Day 5 scribbles

July 24, 2020 11:37 AM

# Geometry of Lattices Day 5

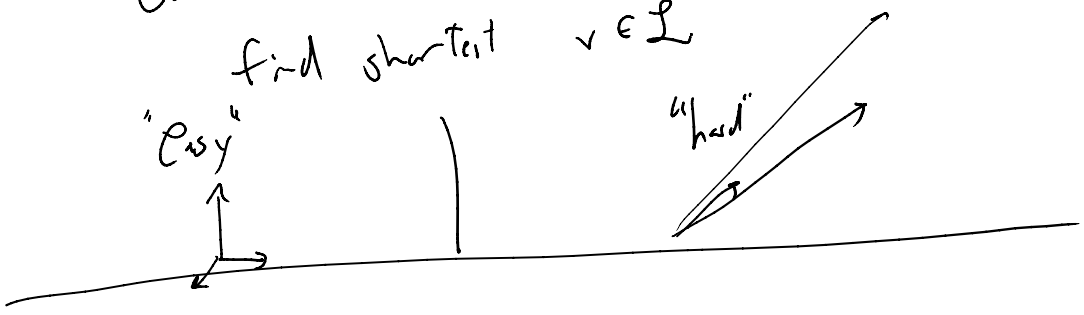
If you have information that you need to keep private, what do you do with it?

Recap

## Shortest Vector Problem (SVP)

Given a basis $b_1, \ldots, b_n$ for a lattice $\mathcal{L}$,

find shortest $v \in \mathcal{L}$




## LLL Reduction

LLL-reduced basis looks like a 2D reduced basis

If you take remainder after projecting onto previous basis vectors.

Day 4 Exp 5: $\frac{\sqrt{3}}{2} \|b_{k-1}^*\| \leq \|b_k^*\|$.

LLL is polynomial time. # of steps is a polynomial in dimension $n$.

E.g. 100-dim lattice, will take $10^6$ steps.

e.g. [illegible]

LLL is efficient, and gives a better basis than before.

$\hookrightarrow \|b_1\| \leq \left(\frac{2}{\sqrt{3}}\right)^n \lambda_1$ ($\lambda_1$ = length of shortest vector)

If $n = 100$, LLL returns a vector that could be 1.7 million times the length of shortest vector.

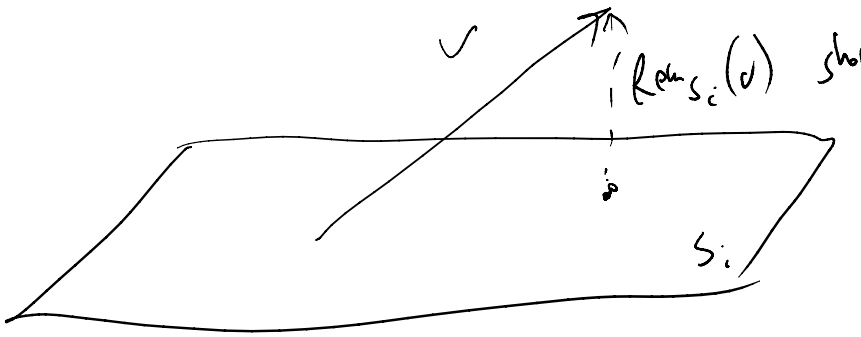
In high dim, even LLL does not give us short vectors!

Sol Brute Force!

Check all coefficients $a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$,

and see which is shortest.

How big can the coefficients get??




If I wrote $\|a_1 b_1 + \cdots + a_n b_n\| < L_1$

↓ $\|\cdot\| < L_1$

If $\perp$ wrt $\|a_1 \cdots$

That forces $\|\mathrm{Rem}_{S_{n-1}}(\ \ )\| < L$.

$$\Rightarrow \|a_n b_n^*\| < L$$

$$\Rightarrow |a_n| < \frac{L}{\|b_n^*\|}.$$

(Exp 1: check the details)

$$|a_k| < \frac{L}{\|b_k^*\|}.$$

We already know one vector that's kinda short: $b_1$. $L = \|b_1\|$

$$|a_k| < \frac{\|b_1\|}{\|b_k^*\|}.$$

Know: $\|b_1\| = \|b_1^*\| \le \left(\frac{2}{\sqrt{3}}\right)\|b_2^*\| \le \left(\frac{2}{\sqrt{3}}\right)^2 \|b_3^*\| \le \cdots \le \left(\frac{2}{\sqrt{3}}\right)^{k-1}\|b_k^*\|$

So $$|a_k| < \frac{\left(\frac{2}{\sqrt{3}}\right)^{k-1}\|b_k^*\|}{\|b_k^*\|} = \left(\frac{2}{\sqrt{3}}\right)^{k-1}.$$

To find a short vector $a_1 b_1 + \cdots + a_n b_n$,

$\le 2$ options for $a_1$

$\le 2\left(\frac{2}{\sqrt{3}}\right)$ " " $a_2$

$\le 2\left(\frac{2}{\sqrt{3}}\right)^2$ " " $a_3$ ...

Total # of vectors to check:

$$(2)\left(2\left(\tfrac{2}{\sqrt{3}}\right)\right)\left(2\left(\tfrac{2}{\sqrt{3}}\right)^2\right)\cdots\left(2\left(\tfrac{2}{\sqrt{3}}\right)^{n-1}\right) = \underbrace{2^n\left(\tfrac{2}{\sqrt{3}}\right)^{\frac{n(n-1)}{2}}}.$$

Plug in $n=100\ldots$

$$\approx 10^{339}.$$

Algorithms to solve SVP = NP-Hard

# of steps polynomial

Impossible ???

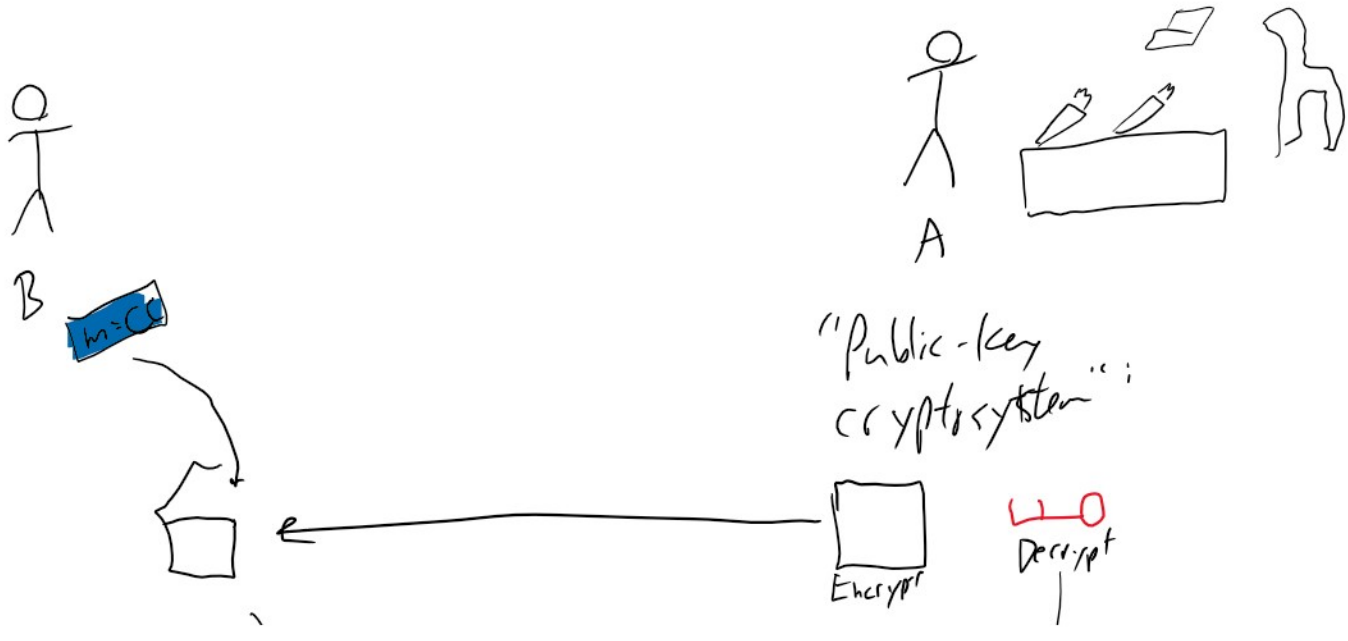
# of steps exponential (or worse)

Basic, brute force, (sieving ...)

find very short vectors (polynomial error)

find kinda short (exponential error)

LLL (HKZ, BKZ, etc)




It is technically always possible to break the box!

Goal: computationally infeasible to do this without key.

| RSA | ECC |
| --- | --- |
| Encrypt using $N$ | Elliptic curve $E$ |
| Decrypt: $N = pq$. | Encrypt using $P$, $kP$ |
| | Decrypt using $k$. |

## Quantum Computers break both!

NIST: search for "post-quantum cryptography"

How can regular computers defend against quantum?

## Lattice Crypto! (based on GGH)

Alice sets up a lattice $L$ w/ basis $u_1, u_2, \ldots, u_n$

Alice sets up a lattice $L$ w/ basis $u_1, u_2, \ldots, u_n$ (orthogonal.)

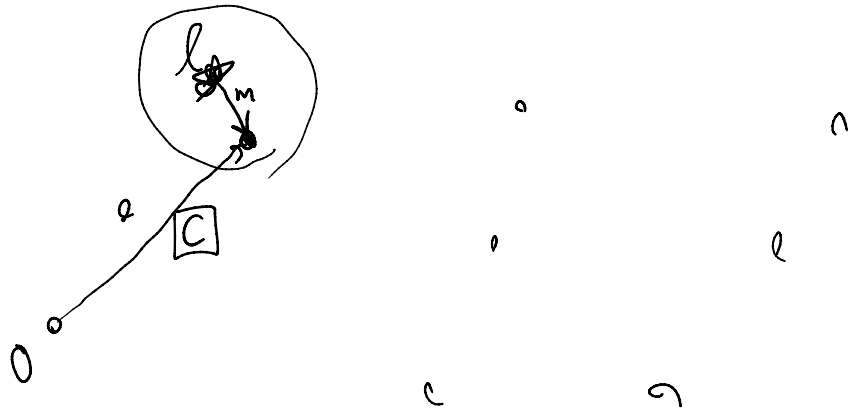
Alg finds a terrible basis generating $L$, $b_1, b_2, \ldots, b_n$

Also: $\ell \leq \frac{\|u_1\|}{2}$.

Encrypt Bob encodes message as a vector $\|m\| < \ell$

Chooses random $a_1, \ldots, a_n$,

publishes $\boxed{a_1 b_1 + \cdots + a_n b_n + m} = c$.




Decrypt: Find $\ell \in L$ closest to $c$, Alice computes $m = c - \ell$.

---

Exp 5: Why can Alice find closest vector? (knowing orthogonal basis)

---

An eavesdropper, Eve, finds $c$, $b_1, \ldots, b_n$.

Can Eve find message $m$?

Closest vector problem (CVP):

Given $b_1, \ldots, b_n$, and $v$ (not in lattice),

find the lattice vector gen by $b_1, \ldots, b_n$ closest to $v$.

---

Prop 6 CVP at least as hard as SVP.

(solving CVP lets ya solve SVP).

Pf idea: to solve SVP, remove vertex from $\mathcal{L}$ and solve CVP.

$\mathcal{L}$ is gen by $b_1, \ldots, b_n$.

Set $\mathcal{L}_i$ to be gen by $b_1, \ldots, b_{i-1}, 2b_i, b_{i+1}, \ldots, b_n$

Solve CVP: Which vector $l_i \in \mathcal{L}_i$ is closest to $b_i$?

Claim: shortest $l_i - b_i$ (over all $i$) is the shortest vector in $\mathcal{L}$.

$v = a_1 b_1 + \cdots + a_n b_n$ is shortest vector in $\mathcal{L}$.

At least one $a_j$ is odd.

$\frac{a_j + 1}{2}$ is an integer.

$$v = \underbrace{\left(a_1 b_1 + \cdots + a_{j-1} b_{j-1} + \left(\frac{a_j + 1}{2}\right)(2b_j) + \cdots + a_n b_n\right)}_{\in \mathcal{L}_j} - b_j$$

$v$ is a difference $(\in \mathcal{L}_j) - (b_j)$

What is the smallest $(\in \mathcal{L}_j) - (b_j)$?

solved with CVP: $\ell_j - b_j$

So $v$ can't be shorter than $\ell_j - b_j$.

$\ell_j - b_j$ is shortest possible in $\mathcal{L}$. □

---

If Eve can find $m$, then Eve could solve CVP,

Then Eve could solve SVP!

So this cryptosystem seems secure

No known way to leverage quantumness against lattice problems!