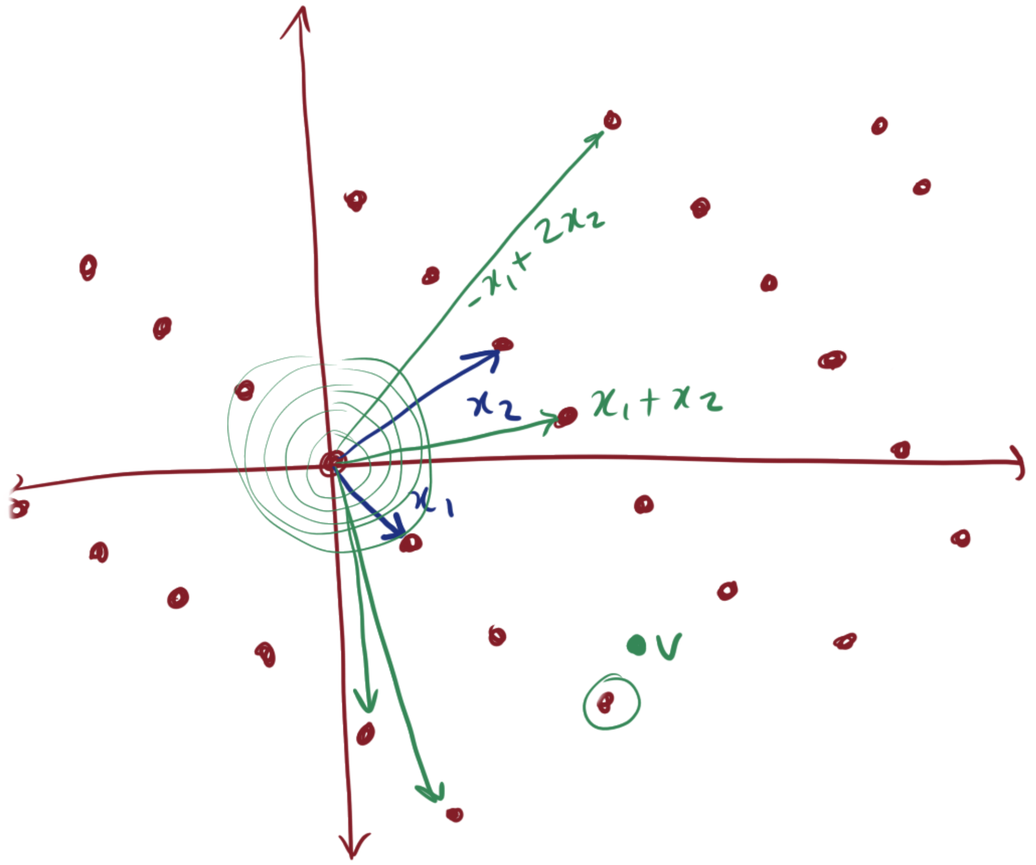
Lattices



Def^n A **lattice** in $\mathbb{R}^n$ is any set of the form

$$\Lambda = \left\{ \sum a_i x_i : a_i \in \mathbb{Z} \right\}$$
$$= x_1\mathbb{Z} + x_2\mathbb{Z} + \cdots + x_n\mathbb{Z}$$

for a fixed **basis** $x_1, \ldots, x_n$ of $\mathbb{R}^n$.

the representation

$$v = \sum a_i x_i$$

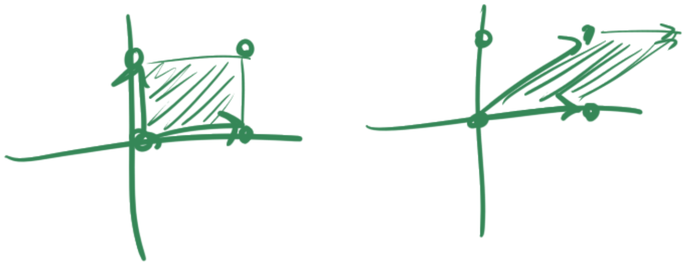
is **unique**

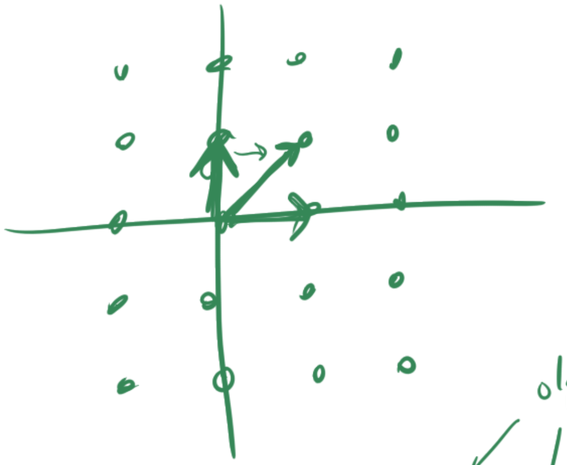
Example

Representing a lattice: $\Lambda = x_1\mathbb{Z} + \cdots + x_n\mathbb{Z}$

$$\begin{pmatrix} | & | & & | \\ x_1 & x_2 & \cdots & x_n \\ | & | & & | \end{pmatrix}$$

columns $= x_i$'s





$\mathbb{Z}^2 \subset \mathbb{R}^2$

$$\begin{pmatrix} | & | \\ v_1 & v_2 \\ | & | \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} | \\ v_1 \\ | \end{pmatrix} + b\begin{pmatrix} | \\ v_2 \\ | \end{pmatrix}$$

vectors; coeff.; lin. comb.

Example. $\Lambda = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\mathbb{Z} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\mathbb{Z}$

$$= \begin{pmatrix} 1 \\ 1 \end{pmatrix}\mathbb{Z} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\mathbb{Z} \quad \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \begin{pmatrix} 1 \\ 2 \end{pmatrix}\mathbb{Z} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\mathbb{Z} \quad \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \begin{pmatrix} 1 \\ 2 \end{pmatrix}\mathbb{Z} + \begin{pmatrix} 1 \\ 3 \end{pmatrix}\mathbb{Z} \quad \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right)$$

old basis; lin. comb; new vector

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

old basis; change; new basis

$\det = 1$

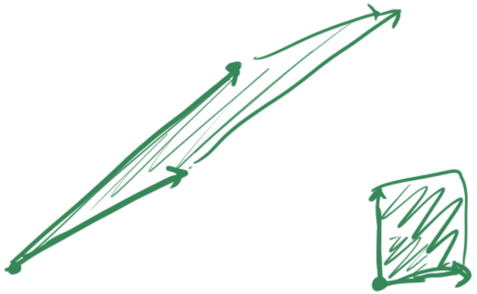
Fact: If we change basis by a matrix of $\det = 1$, the new vectors still form a basis.

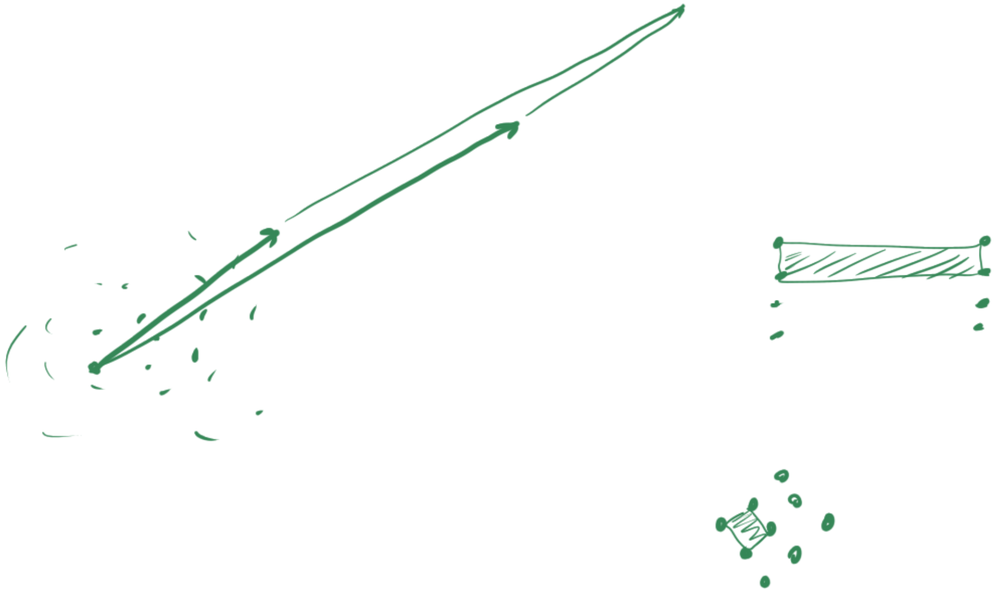
Hard Lattice Problems:

① Shortest Vector Problem: Given a lattice (in a potentially bad basis), find the shortest vector in the lattice (as a linear comb. of basis).

② Closest Vector Problem: Given a lattice (in a potentially bad basis), and given $v \in \mathbb{R}^n$, find the vector in lattice closest to v.

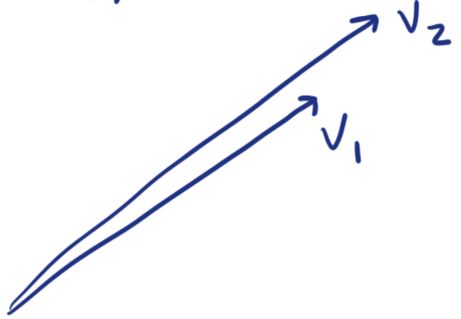
Cryptographic size: $n = 300 - 1500$.



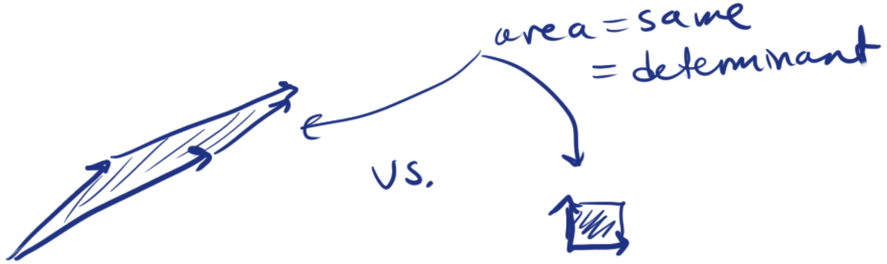


Lattice Reduction in Two Dimensions

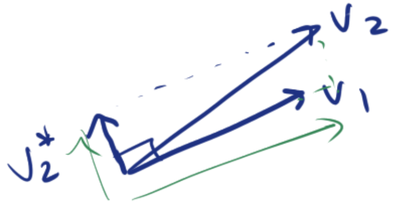
Suppose $\|v_1\| \leq \|v_2\|$.



Idea: Try to make the basis more perpendicular.



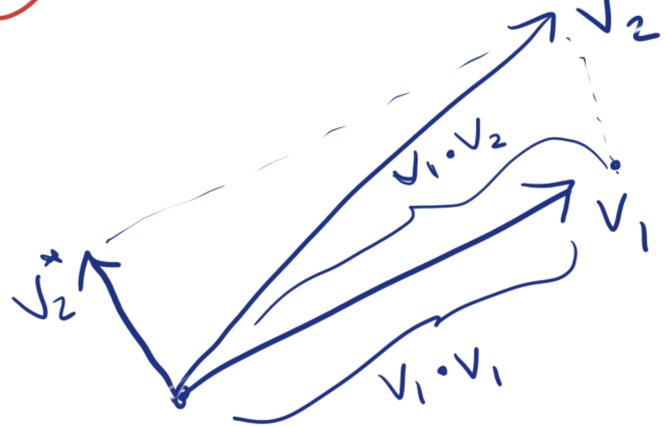
More perpendicular $\Rightarrow$ shorter



v_2^* = projection of v_2 $\perp$ to v_1

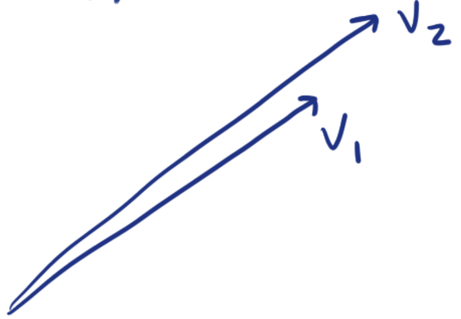
Formula (Gram-Schmidt process):

$$v_2^* = v_2 - \frac{v_1 \cdot v_2}{v_1 \cdot v_1} v_1$$

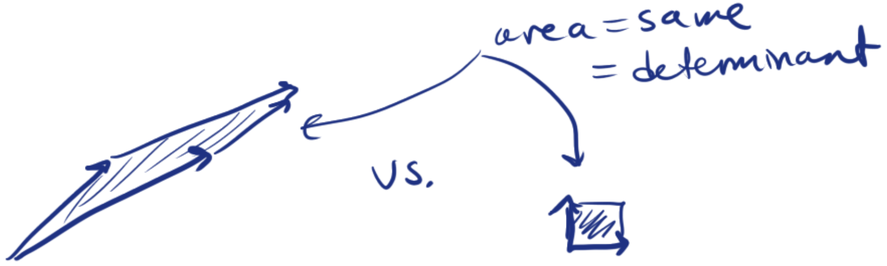


Lattice Reduction in Two Dimensions

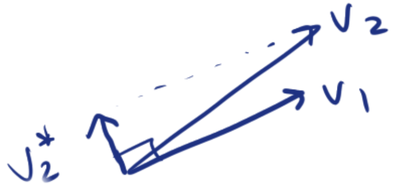
Suppose $\|v_1\| \leq \|v_2\|$.



Idea: Try to make the basis more perpendicular.



More perpendicular $\Rightarrow$ shorter



v_2^* = projection of v_2 $\perp$ to v_1

Nearby in Λ:

$[x]$ = integer closest to x

$$v_2^* = v_2 - \left[\frac{v_1 \cdot v_2}{v_1 \cdot v_1}\right] v_1$$

Guarantee: v_1, v_2^* is a basis $\left(\det\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = 1\right)$

New Basis:

$$v_1, \quad v_2 - \left[\frac{v_1 \cdot v_2}{v_1 \cdot v_1}\right] v_1$$

SWAP AND

REPEAT!

When to stop?

Def^n A basis is reduced when $\|v_1\| \le \|v_2\|$ and $\left[\frac{v_1 \cdot v_2}{v_1 \cdot v_1}\right] = 0$.

Example. $v_1 = \begin{pmatrix} 17 \\ 5 \end{pmatrix}$ $v_2 = \begin{pmatrix} 19 \\ 10 \end{pmatrix}$.

Determinant $= \begin{vmatrix} 17 & 19 \\ 5 & 10 \end{vmatrix} = 170 - 95 = 75$

① $\|v_1\| = 17^2 + 5^2 = 314$, $\|v_2\| = 19^2 + 10^2 = 461$

$\frac{v_1 \cdot v_2}{v_1 \cdot v_1} = \frac{17 \cdot 19 + 5 \cdot 10}{314} = \frac{373}{314} \approx 1$

② $v_2' = \begin{pmatrix} 17 \\ 5 \end{pmatrix}$ $v_1' = v_2 - v_1 = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$

$\|v_2'\| = 314$ $\|v_1'\| = 2^2 + 5^2 = 29$

$\frac{v_1' \cdot v_2'}{v_1' \cdot v_1'} = \frac{17 \cdot 2 + 5 \cdot 5}{29} = \frac{59}{29} \approx 2$

③ $v_2'' = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ $= 29$

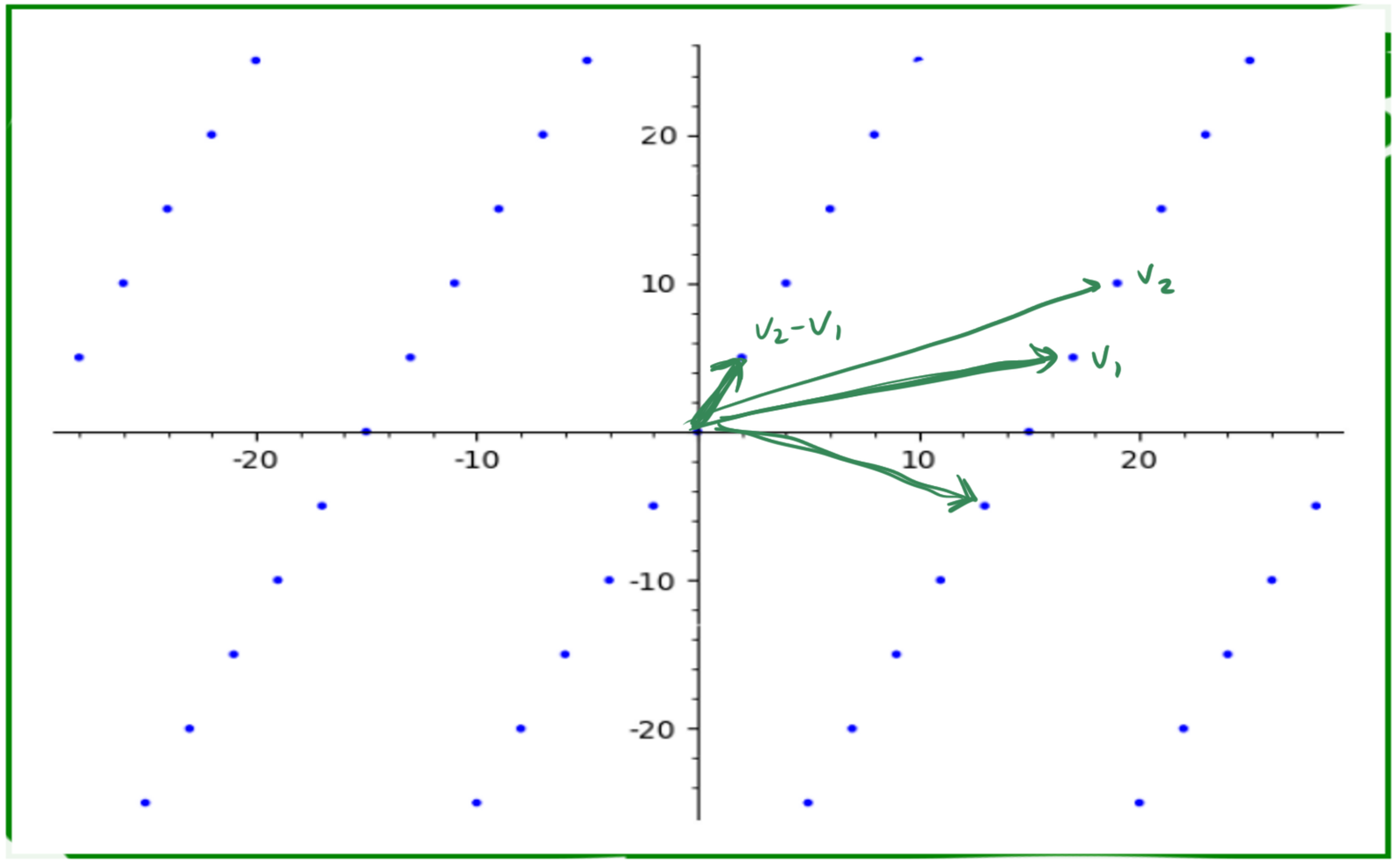
$v_1'' = v_2' - 2v_1' = \begin{pmatrix} 13 \\ -5 \end{pmatrix}$

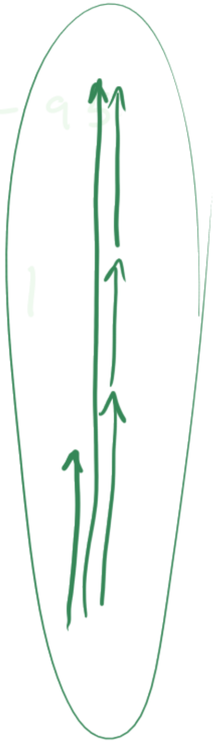
$\|v_1'\| = 194$

$\frac{v_1'' \cdot v_2''}{v_1'' \cdot v_1''} = \frac{2 \cdot 13 - 5 \cdot 5}{194} = \frac{1}{194} \approx 0$

When to stop?

Def^n A basis is reduced when $\|v_1\| \le \|v_2\|$ and $\left\lfloor \frac{v_1 \cdot v_2}{v_1 \cdot v_1} \right\rceil = 0$.





Thm.
This will always terminate with a reduced basis.
When reduced, we have found the shortest vector! (Proof in textbook.)

High Dimensional Reduction: LLL algorithm (Lenstra, Lenstra, Lovász)

(Finds a fairly short vector) n = dimension

$\Lambda = v_1\mathbb{Z} + \dots + v_n\mathbb{Z}$. D = determinant(Λ).

λ = length of shortest vectors $B = \max\{\|v_i\|\}$.

LLL gives new basis $\Lambda = b_1\mathbb{Z} + \dots + b_n\mathbb{Z}$, such that:

a) $\|b_1\| \leq 2^{\frac{n-1}{4}} D^{1/n}$

b) $\|b_1\| \leq 2^{\frac{n-1}{2}} \lambda$ "pretty short"

c) $\|b_1\|\|b_2\|\cdots\|b_n\| \leq 2^{\frac{n(n-1)}{4}} D$ "close to orthogonal"

Running time: $O(n^6(\log B)^3)$