

# CSE206A: Lattice Algorithms and Applications

## Blockwise Basis Reduction

UCSD – Fall 2025

Daniele Micciancio



- Input:  $\Lambda = \mathcal{L}(b_1, \dots, b_n)$
- GSO:  $b_1^*, \dots, b_n^*$ , lengths  $\|b_i^*\|$  are shorter and shorter due to projection
- Goal: ensure  $\|b_{i+1}^*\| \geq \|b_i^*\| / \alpha$  do not decrease too fast
- LLL algorithm: if  $\|b_{i+1}^*\| < \|b_i^*\| / \alpha$ , then swap  $b_i^*, b_{i+1}^*$
- Output:
  - **SVP**:  $\|b_1\| \leq \min_i (\alpha^{i-1} \|b_i^*\|) \leq \alpha^{n-1} \min_i \|b_i^*\| \leq \alpha^{n-1} \lambda(\Lambda)$
  - **HVP**:  $\|b_1\| \leq \sqrt[n]{\prod_i \alpha^{i-1} \|b_i^*\|} = \alpha^{\sum_i (i-1)/n} \det(\Lambda)^{1/n} = \sqrt{\alpha^{n-1}} \det(\Lambda)^{1/n}$
- Best  $\alpha = \gamma_2 = \frac{2}{\sqrt{3}} \approx 1.15$ : make  $\|b_i^*\| = \lambda(\mathcal{L}(\pi_i(b_i, b_{i+1})))$  as small as possible
  - Using Minkowski  $\|b_i^*\| \leq \sqrt{\gamma_2} (\|b_i^*\| \|b_{i+1}^*\|)^{1/2}$  gives  $\|b_i^*\| \leq \gamma_2 \|b_{i+1}^*\|$

- LLL algorithm: if  $\|b_{i+1}^*\| < \|b_i^*\| / \alpha$ , then swap  $b_i \leftrightarrow b_{i+1}$ 
  - Note: when swapping  $b_i \leftrightarrow b_{i+1}$ ,  $\|b_{i+1}^*\|^2$  may grow to  $\|b_{i+1}^*\|^2 + \frac{1}{4} \|b_i^*\|^2$
  - Still, the new  $\|b_i^*\|^2$  goes down to  $\|b_{i+1}^*\|^2 + \frac{1}{4} \|b_i^*\|^2 < \left(\frac{1}{\alpha^2} + \frac{1}{4}\right) \|b_i^*\|^2$
  - For  $\alpha = \gamma_2 = \frac{2}{\sqrt{3}}$ , we have  $\left(\frac{1}{\alpha^2} + \frac{1}{4}\right) = 1$ , and  $\|b_i^*\|^2$  decreases strictly at each swap
  - For  $\alpha > \gamma_2$ ,  $\|b_i^*\|^2$  decreases by a multiplicative constant at each iteration, and running time is polynomial
- Potential function:  $\prod_i \|b_i^*\|^{2(n-i)} = \prod_i \det(\mathbf{b}_1, \dots, \mathbf{b}_i)^2 \geq 1$  because  $\det(\mathbf{b}_1, \dots, \mathbf{b}_i)^2 \in \mathbb{Z}$ 
  - When swapping  $b_i \leftrightarrow b_{i+1}$ , only  $\det(\mathbf{b}_1, \dots, \mathbf{b}_{i+1})^2$  changes.
  - $\det(\mathbf{b}_1, \dots, \mathbf{b}_{i+1})$  changes by a factor  $\|b_i^{*[\text{new}]} \|^2 / \|b_i^{*[\text{old}]} \|^2 < \left(\frac{1}{\alpha^2} + \frac{1}{4}\right) < 1$

- Assume we can solve SVP in dimension  $k$
- Solve  $\text{SVP}(b_1, \dots, b_k)$ , so that
  - $\|b_1\| = \lambda(\mathcal{L}(b_1, \dots, b_k)) \leq \sqrt{\gamma_k} \det(b_1, \dots, b_k)^{1/k}$
  - $\|b_1\|^k \leq \gamma_k^{k/2} \prod_{i \geq 1} \|b_i^*\|$
  - $\|b_1\|^{k-1} \leq \gamma_k^{k/2} \prod_{i \geq 2} \|b_i^*\|$
  - $\|b_1\| \leq \gamma_k^{k/2(k-1)} (\prod_{i \geq 2} \|b_i^*\|)^{1/(k-1)}$
- What can we do next?
  - Solve  $\text{SVP}(\pi_1(b_2, \dots, b_{k+1}))$ : works well in practice, but difficult to analyse (BKZ)
  - Solve SVP on  $\text{dual}(\pi_1(b_2, \dots, b_{k+1})) = (d_2, \dots, d_{k+1})$  to make  $\|b_{k+1}^*\|$  as large as possible

- Primal SVP:  $\|b_1\| \leq \gamma_k^{\frac{k}{2(k-1)}} (\prod_{i \geq 2} \|b_i^*\|)^{\frac{1}{k-1}}$
- Dual SVP:  $\|d_{k+1}\| \leq \gamma_k^{\frac{k}{2(k-1)}} (\prod_{i \geq 2} \|b_i^*\|)^{\frac{-1}{k-1}}$
- Taking the inverse:  $\|b_{k+1}^*\| \geq \gamma_k^{-\frac{k}{2(k-1)}} (\prod_{i \geq 2} \|b_i^*\|)^{\frac{1}{k-1}}$
- Combine:  $\|b_1\| \leq \gamma_k^{\frac{k}{2(k-1)}} (\prod_{i \geq 2} \|b_i^*\|)^{\frac{1}{k-1}} \leq \gamma_k^{\frac{k}{(k-1)}} \|b_{k+1}^*\|$
- Repeat on  $\pi_k(b_{k+1}, \dots, b_{2k+1})$ ,  $\pi_{2k}(b_{2k+1}, \dots, b_{3k+1})$ , etc. up to  $n = ck + 1$ 
  - Similarly,  $\|b_{ik+1}^*\| \leq \gamma_k^{k/(k-1)} \|b_{(i+1)k+1}^*\|$
  - $\|b_1\| \leq \min_i \gamma_k^{ik/(k-1)} \|b_{ik+1}^*\| \leq \gamma_k^{ck/(k-1)} \min_i \|b_{ik+1}^*\| \leq \gamma_k^{(n-1)/(k-1)} \lambda(\Lambda)$

- Run SVP on blocks  $[b_1, \dots, b_k], [b_{k+1}, \dots, b_{2k}], \dots, [b_{(c-1)k+1}, \dots, b_{ck}], (b_n = b_{cn+1})$
- Run Dual SVP on  $(b_1), [b_2, \dots, b_{k+1}], [b_{k+2}, \dots, b_{2k+1}], \dots, [b_{(c-1)k+2}, \dots, b_{ck+1=n}]$
- Approximation SVP  $\gamma_k^{(n-1)/(k-1)} \lambda(\Lambda) \leq k^{(n-1)/(k-1)} \lambda(\Lambda) = \exp\left(\frac{\log k}{k-1}\right)^{n-1} \lambda(\Lambda)$ 
  - LLL is a special case for  $k=2$ , approximation  $\gamma_2^{n-1}$
  - Choosing larger (still constant)  $k$ , reduces the basis of exponential to

$$\lim_{k \rightarrow \infty} \exp\left(\frac{\log k}{k-1}\right) = 1$$

- Solving SVP in single exponential time  $2^{O(k)}$  is still polynomial for  $k = \log n$ , and achieves SVP approximation factor  $2^{n(\log \log n / \log n)} \ll 2^n$ .

- BKZ (Block Korkine-Zolotarev) reduction [Schnorr 1993]
  - Most popular, output is very good in practice, ... but
  - Theoretical approximation factor is worst than  $\gamma_k^{(n-1)/(k-1)}$
- Slide Reduction [Gama & Nguyen 2008]
  - Good theoretical bound  $\gamma_k^{(n-1)/(k-1)}$ , ... but
  - Worst quality than BKZ in practice
- Self-Dual BKZ [Micciancio & Walter 2015]
  - Theoretically as good as Slide Reduction
  - Practically as good as BKZ