Solving ApproxSVP: the LLL and BKZ algorithms

Main motivation: solving SVP is too costly

4. Determinant and Minkowski's thm

Def.: [determinant]: Let $(b_i)_i$ be a basis of L. $\det(L) := (\det B^T B)^{1/2}$

Lemma: it's independant of the basis choice

(R) → This is the volume of the fundamental parallelepiped spanned by the b_i's: $\mathcal{P}(b_i) = \sum_i [0,1) \cdot b_i$.

Minkowski

Thm.: $\lambda_1(L) \leq \sqrt{d} \cdot (\det L)^{1/d}$; $\lambda_1^\infty(L) \leq (\det L)^{1/d}$. with $d = \dim L$

(R) → we also have $\prod_{i \leq d} \lambda_i(L) \leq \sqrt{d}^d \cdot (\det L)$.

Thm.: Let $S \subseteq \mathbb{R}^n$ sym. convex with $\mathrm{vol}(S) > 2^d \cdot \det L$.
Then $|S \cap L| > 1$. If S is compact, $\mathrm{vol}(S) \geq 2^d \cdot \det L$ suffices.

(R) → taking $S = [-\det^{1/d}, \det^{1/d}]^d$ gives Minkowski's thm for λ^∞.
Eq. btw norms gives Minkowski's thm for λ_1.

Thm (Blichfeldt): $L \subseteq \mathbb{R}^n$, $E \subseteq \mathbb{R}^n$ w. $\mathrm{vol}(E) > \det(L)$ [assuming $\dim = n$]
$\Rightarrow \exists z_1 \neq z_2 \in E$ s.t. $z_1 - z_2 \in L$.

(R) → This implies previous thm. Take $E = S/2$. $z_1 - z_2 \in L \setminus 0$

$= 2 \cdot \underbrace{\frac{z_1 - z_2}{2}}_{\in S/2 \text{ by convexity and symmetry}} \in 2 \cdot \frac{S}{2} = S.$

Proof: Consider $\bigcup_{b \in L} \{S((b_i)_i) + b\}$: this partitions $\mathbb{R}^n$.

$\Rightarrow E = \coprod_{b \in L} \{S((b_i)_i) + b \cap E\} \Rightarrow \sum_{b \in L} \mathrm{vol}(S(b_i) + b \cap E) > \det(L)$

PICTURE

$\sum_{b \in L} \mathrm{vol}(S(b_i) \cap (E - b))$

As $\bigcup_{b \in L} S(b_i) \cap E - b \subseteq S(b_i)$, $\exists z \in S(b_i) \cap E - b_1$
$\wedge S(b_i) \cap E - b_2$.

$z_1 = z + b_1$; $z_2 = z + b_2$ ∎

(R) → Non-constructive, pigeonhole principle.

HSVP: given $b_1, \dots, b_n$ basis of L, find $b \in L$: $0 < \|b\| \leq \gamma \cdot \det(L)^{\frac{1}{n}}$.

$\mathrm{SVP}_\gamma \Rightarrow \mathrm{HSVP}_{\gamma \cdot \sqrt{n}}$ by Minkowski's thm.

$\mathrm{HSVP}_\gamma \Rightarrow \mathrm{SVP}_{\gamma^2}$ [Lenstra+ Schnorr '84].

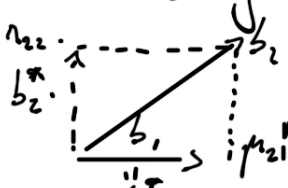
② QR-factorization and size-reduction.

$Q^TQ = QQ^T = I$.

Def.: Let $B \in \mathbb{R}^{n\times n}$ non-singular. There exists Q orthogonal and R upper triangular with $r_{ii} > 0 \ \forall i$ s.t.: $B = Q \cdot R$.
This factorization is unique.

Relationship to Gram-Schmidt orthogonalization: $b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*$.
$\mu_{ij} = \langle b_i, b_j^* \rangle / \|b_j^*\|^2$.

(but QR is more "natural" as it just "rotates" B)



$$B = Q \cdot R = \underbrace{Q \cdot \mathrm{diag}(r_{ii})}_{B^*} \cdot \underbrace{\mathrm{diag}(r_{ii}^{-1}) \cdot R}_{(\mu_{ij})^T_{ij}}$$

$\equiv$) this accounts the same information.

Computing $Q \cdot R$? Q, R are in general not rational → real approximations
B^*, μ are rational with nums/denoms of bitsizes polynomial in $n, \log\|B\|$.

($O(n^3)$ arithmetic ops → exact via Gram-Schmidt
→ approximate via QR [numerical linear algebra provides nice black box framework to get bnds on errors].)

Q is an orthogonal matrix. In particular:
$$\|B \cdot x\| = \|Q \cdot R \cdot x\| = \|R \cdot x\|.$$
we want to find $x \in \mathbb{Z}^n$ s.t. $R \cdot x$ is small $\neq 0$.

LEMMA: $\lambda_1(L) \geq \min_i r_{ii}$. (write $b = \sum x_i b_i$)

Def.: $B = Q \cdot R$ is said size-reduced if $|r_{ij}| \leq r_{ii}/2 \ \forall i < j$.
(equivalently $|\mu_{ij}| \leq 1/2 \ \forall i > j$)