Day 3 scribbles

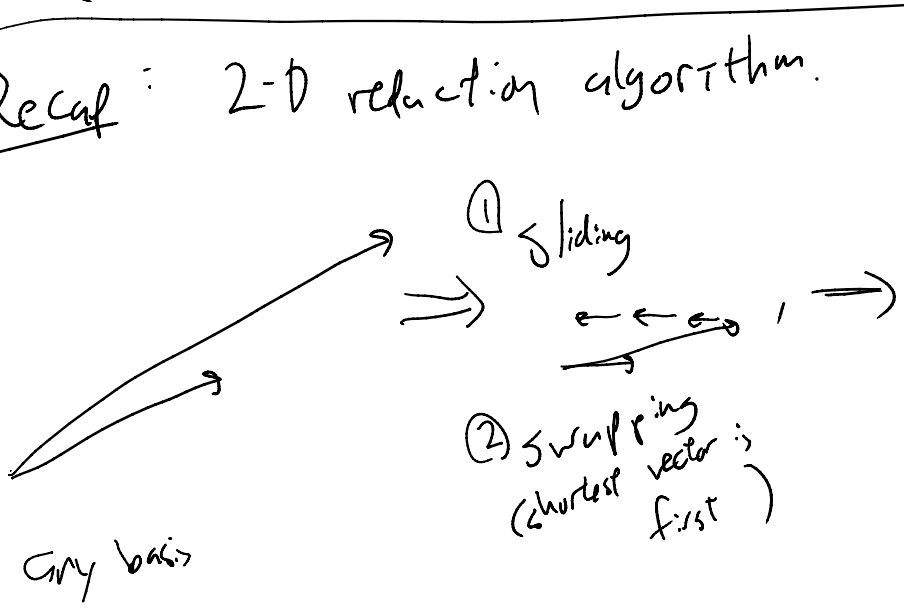
July 21, 2020 1:35 PM

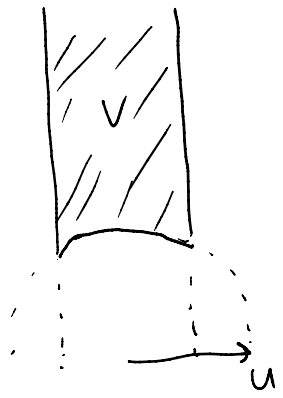
Geometry of Lattices Day 3

When you've lost something how much space do you typically search through before you find it?

(Feel free to share stories)

Recap: 2-D reduction algorithm.





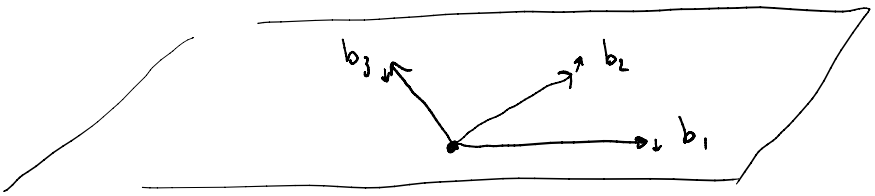
reduced basis

In 3-D, what does "reduced" mean?

$b_1 = \begin{pmatrix} 1 \\ 0 \\ -10^{-6} \end{pmatrix}$, $b_2 = \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \\ 2 \cdot 10^{-6} \end{pmatrix}$ $b_3 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \\ -3 \cdot 10^{-6} \end{pmatrix}$

Sliding does not make them shorter!

BUT they are hiding a surprise short vector:



b_2 very close to $b_3 + b_1$.

$b_2 - b_1 - b_3$ extremely short

Could we have predicted this short vector?

Tool: Volume of the fundamental parallelotope

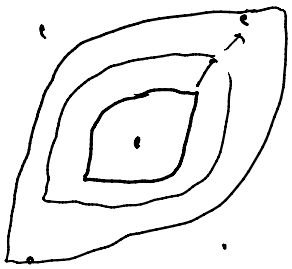
2-D parallelogram 

3-D parallelepiped 

n-D parallelotope

Minkowski's Thm:

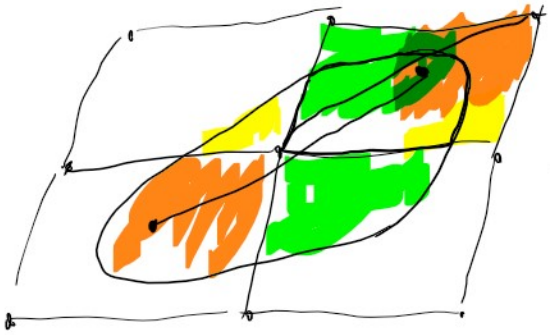
How big does this convex shape need to be in order to contain a nonzero lattice point?



Thm If S convex (If $P, Q \in S$, line segment $\overline{PQ}$ is in S)
symmetric (If $P \in S$, then $-P \in S$)
and $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(P)$ (P is fund. par of a lattice L)
then S must contain a nonzero vector in L.

the S must contain a nonzero vector.

Pf



overlaps:

P, Q map to same pt if

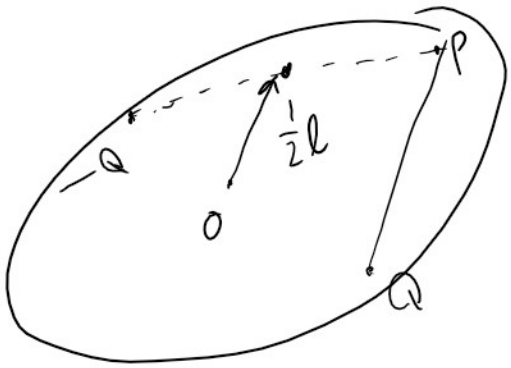
$$\boxed{P - Q = \ell \in L.}$$

$P, Q \in \frac{S}{2}$,

$-Q \in \frac{S}{2}$ (symmetry)

$$\frac{P + (-Q)}{2} \in \frac{S}{2} \quad \text{(convex)}$$

$$\| \quad \frac{1}{2}\ell.$$



Scale by 2.

$\frac{1}{2}\ell \longrightarrow \ell$

$\frac{S}{2} \longrightarrow S$

$\mathrm{Vol}(\frac{S}{2}) \longrightarrow 2^n \mathrm{Vol}(\frac{S}{2}) = \mathrm{Vol}(S)$

$\iff \mathrm{Vol}(S) > 2^n \mathrm{Vol}(P)$. □

Thm S to be a ball of radius r.

Take S to be a ball of radius r.

Then this says that if r is large enough,

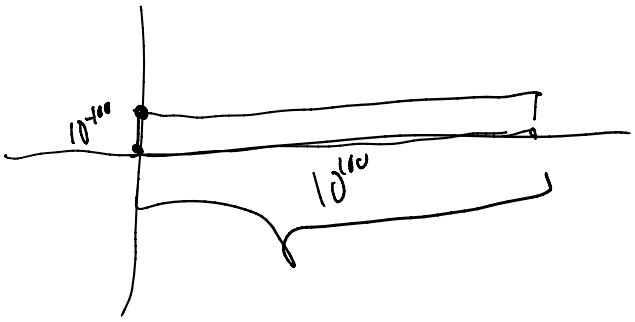
There is a lattice vector in Ball radius r.

(Exp 5).

Apply Minkowski to b_1, b_2, b_3, tells us

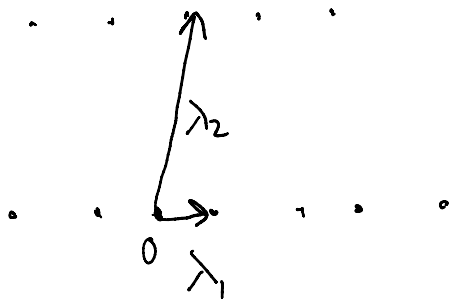
that there is a vector of length ≤ 0.03.

b_1, b_2, b_3 make squashed parallelotope.



$\text{Vol}(P) = 1$

Def Successive minima



λ_1 = length of shortest vector.

λ_2 = length of shortest vector independent vector.

λ_3 = length of shortest vector that is independent of previous 2 ...

$(1,0,0)$	$\lambda_1 = 1$	What about $(1,1,0)$?
$(0,1,0)$	$\lambda_2 = 1$	This is not independent of $(1,0,0)$, $(0,1,0)$
$(0,0,2)$.	$\lambda_3 = 2$	

$(0,1,1)$
$(0,0,2)$.

$\lambda_2 =$.
$\lambda_3 = 2$ | | This is w
of $(1,0,0)$, $(0,1,1)$

Minkowski's 2nd Thm

ball of radius 1

$$\frac{2^n}{n!}\mathrm{Vol}(P) \le \lambda_1\lambda_2\cdots\lambda_n \mathrm{Vol}(B) \le 2^n \mathrm{Vol}(P).$$

Note: Since $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$

$$\lambda_1^n \mathrm{Vol}(B) \le \lambda_1\lambda_2\cdots\lambda_n \mathrm{Vol}(B) \le 2^n \mathrm{Vol}(P)$$

$\lambda_1^n \mathrm{Vol}(B)$: Vol(ball of radius λ_1).

Minkowski 2 $\Rightarrow$ Minkowski 1

Exp 5

Exp 10 (practice using Mink 2)