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 ($\star$)

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.

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 $\det(\mathcal{L})$.

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 $[\mathcal{L}_2 : \mathcal{L}_1]$.

   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 is not tight: construct a lattice with $\det(\mathcal{L}) = 1$ and which contains a non-zero vector v whose euclidean norm is 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 $\mathbb{Z}^n$.

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 $\mathbb{Z}^n$.

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. :)).

3 HNF basis $(\star\star)$

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).

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 $M \cdot U = \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$.

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 $M \cdot U = \begin{pmatrix} \gcd(a,b) & * \\ * & * \end{pmatrix}$. $(\star\star)$

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 $M \cdot U = \begin{pmatrix} \gcd(a,b) & 0 \\ * & * \end{pmatrix}$.

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

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 $M_2 = \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$.

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 $\mathcal{L}$. $(\star\star)$

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 $\Lambda(A) := \{x \in \mathbb{Z}^m \,|\, \exists s \in \mathbb{Z}^n \text{ s.t. } As = x \bmod q\}$.

1. Show that the sets $\Lambda^{\perp}(A)$ and $\Lambda(A)$ are indeed 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 $1 \le i \le m$), where e_i is the vector with a 1 at the i-th position and 0's everywhere else.

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).

4. Assume again that q is prime. Assume also that $m \ge n$ 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 $B' \in \mathbb{Z}^{n\times(m-n)}$.

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 $\le \sqrt{m} \cdot q^{n/m}$ and that the LWE lattice $\Lambda(A)$ contains a non-zero vector of norm $\le \sqrt{m} \cdot q^{1-n/m}$.

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 $(b_i)_{1\le i\le n}$ 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 $\|t - s\| \le 1/2 \cdot n \cdot \max_i \|b_i\|$.

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 $\|b_1\| \le \|b_1 + b_2\|$, then for any $\alpha \in (1, +\infty)$ it holds that $\|b_1 + b_2\| \le \|b_1 + \alpha b_2\|$. $(\star\star)$

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 $x_1 \neq 0$.) $(\star\star\star)$