Lattices and Ajtai hash

Monday, November 29, 2021 3:54 PM

Lattices

- New algebraic object
- Some problems thought to be hard * involving lattices
  $\Longrightarrow$ Construct cryptography

  * Even against quantum attackers.
- Lots of structure $\Rightarrow$ flexible for PKE, Signature, ZK, ...

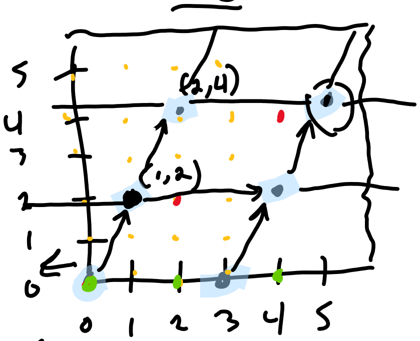
Three equiv definitions:

(I) A lattice Λ is a subgroup of $\mathbb{Z}_q^n$ under $\underset{\text{mod } q}{\underline{\text{addition}}}$ for integers q, n.

ex. lattices over $\mathbb{Z}_6^2$

$\boxed{|\mathbb{Z}_6^2| : 36}$

$\mathbb{Z}_6$



$(0,0) \in \mathbb{Z}_6^2$ is identity

examples of Λ

- $\mathbb{Z}_q^2$
- $|\langle (2,2) \rangle| = 3$
- $\langle (1,2) \rangle$ size 6

  $\{(0,0), (1,2),$
  $2 \cdot (1,2) = (2,4)$
  $3 \cdot (1,2) = (3,0)$
  $\vdots$
  $\}$
- $\langle (2,0) \rangle = 3$

$A = [2,4]$

(II) Integer Span

Let $A \in \mathbb{Z}_q^{m \times n}$ be a matrix

View as a set of m vectors in $\mathbb{Z}_q^n$

$$A^T = \left[\begin{pmatrix} \bar{a}_1 \end{pmatrix} \begin{pmatrix} \bar{a}_2 \end{pmatrix} \cdots \begin{pmatrix} \bar{a}_n \end{pmatrix} \right] \Big\} n$$

The lattice $\Lambda(A)$ is the integer span of these vectors $\vec{a}_1, \dots \vec{a}_n$

$$\Lambda(A) = \left\{ \sum_i s_i \cdot \vec{a}_i \;\middle|\; \vec{s} \in \mathbb{Z}^m \right\}$$

$$= \left\{ x \in \mathbb{Z}_q^n \;\middle|\; \underline{x = A^T s} \text{ for some } s \in \mathbb{Z}^m \right\}$$

III Dual form

$$\Lambda(A) = \left\{ x \in \mathbb{Z}_q^n \;\middle|\; \tilde{A} x = \vec{0} \right\}$$

where $\tilde{A} = \underline{A^T (\underline{A \cdot A^T})^{-1}}$

Assume A is linearly independent in columns and rows.

pseudoinverse.

$$\underline{\tilde{A} A = I = A \cdot \tilde{A}}$$

Lattice Problems:

- Shortest Vector Problem. (SVP)

Given $A \in \mathbb{Z}_q^{m \times n}$

Variants:

- Find the <u>smallest</u> non-zero vector in $\Lambda(A)$

  euclidean distance

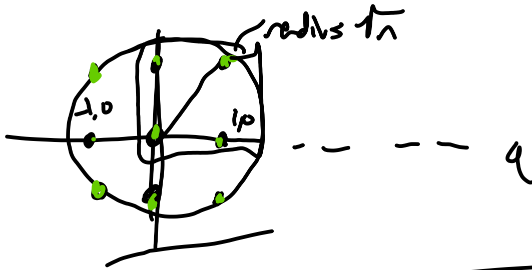
  $$\|x\| = \sqrt{\sum_i (x_i)^2}$$

  This is assumed hard for random matrices A.

- $\sqrt{n}$ - Shortest vector

  Given A, find <u>some</u> $\underline{x \in \Lambda(A)}$ s.t. $\|x\| \leq \sqrt{n}$

This defines a ball contains the hypercube $\{-1,0,1\}^n \subset \mathbb{Z}_q^n$



Collision resistant hash from $\sqrt{n}$ - SVP.

- main idea: Valid preimages lie within $\sqrt{n}$-radius ball

Setup:
- Let $\tilde{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ be the public parameter.
- The preimage space is $\{0,1\}^n$

Hash: - $f_A : \{0,1\}^n \to \mathbb{Z}_q^m$

$$f_A(x) = \tilde{A}^T \cdot x \quad \leftarrow \text{treat } x \in \mathbb{Z}_q^n$$

$$(m \times n)\cdot(n \times 1) \Rightarrow (m \cdot 1)$$

We set $\underline{n} > \underbrace{m \cdot \log_2 q}_{\text{size of digest in bits.}}$

Claim: This is collision resistant if $\sqrt{n}$ - SVP is hard.

Proof: Suppose $\mathcal{A}$ outputs collisions.

Given an instance of $\sqrt{n}$-SVP, A,

we'll output a short vector in $\Lambda(A)$ using $\mathcal{A}$

- Compute $\tilde{A}$. ← pub. param for hash
- $\mathcal{A}(\tilde{A}) \to x, x' \in \{0,1\}^n$

$x \neq x'$ Recall

but $f(x) = f(x')$

$\tilde{A}^T x = \tilde{A}^T x'$

$\tilde{A}^T (x - x') = 0$

$(x - x') \in \Delta(A)$

$\Delta(A) = \{ x \mid A^T x = 0 \}$

ex: $x = [0,1,0,0,1]$ $\quad x - x'$ $[-1,1,-1,0,1]$

$x' = [1,0,1,0,0]$

$\|x - x'\| \le \sqrt{n}$