Basis Reduction

Monday, April 21, 2025 9:53 AM

Given $\alpha_1 \dots \alpha_n \in (0,1)$, $\varepsilon > 0$, integer $Q > 0$, find $p_1, p_2, \dots p_n, q \in \mathbb{Z}$, $0 < q \le Q$ s.t.

$$\left|\alpha_i - \frac{p_i}{q}\right| \le \frac{\varepsilon}{q}.$$

<u>Thm</u> (Dirichlet) $Q \geq \frac{1}{\varepsilon^n}$ suffices.

Hard to find!

$$B = \begin{pmatrix} 1 & & & & & \alpha_1 \\ & 1 & & 0 & & \alpha_2 \\ & & 1 & & & \vdots \\ & 0 & & 1 & & \vdots \\ & & & & 1 & \alpha_n \\ 0 & \cdots & & & 0 & \varepsilon/Q \end{pmatrix} \qquad \mathcal{L}(B)$$

$u \in \mathcal{L}(B)$: $u = Bz$ $\quad p \in \mathbb{Z}^{n+1}$.

If $u \neq 0$, $\|u\|_\infty \le \varepsilon$, then $p_{n+1} \neq 0$. Assume $p_{n+1} < 0$.
and $q = -p_{n+1}$

Then $|u_i| = |p_i - \alpha_i q| \le \varepsilon$ $\quad i = 1 \dots n$.

$$|u_{n+1}| = \frac{\varepsilon}{n} q \le \varepsilon.$$

$$|u_{n+1}| = \frac{\varepsilon}{Q} q \le \varepsilon.$$

By Minkowski's theorem, $\exists u \neq 0$ s.t. $\|u\|_\infty \le (\det(\mathcal{L}))^{\frac{1}{n+1}}$

(soon!)

$$= \left(\frac{\varepsilon}{Q}\right)^{\frac{1}{n+1}}$$

for $Q \geq \varepsilon^{-n}$ $\quad \le \varepsilon.$ ✓

If we approximate shortest nonzero u to within α then $\|u\|_\infty \le \alpha\, (\det(L))^{\frac{1}{n+1}}$

$$Q = \alpha^{n+1} \cdot \varepsilon^{-n} \Rightarrow \quad \le \varepsilon.$$

Even an exponential approximation is useful!

Lattice in $\mathbb{R}^n$ $\quad b = \{b_1 \ldots b_m\}$ $\quad m \le n$.

$$\mathcal{L}(b) = \left\{ \sum \lambda_i b_i \;:\; \lambda_i \in \mathbb{Z} \right\}$$

Any set of vectors closed under subtraction and discrete $(\exists \delta > 0,\ \forall x, y \in \mathcal{L},\ \|x-y\| \geq \delta)$.

$\Lambda_1(\mathcal{L})$ = shortest nonzero vector in $\mathcal{L}$.

Thm $\forall \mathcal{L}$. $\exists u \in \mathcal{L}$ s.t. $\|u\|_\infty \le (\det(\mathcal{L}))^{\frac{1}{n}}$.

Thm. $\forall \mathcal{L}$, $\exists u \in \mathcal{L}$ s.t. $\|u\|_\infty \le (\det(\mathcal{L}))$.

Note $\mathcal{L}$ can have many bases, but all have same determinant.

$$\mathcal{L}(B) = \mathcal{L}(\bar{B}) \iff B = U\bar{B}$$

unimodular U.

$$\det(B) = \det(\bar{B}).$$

Pf. Let $Q = \{x : \|x\|_\infty \le \frac{1}{2}\}$

Assume $\det(\mathcal{L}) = 1$ by scaling. Consider $b + Q$, $b \in \mathcal{L}$.

$\mathrm{Vol}(Q) = 1$. So $\exists\, b_1, b_2$

$$Q + b_1 \cap Q + b_2 \ne \phi$$

$\Rightarrow \|b_1 - b_2\|_\infty \le 1$. $\quad b_1 - b_2 \in \mathcal{L}$.

NP-hard to find such a short vector!

More generally, symmetric convex body K. ($K = -K$).

$\exists V_0$ st. $\mathrm{Vol}(K) \ge V_0 \Rightarrow K$ contains a nonzero integer point?

$\lambda_1(K) = \inf t$: tK contains a nonzero $b \in \mathcal{L}$.

$\Lambda_1(K) = \inf$ ...

$\vdots$

$\Lambda_i(K)$: ______________ i linearly ind. points in $\mathcal{L}$.

Thm (Minkowski). $\forall \mathcal{L}$, $\forall$ symmetric K,

(1) $$\Lambda_1(K)^m \leq 2^m \frac{\det(\mathcal{L})}{\mathrm{Vol}(K)}.$$

(2) $$\Lambda_1(K)\Lambda_2(K)\cdots\Lambda_m(K) \leq 2^m \frac{\det(\mathcal{L})}{\mathrm{Vol}(K)}.$$

Pf. (1). Suppose $\frac{1}{2}tK$ has volume 1.
t s.t.

$\exists\, y_1, y_2 \in \mathcal{L}$: $\frac{1}{2}tK + y_1 \cap \frac{1}{2}tK + y_2 \neq \emptyset$

$y = y_1 - y_2$ $\qquad \frac{1}{2}tK \cap \left(\frac{1}{2}tK + y\right) \ni w$

$w \in \frac{1}{2}tK \Rightarrow -w \in \frac{1}{2}tK$

$w - y \in \frac{1}{2}tK$

$\Rightarrow \frac{1}{2}\left(-w + w - y\right) \in \frac{1}{2}tK$

$-\frac{y}{2} \in \frac{1}{2}tK$

$$\Rightarrow y \in tK.$$

$$\mathrm{Vol}\left(\tfrac{1}{2}tK\right) = \frac{t^m}{2^m}\mathrm{vol}(K) \geq 1$$

$$t \geq 2\,\mathrm{Vol}(K)^{-1/m}$$

$\mathcal{L} = \mathcal{L}(b_1 \dots b_m)$

dual lattice $\mathcal{L}^* = \left\{ y \;\middle|\; \begin{array}{l} y \in \mathrm{Span}(\mathcal{L}) \\ y \cdot x \in \mathbb{Z} \end{array} \right\}$

B^{-1} is a basis of $\mathcal{L}^*$.

<u>Cor.</u> $\lambda_1(\mathcal{L})\,\lambda_1(\mathcal{L}^*) \leq n$.

Finding λ_1 is NP-hard

but certifying $\lambda_1(\mathcal{L})$ to within a factor of n

is in NP $\cap$ co-NP!

$$\begin{pmatrix} \text{---}\; b_1 \;\text{---} \\ \vdots \\ \vdots \end{pmatrix} \xrightarrow{\text{Gram-Schmidt}} \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & \\ & & \ddots & \end{pmatrix}$$

$$\begin{pmatrix} \vdots \\ - \; b_n \; - \end{pmatrix} \qquad \begin{pmatrix} \ddots & \end{pmatrix}$$

$$b_1^* = b_1$$

$b_i^* = b_i \perp$ to $\{b_1 \dots b_{i-1}\}$

$$= b_i - \sum_{j=1}^{i-1} \frac{\langle b_i , b_j \rangle}{\|b_j\|^2} . b_j = b_i - \sum_{j=1}^{i-1} \frac{\langle b_i , b_j^* \rangle}{\|b_j\|^2} b_j^*$$

$$b_{ii} = \| b_i^* \|$$

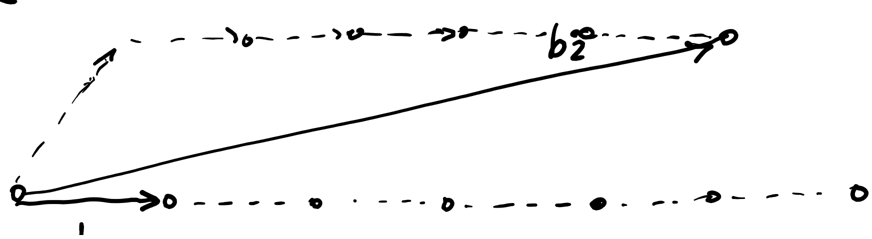
$\det(B) = \|b_1^*\| \dots \|b_n^*\|$

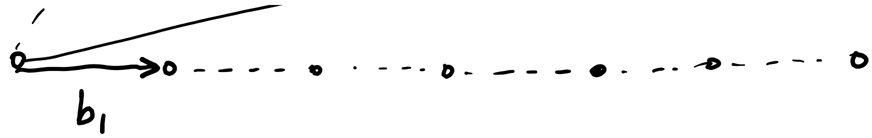
orthogonality defect $= \dfrac{\|b_1\| \dots \|b_n\|}{\det(B)}$.

"Small" ortho. defect $\Rightarrow$ "short" vectors in basis.

How to find a good ($\approx$ "short") basis?

$n = 2$ (Gauss)





$\|b_1\| \le \|b_2\|$

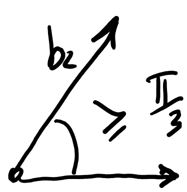
$$\hat{b}_2 \leftarrow \underbrace{b_2 - m\, b_1}_{\text{shortest}} \qquad m \in \mathbb{Z}$$

m = integer closest to $\dfrac{\langle b_2, b_1 \rangle}{\|b_1\|^2}$

If $\|\hat{b}_2\| \ge \|b_1\|$ stop; else swap b_1, b_2 and repeat.

Note: after this step, component of b_2 along b_1 $\le \frac{1}{2}\|b_1\|$. (else not shortest).

$\Rightarrow$



Termination: Stop if $\|\hat{b}_2\| \ge (1-\varepsilon)\|b_1\|$.

So $O(\log \|b\|)$ iterations for ε constant

Proper basis: $\quad b_i - b_i^* \in \left\{ \sum_{j=1}^{i-1} \alpha_j b_j^* : -\frac{1}{2} \le \alpha_j \le \frac{1}{2} \right\}$

Can convert any basis into a proper basis by row reduction.

Lovász basis reduction.

Find basis B s.t. it is proper and

$$\forall i \qquad \|b_{i+1}^*\| \geq \frac{1}{2}\|b_i^*\|.$$

Thm. For an L-reduced basis, (1) $\|b_1\| \leq 2^n \Lambda_1(\mathcal{L})$

$$(2) \quad \frac{\|b_1\| \dots \|b_n\|}{\det(\mathcal{L})} \leq 2^{n^2}.$$

Pf. (1)

$$\|b_j^*\| \geq 2^{i-j}\|b_i^*\|, \quad j \geq i$$

$\forall v \in \mathcal{L} \quad v = \sum \lambda_i b_i^* \qquad \|v\| \geq |\lambda| \|b_i^*\| \geq \|b_i^*\| \geq 2^{1-n}\|b_1^*\|$

$\lambda \neq 0 \qquad \Rightarrow \|b_1\| = \|b_1^*\| \leq 2^{n-1}\|v\| \quad \forall v \in \mathcal{L}.$

(2) $\dfrac{\|b_1\| \dots \|b_n\|}{\|b_1^*\| \dots \|b_n^*\|}$

$$\|b_i\| \leq \|b_i^*\| + \frac{1}{2}\sum_{j=1}^{i-1}\|b_j^*\| \leq \|b_i^*\|\left(1 + \frac{1}{2}\left(2 + 2^2 + \dots 2^{i-2}\right)\right)$$

$$\leq 2^{i-1}\|b_i^*\|$$

$$\leq \prod_{i=1}^{n} 2^{i-1} = 2^{\frac{n(n-1)}{2}}.$$

Algorithm: $V_0 = \{0\}$

$V_i = \text{Span}\{b_1 \dots b_i\}$

If $\exists i$ s.t. $\|b_{i+1}^*\| < \frac{1}{2}\|b_i^*\|$ ($a/_V$ is proj of a $\perp$ to V)

Let $x = b_i/_{V_{i-1}}$ $y = b_{i+1}/_{V_{i-1}}$

Apply Gauss to get u, v with $1-\varepsilon = \frac{\sqrt{3}}{2}$.

$$\begin{pmatrix} u \\ v \end{pmatrix} = U \begin{pmatrix} x \\ y \end{pmatrix}$$ U is unimodular.

and $$\begin{pmatrix} \hat{b}_i \\ \hat{b}_{i+1} \end{pmatrix} = U \begin{pmatrix} b_i \\ b_{i+1} \end{pmatrix}$$

Repeat till $\|b_{i+1}^*\| \geq \frac{1}{2}\|b_i^*\|$ $\forall i$.

Then make proper.

Upon termination $\longrightarrow$ L-reduced.

How many iterations ?!

By Gauss with $1-\varepsilon = \frac{\sqrt{3}}{2}$

$\|v\| \geq \frac{\sqrt{3}}{2}\|u\| \Rightarrow$ component of $v \perp u$

$\|v\| \geq \frac{\sqrt{3}}{2}\|u\| \Rightarrow$ component of $v \perp u$

$\geq \sqrt{\frac{3}{4} - \frac{1}{4}} \; \|u\|$

Since component of v along $u \leq \frac{1}{2}\|u\|$.

$\geq \frac{1}{\sqrt{2}}\|u\|$.

So for $b_1^*, b_2^* \ldots\ldots b_i^*, b_{i+1}^*, \ldots\ldots b_n^*$

$\hat{b}_i^*, \tilde{b}_{i+1}^*, \ldots\ldots b_n^*$

$\|v\| = \|\hat{b}_{i+1}^*\| \geq \frac{1}{\sqrt{2}}\|\hat{b}_i^*\| = \|u\|$.

$\|b_i^*\|\,\|b_{i+1}^*\| = \|\hat{b}_i^*\|\,\|\hat{b}_{i+1}^*\|$ and $\|b_{i+1}^*\| < \frac{1}{2}\|b_i^*\|$

$\Rightarrow \frac{1}{2}\|b_i^*\|^2 \geq \frac{1}{\sqrt{2}}\|\hat{b}_i^*\|^2 \Rightarrow \|\hat{b}_i^*\| \leq \frac{1}{2^{1/4}}\|b_i^*\|$.

So consider the potential

$$\prod_i \|b_i^*\|^{n-i}$$

drops by $2^{1/4}$ in each iteration!

$\Rightarrow$ #iterations $= O(n^2 \log \langle b \rangle)$.