CS6190: Lattices in Computer Science Due Nov 23, 1 pm

Final Exam

Instructors: Shweta Agrawal and Satya Lokam

Total Points:

Advice: Be relaxed, attempt fewer questions better. Best of luck! :)

Problem 1: Size-reduction is not good enough

Recall that the Fibonacci numbers are given by the recurrence

$$F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 3, \text{ and } F_2 = F_1 = 1.$$

Consider the columns of the matrix

$$B_n = \begin{pmatrix} F_{n+1} & F_{n-1} \\ F_{n+2} & F_n \end{pmatrix}.$$

Show that

1. For all $n \geq 2$, the columns of B_n form a basis of the lattice $\mathbb{Z}^2$.
2. These basis vectors are *size-educed.* Recall that a basis is size-reduced if its Gram-Schmidt coefficients are all at most $1/2$ in absolute value.

Yet, since the lengths of basis vectors in B_n go to ∞ as $n \to \infty$, this shows that size-reduction is not a good enough notion of reduction.

Problem 2: Hermite Reduction and Orthogonality Defect

Hermite, in a letter to Jacobi in 1850, proposed the following notion of reduction (among other things):

A basis $B \in \mathbb{R}^{n \times n}$ of a lattice $\mathcal{L}$ is Hermite-reduced if

- it is size-reduced, and
- its Gram-Schmidt orthogonal vectors b_i^* satisfy
$$\|b_i^*\| \leq (4/3)^{(n-i)/4} \cdot (\mathrm{vol}(\pi_i(\mathcal{L})))^{1/(n-i+1)}, \text{ for all } 1 \leq i \leq n.$$
Recall that π_i is the projection onto the orthogonal complement of $\mathrm{span}(b_1, \ldots, b_{i-1})$.

For $0 < \varepsilon < 1$, consider the following basis B and the lattice $\mathcal{L}$ generated by its columns.

$$B = \begin{pmatrix} 1 & 1/2 & 1/2 \\ 0 & \varepsilon & \varepsilon/2 \\ 0 & 0 & 1/\varepsilon \end{pmatrix}.$$

1. Show that B is a Herimte-reduced basis of $\mathcal{L}$ according to the above definition.
2. Yet, this is a bad basis for $\mathcal{L}$ since $\|b_3\| \to \infty$ as $\varepsilon \to 0$. In particular, the *orthogonality defect* of this basis for the lattice goes to ∞, where for a basis $[b_1 \cdots b_n]$ of a lattice $\mathcal{L}$, its orthogonality defect is defined by $\prod \|b_i\| / \mathrm{vol}(\mathcal{L})$. Show that orthogonality defect of a basis is 1 if and only if it is orthogonal.
3. What is the orthogonality defect of an LLL-reduced basis?

Problem 3: Modular Lattices

Let $A = [I, A'] \in \mathbb{Z}_q^{k\times n}$, where I is the $k \times k$ identity matrix and $A' \in \mathbb{Z}^{k\times n-k}$. Give a basis for each of the following lattices and prove your answers correct.

1. $\mathcal{L}_q(A) = \{x \in \mathbb{Z}^n \ : \ Ax = 0 \pmod q\}$.
2. $\mathcal{L}_q^{\perp}(A) = \{x \in \mathbb{Z}^n \ : \ x = A^t s \pmod q \text{ for some } s \in \mathbb{Z}_q^k\}$.
3. The dual of lattice $\mathcal{L}_q(A)$.
4. The dual of lattice $\mathcal{L}_q^{\perp}(A)$.

Problem 4: Guassians

Recall that the *Discrete Gaussian Distribution* $D_{\mathcal{L},s,c}$, on lattice $\mathcal{L} \subseteq \mathbb{R}^n$, with parameter $s \geq 0$, and center $c \in \mathbb{R}^n$, is the probability distribution with support $\mathcal{L}$ assigning to each $x \in \mathcal{L}$ the probability

$$\rho_s(x - c)/\rho_s(\mathcal{L} - c).$$

Show that for any $c \in \mathbb{R}^n$ and any $(n-1)$-dimensional hyperplane $H \in \mathbb{R}^n$, and for parameter $s \geq \sqrt{2} \cdot \eta_\varepsilon(\mathcal{L})$, where $\varepsilon \leq 1/100$,

$$\Pr_{x \in D_{\mathcal{L},s,c}}[x \in H] < 0.9.$$

Hint: Show that it is w.l.o.g. to consider an axis-parallel hyperplane, e.g., $H = \{x \in \mathbb{R}^n : x_1 = r\}$ for $r \geq 0$. Then, use the Poisson summation formula to show that

$$\mathbb{E}_{x \in D_{\mathcal{L},s,c}}[\exp(-\pi((x_1 - r)/s)^2] < 0.9.$$