Hard Lattice Problems

1. Lagrange reduction. (⋆⋆)

Let L be a two-rank lattice. A basis $(\vec{u}, \vec{v})$ of L is *Lagrange-reduced* if $\|\vec{u}\| \leq \|\vec{v}\|$ and $|\langle \vec{u}, \vec{v} \rangle| \leq \|\vec{u}\|^2/2$. Show that :

---

1. *If $(\vec{u}, \vec{v})$ is reduced, then $\|\vec{u}\| = \lambda_1(L) \leq (4/3)^{1/4} \mathrm{vol}(L)^{1/2}$ and $\|\vec{v}\| = \lambda_2(L)$.*
2. *There exists a reduced basis $(\vec{u}, \vec{v})$ of L.*
3. *There exists a lattice L such that $\lambda_1(L) = (4/3)^{1/4} \mathrm{vol}(L)^{1/2}$.*

---

2. Lagrange's Algorithm. (⋆⋆)

In 1773, Lagrange published the following two-dimensional reduction algorithm. Lagrange's reduction algorithm.

Input: a basis $(\vec{u}, \vec{v})$ of a two-rank lattice L.
Output: a Lagrange-reduced basis of L.

1: **if** $\|\vec{u}\| < \|\vec{v}\|$ **then**
2: swap $\vec{u}$ and $\vec{v}$
3: **end if**
4: **repeat**
5: $\vec{r} \longleftarrow \vec{u} - q\vec{v}$ where $q = \left\lfloor \frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{v}\|^2} \right\rceil$ and $\lfloor x \rceil$ denotes an integer closest to x.
6: $\vec{u} \longleftarrow \vec{v}$
7: $\vec{v} \longleftarrow \vec{r}$
8: **until** $\|\vec{u}\| \leq \|\vec{v}\|$
9: Output $(\vec{u}, \vec{v})$.

---

1. *Consider Line 5 of Algorithm : show that this choice of $q \in \mathbb{Z}$ minimizes $\|\vec{u} - q\vec{v}\|$.*
2. *Show that Lagrange's algorithm terminates,* i.e. *that the repeat/until loop is not infinite, and that the output basis is Lagrange-reduced.*
3. *Consider the integer q of Step 5. Show that :*
   — *if $q = 0$, then this must be the last iteration of the loop.*
   — *if $|q| = 1$, then this must be either the first or last iteration of the loop.*
4. *Show that the number τ of iterations of the repeat/until loop is bounded by : $\tau = O(1 + \log B - \log \lambda_1(L))$ where B denotes the maximal Euclidean norm of the input basis vectors $\vec{u}$ and $\vec{v}$.*
5. *Show that when $L \subseteq \mathbb{Z}^n$, the bit-complexity of Lagrange's algorithm is polynomial in $\log B$.*

---

3. <u>CVP is NP-hard.</u> $(\star)$

Given integers $a_1, ; a_n$ and a target t, the NP-complete subset sum problem asks if there exist $x_1, \ldots, x_n \in \{0,1\}$ s.t. $t = \sum_{i=1}^{n} x_i a_i$.

---

1. *Let L be the set of all $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ such that $\sum_{i=1}^{n} z_i a_i = 0$. Show that L is a lattice of $\mathbb{Z}^n$, of rank $n-1$. What is the volume of L ?*
2. *Let d be the gcd of $a_1, \ldots, a_n$. Show that if d does not divide t, then the subset sum has no solution. Otherwise, show that one can compute in polynomial time $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ such that $t = \sum_{i=1}^{n} y_i a_i$.*
3. *Given a CVP-oracle for L, show that one can decide the subset sum problem in polynomial time. This shows that CVP is NP-hard.*

---

4. <u>SIS and LWE Lattices.</u> $(\star)$

Let G be a finite Abelian group : we view G as $\mathbb{Z}$-module, so that the notation ng for $(n, g) \in \mathbb{Z} \times G$ is defined. Let $g_1, \ldots, g_m \in G$. Show that :

---

1. *The set L of $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ such that $\sum_{i=1}^{m} x_i g_i = 0$ in G is a lattice in $\mathbb{Z}^m$.*
2. *The rank of L is m.*
3. *The volume of L divides the order of G.*
4. *The dual lattice of L is the lattice Λ defined as the set of all $(y_1, \ldots, y_m) \in \mathbb{R}^m$ such that there exists a morphism $s : G \to \mathbb{R}/\mathbb{Z}$ satisfying $s(g_i) = y_i \bmod 1$ for all $1 \leq i \leq m$. Such a map s is called an* additive character *of G.*
5. *The set of additive characters of G is an additive group, isomorphic to G.*
