Results

Debadatta Kar
Cryptography Research Lab
Indian Institute of Science Education and Research Bhopal

July 21, 2025

Lecture 6

1. Two bases B_1, B_2 generating the same lattice $\mathcal{L}$ are related by $B_2 = B_1 U$ where U is an unimodular matrix.

2. If $B = \{\tilde{b}_1, \tilde{b}_2, \cdots, \tilde{b}_n\}$ is the GSO basis then $\det(\mathcal{L}) = \prod_{i=1}^{n} ||\tilde{b}_i||$

3. **(Hadamard's Inequality)** If $B = \{b_!, b_2, \cdots b_n\}$ is the basis of lattice $\mathcal{L}$ then

$$\det(\mathcal{L}) \leq ||b_1|| \times ||b_2|| \times \cdots \times ||b_n||$$

4. Let B be a rank-n lattice basis, and B^* be its Gram-Schmidt orthogonalisation, then

$$\lambda_1(B) \geq \min_{1 \leq i \leq n} \{||b_j^*||\}$$

5. **(Blichfield)** For a full rank lattice $\mathcal{L}$ and a measurable set $S \subseteq \mathbb{R}^n$ such that $vol(S) > \det(\mathcal{L})$ there exist $x, y \in S$ such that $x - y \in \mathcal{L}$

6. **(Minkowski's Convex Body Theorem)** For a full rank lattice $\mathcal{L}$ and a centrally convex and symmetric set S with $Vol(S) > 2^n \det(\mathcal{L})$, S contains at least one non-zero lattice point.

7. **(Minkowski's First Theorem)** For any full rank lattice $\mathcal{L}$ of rank n

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det \mathcal{L})^{1/n}$$

8. **(Minkowski's Second Theorem)** For a full rank lattice $\mathcal{L}$

$$\left(\prod_{i=1}^{n} \lambda_i\right)^{1/n} \leq \sqrt{n} \cdot (\det(\mathcal{L}))^{1/n}$$

9. In a 2-dimensional lattice $\mathcal{L}$ with rank 2. If λ is the length of the shortest vector in the lattice, then

$$\lambda \leq \sqrt{\frac{2}{\sqrt{3}} \det(\mathcal{L})}$$

10. Let b_1, b_2 be the initial vectors of an iteration of the algorithm and let $b_1' = b_2 - mb_1$ and $b_2' = b_1$ be next set of vectors considered in the GLRA. Then except for possibly the last two iterations

$$||b_1'|| < \frac{||b_1||^2}{3}$$

11. If b_1, b_2 are some iterations of vectors in the **GLRA** with $||b_1|| \leq ||b_2||$ and $m = \left\lfloor \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \right\rceil$ then for all $k \in \mathbb{Z}$ we have
$$||b_2 - mb_1|| \leq ||b_2 - kb_1||$$

12. If b_1, b_2 are some iterations of vectors in the **GLRA** with $||b_1|| \leq ||b_2||$ and $m = \left\lfloor \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \right\rceil$ with $b_1' = b_2 - mb_1$ and $b_2' = b_1$ then $||b_1'|| \leq ||k'b_2' + b_1'||$ for all $k \in \mathbb{Z}$

13. If $m = \pm 1$ then the GLRA algorithm terminates in the next step.

14. Let $\mathcal{L} \subset \mathbb{R}^2$ be a two dimensional lattice basis with vectors b_1, b_2
    (a) The **GLRA** terminates and yields a good basis.
    (b) Final vector b_1 is the shortest vector in the lattice $\mathcal{L}$, so the algorithm solves the shortest vector problem in two dimensions.
    (c) The angle θ between b_1, b_2 satisfies $|\cos \theta| \leq \frac{||b_1||}{2||b_2||}$

15. Let $b_1, b_2, \cdots b_n \in \mathbb{R}^n$ be a $\delta -$ LLL reduced basis. Then
$$||b_1|| \leq \left(\frac{2}{\sqrt{4\delta - 1}} \right)^{n-1} \lambda_1(\mathcal{L})$$

References

[1] Oded Regev, *Lecture Notes on Lattices in Computer Science*, Tel Aviv University, Fall 2009.

[2] Vinod Vaikuntanathan, *Advanced Topics in Cryptography: From Lattices to Program Obfuscation*, MIT, Fall 2024.

[3] Deng, Xinyue *An Introduction to Lenstra-Lenstra-Lovasz Lattice Basis Reduction Algorithm*, Massachusetts Institute of Technology, 2016

[4] Galbraith, S. D. *Mathematics of public key cryptography* Cambridge University Press, 2012