MATH 6302 PSET 3 TEST V1

AUSTIN WU, RISHI GUJJAR, AND ERIC YACHBES

Date: May 28, 2025.

Problem 1:

a:

Recall that since

$$\eta_\epsilon(\mathcal{L}) \coloneqq \inf\{s > 0 : \rho_{\frac{1}{s}}(\mathcal{L}^*) \leq 1 + \epsilon\}$$

Now recall in chapter 5.2 we are given an equivalent definition in a remark:

$$\eta_\epsilon \coloneqq s \text{ s.t. } \rho_{\frac{1}{s}}(\mathcal{L}^*) = 1 + \epsilon$$

This implies we need to find the value such that

$$\rho_{\frac{1}{s}}(\mathcal{L}^*) = 1 + \epsilon = \sum_{y \in \mathcal{L}^*} e^{-\pi ||y||^2 s^2}$$

Now given a lattice $\alpha\mathcal{L}$, recall that the dual lattice $(\alpha\mathcal{L})^* = \frac{1}{\alpha}\mathcal{L}^*$. Thus

$$\rho_{\frac{1}{s}}(\frac{1}{\alpha}\mathcal{L}^*) = 1 + \epsilon = \sum_{y \in \frac{1}{\alpha}\mathcal{L}^*} e^{-\pi\alpha^2 ||y||^2 s^2} = \sum_{y \in \frac{1}{\alpha}\mathcal{L}^*} e^{-\pi ||y||^2 (\alpha s)^2} = \alpha s$$

So s becomes αs so

$$\eta_\epsilon(\alpha\mathcal{L}) = \alpha s = \alpha \eta_\epsilon(\mathcal{L})$$

b:

Recall that $\rho_s(y - t) = \rho_s(t)\rho_s(y)e^{2\pi<y,t>/s^2}$. Then,

$$\rho_s(\mathcal{L} - y) = \rho_s(\mathcal{L})\rho_s(t)e^{2\pi/s^2<y,t>} = \sum_{y \in \mathcal{L}} \rho_s(y)\rho_s(t)e^{2\pi/s^2<\mathcal{L},t>}$$

$$= \rho_s(t) \sum_{y \in \mathcal{L}} \rho_s(y)e^{2\pi<y,t>}$$

Now due to the symmetry of the lattice sum

$$= \frac{1}{2}\rho_s(y)\left(\sum_{y \in \mathcal{L}} \rho_s(y)e^{2\pi/s^2<y,t>} + \sum_{-y \in \mathcal{L}} \rho_s(y)e^{2\pi/s^2<y,t>}\right) = \rho_s(t)\frac{1}{2}\sum_{y \in \mathcal{L}} \rho_s(y)\big(e^{2\pi<y,t>} + e^{-2\pi<y,t>}\big)$$

However, we note that

$$\cosh(2\pi < y, t >) = \frac{1}{2}(e^{2\pi<y,t>} + e^{-2\pi<y,t>})$$

but $\cosh(x) \geq 2$, so we have

$$\geq \rho_s(t) \sum_{y \in \mathcal{L}} \rho_s(y)\sqrt{e^{2\pi<y,t>}e^{-2\pi<y,t>}} = \rho_s(t) \sum_{y \in \mathcal{L}} \rho_s(y) = \rho_s(t)\rho_s(\mathcal{L})$$

c:

Recall that

$$\eta_\epsilon := \inf\{s > 0 : \rho_{\frac{1}{s}}(\mathcal{L}^*) \leq 1 + \epsilon\}$$

which is equivalent to

$$\forall s \leq \frac{\sqrt{\log(2/\epsilon)}/\pi}{\lambda_1(\mathcal{L}^*)} \implies \rho_{1/s}(\mathcal{L}^*) \geq 1 + \epsilon,$$

Now let y be the shortest vector in the lattice. This implies that Since

$$\rho_{\frac{1}{s}}(\mathcal{L}^*) := \sum_{w \in \mathcal{L}^*} \rho_{\frac{1}{s}} w \geq \rho_{\frac{1}{s}}(0) + \rho_{\frac{1}{s}}(y) + \rho_{\frac{1}{s}}(-y) \geq \rho_{\frac{1}{s}}(0) + \rho_{\frac{1}{s}}(y) + \rho_{\frac{1}{s}}(-y) = 1 + 2e^{-\pi||y||^2 s^2}$$

Now since we know that it is the shortest vector we know that

$$\geq 1 + 2e^{-\pi\lambda_1(\mathcal{L}^*)^2 s^2}$$

We can use that

$$s \leq \frac{\sqrt{\log(2/\epsilon)/\pi}}{\lambda_1(\mathcal{L}^*)}$$

and see that

$$\rho_{1/s}(\mathcal{L}^*) \geq 1 + 2e^{-\pi\lambda_1(\mathcal{L}^*)^2 \left(\frac{\sqrt{\log(2/\epsilon)/\pi}}{\lambda_1(\mathcal{L}^*)}\right)^2} = 1 + \epsilon.$$

Since the statement was equivalent to

$$\eta_\varepsilon(\mathcal{L})\lambda_1(\mathcal{L}^*) \geq \sqrt{\log(2/\epsilon)/\pi}.$$

d:

Not attempted

e:

Recall that

$$\rho_s(\mathcal{L}) := \sum_{y \in \mathcal{L}} \rho_s(y)$$

Thus c

$$\rho_s(\mathbb{Z}^n) = \sum_{y \in Z^n} e^{-\pi||x||^2/s^2} = \sum_{y \in \mathbb{Z}^n} e^{-\pi \sum_{i=1}^n y_i^2/s^2} = \sum_{y \in \mathbb{Z}^n} \Pi_{i=1}^n e^{-\pi/s^2 y_i^2} = e^{-\pi/s^2} \sum_{y \in \mathbb{Z}^n} \prod_{i=1}^n e^{y_i^2}$$

Note you can interchange the sum and product since both will have each will have $(x_1, x_2, \ldots, x_n)$ takes on every value of $\mathbb{Z}^n$ exactly once.

$$= \prod_{i=1}^{n} \sum_{y \in \mathbb{Z}} e^{-\pi/s^2 y^2} = \prod_{i=1}^{n} \rho_s(\mathbb{Z}) = \rho_s(\mathbb{Z})^n$$

f:

Using the same reason as 1c, this statement is equivalent to showing

$$s \leq \sqrt{\log(2n/\epsilon)/\pi} \implies \rho_{1/s}(\mathcal{L}^*) \geq 1 + \epsilon.$$

There are $2n$ shortest vectors coming from $\pm\vec{e}_i$ for $i = 1, \ldots, n$. We can use the bounding of 1c and that $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ and see

$$\rho_{1/s}(\mathcal{L}^*) = \sum_{\vec{z} \in \mathbb{Z}^n} \rho_{1/s}(\vec{z}) \geq \rho_{1/s}(0) + \sum_{i=1}^{n} \rho_{1/s}(e_i) + \rho_{1/s}(-e_i)$$

$$\geq 1 + 2ne^{-\pi(\log(2n/\epsilon)/\pi)^2} = 1 + \epsilon.$$

This shows that we have the inequality.

g:

Recall the poisson summation formula,

$$\rho_s(\mathcal{L}) = s^n/det(\mathcal{L})\rho_{1/s}(\mathcal{L}^*)$$

Then for all $s > 0$

$$\rho_s(\mathbb{Z}) = s\rho_{\frac{1}{s}}(\mathbb{Z}^*) \geq s\rho_{1/s}(0) = s.$$

We can split the sum of $\rho_s(\mathbb{Z})$ as

$$\rho_s(\mathbb{Z}) = \rho(0) + 2\sum_{n=1}^{\infty} \rho_s(n) = 1 + 2\sum_{n=1}^{\infty} \rho_s(n)$$

Now since ρ is strictly decreasing between $(0, \infty)$ implies that

$$\sum_{n=1}^{\infty} \rho_s(n) \leq \int_0^{\infty} \rho_s(x)dx$$

So we know that

$$\rho_s(\mathbb{Z}) \leq 1 + \int_{-\infty}^{\infty} \rho_s(x)dx = s + 1$$

because the integral of the Gaussian with parameter s is s.

Then since $s \leq \rho_s(\mathbb{Z}) \leq (1+s)$ implies that since from the previous question $\rho_s(\mathbb{Z}^n) = \rho_s(\mathbb{Z})^n \forall s$ that

$$s^n \leq \rho_s(\mathbb{Z}^n) \leq (1+s)^n$$

Problem 2:

a:

We are given a matrix A with each entry randomly distributed amongst $\mathbb{Z}_q$ such that the first n columns of the matrix form an invertible matrix.
Now extract the first n columns of the matrix. Call this matrix M. Let M^{-1} be the inverse of this matrix. Let the ramining rows of the matrix be A'. Then $A = [M|A']$ is trivally true. Then this implies that $M^{-1}A = M^{-1}[M|A'] = [I_n|M^{-1}A']$. Note this is the same idea as row reduction. Thus since this form is the same as the matrix form created by row reduction and is invertible, it forms a bijection inside
Mapping back to original SIS, this solution works as

$$Az \cong M^{-1}MAz \mod q \implies$$

Now since $M^{-1}Az \cong 0 \mod q \implies$

$$Az \cong M0 \mod q \implies$$

$$Az \cong 0 \mod q$$

Which solves original SIS and hence showes a reduction between the problems

b:

Let (A, b) be an LWE instance over $\mathbb{Z}_q$, and write

$$A = \begin{pmatrix} G \\ H \end{pmatrix}, \quad b = \begin{pmatrix} u \\ v \end{pmatrix},$$

where G is an $n \times n$ matrix that is invertible mod q, and u is n-dimensional. We know there exists some $s \in \mathbb{Z}_q^n$ and an error vector e such that

$$b = A\,s + e,$$

and we partition e accordingly as

$$e = \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}.$$

Define

$$A' := -\,H\,G^{-1}, \quad b' := v - H\,G^{-1}\,u.$$

Because G is invertible over $\mathbb{Z}_q$, $H\,G^{-1}$ behaves as a uniformly random matrix, so A' is suitable for normal-form LWE. We note

$$v = H\,s + e_2, \quad u = G\,s + e_1.$$

Then

$$b' = v - H\,G^{-1}\,u = (H\,s + e_2) \;-\; H\,G^{-1}(G\,s + e_1) = e_2 - H\,G^{-1}\,e_1 = e_2 + A'\,e_1.$$

Hence, b' is of the form $A' \cdot (\text{something}) + (\text{error})$, which matches normal-form LWE if we treat e_1 as the new "secret" and e_2 as the new "error."
Suppose there is an oracle that solves normal-form LWE on input (A', b') and returns e_1.
Then from the upper part of the original instance,

$$u = G\,s + e_1,$$

we invert G (which is efficient) and get

$$s = G^{-1}\big(u - e_1\big).$$

Thus, once we have e_1, we immediately recover the original secret s in polynomial time.

Problem 3:

a:

Recall that

$$M_{s,r} := \int_{||x|| \geq r} \rho_s(x)dx$$

Then if we let $s' = \alpha s$ implies that

$$M_{\alpha s,r} = \int_{||x|| \geq r} \rho_{\alpha s}(x)dx = \int_{||x|| \geq r} e^{-\pi ||x||^2/(\alpha s)^2}$$

And so if we do

$$= \int_{||x|| \geq r} e^{-\pi ||x||^2/s^2(1-1+\frac{1}{\alpha^2})} = \int_{||x|| \geq r} e^{-\pi ||x||^2/s^2} e^{\pi(1-\frac{1}{\alpha^2})||x||^2/s^2}$$

we know that

$$e^{-\pi ||x||^2/s^2} e^{\pi(1-\frac{1}{\alpha^2})r^2/s^2} \geq e^{-\pi ||x||^2/s^2} e^{\pi(1-\frac{1}{\alpha^2})r^2/s^2} \forall ||x||.$$

Thus we know that

$$\int_{||x|| \geq r} e^{-\pi ||x||^2/s^2} e^{\pi(1-\frac{1}{\alpha^2})||x||^2/s^2} \geq \int_{||x|| \geq r} e^{-\pi ||x||^2/s^2} e^{\pi r^2/s^2(1-\frac{1}{\alpha^2})}$$

$$= e^{\pi(1-\frac{1}{\alpha^2})r^2/s^2} \int_{||x|| \geq r} e^{-\pi ||x||^2/s^2}$$

And since

$$M_{s,r} = \int_{||x|| \geq r} e^{-\pi ||x||^2/s^2}$$

Is trivially known implies that

$$= e^{\pi(1-\frac{1}{\alpha^2})r^2/s^2} M_{s,r}$$

Thus we have that

$$M_{\alpha s,r} \geq e^{\pi(1-\frac{1}{\alpha^2}r^2/s^2)} M_{s,r}$$

b:

Recall that $M_{\alpha s,r} \leq M_{\alpha s,0} = (\alpha s)^n$. and if $r > 0$ then $M_{\alpha s,r} < M_{\alpha s,0} = (\alpha s)^n$ Now since we know from 3.1 that

$$M_{\alpha s,r} \geq e^{\pi(1-\frac{1}{\alpha^2}r^2/s^2)} M_{s,r}$$

So multiplying each side by $e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}$ implies that

$$M_{s,r} \leq e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)} M_{\alpha s,r}$$

But since we directly know that leq $M_{\alpha s,r} < M_{\alpha s,0} = (\alpha s)^n$ Directly implies that

$$M_{s,r} \leq e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}M_{\alpha s,r} < e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}M_{\alpha s,0} = e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}(\alpha s)^n$$

And thus we showed that

$$M_{s,r} < e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}(\alpha s)^n$$

c:

Recall that

$$\frac{1}{s^n}\int_{||x||\geq r}\rho_s(x)dx = \frac{1}{s^n}M_{s,r}$$

Now since we directly know that

$$M_{s,r} < e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}(\alpha s)^n$$

Directly implies that

$$\frac{1}{s^n}\int_{||x||\geq r}\rho_s(x)dx < \frac{1}{s^n}e^{-\pi(1-\frac{1}{\alpha^2}r^2/s^2)}(\alpha s)^n$$

Thus since we know that $r > \sqrt{n/(2\pi)}s$ implies that since this equation holds for any $\alpha > 1$ setting $\alpha = \sqrt{\frac{2\pi}{n}}\frac{r}{s}$ trivially knowing that this is greater than 1 implies that

$$\frac{1}{s^n}\int_{||x||\geq r}\rho_s(x)dx < \frac{1}{s^n}e^{-\pi(1-\frac{1}{e}r^2/s^2)}(\alpha s)^n = e^{-\pi(1-\frac{1}{e}r^2/s^2)}\alpha^n = \alpha^n e^{-\pi r^2/s^2}e^{\pi r^2/(\alpha s)^2}$$

Now replacing α with its value implies that

$$= (\sqrt{\frac{2\pi}{n}}\frac{r}{s})^n e^{-\pi r^2/s^2}e^{\pi r^2/((\sqrt{\frac{2\pi}{n}}\frac{r}{s})s)^2}$$

$$= (\frac{2\pi e r^2}{ns^2})^{n/2}e^{-\pi r^2/s^2}$$

Problem 4:

Let the algorithm be

```
Algo(B): #input the basis
  B'= LLL(δ = 3/4, B) #Calculate the LLL reduced basis
  B*' = B'((B')^T B')^{-1} # Calculate the Dual
  b_1 = B'[1]
  for i in range(1, n):
    y = A(B', 2^{-n/2+i} · ||b_1||)
    if and y ∈ Span(B) and not y == {0}:
      append y to a list
  return the smallest y in the list

```

Now to stuty time complexity:

Now since given that finding B' requires polynomial time complexity it has time complexity of $poly(n, l)$. Now since calculating the dual matrix consists of one transpose (n^2) operation, one multiplication (n^3) operation, one inversion (n^3) operation, and one more multiplication (n^3) operation, this step is polynomial still. After we run $\mathcal{A}$ for n steps, resulting in a time complexity of $T(n, l)$ per step. Thus since checking if it is in the span of a lattice is polynomial (checking by multiplying with the basis of the dual lattice) and checking if its the zero vector is n, We get the time complexity inside the loop is $nT(n, l) + npoly(n, l)$ which implies the total time complexity is

$$nT(n, l) + npoly(n, l) + poly(n, l) = nT(n, l) + poly(n, l)$$

Now to show correctness:

Recall that given $B \in \mathbb{R}^{n\times n}$ is a $\delta = \frac{3}{4}$ LLL reduced basis for a lattice $\mathcal{L}$ then $||\tilde{b}_i|| \geq \lambda_1(\mathcal{L})/2^{n/2}$. (HW 2.1)

Also recall that if $B \in \mathbb{R}^{n\times n}$ is a $\delta = \frac{3}{4}$ LLL basis for $\mathcal{L}$ then (Theorem 2.12)

$$||b_1|| \leq \frac{\lambda_1(\mathcal{L})}{(\delta - \frac{1}{4})^{(n-1)/2}}$$

Now

$$||\tilde{b}_i|| \geq \lambda_1(\mathcal{L})/2^{n/2} \implies 2^{n/2}||\tilde{b}_i|| \geq \lambda_1(\mathcal{L}) \implies 2^{n/2}||b_1|| \geq \lambda_1(\mathcal{L})$$

and

$$||b_1|| \leq \frac{\lambda_1(\mathcal{L})}{(\delta - \frac{1}{4})^{(n-1)/2}} \implies (\delta - \frac{1}{4})^{(n-1)/2}||b_1|| \leq \lambda_1(\mathcal{L}) \implies$$

$$(\frac{1}{2})^{(n-1)/2}||b_1|| \leq \lambda_1(\mathcal{L}) \implies 2^{-(n-1)/2}||b_1|| \leq \lambda_1(\mathcal{L})$$

Thus since $||\tilde{b}_i|| \geq \lambda_1(\mathcal{L})/2^{n/2}$ implies that there exsits some $i \in Range(1, n)$ such that $||\tilde{b}_i|| \geq \lambda_1(\mathcal{L})/2^{-n/2+i}$ suffices (setting $i = n$ returns the orignal equation). Let i' be the i such that the norm is minimial.

Now if $i' = 1$ then we know that $2^{-(n-1)/2}||b_1|| \leq \lambda_1(\mathcal{L})$ and that $\lambda_1(\mathcal{L}) \leq 2^{-n/2+1}$ which by defintiion implies that

$$\lambda_1 \leq ||b_1|| \leq 2^0||b_1|| \leq \sqrt{2}]\lambda_1(\mathcal{L})$$

And thus b for $i' = 1$ is in the range to output the right vector.

Now if $i' > 1$ we know by minimality of i' that

$$2^{-n/2+i'}||b_1|| \geq \mathcal{L}_1(\mathcal{L}) \geq 2^{-n/2+i'-1}$$

so we directly know that

$$\lambda_1(\mathcal{L}) \leq 2^{-n/2+i'}||b_i|| \leq 2\lambda_1(\mathcal{L})$$

and thus b is in the right range such that the output is the right vector for $i' > 1$.

Thus for all $i' \in Range(1, n)$ there exists a output that gives the answer from $\mathcal{A}$ and thus since i' is guarenteed to exist in that range this algorithm will work.

Problem 5:

A lot like 25 hours