The LLL Algorithm

1. Lagrange reduction. (⋆⋆)

Let L be a two-rank lattice. Lagrange's algorithm (from another sheet) shows the existence of a basis $(\vec{u}, \vec{v})$ of L such that if $\|\vec{u}\| \leq \|\vec{v}\|$ and $|\langle \vec{u}, \vec{v} \rangle| \leq \|\vec{u}\|^2/2$. We call reduced any such basis $(\vec{u}, \vec{v})$. Show that in such a case :

---

1. *For any* $(x, y) \in \mathbb{Z}^2$ *:*

$$\|x\vec{u} + y\vec{v}\|^2 \geq (x^2 - |xy|)\|\vec{u}\|^2 + y^2\|\vec{v}\|^2.$$

2. *Deduce that* $\|\vec{u}\| = \lambda_1(L)$ *and* $\|\vec{v}\| = \lambda_2(L)$.
3. *Show that* $\|\vec{u}\| \leq (4/3)^{1/4}\mathrm{vol}(L)^{1/2}$.
4. *There exists a lattice* L *such that* $\lambda_1(L) = (4/3)^{1/4}\mathrm{vol}(L)^{1/2}$.

---

2. Hermite's Inequality. (⋆⋆)

Let L be a d-rank lattice of $\mathbb{R}^n$, and $\vec{u}$ be a shortest non-zero vector of L. Let π denote the (orthogonal) projection over the hyperplane $\vec{u}^\perp$ orthogonal to $\vec{u}$. Let $L' = \pi(L)$.

---

1. *Show that* L' *is a lattice of* $\mathbb{R}^n$ *: what is the rank of* L' *?*
2. *Show that* $\mathrm{vol}(L) = \|\vec{u}\|\mathrm{vol}(L')$.
3. *Show that for any* $\vec{v'} \in L'$ *there exists* $\vec{v} \in L$ *such that* $\vec{v'} = \pi(\vec{v})$ *and :*

$$\|\vec{v}\|^2 \leq \|\vec{v'}\|^2 + \|\vec{u}\|^2/4.$$

4. *Show that :*

$$\|\vec{u}\| \leq (4/3)^{(d-1)/4}\mathrm{vol}(L)^{1/d}.$$

This was proved by Hermite in the middle of the 19th century : it is equivalent to Hermite's inequality $\gamma_d \leq (4/3)^{(d-1)/2}$. *The LLL algorithm is an efficient algorithmic version of Hermite's inequality : given any basis of* $L \subseteq \mathbb{Q}^n$ *and* $\varepsilon > 0$, *LLL finds, in time polynomial in* $1/\varepsilon$ *and the size of the input basis, a non-zero* $\vec{v} \in L$ *such that* $\|\vec{v}\| \leq (4/3 + \varepsilon)^{(d-1)/4}\mathrm{vol}(L)^{1/d}$.

---

3. Siegel reduction. (⋆)

Let $B = (\vec{b}_1, \ldots, \vec{b}_d)$ be a basis of a lattice L. Assume that B is Siegel-reduced for some $\alpha \geq 1$, that is, B is size-reduced and its Gram-Schmidt orthogonalization satisfies : $\|\vec{b}_i^\star\|/\|\vec{b}_{i+1}^\star\| \leq \alpha$ for all $i \in \{1, 2, \ldots, d-1\}$. Notice that an LLL-reduced basis is Siegel-reduced.

---

1. *Show that* $\|\vec{b}_1\| \leq \alpha^{(d-1)/2}\mathrm{vol}(L)^{1/d}$.
2. *Show that* $\prod_{i=1}^d \|\vec{b}_i\| \leq \alpha^{d(d-1)/2}\mathrm{vol}(L)$.
3. *Show that* $\|\vec{b}_i\| \leq \alpha^{d-1}\lambda_i(L)$ *for all* $i \in \{1, 2, \ldots, d\}$.

---

4. Approximating the Closest Vector Problem. (⋆⋆)

Let $B = (\vec{b}_1, \ldots, \vec{b}_d)$ be a Siegel-reduced basis of a lattice $L \subseteq \mathbb{Z}^n$ for some $\alpha > 0$.

---

1. *Show that for any* $\vec{t} \in \operatorname{span}(L) \cap \mathbb{Q}^n$*, there exists* $\vec{w} \in L$ *and* $(w_1, ..., w_d) \in \mathbb{Q}^n$ *such that* $\vec{t} - \vec{w} = \sum_{j=1}^{d} w_j \vec{b}_j^\star$ *and all* $|w_j| \leq \frac{1}{2}$*. How can one compute* $\vec{w}$ *?*
2. *Assume that there exists* $\vec{u} \in L$ *such that* $\|\vec{t} - \vec{u}\| < \frac{1}{2} \min_{j=1}^{d} \|\vec{b}_j^\star\|$*. Show that* $\vec{w} = \vec{u}$*. (Hint :* $\vec{w} - \vec{u} \in L$*).*
3. *Let* $\vec{u} \in L$ *be a closest vector to* $\vec{t}$ *in the lattice* L *such that* $\vec{u} \neq \vec{w}$*. Show that* $\|\vec{t} - \vec{u}\| \geq \frac{1}{2} \min_{j=1}^{d} \|\vec{b}_j^\star\|$*.*
4. *Show that* $\|\vec{t} - \vec{w}\| \leq \alpha^d \operatorname{dist}(\vec{t}, L)$*. Thus,* $\vec{w}$ *approximates CVP to within an exponential factor.*
