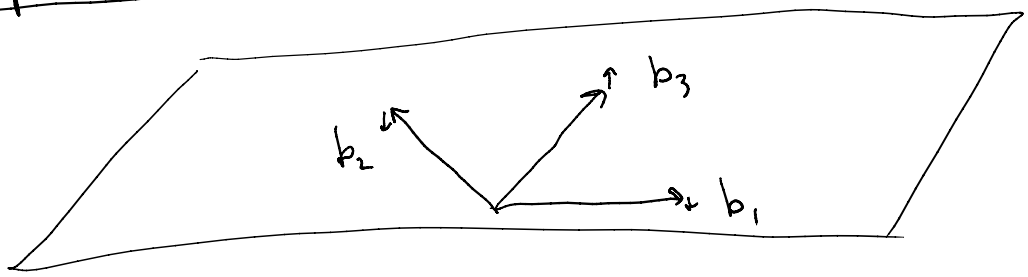
Day 4 scribbles

July 22, 2020 3:13 PM

Geometry of Lattices Day 4

What are some things that become easier to study by projecting an image of them onto somewhere else?

Recap yesterday



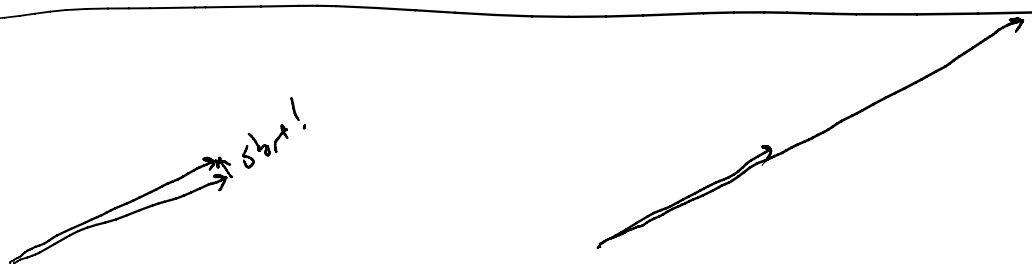
$b_3 - b_1 - b_2$ is extremely small.

BUT no sliding one vector along another helps!

How to find short vectors?

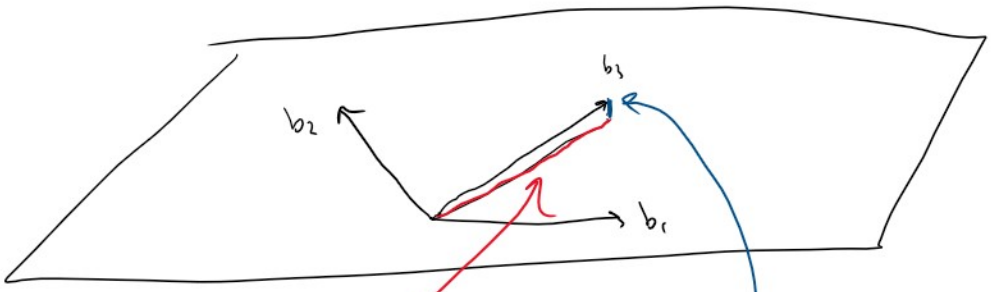
Minkowski: If the volume of the fundamental parallelepiped is small, then there's a short vector

Unfortunately: doesn't tell us where it is!!



projections

projections



Def Write

$$b_3 = \mathrm{Proj}_{\{b_1,b_2\}}(b_3) + \mathrm{Rem}_{\{b_1,b_2\}}(b_3)$$

small remainder...
implies that maybe we can cancel out most of $\mathrm{Proj}_{\{b_1,b_2\}}(b_3)$ using combinations of b_1, b_2.

Exp 1 $v = a_1 b_1 + \cdots + a_j b_j \xrightarrow{\text{Rem}} a_j b_j^*$ $\quad (b_j^* = \mathrm{Rem}_{S_{j-1}}(b_j))$

project onto S_{j-1} ↓

$$\|b_j^*\| \le \|a_j b_j^*\| \le \|v\|$$

⇓ Prop 2

$$a_1 b_1 + a_2 b_2 + \cdots + a_{j-1} b_{j-1} + \mathrm{Proj}_{S_{j-1}}(a_j b_j)$$

$\|b_3^*\| \approx 5.997\ldots \times 10^{-6}$.

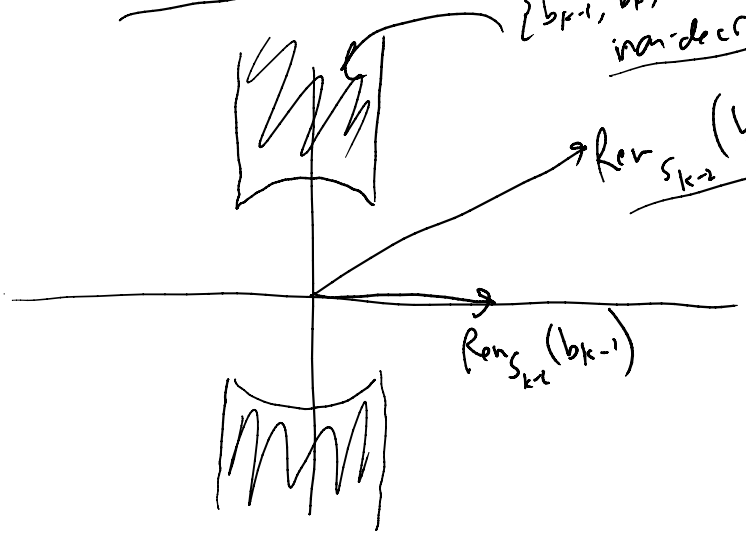
Use 2-D idea, not on basis vectors, but on remainders.

LLL-reduced: (see definition in handout)

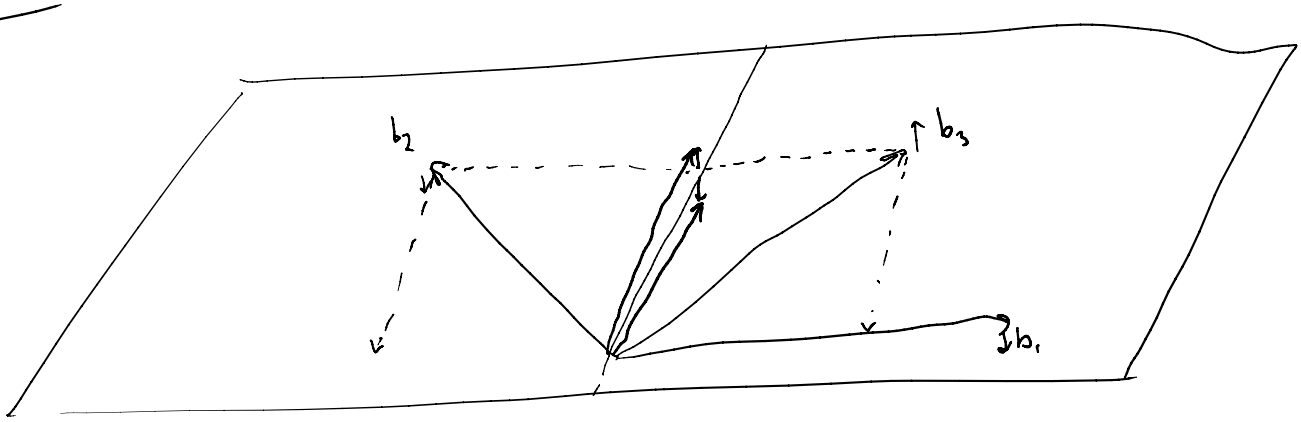
suppose b_{k-1}, b_k adjacent.

Suppose b_{k-1}, b_k adjacent.

Compute $\mathrm{Rem}_{S_{k-2}}$ of each



Exp 4



$\mathrm{Rem}_{S_1}(b_2)$ vs $\mathrm{Rem}_{S_1}(b_3)$ very very close.

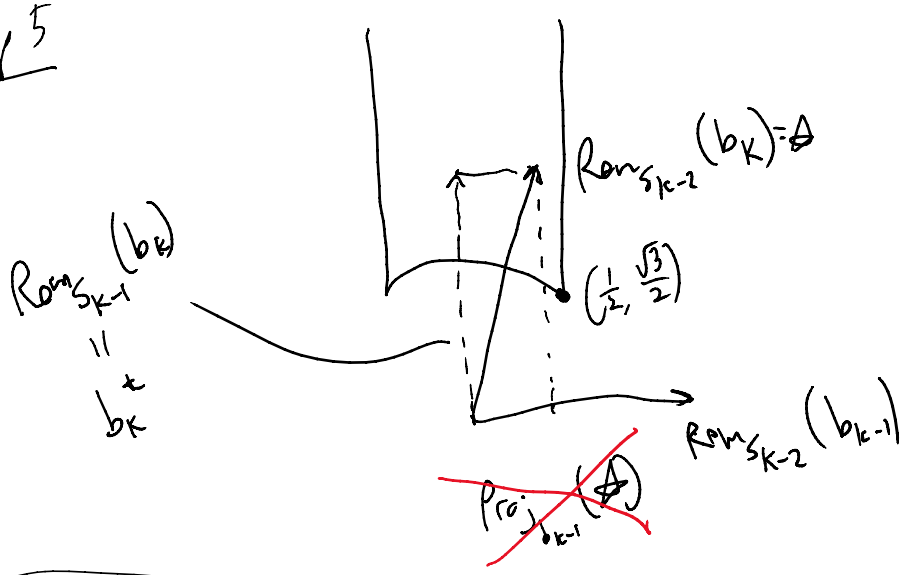
contradicts size-reduction.

If I replace b_3 with $b_3 - b_2$,

then $\mathrm{Rem}_{S_1}(b_3 - b_2)$ very very small.

Ex. 5

Exp 5



UPDATE
see below

Prop 6 $\quad \|b_1\| \leq \left(\frac{2}{\sqrt{3}}\right)^{n-1} \lambda_1$

Recall: Exp 7-11 (Exp 11)

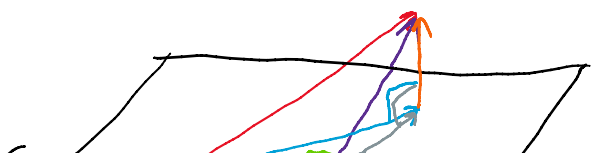
or: just read the algorithm, apply it to b_1, b_2, b_3.

Update: In order to prove Exp 5, we need the following lemma:

Lem If $i < j$, then

$$\text{Rem}_{S_j}(\text{Rem}_{S_i}(v)) = \text{Rem}_{S_j}(v).$$

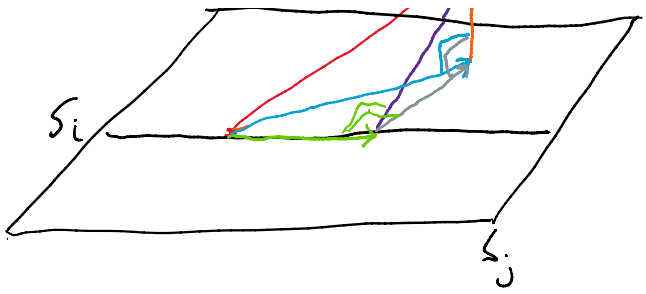
Idea:



v

$\text{Proj}_{S_i}(v)$

$\text{Rem}_{S_i}(v)$



$\text{Rem}_{S_i}(v)$

$\text{Proj}_{S_j}(v)$

$\text{Rem}_{S_j}(v) = \text{Rem}_{S_j}(\text{Rem}_{S_i}(v))$

Pf Write $b_k = \text{Proj}_{S_j}(v) + \text{Rem}_{S_j}(v)$.

Now project ↑ onto S_i:

$$\text{Proj}_{S_j}(v) = \text{Proj}_{S_i}(\text{Proj}_{S_j}(v)) + \text{Rem}_{S_i}(\text{Proj}_{S_j}(v))$$

That is,

$$b_k = \underbrace{\text{Proj}_{S_i}(\text{Proj}_{S_j}(v))}_{\text{in } S_i} + \underbrace{\text{Rem}_{S_i}(\text{Proj}_{S_j}(v)) + \text{Rem}_{S_j}(v)}_{\text{orthogonal to everything in } S_i}$$

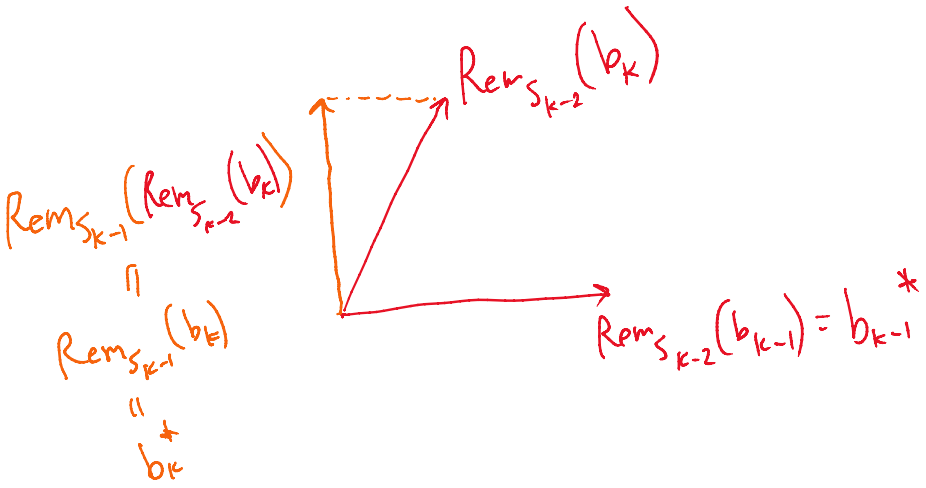
$$\text{Proj}_{S_i}(v) \qquad \text{Rem}_{S_i}(v)$$

so by definition of Proj, Rem.

Now $\text{Rem}_{S_i}(v) = \underbrace{\text{Rem}_{S_i}(\text{Proj}_{S_j}(v))}_{\text{in } S_j} + \underbrace{\text{Rem}_{S_j}(v)}_{\text{orthogonal to everything in } S_j}$

so $\text{Proj}_{S_j}(\text{Rem}_{S_i}(v)) + \text{Rem}_{S_j}(\text{Rem}_{S_i}(v))$. □

As a result, we have the following picture:


$\mathrm{Rem}_{S_{k-2}}(b_k)$
$\mathrm{Rem}_{S_{k-1}}(\mathrm{Rem}_{S_{k-2}}(b_k))$
$\mathrm{Rem}_{S_{k-2}}(b_{k-1}) = b_{k-1}^*$
$\mathrm{Rem}_{S_{k-1}}(b_k)$
b_k^*