EXERCISES

In all the exercises, unless specified otherwise, we take $P = X^d + 1$ for d a power-of-two, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$.

1 Canonical and coefficient embeddings

In this exercise, we take $P = X^d + 1$ for d a power-of-two, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$.

1. Show that the map from $\mathbb{Q}^d$ to $\mathbb{C}^d$ sending $\Sigma(a)$ to $\tau(a)$ (for $a \in K$) is a $\mathbb{Q}$-linear morphism. Exhibit the matrix $M \in \mathrm{GL}_d(\mathbb{C})$ such that $\tau(a) = M \cdot \Sigma(a)$ for all $a \in K$.
2. How can we compute $\Sigma(a)$ in polynomial time from $\tau(a)$? (this is equivalent to inverting the map τ, since recovering a from $\Sigma(a)$ is immediate).
3. Show that $M \cdot M^* = d \cdot I_d$, where $M^* = \overline{M}^T$.
   (Hint 1: you may want to prove first that if $\zeta \in \mathbb{C}$ is a m-th root of unity different from 1, then $\sum_{i=0}^{m-1} \zeta^i = 0$)
   (Hint 2: to prove Hint 1, you can consider the equality $(\sum_{i=0}^{m-1} X^i) \cdot (X-1) = X^m - 1$
4. Deduce from the previous question that we also have $M^* \cdot M = d \cdot I_d$.
5. Conclude that $\|\tau(a)\| = \sqrt{d} \cdot \|\Sigma(a)\|$ for all $a \in K$.

2 Ideal lattices

In this exercise again, we take $P = X^d + 1$ for d a power-of-two, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$.

1. Show that if $a \in K$ is non-zero, then the d vectors $\tau(a \cdot X^i)$ for $i = 0$ to $d-1$ are $\mathbb{Q}$-linearly independent.
   (Hint: you may want to use the fact that $\sigma : K \to \mathbb{C}^d$ is injective)
2. Show that for any $a, b \in R$ with $a \neq b$, then $\|\tau(a) - \tau(b)\| \geq \sqrt{d}$.
   (Hint: you may want to use the fact that $\|\tau(x)\| = \sqrt{d} \cdot \|\Sigma(x)\|$)
3. Conclude that for any non-zero ideal $\mathfrak{a}$, the set $\tau(\mathfrak{a})$ is a lattice of rank d in $\mathbb{C}^d$.
4. Show that in any non-zero ideal $\mathfrak{a}$, it holds that $\lambda_1(\tau(\mathfrak{a})) = \cdots = \lambda_d(\tau(\mathfrak{a}))$.
   (Hint: you may want to use question 1 again.)
5. Prove that if one knows a solution to SVP_γ in $\mathfrak{a}$, then one can construct in polynomial time a solution to SIVP_γ in $\mathfrak{a}$.
6. Prove that the reciprocal is also true: if one knows a solution to SIVP_γ in $\mathfrak{a}$, then one can construct in polynomial time a solution to SVP_γ in $\mathfrak{a}$.

3 Albrecht-Deo's reduction

In this exercise again, we take $P = X^d + 1$ for d a power-of-two, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$. All the vectors are by default column vectors.

We will admit that if q is a prime integer and if the a_i are sampled uniformly in R_q^n for some $n > 1$, then with overwhelming probability, it suffices to sample a polynomial number of a_i's to be able to extract n of them $a'_1, \ldots, a'_n$ such that the matrix whose rows are the $(a'_i)^T$'s is invertible in R_q.

1. Assume that we have access to an oracle computing samples from the distribution $D^{\mathrm{MLWE}}_{n,q,\chi}(s)$ (for some $s \in R_q^n$), and assume that we have n samples $(a_i, b_i) \in R_q^n \times R_q$ from $D^{\mathrm{MLWE}}_{n,q,\chi}(s)$ such that the matrix $\overline{A}$ whose rows are the a_i is invertible in R_q. Let $b_i = \langle a_i, s\rangle + e_i$ with $e_i \leftarrow \chi$ and let us write $\overline{e} = (e_1, \ldots, e_n)^T$ and $\overline{b} = (b_1, \ldots, b_n)^T$. Observe that, by definition, we have $\overline{b} = \overline{A} \cdot s + \overline{e}$.

   Let $(a, b) \leftarrow D^{\mathrm{MLWE}}_{n,q,\chi}(s)$. Define $a' = \overline{A}^{-T} \cdot a$ and $b' = \langle a', \overline{b}\rangle - b$. Show that (a', b') is a sample from $D^{\mathrm{MLWE}}_{n,q,\chi}(\overline{e})$.

2. Conclude that there is a polynomial time reduction from $\mathrm{MLWE}_{n,q,\chi}$ to $\mathrm{HNF\text{-}MLWE}_{n,q,\chi}$, which is a variant of MLWE where the secret is sampled from the distribution χ^n instead of being chosen uniformly in R_q^n.

3. Let $e \in R$ be such that $\|\tau(e)\| \leq \beta$ for some $\beta > 0$. Let $X = \{x \in R \,|\, \|\Sigma(x)\|_\infty \leq \beta'\}$ and $Y = \{x \in R \,|\, \|\Sigma(x - e)\|_\infty \leq \beta'\}$ for some $\beta' > 0$ not in $\mathbb{Z}$. Show that $|X| \leq (2\beta')^d$ and that $|X \cap Y| \geq (2(\beta' - \beta))^d$.

4. Let χ' be the uniform distribution over $\{x \in R \,|\, \|\Sigma(x)\|_\infty \leq \beta'\}$ where $\beta' = \beta \cdot 2^{d+1} d$. Assume that $\beta' \notin \mathbb{Z}$, using the previous question, show that the statistical distance between χ' and $e + \chi'$ is $\leq 2^{-d}$.

5. Conclude the proof of Albrecht-Deo's reduction from the course.

4 Subfields and automorphisms

In this exercise, we take $P = X^4 + 1$, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$.

1. What are the automorphisms of K? Show that $\mathrm{Gal}(K)$ is isomorphic as a group to $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

2. Deduce from the previous question that K admits one subfield of degree 1, three subfields of degree 2 and one subfield of degree 4.

3. Exhibit a basis for all the subfields from the previous question.

5 Canonical embedding and automorphisms

In this exercise, we take $P = X^d + 1$ for d a power-of-two, $K = \mathbb{Q}[X]/P(X)$ and $R = \mathbb{Z}[X]/P(X)$. Let ζ be a primitive $(2d)$-th root of unity in $\mathbb{C}$, and define, for $i = 1$ to d the maps

$$\begin{aligned} \sigma_i : \quad & K \to \mathbb{C} \\ & a(X) \mapsto a(\zeta^{2i-1}) \end{aligned}$$

These maps σ_i are called the complex embeddings of K. Recall that the canonical embedding τ of an element $a \in K$ is defined as $\tau(a) := (\sigma_1(a), \ldots, \sigma_d(a)) \in \mathbb{C}^d$. Let φ be some automorphism of K.

1. Show that for all $i \in \{1, \ldots, d\}$, there exists $k \in \{1, \ldots, d\}$ such that $\sigma_i \circ \varphi = \sigma_k$.

2. Show that the map $\sigma \mapsto \sigma \circ \varphi$ is actually a permutation over the set of complex embeddings $(\sigma_i)_{1 \leq i \leq d}$.

3. Conclude that for all $a \in K$, it holds that $\|\tau(\varphi(a))\| = \|\tau(a)\|$.

6 Short vectors in special ideals

Let $\mathfrak{a}$ be an ideal of $K = \mathbb{Q}[X]/(X^d + 1)$. Let H be its decomposition group (i.e., $H = \{\varphi \in \mathrm{Gal}(K) \mid \varphi(\mathfrak{a}) = \mathfrak{a}\}$), and let K_H be the fixed field of H (i.e., $K_H = \{x \in K \mid \varphi(x) = x,\, \forall \varphi \in H\}$).

1. Let $x \in \mathfrak{a}$ be non-zero. Define $w_i = \mathrm{Tr}_{K/K_H}(x \cdot X^{i-1})$ for $i \in \{1, \dots, d\}$. Show that there exists an index i_0 for which w_{i_0} is non-zero.
   (Hint: recall from Exercise 2 that the vectors $x \cdot X^{i-1}$ are linearly independent, hence they form a $\mathbb{Q}$-basis of K.)

2. Prove that, for all i, it holds that $\|\tau(w_i)\| \leq |H| \cdot \|\tau(x)\|$.
   (Hint: recall that $\|\tau(y \cdot X)\| = \|\tau(y)\|$ for all $y \in K$.)

3. Show that $w_i \in \mathfrak{b} := \mathfrak{a} \cap K_H$ for all i's.
   (Hint: this is where we use that H is the decomposition group of $\mathfrak{a}$.)

4. Conclude that $\lambda_1(\tau(\mathfrak{b})) \leq |H| \cdot \lambda_1(\tau(\mathfrak{a}))$.

7 NTRU

For the first 3 questions, assume that $K = \mathbb{Q}$, and that q is a prime integer.

1. Let $(f, g) \in \mathbb{Z}^2$ with $(f, g) \neq (0, 0)$ and $|f|, |g| < q$. Let $h, h' \in \mathbb{Z}$ such that $gh = f \bmod q$ and $gh' = f \bmod q$. Show that $h = h' \bmod q$.
   (Hint: it may be useful to prove that q is invertible modulo q.)

2. Show that for any $B > 0$, the number of pairs $(f, g) \in \mathbb{Z}^2$ with $|f|, |g| \leq B$ is at most $(2B + 1)^2$.

3. Deduce from the previous two questions that for $B < q$, the proportion of NTRU$_{q,B}$ instances in $\mathbb{Z}$ is $\leq \frac{(2B+1)^2}{q}$.
   (Hint: observe that if h is an NTRU$_{q,B}$ instance, then any $h' = h \bmod q$ is also an NTRU$_{q,B}$ instance, so it suffices to consider the h in $\{0, \dots, q-1\}$.)

From now on, $K = \mathbb{Q}[X]/(X^d + 1)$ as usual, and let $q \geq 5$. Let χ be the uniform distribution over polynomials of $\mathbb{Z}[X]/(X^d + 1)$ with coefficients in $\{-1, 0, 1\}$, and let ψ be the distribution obtained by sampling $f, g \leftarrow \chi$ until g is invertible mod q, and returning $h = f/g \bmod q$. Note that ψ is a distribution over NTRU$_{q,B}$ instances for $B = d$ (because $\|\tau(f)\| = \sqrt{d} \cdot \|\Sigma(f)\| \leq d$ if $f \leftarrow \chi$). Recall that the dec-NTRU$_{q,B,\psi}$ problem asks to distinguish $h \leftarrow \psi$ from $h \leftarrow \mathcal{U}(R_q)$.

1. Show that dec-NTRU$_{q,B,\psi}$ would be easy to solve if we had taken $h = f \bmod q$ instead of $h = f/g \bmod q$.

2. Show that dec-NTRU$_{q,B,\psi}$ would be easy to solve if we had taken $h = 1/g \bmod q$ instead of $h = f/g \bmod q$.