Homework 3

Instructor: Chris Peikert
Student: YOUR NAME HERE

This homework is due by the **start of class on October 16** via the course page on T-Square. 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*, *clarity*, and *conciseness*. 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/sources*** for each problem.

IMPORTANT NOTE: work hard on these questions yourself before looking at outside sources.

1. Using an oracle for SVP_γ for some $\gamma \geq 1$, show that one can efficiently solve subset-sum for densities as large as $C/\log\gamma$, where $C > 0$ is some universal constant. *Hint:* describe how to adapt Frieze's attack and analysis. To handle the case $\gamma = o(\sqrt{n})$, you will need a tighter analysis of the number of integer vectors of length at most $\gamma\sqrt{n}$. Consider centering unit cubes at all such points, and use a volume argument.

2. Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a set of linearly independent vectors and let $\mathbf{D} = (\mathbf{d}_1, \ldots, \mathbf{d}_n) = \mathbf{B}^{-t}$ be its dual set. Let $(\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n)$ be the Gram-Schmidt orthogonalization of $\mathbf{B}$, and $(\widetilde{\mathbf{d}}_1, \ldots, \widetilde{\mathbf{d}}_n)$ be the GS orthogonalization of $\mathbf{D}$ *in reverse order*, i.e., $\widetilde{\mathbf{d}}_n = \mathbf{d}_n$, $\widetilde{\mathbf{d}}_{n-1}$ is the component of $\mathbf{d}_{n-1}$ orthogonal to $\mathbf{d}_n$, etc.

   Prove that $\widetilde{\mathbf{d}}_i = \widetilde{\mathbf{b}}_i / \|\widetilde{\mathbf{b}}_i\|^2$.

3. We saw in class that $\rho((\mathbf{c}+\mathcal{L}) \setminus \sqrt{n}\mathcal{B}) \leq 5^{-n} \cdot \rho(\mathcal{L})$ for any lattice coset $\mathbf{c}+\mathcal{L}$, where $\mathcal{B}$ is the unit ball.

   Prove that $\rho((\mathbf{c}+\mathcal{L}) \setminus r\mathcal{B}^\infty) \leq 2n\exp(-\pi r^2) \cdot \rho(\mathcal{L})$ for any $r \geq 0$, where $\mathcal{B}^\infty$ denotes (any rigid rotation of) the unit ball in ℓ_∞ norm, i.e., an origin-centered cube of side length 2.

4. Define the lattice parameter $\widetilde{bl}(\mathcal{L}) := \min_{\mathbf{B}} \|\widetilde{\mathbf{B}}\|$, where the minimum is taken over all sets $\mathbf{B}$ of n linearly independent vectors in $\mathcal{L}$.

   Prove that $\eta_\varepsilon(\mathcal{L}) \leq \widetilde{bl}(\mathcal{L}) \cdot \sqrt{\ln(2n(1+1/\varepsilon))/\pi}$, and argue that this is a tighter bound than the one we saw in class (which had λ_n in place of $\widetilde{bl}$).