

MATH 6302 PSET 2

AUSTIN WU, RISHI GUJJAR, AND ERIC YACHBES

Problem 1:**a:**

Now since there are $n + 1$ vectors in a series of vectors of rank n implies since there for any point in the lattice it can be created with

$$n_1\hat{b}_1 + \cdots + n_{i-1}\hat{b}_{i-1} + n_{i+1}\hat{b}_{i+1} + \cdots + n_{n+1}\hat{b}_{n+1}$$

Now since by definition a lattice of rank n is created by n basis vectors and this set of vectors is a basis for the lattice, then there will exist some basis vector such that removing it still generates the lattice. Let this vector be b_i . Now given $n_i b_i$ since $n_i b_i \in \mathcal{L}$, there is some equivalent construction $n_1\hat{b}_1 + \cdots + n_{i-1}\hat{b}_{i-1} + n_{i+1}\hat{b}_{i+1} + \cdots + n_{n+1}\hat{b}_{n+1}$ since

$$\forall p \in \mathcal{L}, \exists n_1, \cdots, n_{i-1}, n_{i+1}, \cdots, n_{n+1}$$

$$n_1\hat{b}_1 + \cdots + n_{i-1}\hat{b}_{i-1} + n_{i+1}\hat{b}_{i+1} + \cdots + n_{n+1}\hat{b}_{n+1} = p$$

This implies that there are a set of integers such that

$$n_1\hat{b}_1 + \cdots + n_{i-1}\hat{b}_{i-1} + n_{i+1}\hat{b}_{i+1} + \cdots + n_{n+1}\hat{b}_{n+1} = n_i\hat{b}_i$$

which is the same thing as saying

$$n_1\hat{b}_1 + \cdots + n_{i-1}\hat{b}_{i-1} + n_{i+1}\hat{b}_{i+1} + \cdots + n_{n+1}\hat{b}_{n+1} - n_i\hat{b}_i = 0$$

and thus we have showed a set of integers such that the linear combination of them is equal to 0. Now since the integers is a subset of the rational numbers implies that we have a set of rational numbers such that

$$\sum_{i=1}^{n+1} q_i \hat{b}_i = 0$$

which directly implies \mathbb{Q} -linear dependence.

b:

Now since $b_{n+1} \in \text{span}(b_1, \cdots, b_n)$ implies there exists $\hat{c} \in \mathbb{R}^n$ such that

$$b_{n+1} = \sum_{k=1}^i c_k b_k$$

And thus rearranging

$$b_i = \frac{1}{c_i} \left(b_{n+1} - \sum_{k=1}^{i-1} c_k b_k \right)$$

.

Now this implies since span is the set of linear combination of all the vectors, given $\forall \hat{t} \in \text{span}(b_1, \dots, b_i)$, let

$$\hat{t} = \sum_{k=1}^i a_i k_i$$

for any arbitrary coefficients $c_i \in \mathbb{R}$. Which is guaranteed to exist by definition of span. Then

$$\begin{aligned} \hat{t} &= \sum_{k=1}^i a_k b_k = \\ \sum_{k=1}^{i-1} a_k b_k + a_i b_i &= \sum_{k=1}^{i-1} a_k b_k + a_i \left(\frac{1}{c_i} \left(b_{n+1} - \sum_{k=1}^{i-1} c_k b_k \right) \right) \end{aligned}$$

Which consists of a linear sum of vectors entirely inside of $\text{span}(b_1, \dots, b_{i-1}, b_{n+1})$ and thus any vector in $\text{span}(b_1, \dots, b_i)$ can be represented by a sum of vectors in $\text{span}(b_1, \dots, b_{i-1}, b_{n+1})$. Which implies it is in that span.

Now suppose $\forall \hat{v} \in \text{span}(b_1, \dots, b_{i-1}, b_{n+1})$. Then there is guaranteed by definition of span to exist some combination

$$\hat{v} = a_{n+1} b_{n+1} + \sum_{k=1}^{i-1} a_k b_k$$

Then

$$= a_{n+1} \sum_{k=1}^i c_k b_k + \sum_{k=1}^{i-1} a_k b_k$$

Which consists of a linear sum of vectors entirely inside of $\text{span}(b_1, \dots, b_i)$ and thus any vector in $\text{span}(b_1, \dots, b_{i-1}, b_{n+1})$ can be represented by a sum of vectors in $\text{span}(b_1, \dots, b_i)$. Which implies it is in that span.

Thus we have proved both directions so it implies a vector in one span can be represented in the other span so we proved equality

$$\text{span}(b_1, \dots, b_i) = \text{span}(b_1, \dots, b_{i-1}, b_{n+1})$$

C:

Now given the procedure listed above as assume initially that b_1, \dots, b_n are linearly independent. Then at each procedure

- (1) Size reduction: This step does not affect set of vectors from b_1, \dots, b_n .
- (2) Output step: This step doesn't change the set of vectors so it keeps them independent
- (3) Swap: Now since the only vector we are changing is between b_i and b_{n+1} and we start with a set that is linearly independent the rest of the elements will remain linearly independent. Now when we switch elements, it implies that $\mu_{i,n+1} \neq 0$ otherwise the algorithm would have terminated. This implies that there is a part

of the sized reduced b_{n+1} that is in the part of the vector b_i and not in the rest of the vectors. This implies linear independence for this step.

- (4) Repeat: Since any repetition step consists of the first 3 steps and we showed the first 3 steps keep the set linearly independent any repetition will also keep the set linearly independent

Thus since we assumed the base case which is that b_1, \dots, b_n is linearly independent and at every step in the algorithm each step keeps b_1, \dots, b_n linearly independent implies by induction that at every step of the procedure the vector set remains linearly independent.



d:

Now to show this program never terminates since this program only terminates when $b_{n+1} = 0$, we must show that b_{n+1} never equals 0.

Now since we assume we start with \mathbb{Q} linear independence implies that we cannot write one vector as the sum of linear \mathbb{Q} coefficients with the rest of the vectors such that no vector can be the zero vector, otherwise we could write it as the sum of vectors with coefficient $0 \in \mathbb{Q}$. We also showed that the vectors b_1, \dots, b_n are always \mathbb{R} linearly independent throughout the algorithm. This inherently implies \mathbb{Q} linear independence. Now since all vectors start not 0 and process 3 is simply a swap, the only way they could ever change in value could be in process 1. Now since the size reduction operation consists of adding integer multiples of the basis, this operation does not change the linear independence of \mathbb{Q} . Thus the vectors are always \mathbb{Q} independent. Now suppose all vectors are \mathbb{Q} independent in the set b_1, \dots, b_i, b_{n+1} . Then this implies that b_{n+1} can never be 0 since otherwise it could be made out of sum of vectors with coefficient 0. Thus since at every step the whole set is \mathbb{Q} linearly independent even on the size reduction step the values of the vectors will never be 0 and thus the program will never terminate.

e:

We define

$$\Phi = \prod_{i=1}^n \|\tilde{b}_i\|$$

Then before the swap step let the set be $\{b_1, \dots, b_n + 1\}$ which implies that the vectors after the swap step will be written as $\{b_1, \dots, b_{i-1}, b_{n+1}, b_{i+1}, \dots, b_n, b_i\}$. Then let Φ' be Φ after the swap step. Then

$$\frac{\Phi'}{\Phi} = \frac{\prod_{k=1}^n \|\tilde{b}'_k\|}{\prod_{k=1}^n \|\tilde{b}_k\|} = \frac{\tilde{b}'_i}{\tilde{b}_i} = \frac{b_{n+1}'}{\tilde{b}_i}$$

This is true since from problem 1.2 the span of b_1, \dots, b_{i-1}, b_n and b_1, \dots, b_i is equivalent so the gram schmidt process is the same. Where b_{n+1}' is size reduced such that $|u_{i,n+1}| < \frac{1}{2}$.

Now since the spans of basis $b_1 \cdots b_i$ and $b_1 \cdots b_{i-1}, b_n$ are equivalent implies that the gram schmidt orthogonalization of both leaves the i th basis vector (b_i or b_{n+1}) equivalent up to a scaling factor. Thus the size reduction

$$\left| \mu_{i,n+1} < \frac{1}{2} \right| \implies \langle \tilde{b}_{n+1}, \tilde{b}_i \rangle < \frac{\langle \tilde{b}_i, \tilde{b}_i \rangle}{2} \implies c < \frac{|\tilde{b}_i|}{2|\tilde{b}_i|} \implies c < \frac{1}{2}$$

Where c is the scaling factor between the two vectors since they are equivalent. This directly implies $\frac{\Phi'}{\Phi} < \frac{1}{2}$

f:

Minkowski

g:

We know from 1.5 that every run of the algorithm decreases Φ by two. Thus since Φ is guaranteed not to terminate, we know that we can run this algorithm enough to achieve a set of basis pairs that satisfies this property.

Now let $i = \log_2\left(\frac{C}{(\epsilon/2\sqrt{n})^n}\right) + 1$. Then running the algorithm i iterations implies that

$$\Phi < \frac{C}{2^n} < \frac{C}{\frac{C}{(\epsilon/2\sqrt{n})^n} + 1} < \frac{C}{\frac{C}{(\epsilon/2\sqrt{n})^n}}$$

Where $C = \Phi'$, or Φ of the initial basis set. This implies that $\sqrt{n}\Phi^{1/n} < \epsilon$. And thus from 1.7 there exists

$$0 < \|y\| < \sqrt{n}\Phi^{1/n}$$

which implies there exists a vector such that

$$0 < \|y\| < \epsilon \quad \text{👉}$$

Problem 2:**a:**

Let y_i be the coefficients for the linear combination of \tilde{b}_i gram schmidt basis vectors such that it is equal to y . Then


$$y_i = z_i + \sum_{k=i+1}^n z_k \mu_{k,i}$$

This implies that $|y_i| \leq 2^{n/2}$. Thus

$$|z_i| \leq |y_i| + \left| \sum_{k=i+1}^n z_k \mu_{k,i} \right| \leq |y_i| + \frac{1}{2} \sum_{k=i+1}^n |z_k|$$

Directly implies $(\lambda_1(\mathcal{L}))^2 = \sum_{i=1}^n y_i^2 \|\tilde{b}_i\|^2$. This implies our base case.

Now let $|z_{n-k}| \leq |y_{n-k}| + \frac{1}{2} \sum_{j=1}^k |z_{n-j}| \leq 2^{n/2} + \frac{1}{2} \sum_{j=1}^k 2^{n/2} (3/2)^j \leq 2^{n/2} (3/2)^k$

Now since our base case satisfies and we showed the recurring step implies that by induction this holds. 

b:

Create an algorithm defined by iterating in order by i through all vectors such that $|z_{n-i}| \leq 2^{n/2+i}, z \neq 0$. Then if $\|B\hat{z}\| < \text{current shortest vector}$ then set it as the shortest vector. Then output at the end.

Now since we enumerate over $|z_{n-i}| \leq 2^{n/2+i}, z \neq 0$, our number of steps is

$$\prod_{i=1}^n 2^{n/2+n-1} = 2^{n^2}$$

which implies a total complexity of $2^{\mathcal{O}(n^2)}$

Now since there exists some vector v in the set described such that $Bv = y \in \mathcal{L}$ with $\|y\| = \lambda_1(\mathcal{L})$ and we are finding it by looping over the set such that we find the smallest one we will find the shortest nonzero vector. Note that it is nonzero since the matrix B spans the space.

c:

subproblem **Part C:**

Proof derived from <https://pubsonline.informs.org/doi/10.1287/moor.12.3.415>, section 4.

Claim 0.1:

There exists an algorithm for exact CVP that runs in $2^{\mathcal{O}(n^2)}$.

Recall

Definition 0.2 (CVP):

Given a vector $t \in \mathbb{R}^n$ and lattice $\mathcal{L} \subset \mathbb{R}^n$

$$CVP(\mathcal{L}, t) := \min_{y \in \mathcal{L}} \|y - t\|$$


Proposition 0.3:

Suppose that $\mathcal{L}(b_1, \dots, b_n)$ is a lattice in \mathbb{R}^k , $k \geq n$ with all b_i independent and $b_0 \in \mathbb{R}^k$. Let b'_0 be the projection of b_0 onto the span of b_1, \dots, b_n . Then there exists a point $b \in \mathcal{L}$ such that

$$\|b - b'_0\| \leq \frac{1}{2} \left(\sum_{j=1}^n (b_j(j))^2 \right)^{\frac{1}{2}}$$

Proof. Since $b(1,1), b(n,n)$ forms an orthogonal basis for their vector space with b'_0 in that vector space, this implies we can successively choose integers with ordering $\alpha_n, \alpha_{n-1}, \dots, \alpha_1$ such that

$$\left| \left(\sum_{i=j}^n \alpha_i b_i - b'_0, b(j,j) \right) \right| \leq (b_j(j))^2 / 2 \forall j$$

is true given arbitrary choice of α_j . This implies the proposition. 

Proposition 0.4:

There exists a easily determined set $T \subset \mathcal{L}^{n-i+1}$ with $|T| \leq (n + \sqrt{n})^{n-i+1}$ such that if $\sum_{j=1}^n \lambda_j b_j$ is closest in the lattice to b_0 then $(\lambda_i, \dots, \lambda_n)$ belongs to T .

Proof. Now since

$$\sum_{j=1}^n \lambda_j b_j = v$$

is one of the closest (nonunique) points in \mathcal{L} to b_0 implies v is the closest point to b'_0 in \mathcal{L} . Now proposition 0.3 implies that $|v - b'_0| \leq (\sqrt{n}/2)b_i(i)$. Yet $|v - b'_0| \geq |((v - b'_0), b(n, n))|/b_n(n) = |\lambda_n b_n(n) - (b'_0, b(n, n))|/b_n(n) = |\lambda_n - t|b_n(n)$ for some $t \in \mathbb{R}$. This implies at most $1 + \sqrt{n}b_i(i)/b_n(n)$ candidates for λ_n . This implies we can show a similar bound for $\lambda_1, \dots, \lambda_n$ using (TODO). Now suppose $\lambda_{j+1}, \dots, \lambda_n$ are fixed integers, $j \geq i + 1$. Then this implies by (TODO) that there are at most $1 + \sqrt{n}b_i(i)/b_j(j) \leq (1 + \sqrt{n})b_i(i)/b_j(j)$ possible values of λ_j s.t. the length of $v - b'_0$ in direction of $b_j(j)$ is bounded by $\frac{\sqrt{n}}{2}b_i(i)$. This since $b_i(i) \geq b_j(j)$ that given a set T candidate $\lambda_1, \dots, \lambda_n$ we get

$$|T| \leq \prod_{j=1}^n (1 + \sqrt{n})b_i(i)/b_j(j)$$

So this implies that $b_i(i)$ is the length of the shortest vector in \mathcal{L}



Theorem 0.5:

CVP solves for the closest vector in $\mathcal{O}(n^s)$ arithmetic operations where s is the length of the input

Proof. Now let $T(n)$ be the number of arithmetic operations performed by CVP. Then

$$T(n) \leq (n + \sqrt{n})^{n-1+1}T(i-1) + q(n),$$

$q(n)$ is a polynomial with no s dependence. This implies that between $1 \leq i \leq n$,

$$\max(((i-1)/(n + \sqrt{n}))^{i-1})$$

occurs at $i = n$ and

$$\lim((n-1)/n)^{n-1} = \frac{1}{e}.$$

This implies that $T(n)$ is $\mathcal{O}(n^n)$ by inducting over n . This implies that $T(n) = \mathcal{A}_0(n) + \mathcal{A}_1(n)$ where $\mathcal{A}_0(n), \mathcal{A}_1(n)$ represent the number of operations required for $\mathcal{A}_0, \mathcal{A}_1$. Thus since max time complexity between the two algorithms is $\mathcal{A}_0(n) = \mathcal{O}(n^n)$ implies that this is the time complexity of the algorithm.



```

1  A0(n, L):# aka shortest
2      if n=1
3          return [L[1]]
4      L = LLL(L) #LLL reduce the basis
5      def: LProjGoto
6      LProject
7      for i in range(i):

```



```

8         LProject[i] = Project(B[i], L-{L[i]})
9         LNew = A0(n-1, LProject)
10        for i in range(2,n)
11            Lift(Lnew[i], L[i])
12        if Norm(L[2]) < sqrt(3)*Norm(L[2])/2:
13            Swap(L[1],L[2])
14            Goto LProjGoto
15        for i in range j
16            if Norm(L[j] >= L[1]):
17                j0 = min j such that its true
18            else:
19                j0 = n+1
20        for i in range(1, j0-1):
21            LBasis.append(Lnew[i])
22        Enumerate(Basis)# enumerates the basis
23
24        return: a basis L containing v_1
25

```

```

1    A1()
2

```

```

1    CVP(n L):
2        NewBasis = A0(L)
3        Candidates = null
4        forall lambda i:
5            if i = 1
6                a1 =
7
8

```

Problem 3:**a:**

Now suppose that $r = \max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L})$. Then for any point $t \in \mathbb{R}^n$, it is always at most r away from any point in the lattice. Now since any volume ball of radius r will contain all the points at most r distance away from it implies that any volume balls around every set of lattice points will contain all points in \mathbb{R}^n . Thus $\max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L}) \in \{r | \mathcal{L} + B^n(r) = \mathbb{R}^n\}$

Now suppose $r' < \max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L})$. Then since r' is less than the maximum distance from the lattice to any point, there exists a point $p \in \mathbb{R}^n$ such that the distance from p to any point in the lattice is greater than r' . This then directly implies that there exists a point not in $\mathcal{L} + B^n(r)$ which implies that $\mathcal{L} + B^n(r) \neq \mathbb{R}^n$. Thus r' is not in the set $\{r | \mathcal{L} + B^n(r) = \mathbb{R}^n\}$.

Thus we have showed that $\max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L}) \in \{r | \mathcal{L} + B^n(r) = \mathbb{R}^n\}$ and that given $r' < \max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L})$ then $r' \notin \{r | \mathcal{L} + B^n(r) = \mathbb{R}^n\}$. Thus

$$\max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L}) = \min\{r | \mathcal{L} + B^n(r) = \mathbb{R}^n\} \quad \text{👤}$$

b:

Let

$$S_r := \cup_{y \in \mathcal{L} \cap B^n(r)} (B^n(\mu(\mathcal{L})) + 1), r \geq \mu(\mathcal{L})$$

Then since they are disjoint implies that

$$\text{vol}(B^n(\mu(\mathcal{L}))) (\mathcal{L} \cap B^n(r)) \geq \text{vol}(S_r)$$

But since any distance in the lattice is bounded by $\mu(\mathcal{L})$ implies that

$$\forall v \in B^n(r - \mu(\mathcal{L}))$$

there exists a point such that $v = x + y$ where $x \in \mathcal{L}$ $y \in B^n(\mu(\mathcal{L}))$. Thus since $\|v\| + \|x\| < r$ implies by triangle inequality that $\|v\| < r$.

This implies that all $\forall v \in B^n(r - \mu(\mathcal{L})), v \in S_r$. Thus since

$$B^n(r - \mu(\mathcal{L})) \leq \text{vol}(B^n(\mu(\mathcal{L}))) (\mathcal{L} \cap B^n(r))$$

implies that

$$\frac{B^n(r - \mu(\mathcal{L}))}{\mathcal{L} \cap B^n(r)} \leq \text{vol}(B^n(\mu(\mathcal{L}))) \forall r$$

Thus

$$\lim_{r \rightarrow \infty} \frac{B^n(r - \mu(\mathcal{L}))}{\mathcal{L} \cap B^n(r)} = \frac{B^n(r)}{\mathcal{L} \cap B^n(r)} = \det(\mathcal{L})$$

Which we just showed is less than $\text{vol}(B^n(\mu(\mathcal{L})))$. Thus


$$\det(\mathcal{L}) \leq \text{vol}(B^n(\mu(\mathcal{L})))$$

c:

Suppose this is false. Then there must exist some coefficient less than $\frac{\lambda_n(\mathcal{L})}{2}$ such that it is equal to $\mu(\mathcal{L})$.

Now for a given set of $\lambda_1(\mathcal{L}) \cdots \lambda_n(\mathcal{L})$ find a working configuration of associated vectors for this set of lattices. This is guaranteed to exist since if you sort the vectors $\mathbf{y}_1, \dots, \mathbf{y}_n$ by norm and sort in arbitrary order for vectors of equivalent norm, then for each $1 \leq i \leq n$ the definition satisfies and you have an associated \mathbf{y}_i for every $\lambda_i(\mathcal{L})$. Associate each basis vector associated with $\lambda_i(\mathcal{L})$ as \mathbf{y}_i

Now define a new lattice \mathcal{L}' as the set of basis vectors $\{\mathbf{y}_1, \dots, \mathbf{y}_{n-1}, \frac{1}{2} \cdot \mathbf{y}_n\}$. Now since $\mathbf{y}_1, \dots, \mathbf{y}_n$ are linearly independent imply $\mathbf{y}_1, \dots, \mathbf{y}_{n-1}$ is also linearly independent. Recall from the definition of linear independence on the reals that no set of coefficients $\hat{c} \in \mathbb{R}^n$ where $\sum_{i=1}^{n-1} c_i \hat{v}_i = c_n v_n$. This directly implies that no set of sum of linear real coefficients of $\mathbf{y}_1, \dots, \mathbf{y}_{n-1}$ can be equal to any vector in the linear span of $\frac{1}{2} \cdot \mathbf{y}_n$. This directly implies since the integers are a subset of the reals that no sum of integer coefficients for $\mathbf{y}_1, \dots, \mathbf{y}_{n-1}$ can reach point $\frac{1}{2} \cdot \mathbf{y}_n$ without using vector $\frac{1}{2} \cdot \mathbf{y}_n$ in its sum. Now since \mathcal{L}' is a lattice, the all its coefficients must be integers which implies that since we need to use at least $\pm 1 \cdot \frac{1}{2} \cdot \mathbf{y}_y$ to reach $\frac{1}{2} \cdot \mathbf{y}_n$ from any point in the linear span of $\mathbf{y}_n - \{\vec{0}\}$, using the triangle inequality we get a bound on the norm of the vector to reach any lattice point in the span of $\frac{1}{2} \cdot \mathbf{y}_n$ point of $\frac{1}{2} \lambda_n(\mathcal{L})$.

Now going back to \mathcal{L} , since they differ by a scaling factor on a single vector, we know that the only difference between the set of lattice vectors is that $(n + \frac{1}{2})\mathbf{y}_n$ is in \mathcal{L}' but not in \mathcal{L} . Since we know a bound on the distance to $\frac{1}{2}\mathbf{y}_n$, \mathcal{L}' implies that we know there is a point at least $\frac{1}{2}\lambda_n(\mathcal{L})$ away from any point on the lattice, for there to be a $r|\mathcal{L} + B^n(r) = \mathbb{R}^n$, r must be at least $\frac{1}{2}\lambda_n(\mathcal{L})$. This implies a bound on the $\frac{1}{2}\lambda_n(\mathcal{L}) \leq \min\{r|\mathcal{L} + B^n(r) = \mathbb{R}^n\} = \mu(\mathcal{L})$ which implies the bound. 

Problem 4:**a:****Definition 0.6 (Poisson summation formula):**

Defined in (5.3)

$$\sum_{\mathbf{y} \in \mathcal{L}} f(\mathbf{y} - \mathbf{t}) = \frac{1}{\det \mathcal{L}} \sum_{\mathbf{w} \in \mathcal{L}^*} \cos(2\pi \langle \mathbf{w}, \mathbf{t} \rangle) \hat{f}(\mathbf{w})$$

Now given

$$\rho_s(\mathcal{L}) := \sum_{\mathbf{y} \in \mathcal{L}} \rho_s(\mathbf{y}) = \sum_{\mathbf{y} \in \mathcal{L}} e^{-\pi \|\mathbf{y}\|^2 / s^2}$$

Setting $\mathbf{t} = 0$ implies that

$$\sum_{\mathbf{y} \in \mathcal{L}} f(\mathbf{y}) = \frac{1}{\det \mathcal{L}} \sum_{\mathbf{w} \in \mathcal{L}^*} \cos(2\pi \langle \mathbf{w}, \mathbf{0} \rangle) \hat{f}(\mathbf{w}) = \frac{1}{\det \mathcal{L}} \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{f}(\mathbf{w})$$

and since the determinant of the lattice is defined as 1, $\frac{1}{\det \mathcal{L}} = 1$. Thus

$$\sum_{\mathbf{y} \in \mathcal{L}} f(\mathbf{y}) = \frac{1}{\det \mathcal{L}} \sum_{\mathbf{w} \in \mathcal{L}^*} \cos(2\pi \langle \mathbf{w}, \mathbf{0} \rangle) \hat{f}(\mathbf{w}) = \frac{1}{\det \mathcal{L}} \sum_{\mathbf{w} \in \mathcal{L}^*} \hat{f}(\mathbf{w})$$

We also know that the gaussian function is equivalent up to a scaling factor, i.e. $\hat{\rho}_s(\mathbf{w}) = s^n \rho_s^{\frac{1}{s}}(\mathbf{w})$

So applying the poisson summation formula to the gaussian function and using its scaling property implies that

$$\begin{aligned} \rho_s(\mathcal{L}) &= \sum_{y \in \mathcal{L}} \rho_s(y) = \frac{1}{\det \mathcal{L}} \sum_{w \in \mathcal{L}^*} \hat{\rho}(w) = \sum_{w \in \mathcal{L}^*} s^n \rho_{1/s}(w) \\ &= s^n \rho_{1/s}(0) + \sum_{w \in \mathcal{L} - \{0\}} \rho_{1/s}(w) \geq s^n \end{aligned}$$

since $\rho_{1/s}$ and s are positive values.**b:**

Recall that

$$\rho_{s,r}(\mathcal{L}) \leq e^{-\pi x^2} \rho_s(\mathcal{L})$$

where $r = \sqrt{\frac{n}{2\pi}}s + xs$ and $x \geq 0$. Thus since $x = 10 \geq 0$ implies that we know

$$\rho_{s,r}(\mathcal{L}) \leq e^{-\pi 100} \rho_s(\mathcal{L})$$

Now since we know that $\rho_s(\mathcal{L}) \geq 2$ implies that given

$$e^{-\pi 100} \rho_{s,r}(\mathcal{L}) < \rho_s(\mathcal{L}) - 1$$

thus

$$\rho_{s,r}(\mathcal{L}) < e^{100\pi}(\rho_s(\mathcal{L}) - 1)$$

Directly implies that

$$\rho_{s,r}(\mathcal{L}) \leq e^{-\pi 100} \rho_s(\mathcal{L}) < \rho_s(\mathcal{L}) - 1$$

that $\rho_{s,r}(\mathcal{L}) < \rho_s(\mathcal{L}) - 1$.



c:

Now let

$$s(n) := 1 + \frac{2n}{\sqrt{n/(2\pi)}}$$

Then since 4.1 shows

$$\rho_s(\mathcal{L}) \geq s^n \forall s > 0$$

Then it will hold that

$$s(n)^n \geq 1 + \frac{2}{\sqrt{n/(2\pi)}}$$

regardless of the n dependence on s .

Now since

$$1 + \frac{2n}{\sqrt{n/(2\pi)}} \geq 1 + \frac{2(n-1)}{\sqrt{(n-1)/(2\pi)}}$$

is equivalent to $\sqrt{n} \geq \sqrt{(n-1)}$ which is trivially true given $n > 1$ then $s(n) \leq s(n-1)$ for $n > 1$.

And since $s(1) = 2$ implies $s(n) \geq 2 \forall n$.

Thus since

$$\rho_{s,r}(\mathcal{L}) < \rho_s(\mathcal{L}) - 1$$

implies that

And since $\lambda_1(\mathcal{L}) \leq r$ implies that since we know $\rho_{s,r}(\mathcal{L}) < \rho_s(\mathcal{L}) - 1$ and

$$\rho_s(\mathcal{L}) = \rho_{s,r}(\mathcal{L}) + \sum_{y \in \mathcal{L} \cap B^n(r)} \rho_s(y)$$

That $\sum_{y \in \mathcal{L} \cap B^n(r)} \rho_s(y) > 1$ which implies that $\sum_{y \in \mathcal{L} \cap B^n(r) - \{0\}} \rho_s(y) > 0$ Which means that since the sum of the fourier components is geq 0 then there must exist a vector in the lattice such taht $\|y\| < r$.

$$\lambda_1(\mathcal{L}) \leq r = (1 + \frac{2}{\sqrt{n/(2\pi)}})(\sqrt{\frac{n}{2\pi}} + 10) < \sqrt{\frac{n}{2\pi}} + 100$$

Shows that $\lambda_1(\mathcal{L}) \leq \frac{n}{2\pi} + 100$

Problem 5:

A bit