1. (10 points) **LLL vs KZ bases**
   (a) (4 points) For any LLL-reduced (with $\delta = 3/4$) basis $B = [b_1, b_2, ..b_n]$ of a lattice $\mathcal{L} = \mathcal{L}(B)$, and for every $1 \leq i \leq n$, show that

$$2^{-i+1} \leq ||\widetilde{b_i}||^2 \lambda_i(\mathcal{L})^{-2} \leq ||b_i||^2 \lambda_i(\mathcal{L})^{-2} \leq 2^{n-1}$$

Solution:

Proof. We first prove the left side of the inequality, we use the upper bound on $\lambda_i(\mathcal{L})$. We know that $B = b_1, b_2...b_n$ are all independent lattice vectors. Considering the i minimum vectors among all the basis vectors, we can observe that
$\lambda_i(\mathcal{L}) \leq i^{th}$ minimum in the set B.
We also note that i^{th} minimum in the set B $\leq i^{th}$ minimum in the set C where each element of B can be mapped to distinct bigger elements in C.
Also from LLL basis we have the property that $||b_i||^2 \leq 2^{i-1}||\widetilde{b_i}||^2$.

$$b_i = \widetilde{b_i} + \sum_{j=1}^{i-1} \mu_{i,j} \widetilde{b_j}$$

$$\mu_{i,j} \leq \frac{1}{2}$$

Applying General Pythogaros theorem, since all graham-schmidt vectors are orthogonal

$$||b_i||^2 = ||\widetilde{b_i}||^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 ||\widetilde{b_j}||^2$$

$$||b_i||^2 \leq ||\widetilde{b_i}||^2 + \frac{1}{4} \sum_{j=1}^{i-1} ||\widetilde{b_j}||^2$$

Using the second property of LLL basis with the given δ we know that,

$$||\widetilde{b_{i+1}}||^2 \geq (\delta - \frac{1}{4})||\widetilde{b_i}||^2 \tag{1}$$

$$\implies 2||\widetilde{b_{i+1}}||^2 \geq ||\widetilde{b_i}||^2 \tag{2}$$

$$\implies ||\widetilde{b_j}||^2 \leq 2^{i-j}||\widetilde{b_i}||^2 \qquad i \geq j \tag{3}$$

$$\implies ||b_i||^2 \leq ||\widetilde{b_i}||^2 + \frac{1}{4} \sum_{j=1}^{i-1} 2^{i-j} ||\widetilde{b_i}||^2 \tag{4}$$

$$\implies ||b_i||^2 \leq ||\widetilde{b_i}||^2 (1 + \frac{1}{4}(2^i - 2)) \tag{5}$$

$$\implies ||b_i||^2 \leq 2^{i-1}||\widetilde{b_i}||^2 \tag{6}$$

$$\lambda_i(\mathcal{L}) \leq i^{th}_{min}(B)$$

Let C be a set where each b_i in B is replaced by $2^{\frac{i-1}{2}}\widetilde{b_i}$.

$$\lambda_i(\mathcal{L}) \leq i^{th}_{min}(C)$$

We note that by 2, all elements in C are increasing with increasing i, hence i^{th} minimum of C is $2^{\frac{i-1}{2}}\widetilde{b_i}$. Hence,

$$\lambda_i(\mathcal{L})^2 \leq 2^{i-1}||\widetilde{b_i}||^2$$
$$2^{-i+1} \leq ||\widetilde{b_i}||^2\lambda_i(\mathcal{L})^{-2}$$

We notice the middle inequality is obvious since $||\widetilde{b_i}|| \leq ||b_i||$. A projection of a vector is always smaller than the vector itself. Hence,

$$||\widetilde{b_i}||^2\lambda_i(\mathcal{L})^{-2} \leq ||b_i||^2\lambda_i(\mathcal{L})^{-2}$$

To consider the final inequality we remember that in class we proved an upper bound on $\lambda(\mathcal{L})$ by showing that any vector of the form $||Bx|| \geq ||\widetilde{b_j}||$, where j is the largest integer from 1 to n where n is the rank of the lattice such that x has a component along b_j when x is written as a discrete sum of the basis vector b's.
Let $V = v_1, v_2..., v_i$ be the linearly independent vector set achieving the ith successive minima. Clearly, $max(||v_i||)) = \lambda_i(\mathcal{L})$. Also from previous argument, $\forall i$, $||v_i|| \geq ||\widetilde{b_{j_i}}||$ where each j_i is dependent on v_i and defined as above.

$$\lambda_i(\mathcal{L}) = \max_{k=1}^{i}(||v_k||) \geq \max_{k=1}^{i}(\widetilde{||b_{j_k}||})$$
$$\lambda_i(\mathcal{L})^2 \geq \max_{k=1}^{i}(\widetilde{||b_{j_k}||}^2)$$
$$\lambda_i(\mathcal{L})^2 2^{n-1} \geq \max_{k=1}^{i}(\widetilde{||b_{j_k}||}^2)2^{n-1}$$

Now we notice the fact that the max of j_k(let it be j') must be greater than equal to i, otherwise, all the i linearly independent vectors in V can be represented by a span of $\widetilde{b_1}, ..., \widetilde{b_{i-1}}$. Hence a contradiction. Thus $j' \geq i$.

$$\lambda_i(\mathcal{L})^2 2^{n-1} \geq (\widetilde{||b_{j'}||}^2)2^{n-1}$$
$$\lambda_i(\mathcal{L})^2 2^{n-1} \geq (\widetilde{||b_{j'}||}^2)2^{j'-i}2^{n-1-j'+i}$$
$$\lambda_i(\mathcal{L})^2 2^{n-1} \geq (||b_i||^2)2^{n-1-j'+i}$$
$$\lambda_i(\mathcal{L})^2 2^{n-1} \geq (||b_i||^2)$$
$$\lambda_i(\mathcal{L})^{-2}(||b_i||^2) \leq 2^{n-1}$$

Hence Proved. □

(b) (6 points) In contrast, for any KZ-reduced basis, $B = [b_1, b_2, ..b_n]$ of a lattice $\mathcal{L} = \mathcal{L}(B)$, and for every $1 \leq i \leq n$, show that

$$\frac{4}{i+3} \leq ||b_i||^2 \lambda_i(\mathcal{L})^{-2} \leq \frac{i+3}{4}$$

Solution:

Proof. We first prove the right inequality. We show a lowerbound on $\lambda_i(\mathcal{L})$. We show that $\lambda_i(\mathcal{L}) \geq ||\widetilde{b_i}||$. Assume otherwise, if $\lambda_i(\mathcal{L}) < ||\widetilde{b_i}||$, then $\lambda_j(\mathcal{L}) < ||\widetilde{b_i}||$, where $1 \leq j \leq i$. We note that $\widetilde{b_i}$ lies in the space perpendicular to the previous b's. And it is the smallest vector for the projected lattice in this space. Since all the i successive minima's are smaller than $||\widetilde{b_i}||$, the projections of the vectors achieving the minima in the space $span\{b_1, ..., b_{i-1}\}^{\perp}$ will also be smaller. As all $v_1 tov_i$ are i vectors achieving successive minima, one of them must have a non-zero component along $\widetilde{b_i}$. (Otherwise the i vectors lie in a smaller span of vectors). This non-zero component of a lattice vector along $\widetilde{b_i}$ is smaller than $||\widetilde{b_i}||$, thus it means we have found a shorter vector that is in the projected lattice space. This is a contradiction, hence our original assumption must be false.

To move further, we introduce a notation for the K-Z basis vectors, where the vector $b_{i,j}$ denotes the component of b_i when we are considering the n+1-j dimension of the projected lattice. When j is 1, we get the full lattice and hence the final basis vectors, $\implies$ $b_{i,1}$ is equal to the basis b_i. We also note that $b_{i,i}$ is equal to $\widetilde{b_i}$. This is because it is the component of b_i when a lattice of n+1-i dimension is considered, when this lattice is considered, we have already projected i-1 times (as n+1-i = n-(i-1)), hence this is the shortest vector that is guessed on the projected lattice, which is same as the graham schmidt vector. We state the following equality $\forall j \leq i$,

$$b_{i,j} = b_{i,i} + \sum_{k=j}^{i-1} \alpha_k b_{k,k}$$

where alpha are the corresponding lifts. This can be proved using induction. We use this equality to state that,

$$b_i = \widetilde{b_i} + \sum_{k=1}^{i-1} \alpha_k \widetilde{b_k}$$

We also note from class that all the lifts can be written in a range of -half to

half.

$$||b_i||^2 \leq ||\widetilde{b_i}||^2 + \sum_{k=1}^{i-1} \alpha_k^2 ||\widetilde{b_k}||^2$$

$$||b_i||^2 \leq ||\widetilde{b_i}||^2 + \frac{1}{4} \sum_{k=1}^{i-1} ||\widetilde{b_k}||^2$$

$$||b_i||^2 \leq \lambda_i(\mathcal{L})^2 + \frac{1}{4} \sum_{k=1}^{i-1} \lambda_k(\mathcal{L})^2$$

$$||b_i||^2 \leq \lambda_i(\mathcal{L})^2 + \frac{1}{4} \sum_{k=1}^{i-1} \lambda_i(\mathcal{L})^2$$

$$||b_i||^2 \leq \lambda_i(\mathcal{L})^2 \frac{i+3}{4}$$

Hence Proved.
We now prove the left side of the inequality, we state first the observation that $\lambda_i(\mathcal{L}) \leq max_{j=1}^{i}(||b_j||)$. We note this because, $b_1, b_2, ...b_i$ are i independent lattice vectors, hence the ith successive minima must be smaller than the maximum of all these.
We also note the fact that $||\widetilde{b_j}|| \leq ||b_i||$ where $j \leq i$, because these are the shortest vectors in the lattice when the reduced lattice was being considered, hence they must be shorter than b_i in the projected lattice, and since after that only additions/lifts have been made in perpendicular directions the vector only grows bigger, hence $||b_i||$ is a bigger vector.

$$||b_i||^2 \leq ||\widetilde{b_i}||^2 + \frac{1}{4} \sum_{k=1}^{i-1} ||\widetilde{b_k}||^2$$

$$\lambda_i(\mathcal{L}) \leq max_{j=1}^{i}(||b_j||)$$

$$\lambda_i(\mathcal{L})^2 \leq max_{j=1}^{i}(||b_j||^2)$$

$$\lambda_i(\mathcal{L})^2 \leq max_{j=1}^{i}(||\widetilde{b_j}||^2 + \frac{1}{4} \sum_{k=1}^{j-1} ||\widetilde{b_k}||^2)$$

$$\lambda_i(\mathcal{L})^2 \leq max_{j=1}^{i}(||b_i||^2 + \frac{1}{4} \sum_{k=1}^{j-1} ||b_i||^2)$$

$$\lambda_i(\mathcal{L})^2 \leq \frac{i+3}{4}(||b_i||^2)$$

Hence Proved □

2. (10 points) **Sublattices**

Let $\mathcal{L}$ be a full rank sublattice of $\mathcal{L}$'

(a) (2 points) $det(\mathcal{L}')|det(\mathcal{L})$

Solution:

Proof. Since L is a full rank sublattice of L', we know that all the basis vector in L can be written as an integer combination of the basis of L'. Hence B can be expressed as B'U where U is a n by n matrix with integer coordinates. Note that since the sublattice is a full rank matrix, the parent lattice is also full rank. Hence $det(B) = det(B')det(U)$ since U has all integer entries, det(U) is an integer, hence, $det(\mathcal{L}) = det(\mathcal{L}') * m$, where m is an integer, this implies that the determinant of a parent lattice divides the sublattice. □

(b) (2 points) $\mathcal{L} = \mathcal{L}'$ if and only if $det(\mathcal{L}) = det(\mathcal{L}')$

Solution:

Proof. If $\mathcal{L} = \mathcal{L}'$, then their determinants are obviously same, hence this side is trivial.
If $det(\mathcal{L}) = det(\mathcal{L}')$, then as in previous part $det(B) = det(B')det(U)$ where U is an integer matrix, this implies that U is a unimodular integer matrix such that $B = B'U$. By the theorem studied in class this implies that the two lattices are same. (Since any integer linear combinations of B' can denoted by B'x. By cramer's rule since $det(U) = 1$, we can find an x' such that $Ux' = x$. Since $det(U) = 1$, cramers rule suggests that x' is also all integers. Hence $B'x = B'Ux' = Bx'$, since any point in $\mathcal{L}'$ is shown to be in $\mathcal{L}$, $\mathcal{L}'$ is a sublattice of $\mathcal{L}$, combining with the assumption we get that both are the same lattices.) □

(c) (3 points) Show that the successive minimum v_1, v_2 form a basis of $\mathcal{L}$, if $\mathcal{L}$ is a 2-dimensional full rank lattice.

Solution:

Proof. First we show the hint part, that projection of v_2 in $\{v_1\}^\perp$ must be a basis for the lattice obtained by projecting on $\{v_1\}^\perp$. Let,
$v_2 = v_2' + \alpha v_1$, where v_2' is the projection of v_2 in the perpendicular space. Let v_2' not be the basis for the projected lattice. Let the basis be a vector x, since v_2' is a point on the lattice, $v_2' = k * x$, where k is an integer not equal to 1, wlog let x be chosen such that k is positive, this implies that k is greater than equal to 2. We write the lifted vector of x as l(x), $l(x) = x + \beta v_1$, $l(x) = \frac{v_2'}{k} + \beta v_1$.

Note that β lies in the range $\{-\frac{1}{2}, \frac{1}{2}\}$

$$||l(x)||^2 = (\frac{||v_2'||}{k})^2 + \beta^2||v_1||^2$$
$$||l(x)||^2 \leq (\frac{||v_2'||}{2})^2 + \beta^2||v_1||^2$$
$$||l(x)||^2 \leq (\frac{||v_2'||}{2})^2 + \frac{1}{4}||v_1||^2$$
$$||l(x)||^2 \leq (\frac{||v_2||}{2})^2 + \frac{1}{4}||v_2||^2$$
$$||l(x)||^2 \leq \frac{3}{4}||v_2||^2$$

Hence we have found a smaller vector than v_2, that belongs in the lattice, is independent from v_1, hence this is a contradiction to the minimality of v_2. Hence v_2' is a basis in the projected space.
We note that any vector x in lattice can be written as $x = kv_2' + \gamma v_1$ where k is an integer. Considering the vector $x - kv_2$, (notice that this vector lies in the lattice, since x and v_2 are both in lattice.)

$$x - kv_2 = (\gamma - k\alpha)v_1$$

We claim that $Z = \gamma - k\alpha$ is an integer since v_1 is the shortest vector in the lattice.
If Z was not an integer, then $(Z - \text{ceil(Z)})v_1$ is also a lattice vector, since Zv_1 and v_1 are both lattice vectors. Note that this is smaller than v_1 and hence contradicts the minimality of v_1. Hence Z is an integer and any vector can be written as an integer combination of v_1 and v_2. □

(d) (3 points) Part d of the problem

Solution:

Proof. If $\mathcal{L}(B) \subseteq \mathcal{L}(C)$, then we know that an integer combination of the basis of C, must be able to represent all the lattice points of B. Since the basis of B are also lattice points in B. Hence an integer combination of C must be able to represent the basis of B, thus $B = CU$, where U is an integer matrix, the dimensions of U are n by k, n rows for the n columns of C, and k columns for that many vectors are produced(the number of basis vectors of B). If $B = CU$, then B is a sublattice of C. To prove this fact we consider any lattice vector of $\mathcal{L}(B)$, it can be denoted by Bx where $x \subseteq \mathbb{Z}^{k\times 1}$. $Bx = CUx = C(Ux)$. Note since U and x both contain only integers, hence $Ux \subseteq \mathbb{Z}^{n\times 1}$. □

3. (10 points) **Covering Radius**

(a) (4 points) B is a basis of $\mathcal{L}$, $\mu(\mathcal{L}) \leq \sqrt{\sum_i ||\widetilde{b_i}||^2}$

Solution:

Proof. We use induction on the dimensions of the lattice to prove this theorem. The given theorem is obvious for one dimensional lattices as the point $||b_1||/2$ satisfies this condition.
We procede to the induction step, let us assume that the lattice made by the basis vectors $b_1, b_2, ...b_k$, has a covering radius less than equal to $\frac{1}{2}\sqrt{\sum_{i=1}^{k} ||\widetilde{b_i}||^2}$. We now try to show the theorem for $k+1$, i.e. to prove that $\mu(\mathcal{L}_{k+1}) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{k+1} ||\widetilde{b_i}||^2}$.
We note that any vector in the span of $b_1, ...b_k$ is at max at a distance of $\frac{1}{2}\sqrt{\sum_{i=1}^{k} ||\widetilde{b_i}||^2}$ from $\mathcal{L}_k$, as $\mathcal{L}_k \subseteq \mathcal{L}_{k+1}$, hence it will also be at max at a distance of of $\frac{1}{2}\sqrt{\sum_{i=1}^{k} ||\widetilde{b_i}||^2}$ from $\mathcal{L}_{k+1}$.
Any vector(v) in the span of $b_1, ..., b_k, b_{k+1}$ can be written as $x\widetilde{b_{k+1}}+v'$, where v' is a vector in the span of $b_1, ..., b_k$. We note that the minimum distance of a vector from a lattice doesnt change if we shift the vector by a lattice point. Hence considering $w = x\widetilde{b_{k+1}} + v''$, where x lies between -half to half, by subtracting by suitable number of b_{k+1}'s. Also v'' is a vector in the span of $b_1, ..., b_k$. If we find the closest vector to v'' in $\mathcal{L}_k$, and calculate the distance of the same lattice vector from w, we find that its norm is $\leq x^2\widetilde{b_{k+1}} + (\frac{1}{2}\sqrt{\sum_{i=1}^{k} ||\widetilde{b_i}||^2})^2$. As x is within range of -1/2 to 1/2, we have found that for every point in the span, there are lattice points that are at a distance of $\frac{1}{2}\sqrt{\sum_{i=1}^{k+1} ||\widetilde{b_i}||^2}$. Hence Proved. □

(b) (2 points) Give a lattice such that, $\frac{\mu(\mathcal{L})}{\lambda_1(\mathcal{L})} = \Omega(\sqrt{n})$

Solution:

Proof. The Lattice $\mathbb{Z}^n$ achieves this, clearly the shortest vector here has norm 1, but the vector where all coordinates are half is atleast a distance of half on all coordinates away from every integer point, hence $\mu(\mathcal{L}) \geq \sqrt{(}n)/2$, hence this matrix satisfies the required property. □

4. (10 points) SVP vs GapSVP

(a) (2 points) $GapSVP_\gamma$ can be reduced to approximation algo.

Solution:

Proof. Here we assume an oracle for the approximation algo with factor γ, and we use this to answer a decision $GapSVP_\gamma$ that has as input a lattice L, real number r.
Reduction is as follows, run the approximation algo on the same input lattice, the output of the algorithm is a r' st $\lambda \leq r' < \gamma\lambda$. We now note the relation between r and r'. If $r \leq r'$, answer YES to the GapSVP problem, otherwise answer NO. We claim that this will always be a correct strategy, as if r was smaller than lambda i.e a YES, it will always be smaller than the output of the algorithm, and if it was a NO, it will always be greater than the output of the algorithm. □

(b) (2 points) approximation algo can be reduced to $GapSVP_\gamma$.

Solution:

Proof. Here we assume an oracle for the $GapSVP_\gamma$ and we use this to output a real with approximation factor γ.
Reduction is as follows. We do binary search, we set the lower bound of the search as zero, and the upper bound of the search as $||x|| + 1$, where x is any lattice vector. We know that on the lower bound the GapSVP oracle answers NO and on the upper bound it answers YES. We keep running binary search on the two ranges and stop when the range is smaller than an epsilon, at this point we have a small range where the left value(l) answers NO, and the right value(r) had answered YES. Since l answered NO we know that $\lambda > l$, also since r answered YES, we know that $r \geq \frac{\lambda}{\gamma}$. Since l is approximately close to r, we can write, $\frac{\lambda}{\gamma} \leq r < \lambda$, multiply r by γ and output as the output of the algo.
$\lambda \leq \gamma r < \lambda\gamma$
Choose epsilon such that the range is much smaller than the approximation range. We can use exponential bounds on λ to be accurate. Since binary search is logarithmic, even an exponential bound would be polynomial in running time. □

(c) (3 points) $GapSVP_\gamma$ can be reduced to SVP_γ.

Solution:

Proof. Here we assume an oracle for SVP_γ, and we use this to answer a decision $GapSVP_\gamma$ that has as input a lattice L, real number r.
Reduction is as follows, run the SVP_γ on the same input lattice, the output of the algorithm is a vector v, such that $||v|| \leq \gamma\lambda$. We now note the relation between r and $||v||$. If $r \leq ||v||$, answer YES to the GapSVP problem, otherwise answer NO. We claim that this will always be a correct strategy, as if r was smaller than lambda i.e a YES, it will always be smaller than the output of the

algorithm, and if it was a NO, it will always be greater than the output of the algorithm. □

(d) (3 points) SVP_1 can be reduced to $GapSVP_1$.

Solution:

Proof. Here we assume an oracle for $GapSVP_1$, and we use this to find a vector satisfying SVP_1 that has as input a lattice L.
Basically we have to show that search is not harder than decision. Given the exact decision version, we can conduct binary search and find the exact magnitude of the shortest vector.
We also have to find a vector that achieves this magnitude. To find this vector, we can make the lattice sparser and sparser and try to approximate the sparse matrix using LLL algorithm. □