solution;

- find a solution in polynomial time?

Dirichlet's Theorem provides an answer to the existence question:

Theorem 3.1 (Dirichlet). *There exists a solution to the above problem with $Q = \epsilon^{-n}$.*

Recall our second proof of Dirichlet's theorem which used Minkowski's theorem. We examined the matrix:

$$\begin{bmatrix} -1 & 0 & \dots & 0 & \alpha_1 \\ 0 & -1 & & & \vdots \\ \vdots & & \ddots & & \alpha_{n-1} \\ 0 & & & -1 & \alpha_n \\ 0 & \dots & 0 & 0 & \epsilon/Q \end{bmatrix}$$

We took integer linear combinations of the columns with coefficients $\{p_1 \cdots p_{n+1}\}$, with $\sum p_i \mathbf{b}_i = x$, and $\|x\|_\infty \leq \epsilon$. Setting $p_{n+1} = q$, we get the desired result. The question now is for what value of Q can we *construct* such a vector (not just guarantee its existence).

From part (b) of Theorem 2.11, we can find a Lovasz-reduced basis for the lattice spanned by the columns of this matrix, and that gives a vector x, such that

$$\|x\|_\infty \leq \|x\| \leq 2^{n/4}\Delta^{1/(n+1)} \leq 2^{n/4}\left(\frac{\epsilon}{Q}\right)^{1/(n+1)}.$$

For this to be less than ϵ, we want

$$Q = \frac{2^{n(n+1)/4}}{\epsilon^n}.$$

So for this value of Q, Lovasz's Lattice Reduction algorithm finds a solution in polynomial time.

4 Application: integer relations between real numbers

Exercise 4.1. Let $a = 2\mathrm{e} + \pi$, $b = \mathrm{e} + 3\pi$, and $c = 2\mathrm{e} - 5\pi$. Find small integers k, ℓ, m, not all zero, such that $ka + \ell b + mc = 0$. *Hint.* Treat e, π as abstract symbols).

Exercise 4.2. Find the "smallest" such coefficient triple in ℓ_2 and in ℓ_∞-norms.

More generally, given real numbers α_j, we need integers p_i, not all zero, such that $|\sum p_i| < \epsilon$. What we would like to know is for what Q, can we find such integers, p_i, such that $p_i < Q$? To this end, we construct the following matrix:

$$\begin{bmatrix} \alpha_1 & \cdots & \alpha_n \\ \epsilon/Q & & 0 \\ & \ddots & \\ 0 & & \epsilon/Q \end{bmatrix}$$

(Notice that this is not a square matrix.) Now we would like a vector x, such that $x = \sum p_i \mathbf{b}_i$ and $\|x\|_\infty \leq \epsilon$. Such a vector with repsect to this matrix would be a solution to our problem. Again applying part b of Theorem 2.11, we know that

$$\|x\|_\infty \leq \|x\| \leq 2^{n/4}\Delta^{1/(n+1)}.$$

Now we need only compute Δ, and solve $2^{n/4}\Delta^{1/(n+1)} = \epsilon$ for Q. Recall that we can compute Δ using the Gram matrix, $\Delta^2 = \det(A^T A)$.

Exercise 4.3. Let A be the matrix:

$$\begin{bmatrix} \alpha_1 & \cdots & \alpha_n \\ \beta & & 0 \\ & \ddots & \\ 0 & & \beta \end{bmatrix}$$

and show that $\Delta = |\beta|^{n-1}\sqrt{\beta^2 + \sum \alpha_i^2}$.

Exercise 4.4. Find the appropriate Q for the above example.

5 Factoring polynomials

Definition 5.1. If $f \in \mathbb{Z}[x]$, we let the **norm** of f be the norm of the vector of its coefficients. That is,

$$\|x \mapsto ax^2 + bx + c\| = \sqrt{a^2 + b^2 + c^2}$$

Exercise 5.2 (Mignotte's Lemma). If $g, f \in \mathbb{Z}[x]$, and $g \mid f$, then $\|g\| \leq 2^{\deg(g)}\|f\|$.