The Simplest Cases :

For the 2-d case, consider the problem of finding an integer pt inside a triangle. [Peter van Emde Boas & Marchetti-Spaccamela's question to H.W. Lenstra].

Algo: transform the triangle into an equilateral triangle Δ. (say unit side lengths)
But this transforms the integers into another lattice Λ with basis $\{b_1, b_2\}$.

Now do Gauss-Lagrange Basis Reduction

Say $|b_1| \le |b_2|$.

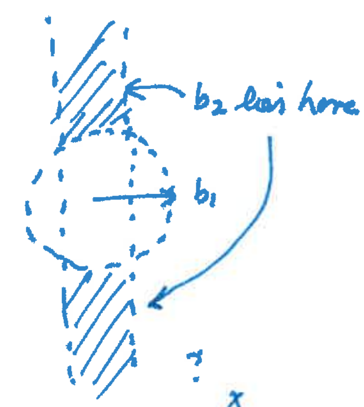
Define $\mu_{12} = \dfrac{\langle b_2, b_1\rangle}{\|b_1\|^2}$ and if $|\mu_{12}| > 1/2$
then choose ℓ and define $b_2 \leftarrow b_2 - \ell b_1$
s.t. $|\mu_{12}| < 1/2$.
new $\mu_{12} = \mu_{12}^{old} - \ell$.

swap b_1 & b_2 if lengths have swapped.

Good. So $|b_2| \ge |b_1|$ and projection $\le 1/2$.

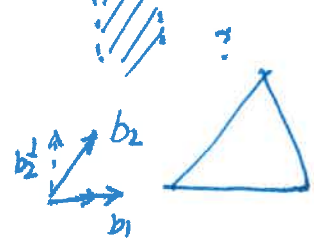
So angle is at least $60°$.

"good" basis.



Now: if $|b_2| \le 1/10$ (actually $\frac{1}{\sqrt{6}}$ apparently)

then $\Delta \leftarrow$ unit side lengths, recall contains lattice pt.



Else the $|b_2| > \frac{1}{10}$. $\Rightarrow |b_2^\perp| \ge \frac{\sqrt{3}}{2}\frac{1}{10}$

So there are at most $O(1)$ hyperplanes of the form $b_2 + b_1\mathbb{Z}$ intersecting Δ.

try them all.

Lattices:

Suppose vectors $b_1, b_2 \ldots b_d \in \mathbb{R}^d$, linearly independent $B = (b_1 \; b_2 \cdots b_d)$

define $\Lambda(B) = \{ \sum_i \lambda_i b_i : \lambda_i \in \mathbb{Z} \} = \{ B\lambda \mid \lambda \in \mathbb{Z}^d \}$

to be all integer combinations of these <u>basis</u> vectors.

$\Lambda(B)$ = lattice generated by Basis B.

Non unique Bases

Adding an integer multiple of b_i to b_j $(j \neq i)$ does not change the lattice.

Negating b_i does not change the lattice

These are both "unimodular" operations.

<u>Lemma</u>: · integer matrix U is called <u>unimodular</u> if $\det(U) \in \pm 1$

· B_1 & B_2 generate the same lattice iff $B_1 = B_2 U$ for some unimodular U.

(Observe that U unimodular $\Leftrightarrow$ U^{-1} unimodular)

Fundamental Parallelopiped

$P(B) = \{ \sum_i x_i b_i \mid x_i \in [0,1) \}$

- $vol(P(B)) = \det(B)$.

- Applying Gram-Schmidt to $B = b_1 b_2 \ldots b_d \rightarrow b_1^*, b_2^* \ldots b_d^*$ (written as B^*).

$$vol(P(B)) = \prod \|b_i^*\|_2 = |\det(B^*)| = |\det(B)|.$$

$$\prod |b_i| = \sqrt{\prod |b_i|^2} = \sqrt{\det(B^{*T} B)} = \det(B^*)$$

$$\det(b_1, b_2 \ldots b_d) = \det(b_1 - \alpha b_2, b_2 \ldots b_d) \text{ etc.}$$

- <u>Fact</u>: $vol(P(B)) = vol(P(B'))$

for two bases since $|\det(B)| = |\det(B'U)| = |\det(B')| \cdot \underbrace{|\det(U)|}_{1} =$
$\uparrow$ unimod.

So can call it $\det(\Lambda)$, since it does not depend on basis.

and $\frac{1}{\det(\Lambda)}$ called the density of the lattice.

Questions we want to ask:

Find short vectors (non zero)
Find good bases.
Solve ILPs.

Crucial tools: Gram Schmidt, Minkowski theorems, ...

Minkowski Thm:

- K convex set, symmetric if $x \in K \Leftrightarrow -x \in K$.
- $cK = \{cx \mid x \in K\}$. $\quad \|x\|_K = \min\{c \mid x \in cK\}$. $\quad x \in K \Leftrightarrow \|x\|_K \le 1$.
  $z + K = \{z + y \mid y \in K\}$.

Thm: if K symmetric, bounded convex set with $\mathrm{vol}(K) > 2^d \Rightarrow$

$$\Rightarrow K \cap (\mathbb{Z}^d \setminus \{0\}) \neq \emptyset.$$

Pf: $K' = \frac{1}{2}K$. Now consider $\mathbb{Z}^d + K'$ (copies of K' on each integer point)

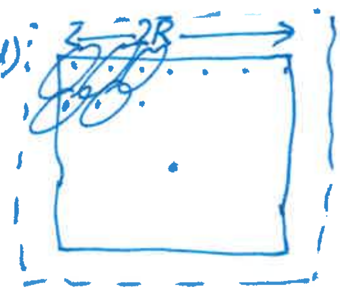
Claim: some points in two different copies.

Suppose not. ~~take~~ suppose $K \subseteq [-c, c]^d$. (b/c bounded);

then $(2R+1)^d \cdot \mathrm{vol}(K) \le (2R+2c)^d$

b/c disjoint

$$\Rightarrow \mathrm{vol}(K) \le \left(1 - \frac{2c-1}{2R+1}\right)^d$$



But $\mathrm{vol}(K') > 1$
and RHS $\to 1$ so smaller than $\mathrm{vol}(K')$ for large R. contradiction

OK sps. $x + K'$ intersects $y + K'$ in z.

then $\|x-y\|_K = \|x-z\|_K + \|z-y\|_K \le \frac{1}{2} + \frac{1}{2} = 1$.

∎

So any large symmetric convex set must contain a nonzero integer point.

Extension to any lattice Λ: K symm. bdd as above.

if K has volume $> 2^d \cdot \mathrm{vol}(\Lambda)$ then $K \cap (\Lambda \setminus \{0\}) \neq \emptyset$.

Pf: define $\tilde{K} = \{\lambda \in \mathbb{R}^d \mid B\lambda \in K\} = B^{-1}K$. so $\mathrm{vol}(\tilde{K}) = \frac{1}{\mathrm{vol}(B)} \cdot \mathrm{vol}(K) > 2^d$.

then $\tilde{K}$ has an integer nonzero point $\Rightarrow K$ has nonzero lattice pt.

$\Rightarrow$ take box of side $(2\mathrm{vol}(\Lambda))^{1/d}$ contain a pt $\Rightarrow$ has ℓ_2 length $\sqrt{d} \cdot \mathrm{vol}(\Lambda)^{1/d}$.

How do you algorithmically find a vector like Minkowski promises?

Seems difficult. If doable $\Rightarrow$ solve other hard lattice problems. (later).

Application of Minkowski's Thm: (Dirichlet's theorem)

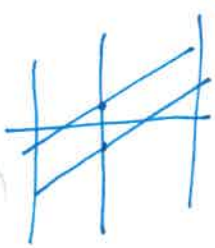
Given $\alpha_1 \alpha_2 \ldots \alpha_d \in [0,1]^d$ find p_i/q st. $|\alpha_i - p_i/q| <$ small

same denominator — small.

- if $q \le Q$, can set $p_i = [\alpha_i Q]$ to get error $1/2Q$.
- Thm: $\exists\ p_i, q$ st. $|\alpha_i - p_i/q| \le \frac{1}{q Q^{1/d}}$, $q \le Q$

want to get ε/Q actually ε/q.

Pf: set $\varepsilon = 1/Q^{1/d}$, we want $p_i, q \in \mathbb{Z}$ st $|\alpha_i q - p_i| \le \varepsilon$.



so want $K = \{(p_1, p_2 \ldots p_d, q) \in \mathbb{R}^{d+1} \mid |\alpha_i q - p_i| \le \varepsilon,\ |q| \le Q\}$

symmetric (so we allow negative q), bounded, convex.

$\mathrm{vol}(K) = (2\varepsilon)^d \cdot (2Q) = 2^{d+1} \cdot \underbrace{\varepsilon^d \cdot Q}_{=1 \text{ by def}}$ $\Rightarrow$ can use Minkowski to claim $\exists$ integer points. (nonzero).

Btw: can $q = 0$? No, $|p_i| \le \varepsilon < 1$ so all $p_i = 0$.

Used in the Ellipsoid algorithm (see GLS)

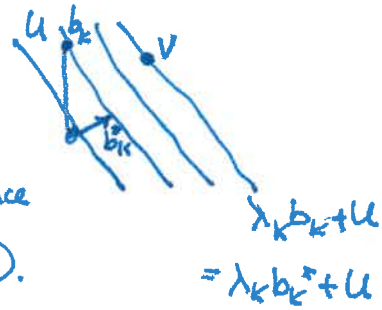
~~Application #2~~ Shortest vector problem $SVP(\Lambda)$ ~~upper bound~~ lower bound.

Say $b_1^*, b_2^* \ldots b_d^*$ output of GramSchmidt. then $SVP(\Lambda) \ge \min_i \|b_i^*\|$

Say v is the shortest vector, say b_k last non zero vector in $v = \sum_i \lambda_i b_i$.

let $U = \mathrm{span}(b_1, b_2 \ldots b_{k-1})$.

then v lies on some translate of U, and that is at least $\|b_k^*\|$ away from U (and hence from the origin).



$\Rightarrow SVP(\Lambda) \ge \min_i \|b_i^*\|$.

So to get ρ-apx, need to find a vector that is ρ times this.

H.W. Arjen Laszlo
Lenstra Lenstra Lovasz Algorithm for Basis Reduction

Want a basis that is (a) somewhat orthogonal and

(b) where $\|b_1\| = \|b_1^*\| \le$ small. $\min_i \|b_i^*\|$.
$\uparrow 2^{n/2}$

Used for ILP, breaking cryptosystems, polynomial factorization, ...

---

① Subtract vectors from each other

② changing ordering of G-S to avoid super small vectors at end.

do 2-d example!!

Ideas: define $\mu_{ij} = \dfrac{\langle b_j, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle}$ so that $b_j^* = b_j - \sum_{i<j}' \mu_{ij} \cdot b_i^*$.

Make $|\mu_{ij}| \le \frac{1}{2}$. (Coefficient reduced)

Note: by replacing b_j by $b_j - c b_\ell$,

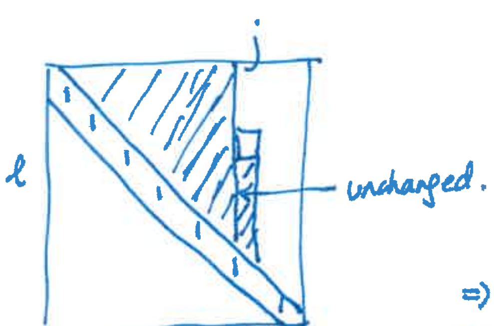
$\forall i<j$: new $b_i^* = b_i$, μ's remain same.

Afterwards things may change. — the b_i^* vectors remain the same
μ's
since we'll subtract off the $c \cdot b_\ell$ part.

now: $\hat{b}_j = b_j - c b_\ell = b_j^* + \sum_{i<\ell}' (\mu_{ij} + c \cdot \mu_{i\ell})\, b_i^*$ ← changed.

$+ (\mu_{\ell j} + c \cdot 1)\, b_\ell^*$ ← changed.

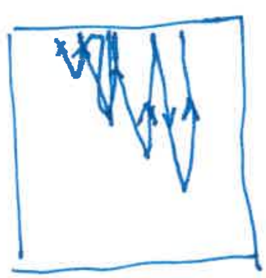
$+ \sum_{i=\ell+1}^{j-1} \mu_{ij} \cdot b_i^*$ ← unchanged.



⇒ do it in the order

$\begin{cases} j = 1 \text{ to } n \\ \ell = j \text{ downto } 1. \end{cases}$

fix $\mu_{j\ell}$.



Basis is LLL reduced if $\quad b_1, b_2 \dots b_d$ ← ordered!

① Coefficient reduced $\quad |\mu_{ij}| \le \frac{1}{2} \ \forall i<j$

② Lovasz condition: $\quad |b_i^*|^2 \le 2 \cdot |b_{i+1}^*|^2$. $\quad \Rightarrow |b_1^*| \le \sqrt{2}^{d} \cdot \min_i |b_i|$ $\le 2^{d/2} \cdot SVP(\Lambda)$.

↑ lengths don't fall too fast.

How to get such basis?

OK: so first coefficient-reduce things. (as above)

Sps. $\exists i$ st Lovasz condition violated. then swap.

Idea:

so b_{i+1}^{**} must be shorter than b_i^*
(new one)

Lemma: ~~Sps. b_1, b_2 only 2 vectors. st $|\mu_{12}| \le 1/2$ and $|b_1^*|^2 = |b_1|^2 > 2|b_2^*|^2$ then swap them to get (b_2^{**}, b_1^{**}) $|b_2^{**}|^2 = |b_2|^2 \le |b_1|^2 \cdot 3/4$.~~

Lemma: a_1, a_2 vectors. st $|\mu_{12}| = \left|\frac{\langle a_2, a_1\rangle}{\langle a_1, a_1\rangle}\right| \le \frac{1}{2}$ and $|a_2^*|^2 < \frac{1}{2}|a_1^*|^2$

then $|a_2| \le \sqrt{3/4}\, |a_1|$.

Pf: $\quad a_2 = a_2^* + \mu_{12} a_1 = a_2^* + \mu_{12} a_1^*$

$\Rightarrow |a_2|^2 = |a_2^*|^2 + \mu_{12}^2 \cdot |a_1^*|^2 < (1/2 + 1/4)|a_1|^2$ ∎

So now conditioning on $b_1^*, b_2^* \dots b_{i-1}^*$, if $|b_i^*|^2 > |b_{i+1}^*|^2 \cdot 2$ and coeff reduced.

then we can ensure that the ~~new~~ swap makes the new

$|b_i^{**}|$ ~~is~~ smaller than old one by $\sqrt{3/4}$ factor.

Formally: potential $\Phi = \prod_{i=1}^{d} \text{volume}_i(b_1, b_2 \ldots b_i)$ ← assume integers for simplicity

$$= \prod_i \left(\prod_{j=1}^{i} |b_j^*| \right). \qquad = \prod_i \sqrt{\det B_{1:i}^T B_{1:i}} \in \mathbb{Z}.$$

Now: if swap b_i & b_{i+1} then all other terms remains same except $\text{vol}_i(b_1 \ldots b_i)$ which falls by $\sqrt{3/4}$.

(Also coeff reduction does not change potential!)

Initial potential is at most $\left(\text{poly}(d) \cdot \max_{ij} |B_{ij}|\right)^{\text{poly}(d)}$. And falls by $O(1)$ factor

& also always integer $\Rightarrow$ poly$(d, \log \max B_{ij})$ steps.
↳ volume (squared)

Big open question: get better basis reduction algorithms!

Another property of LLL basis: small "Orthogonality defect".

Simple idea. $\quad od(B) = \dfrac{\prod |b_i|}{\prod |b_i^*|}.$

Lemma: $od(B_{LLL}) \le 2^{O(d^2)}$.

Pf: $b_k = b_k^* + \sum_{j<k}' \mu_{jk} b_j^*$. so. $|b_k|^2 \le |b_k^*|^2 + \sum_{j<k} \left(\frac{1}{2}\right)^2 \cdot 2^{k-j} \cdot |b_k^*|^2$

$$= 2^{O(k)} \cdot |b_k^*|^2.$$

$\Rightarrow$ Product off by $2^{O(k^2)}$. ∎

Will be useful for the ILP algorithm.

—— x ——