TUTORIAL 1

1 Equivalent definition

Recall that we defined a lattice $\mathcal{L}$ in $\mathbb{R}^n$ as a set of the form $\{\sum_{i=1}^{n} x_i b_i \,|\, x_1, \cdots, x_n \in \mathbb{Z}\}$, where the vectors $(b_i)_i$ are n linearly independent vectors in $\mathbb{R}^n$ and are called a basis of $\mathcal{L}$. This definition actually defines what we usually call "full rank lattices", i.e., lattices generated by n linearly independent vectors in a space of dimension n, as opposed to those generated by n linearly independent vectors in a space of dimension $m > n$. In the lectures and the tutorials, we will assume that the lattices are always full rank (and will omit to say so).

In the rest of this exercise sheet, we will admit the following result:

Lemma: *$\mathcal{L} \subset \mathbb{R}^n$ is a lattice if and only if the three following conditions hold*

1. *$\mathcal{L}$ is closed under addition and subtraction (i.e., $\mathcal{L}$ is an additive subgroup of $\mathbb{R}^n$);*
2. *$\mathcal{L}$ is discrete (i.e., there exists some $c > 0$ such that for any $x, y \in \mathcal{L}$, we have $\|x - y\| \geq c$);*
3. *$\mathcal{L}$ contains n linearly independent vectors.*

2 Lattice bases (⋆)

The objective of this exercise is to prove a bunch of properties regarding bases of lattices. Throughout this exercise, the matrix B (or the matrices B_1, B_2) are invertible matrices in $\mathrm{GL}_n(\mathbb{R})$ for some dimension $n > 0$. Recall that we write $\mathcal{L}(B)$ for the lattice spanned by the columns of the matrix B.

1. Let $B_1, B_2 \in \mathrm{GL}_n(\mathbb{R})$. Show that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ if and only if $B_1 = B_2 \cdot U$ for some $U \in \mathbb{Z}^{n \times n}$ such that $\det(U) = \pm 1$. Such a matrix U is called unimodular. It is an invertible integer matrix whose inverse is also an integer matrix.

   A: Assume first that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Then, every column of B_1 belongs to $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Hence, by definition of the lattice $\mathcal{L}(B_2)$ (integer linear combinations of the columns of B_2), we know that there exists an integer square matrix U_1 such that $B_1 = B_2 \cdot U_1$. Since B_1 and B_2 are both invertible, then U_1 is also invertible (over $\mathbb{R}$). Our objective is to show that U_1 is invertible over $\mathbb{Z}$ (i.e., it's inverse is also an integer matrix). By a similar argument, we know that there exist an invertible (over $\mathbb{R}$) integer matrix U_2 such that $B_2 = B_1 \cdot U_2$.

   Combining both equations, we obtain $B_1 = B_2 \cdot U_1 = B_1 \cdot U_2 \cdot U_1$. Since B_1 is invertible, we can simplify this into $I_n = U_2 \cdot U_1$. Since U_1 and U_2 are invertible over $\mathbb{R}$, their inverse is unique and we conclude that $U_1^{-1} = U_2$ is an integer matrix as desired.

   To conclude, observe that since U_1 and U_2 are integer matrices, then their determinant is also an integer. But we have $1 = \det(I_n) = \det(U_1 \cdot U_2) = \det(U_1) \cdot \det(U_2)$. Hence, the only possibility for $\det(U_1)$ is 1 or -1 (these are the only invertible elements in $\mathbb{Z}$).

   In the other direction, assume that $B_1 = B_2 \cdot U$ with U integer and $\det(U) = \pm 1$. Then, U is invertible over $\mathbb{R}$ and its inverse matrix U^{-1} has integer coefficients (recall that $U^{-1} = 1/\det(U) \cdot \mathrm{adj}(U)$ where the adjugate matrix $\mathrm{adj}(U)$ is integral since U is).

   Since U is integral, then by definition every column of $B_1 = B_2 \cdot U$ is in the lattice spanned by B_2. Hence we have $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$. Since U^{-1} is also integral, then every column of $B_2 = B_1 \cdot U^{-1}$ is in the lattice spanned by B_1, and we conclude that $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$.

2. Let B_1 and B_2 be two bases of the same lattice $\mathcal{L}$. Prove that $|\det(B_1)| = |\det(B_2)|$.
This shows that the quantity $|\det(B)|$ does not depend on the choice of the basis B of $\mathcal{L}$, but only on the lattice $\mathcal{L}$. It is usually called the volume or the determinant of the lattice $\mathcal{L}$, and written $\mathrm{vol}(\mathcal{L})$ or $\det(\mathcal{L})$.

A: We have seen in the previous questions that if $\mathcal{L}(B_1) = \mathcal{L}(B_2)$, then $B_1 = B_2 \cdot U$ for some matrix U with $\det(U) = \pm 1$. Taking the absolute value of the determinant of this equation proves that $|\det(B_1)| = |\det(B_2)|$.

3. Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two lattices of rank n. Show that if $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then $\det(\mathcal{L}_1) = k \cdot \det(\mathcal{L}_2)$ for some integer $k > 0$. This integer k is called the index of $\mathcal{L}_1$ inside $\mathcal{L}_2$ and is written $[\mathcal{L}_2 : \mathcal{L}_1]$.

A: Let B_1 be a basis of $\mathcal{L}_1$ and B_2 be a basis of $\mathcal{L}_2$. Since $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then every column of B_1 is in $\mathcal{L}(B_2)$, i.e., there is an integer matrix X such that $B_1 = B_2 \cdot X$. Taking the determinant, we have $\det(B_1) = \det(B_2) \cdot \det(X)$. Hence, $k = |\det(X)|$ and k is indeed an integer since X has integer coefficients (and k is non-zero since B_1 and B_2 are both invertible).

The determinant of a lattice is an important quantity, mostly useful in cryptography thanks to Minkowski's first theorem. This theorem states that in any lattice $\mathcal{L}$ of dimension n, there exists a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$.

4. Show that the upper bound in Minkowski's first theorem can be quite loose for some lattices: construct a lattice with $\det(\mathcal{L}) = 1$ and which contains a non-zero vector v whose euclidean norm is arbitrarily close to 0.

A: Take $\varepsilon > 0$ and define $\mathcal{L}$ to be the lattice with basis $b_1 = (\varepsilon, 0)^T$ and $b_2 = (0, \varepsilon^{-1})^T$. Then $\det(\mathcal{L}) = 1$ but $\mathcal{L}$ contains the vector b_1 whose norm can be arbitrarily close to 0.

The objective of the next questions is to observe that when dealing with lattices, a maximal set of independent vectors is not always a basis, and a minimal set of generating vectors is also not always a basis (which differs from what we are used to in vector spaces).

5. Exhibit a family of n linearly independent vectors in $\mathbb{Z}^n$ which do not form a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

A: One example is the family $b_i = (0, \ldots, 0, 2, 0, \ldots, 0)$ with a 2 in i-th position, for $i = 1$ to n. Those vectors are linearly independent but they generate the lattice $(2\mathbb{Z})^n$, which is included strictly in $\mathbb{Z}^n$. Note that one cannot add a vector to this family of vectors and still have independent vectors (because independence is defined over $\mathbb{R}$, where things work as expected: the maximal size of an independent set of vectors in $\mathbb{R}^n$ is n).

6. Exhibit a family of $n + 1$ vectors generating $\mathbb{Z}^n$ such that it is not possible to remove any vector from this set to obtain a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

A: Take $b_0 = (2, 0, \ldots, 0)$, $b_1 = (3, 0, \ldots, 0)$ and $b_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with a i at the i-th position for $i = 2$ to n. Then $(b_i)_{0 \leq i \leq n}$ generates $\mathbb{Z}^n$. This is because 2 and 3 are coprime, hence one can find an integer linear combination of b_1 and b_2 with a 1 in its first coordinate (just take $b_1 - b_0 = (1, 0, \ldots, 0)$).

However, one can check that removing b_0 or b_1 from the list of generator does not generate $\mathbb{Z}^n$ anymore: the first coordinate will always be a multiple of 2 or 3. Similarly, we cannot remove one of the b_i for $i \geq 2$ since the i-th coordinate would always be 0.

7. Compute a basis for the lattice generated by $c_1 = (2\pi, 4)^T$, $c_2 = (0, 3)^T$ and $c_3 = (4\pi, 4)^T$. Same question for $c_1 = (1, 0)^T$, $c_2 = (1, 1)^T$ and $c_3 = (1, \pi)^T$. $(\star\star)$
(Hint: the question might be lying to you. In this case, show what is wrong in the question. :)).

A: A basis for the first lattice is given by $b_1 = (2\pi, 0)^T$ and $b_2 = (0, 1)^T$. A way to check that this is indeed a basis of the lattice generated by c_1, c_2 and c_3 is to check that each of the b_i is in the $\mathbb{Z}$-span of the c_i-s (note: $b_2 = 2c_1 - c_3 - c_2$ and $b_1 = c_1 - 4b_2$) and that reciprocally each of the c_i is in the $\mathbb{Z}$-span of the b_i's. This shows that the b_i an the c_i generates the same lattice. Then observe that the b_i are 2 linearly independent vectors in $\mathbb{R}^2$ hence they form a basis of their lattice.

For the second example, it turns out that the $\mathbb{Z}$-span of c_1, c_2 and c_3 is not a lattice. A way to see this is that a lattice must be discrete (see the alternative definition in Section 1). But the $\mathbb{Z}$-span of c_1, c_2 and c_3 is not discrete. Indeed, we have $(0, 1)^T$ and $(0, \pi)^T$ in the $\mathbb{Z}$-span. Since π is not a rational number, we can create a vector $(0, \varepsilon)^T$ with ε as small as we want by taking integer linear combinations of those two vectors. This shows that the $\mathbb{Z}$-span of the c_i contains an accumulation point at 0, and so it is not a lattice.

3 HNF basis (⋆⋆)

In this exercise, we will see how to compute the HNF basis of a lattice $\mathcal{L}$. The algorithm to compute the HNF basis is very similar to the way one would use Gaussian elimination to compute the echelon form of matrices over a field. The main difference is that since we are only allowed to perform integer linear combinations over the vectors of our basis, we cannot multiply by the inverse of a coefficient, in order to annihilate the other coefficients on the same row.

1. Let's review Gaussian elimination a little. Run Gaussian elimination (over $\mathbb{R}$) on the columns of the matrix $M = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$ in order to obtain a triangular matrix of the form $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$. (Here, running Gaussian elimination on the columns means that you are only allowed to perform operations on the columns of the matrix. Said differently, you can only multiply M by invertible matrices on the right).

   A: In order to obtain a 0 on the top-right part of the matrix, we perform the operation $C_2 \leftarrow C_2 - 3/2 \cdot C_1$ (where C_1 and C_2 are the columns of the matrix M). This corresponds to multiplication on the right by the matrix $\begin{pmatrix} 1 & -3/2 \\ 0 & 1 \end{pmatrix}$. We then obtain the matrix $\begin{pmatrix} 2 & 0 \\ 3 & -1/2 \end{pmatrix}$, which has the desired shape.

2. In the previous question, the operations we performed on the columns were not integer. We now want to focus on integer operations on the columns of M. Show that there exists an integer matrix U with determinant 1 such that $M \cdot U = \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$.

   A: The matrix $U = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$ has integral coefficient, determinant 1 and satisfies $M \cdot U = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 1 & -4 \end{pmatrix}$ as desired.

3. More generally, show that for any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ there is a unimodular matrix U such that $M \cdot U = \begin{pmatrix} \gcd(a, b) & * \\ * & * \end{pmatrix}$. (⋆⋆)

   A: We know by Bézout's identity that there exists u, v integers such that $au + bv = \gcd(a, b)$. Moreover, this equality also shows that such u and v must be coprime, since $\gcd(a, b)$ already divides a and b. Hence, applying Bézout's identity once more to u and v, we have x and y such that $ux + vy = 1$. Take the matrix $U = \begin{pmatrix} u & -y \\ v & x \end{pmatrix}$. The first column of this matrix is constructed such that the top-left coefficient of $M \cdot U$ is equal to $au + bv = \gcd(a, b)$. The second column of the matrix is added so that the matrix U has determinant 1 (so that it is invertible over $\mathbb{Z}$). This is ensured by the second Bézout's identity, which shows that $\det(U) = ux + yv = 1$, i.e., U is unimodular.

4. Using the previous question, show that for any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ there is a unimodular matrix U such that $M \cdot U = \begin{pmatrix} \gcd(a,b) & 0 \\ * & * \end{pmatrix}$.

A: Once we have applied the unimodular matrix U from the previous question, we obtain a basis of the form $\begin{pmatrix} \gcd(a,b) & z \\ * & * \end{pmatrix}$. Moreover, we know that z must be a multiple of $\gcd(a,b)$, since it is an integer linear combination of a and b (all top coefficient of vectors in $\mathcal{L}(M)$ must be integer linear combinations of a and b). Hence, from now on, we can use regular Gaussian elimination and perform $C_2 \leftarrow C_2 - z/\gcd(a,b)C_1$ to annihilate the top-right coefficient (where C_1 and C_2 are the columns of the matrix $M \cdot U$). This operation is obtained by multiplying on the right by the matrix $U' = \begin{pmatrix} 1 & -z/\gcd(a,b) \\ 0 & 1 \end{pmatrix}$ which is integer and unimodular as desired.

5. Compute a matrix U as in the previous question for $M = \begin{pmatrix} 9 & 2 \\ 3 & 1 \end{pmatrix}$.

A: $U = \begin{pmatrix} -1 & -2 \\ 5 & 9 \end{pmatrix}$ which gives $M \cdot U = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$

6. Let $M_1 = \begin{pmatrix} 2 & 1 & 0 \\ 8 & 1 & 4 \\ 0 & 1 & 7 \end{pmatrix}$. Generalize the algorithm from the previous questions to compute a matrix M_2 such that $M_2 = M_1 \cdot U$ for some unimodular matrix U and M_2 is of the form $M_2 = \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$.

A: $U = \begin{pmatrix} 0 & -1 & -2 \\ 1 & 2 & 4 \\ 0 & 2 & 3 \end{pmatrix}$ and $M_2 = M_1 \cdot U = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 16 & 25 \end{pmatrix}$

7. Let $\mathcal{L}$ be a lattice of dimension n. Show that there is a unique basis B of $\mathcal{L}$ such that $b_{i,j} = 0$ when $j > i$, $b_{i,i} > 0$ and $0 \leq b_{i,j} < b_{i,i}$ for $j < i$. This basis is called the Hermite normal form (HNF) basis of $\mathcal{L}$. $(\star\star)$

A: First, observe that the algorithm that we described in the previous question provides an algorithmic proof that such a basis exists (the condition that $b_{i,j} \in [0, b_{i,i})$ for $j < i$ is ensured by reducing the non-diagonal coefficients modulo the diagonal coefficients, from top to bottom).

Let us now prove that such a basis is unique. Assume for a contradiction that there exists two such bases B and C, with columns b_j and c_j. Let j_0 be maximal such that $b_{j_0} \neq c_{j_0}$. Since B and C span the same lattice, then b_{j_0} is an integer linear combination of the vectors $(c_j)_{1 \leq j \leq n}$. Moreover, because of the special shape of C and since the top coefficients of b_{j_0} are 0, then is must be that b_{j_0} is a combination of the columns c_j for $j \geq j_0$. This implies that the diagonal coefficient b_{j_0,j_0} is an integer multiple of c_{j_0,j_0}. But a similar argument shows that c_{j_0,j_0} is an integer multiple of b_{j_0,j_0}, hence we conclude that $|b_{j_0,j_0}| = |c_{j_0,j_0}|$. Since both are positive by assumption, we conclude that $b_{j_0,j_0} = c_{j_0,j_0}$.

From this, we know that $b_{j_0} = c_{j_0} + \sum_{j > j_0} a_j \cdot c_j$ for some integers a_j's. However, we know that $c_j = b_j$ for any $j > j_0$ by choice of j_0, which means that the diagonal coefficients $b_{j,j}$ and $c_{j,j}$ are the same for $j > j_0$. We also know that the bottom coefficients of both b_{j_0} and c_{j_0} are reduced modulo those diagonal coefficients $c_{j,j} = b_{j,j}$. Hence, a recursive argument shows that a_j must be equal to 0 for all $j > j_0$, and we conclude that $b_{j_0} = c_{j_0}$, which is a contradiction.

4 LWE and SIS lattices ($\star\star$)

Let $q, m, n > 0$ be integers and $A \in \mathbb{Z}_q^{m \times n}$. Recall that the SIS lattice associated to A is defined by $\Lambda^\perp(A) := \{x \in \mathbb{Z}^m \,|\, x^T \cdot A = 0 \bmod q\}$. Recall similarly that the LWE lattice associated to A is $\Lambda(A) := \{x \in \mathbb{Z}^m \,|\, \exists s \in \mathbb{Z}^n$ s.t. $As = x \bmod q\}$.

1. Show that the sets $\Lambda^\perp(A)$ and $\Lambda(A)$ are indeed lattices in $\mathbb{R}^m$.

   A: We use the definition of a lattice given in Section 1. First, one can check from the definitions that $\Lambda^\perp(A)$ and $\Lambda(A)$ are stable by addition and subtraction. Second, since $\Lambda^\perp(A)$ and $\Lambda(A)$ are both included in $\mathbb{Z}^m$, they are discrete.

   It remains to show that they contain m linearly independent vectors. Both lattices are what we call q-ary lattices, meaning that they contain $q\mathbb{Z}^m$, hence they indeed contain m linearly independent vectors: the vectors $(0, \ldots, 0, q, 0, \ldots, 0)$ with q ranging from position 1 to m. This shows that the two sets are lattices in $\mathbb{R}^m$.

2. Show that $\Lambda(A)$ is generated by the columns of A and the m vectors $q \cdot e_i$ (with $1 \leq i \leq m$), where e_i is the vector with a 1 at the i-th position and 0's everywhere else.

   A: First, one can check that $\Lambda(A)$ indeed contains the column vectors of A (take $s = (0, \ldots, 0, 1, 0, \ldots, 0)$ in the definition of $\Lambda(A)$) and the m vectors $q \cdot e_i$ (take $s = 0$).

   Let us then show the reverse inclusion. Let $x \in \Lambda(A)$. By definition, there must exist a vector $s \in \mathbb{Z}^n$ and $z \in \mathbb{Z}^m$ such that $x = A \cdot s + q \cdot z$. This shows that x is an integer linear combination of the columns of A and the $q \cdot e_i$ vectors. Hence, those vectors indeed generate the lattice $\Lambda(A)$.

3. Assume that q is prime. Using the previous question, exhibit a set of generating vectors for the lattice $\Lambda^\perp(A)$. (Hint: you might want to show that $\Lambda^\perp(A) = \Lambda(B)$ for some well chosen matrix B).

   A: Let $B \in \mathbb{Z}^{m \times k}$ be a basis (in columns) of the left kernel of A modulo q, i.e., $B^T \cdot A = 0 \bmod q$ (here, we use the fact that q is prime so that $\mathbb{Z}_q$ is a field and the kernel of A is a vector space). We know that $k \geq m - n$, but it could be bigger if the rank of A modulo q is $< n$. We have that $x \in \Lambda^\perp(A)$ if and only if $x^T \cdot A = 0 \bmod q$, which is equivalent to x belongs to the span of the columns of B modulo q, i.e., $x \in \Lambda(B)$. Using the previous question, we conclude that the column vectors of B together with the $q \cdot e_i$ vectors form a generating set of $\Lambda^\perp(A)$.

4. Assume again that q is prime. Assume also that $m \geq n$ and that the rank of A modulo q is n (i.e., the n column vectors of A are linearly independent modulo q). Show that up to permuting the rows of A (i.e., permuting the coefficients of the vectors in $\Lambda(A)$), there exists a basis of $\Lambda(A)$ of the form $\begin{pmatrix} I_n & 0_{n \times (m-n)} \\ A' & q \cdot I_{m-n} \end{pmatrix}$, for some integer matrix $A' \in \mathbb{Z}^{(m-n) \times n}$. ($\star\star$)

   Similarly, show that up to permuting the rows of A, there exists a basis of $\Lambda^\perp(A)$ of the form $\begin{pmatrix} I_{m-n} & 0_{(m-n) \times n} \\ B' & q \cdot I_n \end{pmatrix}$, for some integer matrix $B' \in \mathbb{Z}^{n \times (m-n)}$.

   A: First, observe that by definition of $\Lambda(A)$, the lattice only depends on the span over $\mathbb{Z}_q$ of the columns of A, and not the actual choice of the basis A. Also, since the rank of the columns of A is n, then up to permuting the rows of A, we can assume that $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ with $A_1 \in \mathbb{Z}^{n \times n}$ invertible modulo q.

   Hence, we have $\Lambda(A) = \Lambda(A \cdot A_1^{-1})$, where $A \cdot A_1^{-1} = \begin{pmatrix} I_n \\ A' \end{pmatrix}$, with $A' = A_2 \cdot A_1^{-1}$.

   By a previous question, we know that the columns of $\tilde{A} := \begin{pmatrix} I_n \\ A' \end{pmatrix}$ together with the $q \cdot e_i$ vectors generate the lattice $\Lambda(A)$.

   Observe now that because of the special shape of $\tilde{A}$, the first n vectors $q \cdot e_i$ are already in the span of the columns of $\tilde{A}$ and the other $q \cdot e_j$ vectors for $j > n$ (for $i \leq n$, the vector $q \cdot e_i$ can be obtained by multiplying the i-th column of $\tilde{A}$ by q

and annihilating the bottom $m-n$ coordinates using the $q \cdot e_j$ with $j > n$ since those coordinates will be integer multiples of q).

Hence, the n column vectors of A together with the $(m-n)$ vectors qe_j for $j > n$ generate the lattice $\Lambda(A)$. Since those are exactly m vectors, they form a basis of the lattice, with the desired shape.

Regarding $\Lambda^\perp(A)$, we have already seen in a previous question that this lattice is equal to $\Lambda(B)$ where B forms a basis of the kernel of A. Since A has rank n modulo q, then we know that B has dimension $m \times (m-n)$ and rank $m-n$ modulo q. Applying what we have done above to the matrix B solves the second part of the question.

5. Assuming that q is prime and that A has rank n modulo q, show that the SIS lattice $\Lambda^\perp(A)$ contains a non-zero vector of norm $\leq \sqrt{m} \cdot q^{n/m}$ and that the LWE lattice $\Lambda(A)$ contains a non-zero vector of norm $\leq \sqrt{m} \cdot q^{1-n/m}$.

   A: From the previous question, we know that $\det(\Lambda(A)) = q^{m-n}$ and $\det(\Lambda^\perp(A)) \leq q^n$ (permuting the coefficients of the vectors does not change the volume of the lattices). The shortness of the vectors then follows from Minkowski's first theorem.

5 Solving the closest vector problem ($\star$)

Babai's round-off algorithm solves the approximate closest vector problem as follows. Given as input a basis $(b_i)_{1 \leq i \leq n}$ of the lattice $\mathcal{L}$ (of dimension n) and a target t, the algorithm writes $t = \sum_{i=1}^n t_i b_i$ with $t_i \in \mathbb{R}$ and output the vector $s = \sum_i \lceil t_i \rfloor b_i$.

1. Show that Babai's round-off algorithm finds a point $s \in \mathcal{L}$ such that $\|t - s\| \leq 1/2 \cdot n \cdot \max_i \|b_i\|$.

   A: Since the $\lceil t_i \rfloor$'s are integers, then s belongs indeed to the lattice $\mathcal{L}$.

   Let us now compute the distance to t. For $x \in \mathbb{R}$, we write $\{x\} = x - \lceil x \rfloor$ the fractional part of x. It belongs to $[-1/2, 1/2]$.

$$\begin{aligned} \|s - t\| &= \|\sum_i \{t_i\} \cdot b_i\| \\ &\leq \sum_i |\{t_i\}| \cdot \|b_i\| \\ &\leq 1/2 \cdot n \cdot \max_i \|b_i\|. \end{aligned}$$

6 Lagrange-Gauss algorithm ($\star\star\star$)

Recall the Lagrange-Gauss algorithm: given as input a basis (b_1, b_2) of a lattice in $\mathbb{R}^2$, the algorithm finds $x \in \mathbb{Z}$ that minimizes $\|b_2 - xb_1\|$ and replaces b_2 by $b_2 - xb_1$ (finding x efficiently is done by computing the QR factorization of the basis B, this step is not important for this exercise). The algorithm then switches b_1 and b_2 and starts again. The algorithm stops when no progress is made for two consecutive iterations (which means that we cannot reduce b_1 by b_2 nor b_2 by b_1 anymore).

1. Let b_1 and b_2 be two non-zero vectors in $\mathbb{R}^2$. Show that if $\|b_1\| \leq \|b_1 + b_2\|$, then for any $\alpha \in (1, +\infty)$ it holds that $\|b_1 + b_2\| \leq \|b_1 + \alpha b_2\|$. ($\star\star$)

   A: Let us consider the function

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}_+ \\ \alpha &\mapsto \|b_1 + \alpha b_2\| \end{aligned}$$

   A drawing shows that this is a convex function which has a unique minimum at α_0, is decreasing on $(-\infty, \alpha_0]$ and increasing on $[\alpha_0, +\infty)$. Since $\|b_1\| \leq \|b_1 + b_2\|$ (i.e., $f(0) \leq f(1)$) by assumption, then it must be that $\alpha_0 \leq 1$. From this we conclude that f is increasing on $[1, +\infty)$ which implies that $\|b_1 + b_2\| \leq \|b_1 + \alpha b_2\|$ for any $\alpha \geq 1$.

2. Show that if the Lagrange-Gauss algorithm terminates, then either b_1 or b_2 is a shortest non-zero vector of $\mathcal{L}$. (Hint: you may want to consider a shortest non-zero vector $s = x_1 b_1 + x_2 b_2$ and write it as $s = x_1 \cdot (b_1 + \alpha b_2)$ with $\alpha = x_2/x_1$ if $x_1 \neq 0$.) $(\star\star\star)$

A: Without loss of generality, assume that $\|b_1\| \leq \|b_2\|$. Let's use the hint and take $s = x_1 b_1 + x_2 b_2$ be a shortest non-zero vector in $\mathcal{L}$ (with x_1 and x_2 integers). Without loss of generality, we can assume that $x_1, x_2 \geq 0$ (otherwise we can multiply b_1 and/or b_2 by -1, which does not change their size nor the fact that the algorithm cannot reduce them anymore).

If $x_1 = 0$, then we must have $x_2 \geq 1$ (since $x_2 \neq 0$ is a non-negative integer). Then we have $\|b_1\| \leq \|b_2\| \leq \|x_2 b_2\| = \|s\|$, from which we conclude that b_1 is a shortest non-zero vector of $\mathcal{L}$.

Similarly, if $x_2 = 0$, then $\|b_1\| \leq \|x_1 b_1\| = \|s\|$ and so b_1 is a shortest non-zero vector.

Let us now assume that x_1 and x_2 are both non-zero. Assume that $x_1 \geq x_2$, then $s = x_2 \cdot (\alpha b_1 + b_2)$, with $\alpha = x_1/x_2 \geq 1$. Since the algorithm terminated, we know that b_2 cannot be reduced anymore be adding to it multiples of b_1, which implies in particular that $\|b_2\| \leq \|b_2 + b_1\|$. From the previous question, we conclude that $\|b_2 + b_1\| \leq \|b_2 + \alpha b_1\| \leq \|s\|$ (since $x_2 \geq 1$). We finally conclude that $\|b_1\| \leq \|b_2\| \leq \|b_2 + b_1\| \leq \|s\|$ as desired.

If $x_1 \leq x_2$, the situation is very similar. We have

$$\begin{aligned} \|b_1\| &\leq \|b_1 + b_2\| \\ &\leq |x_1| \cdot \|b_1 + b_2\| \\ &\leq |x_1| \cdot \|b_1 + (x_2/x_1) \cdot b_2\| \\ &= \|s\|. \end{aligned}$$