Homework 1

Instructor: Chris Peikert
Student: YOUR NAME HERE

This homework is due by the **start of class on September 23** via the course Canvas page. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators and/or sources*** for each problem.

1. A set of vectors $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\} \subset \mathbb{R}^n$ is called a *generating set* of a lattice $\mathcal{L}$ if every $\mathbf{v} \in \mathcal{L}$ can be expressed as an integer linear combination of vectors in $\mathbf{B}$. (This differs from the notion of *basis* in that the representation need not be unique, so the vectors $\mathbf{b}_i$ need not be linearly independent.)

   Describe an efficient algorithm that, given a generating set $B = \{b_1, \ldots, b_m\} \subset \mathbb{Z}$ of a one-dimensional lattice $\mathcal{L} \subset \mathbb{Z}$, outputs a shortest nonzero element of $\mathcal{L}$. Make sure the algorithm runs in time polynomial in the *bit length* of the input set B.

2. Construct a basis $\mathbf{B}$ of a lattice $\mathcal{L}$ for which both inequalities $\min_i \|\widetilde{\mathbf{b}}_i\| \leq \lambda_1(\mathcal{L})$ and $\lambda_1(\mathcal{L}) \leq \sqrt{n}\det(\mathcal{L})^{1/n}$ are very loose, by large multiplicative factors. Do so in the smallest dimension n you can.

3. *Fundamental regions.*

   (a) Prove the following: let $\mathcal{F}$ be any fundamental region of a lattice $\mathcal{L}$. Then for any lattice coset $\mathbf{x} + \mathcal{L}$, the intersection $(\mathbf{x} + \mathcal{L}) \cap \mathcal{F}$ consists of a single point. (This point is called the "distinguished representative" of the coset in the region $\mathcal{F}$.)

   Also prove that given any vector $\mathbf{x}$ defining a coset $\mathbf{x} + \mathcal{L}$, finding its distinguished representative in $\mathcal{F}$ is equivalent to finding the unique $\mathbf{v} \in \mathcal{L}$ such that $\mathbf{x} \in \mathbf{v} + \mathcal{F}$.

   (b) We showed in class that $\mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot [-\frac{1}{2}, \frac{1}{2})^n$ is a fundamental region of $\mathcal{L} = \mathcal{L}(\mathbf{B})$. Describe an efficient algorithm (and prove it correct) that, given $\mathbf{B}$ and an arbitrary point $\mathbf{x} \in \mathbb{R}^n$ specifying a coset $\mathbf{x} + \mathcal{L}$, outputs the distinguished representative of the coset in $\mathcal{P}(\mathbf{B})$.

   (c) Let $\widetilde{\mathbf{B}}$ denote the Gram-Schmidt orthogonalization of $\mathbf{B}$. Prove that $\mathcal{P}(\widetilde{\mathbf{B}}) = \widetilde{\mathbf{B}} \cdot [-\frac{1}{2}, \frac{1}{2})^n$ is a fundamental region of $\mathcal{L} = \mathcal{L}(\mathbf{B})$. Also, describe an efficient algorithm (and prove it correct) that, given $\mathbf{B}$ and an arbitrary point $\mathbf{x} \in \mathbb{R}^n$ specifying a coset $\mathbf{x} + \mathcal{L}$, outputs the distinguished representative of the coset in $\mathcal{P}(\widetilde{\mathbf{B}})$. (*Hint*: for intuition, it may help to find solutions for two-dimensional lattices first.)

4. Minkowski's theorem says that $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$, where $\lambda_1(\mathcal{L})$ denotes the minimum distance in the standard *Euclidean* norm $\|\mathbf{x}\| = \sqrt{\sum_i x_i^2}$, which is also known as the ℓ_2 norm.

   Consider now the ℓ_p norm for $1 \leq p \leq \infty$, defined as $\|\mathbf{x}\|_p = (\sum_i |x_i|^p)^{1/p}$ and $\|\mathbf{x}\|_\infty = \max_i |x_i|$. Let $\lambda_1^{(p)}$ denote the minimum distance of a lattice in the ℓ_p norm. Generalize Minkowski's theorem and proof to give as tight of an upper bound on $\lambda_1^{(p)}$ as you can.

5. Define the *Voronoi cell* $\mathcal{V}(\mathcal{L})$ of a lattice $\mathcal{L}$ as the (open) set of all points that are closer to the origin than to any other lattice point. Formally,

$$\mathcal{V}(\mathcal{L}) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| < \|\mathbf{x} - \mathbf{v}\| \text{ for all } \mathbf{v} \in \mathcal{L} \setminus \{\mathbf{0}\}\}.$$

Prove that the Voronoi cell is "essentially" a fundamental region of $\mathcal{L}$, in that its translates by lattice points are pairwise disjoint, and cover all of $\mathbb{R}^n$ except for some rare "exceptional" points. Describe these exceptional points, and for any non-exceptional point, describe which translate $\mathbf{v} + \mathcal{V}(\mathcal{L})$ it lies in.

Extra credit: show how to modify $\mathcal{V}(\mathcal{L})$ to make it "half-open" (analogously to how we've defined the fundamental parallelepiped of a lattice), and prove that the modified body is a true fundamental region.