Lattices

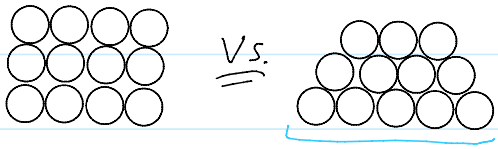
Monday, April 19, 2021 4:47 PM

Post-Quantum Cryptography

Quiz 5 on Thursday at 10 pm.

What are Lattices?

e.g. Stack of oranges



vs.

more dense

"Sphere packing"

1] Def^n. a Lattice is a discrete additive subgroup Λ of $\mathbb{R}^n$

i.e.

① subgroup $\begin{cases} \Lambda \subseteq \mathbb{R} \\ \Lambda \text{ is closed under addition} \\ \text{there is } \vec{v_0} \in \Lambda \\ \forall\, \vec{v} \in \Lambda,\ \exists\, \vec{v}' \in \Lambda,\ \vec{v}+\vec{v}' = \vec{v_0} \end{cases}$

② discrete:

$\exists\, \varepsilon > 0$, for any two distinct points $x, y \in \Lambda$, the distance $\|x-y\| \geq \varepsilon$

2] e.g. 1, $\mathbb{Q}^m \subseteq \mathbb{R}^m$, but $\mathbb{Q}^m$ is not a lattice (not discrete)

e.g. 2, $\mathbb{Z}^m \subseteq \mathbb{R}^m$ is a lattice because it is subgroup and discrete for $\varepsilon = 0.1$

3] Applications:

① Sphere packing:

① Sphere packing:

for $m = 3$ (3D), 74.05 %

for $m > 3$, it is an open problem

② Number Theory. Lattices are discrete subgroups of $\mathbb{R}^m$

③ Cryptography:

- lattices have been used to break cryptosystems.
- lattice-based cryptosystems for post-quantum cryptography.

4] Def^n. Given n linearly independent vectors $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ the lattice generated by them is:

$$\mathcal{L}(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

Here, $b_1, \dots, b_n$ are called the basis of

n is the rank of the lattice

m is the dimension of the lattice, $n \leq m$

if $n = m$ then we have full-rank lattice.

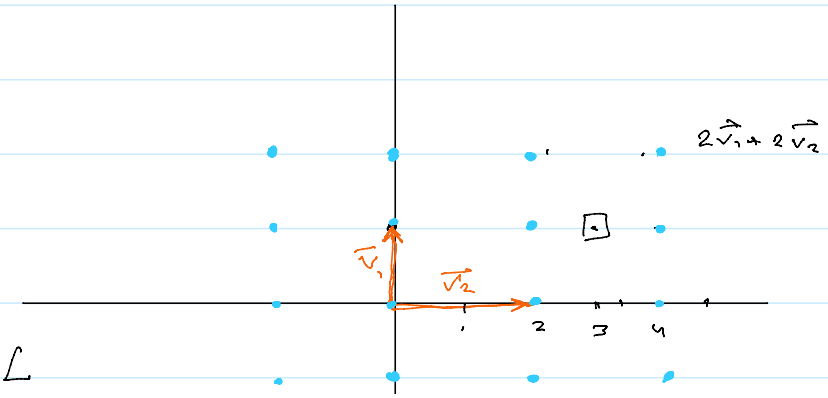
5] Examples:

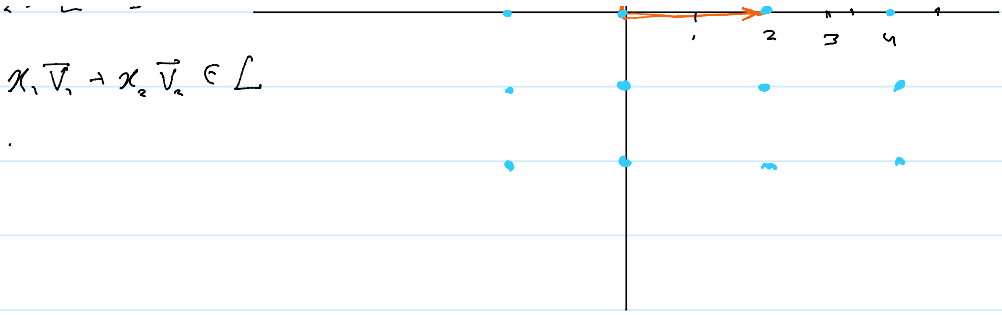
①

$\vec{v}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$\vec{v}_2 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$

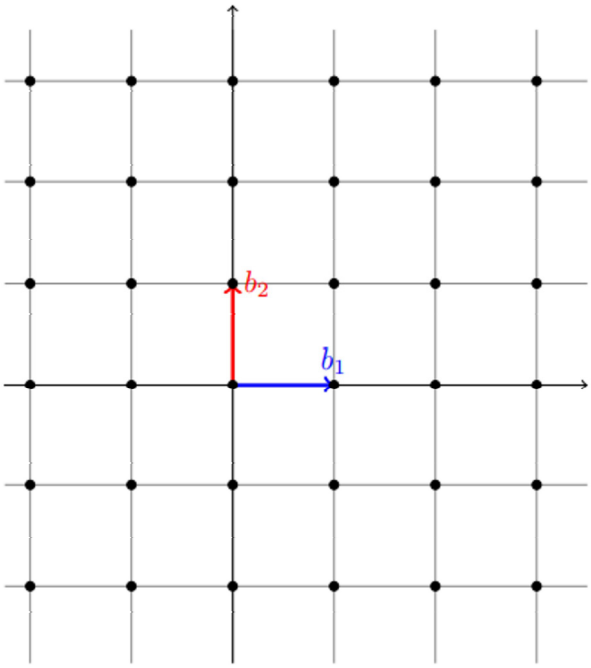
$x_1 \vec{v}_1 + x_2 \vec{v}_2 \in L$





$x_1 \vec{v}_1 + x_2 \vec{v}_2 \in L$

(2)



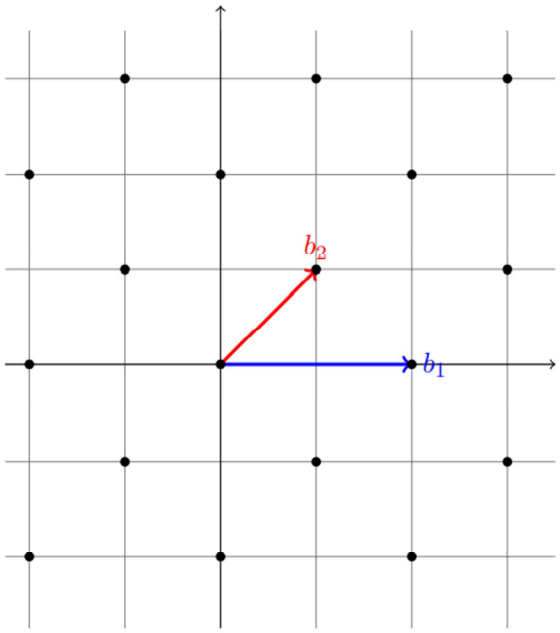
(a) The lattice $\mathbb{Z}^2$ with basis vectors $(0, 1)$ and $(1, 0)$.

$\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$

(3)

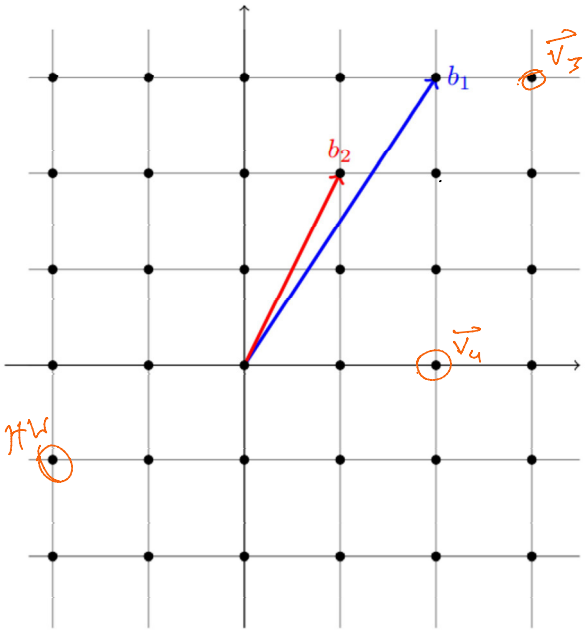
$\vec{v}_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$

$\vec{v}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$



(c) A full-rank lattice generated by the basis vectors $(1, 1)$ and $(2, 0)$. Note that this is a sub-lattice of $\mathbb{Z}^2$.

(4)



(b) The lattice $\mathbb{Z}^2$ with a different basis consisting of vectors $(1, 2)$ and $(2, 3)$. In fact, any lattice has infinitely many bases.

$\vec{v}_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$

$\vec{v}_2 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

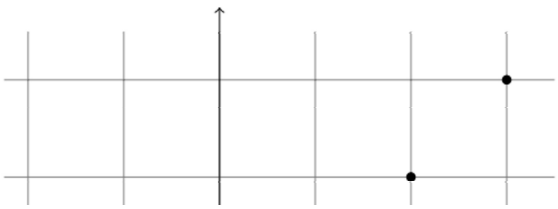
$3\vec{v}_1 - 3\vec{v}_2$

$\vec{v}_3 = 3\begin{bmatrix} 2 \\ 3 \end{bmatrix} - 3\begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$

$\vec{v}_4 = 4\vec{v}_1 - 6\vec{v}_2$ بلا

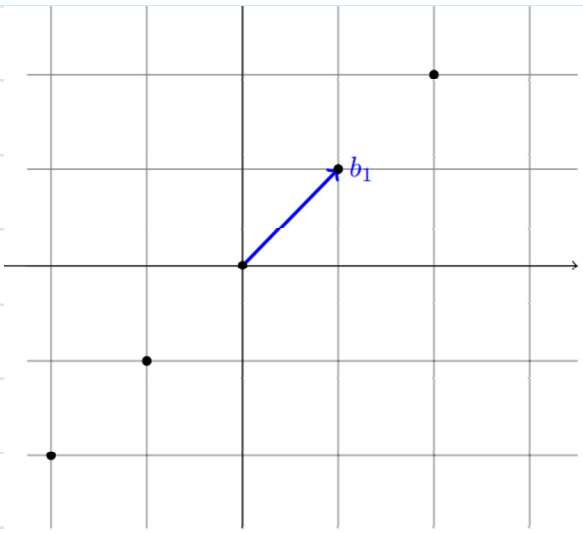
$= 4\begin{bmatrix} 2 \\ 3 \end{bmatrix} - 6\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ ✓

(5)



$\vec{v}_1 = \vec{G}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$\vec{v_1} = \vec{G_1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$



(d) A *non full-rank* lattice with basis vector $(1, 1)$

6] Notation: $\mathcal{L}(b_1, b_2, \ldots, b_n)$

Let $B = \begin{bmatrix} | & | & & | \\ b_1 & b_2 & \cdots & b_n \\ | & | & & | \end{bmatrix}$ (m rows, n columns)

be an $n \times m$ matrix, with $n \leq m$,

where the columns are the bases,

then

$$\mathcal{L}(B) = \{ Bx \mid x \in \mathbb{Z}^n \}$$

7] Note: Same lattice can have many bases.

e.g. $B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $B_2 = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ for $\mathbb{Z}^2$