Improved Progressive BKZ Algorithms and Their Precise Cost Estimation by Sharp Simulator

Yuncong Zhang

April 10, 2020

Introduction

The *Shortest Vector Problem* (SVP):

- Given the lattice $L = L(\vec{b}_1, \cdots, \vec{b}_n)$
- Find the shortest non-zero vector $\vec{v}^* \in L$

Introduction

Current algorithms for solving SVP:

- Blockwise: LLL, BKZ
- Enumeration
- Seiving

Introduction

Blockwise algorithms:

- Efficiency: polynomial time for appropriate parameters
- Quality: exponential approximation factor

Enumeration algorithms:

- Efficiency: exponential
- Quality: exact solution

Relationships:

- Blockwise algorithms invokes enumeration algorithm on local blocks
- Enumeration algorithm requires preprocessing by blockwise algorithms

Introduction

BKZ Algorithms:

- Basic BKZ (proposed by C. P. Schnorr in 1994)
- BKZ 2.0
- Progressive BKZ

Preliminaries

- Mathematical Definitions
- Enumeration Algorithm
- LLL Algorithm

Mathematical Definitions

Gram-Schmidt Basis for $B = (\vec{b}_1, \cdots, \vec{b}_n)$:

- $B^* := (\vec{b}_1^*, \cdots, \vec{b}_n^*)$
- $\vec{b}_i^* := \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \cdot \vec{b}_j^*$
- $\mu_{ij} := \langle \vec{b}_i, \vec{b}_j^* \rangle / \|\vec{b}_j^*\|^2$ called GS coefficients

Properties:

- $\mathrm{vol}(L) := \det(L) := \det(B) = \det(B^*) = \prod_{i=1}^{n} \|\vec{b}_i^*\|$
- Gram-Schmidt Assumption (GSA): $\|\vec{b}_i^*\|^2 / \|\vec{b}_1\|^2 = r^{i-1}$, where $r \in [3/4, 1)$ is GSA constant

Mathematical Definitions

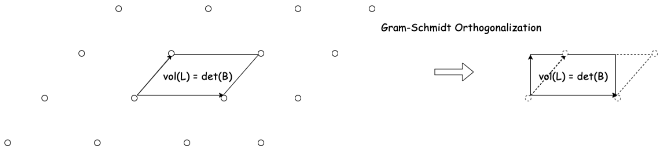

Figure: Gram-Schmidt orthogonalization and volume of lattice

Mathematical Definitions

Projection $\pi_i : \mathbb{R}^n \to \text{span}(\vec{b}_1, \cdots, \vec{b}_{i-1})^\perp$

$$\pi_i(v) := \vec{v} - \sum_{j=1}^{i-1} \langle \vec{v}, \vec{b}_j^* \rangle \vec{b}_j^* / \|\vec{b}_j^*\| \tag{1}$$

which effectively removes the proportion of the vector inside the space $\text{span}(\vec{b}_1, \cdots, \vec{b}_{i-1})$.

Remark

Gram-Schmidt reduction can be rewritten as: $\vec{b}_i^* = \pi_i(\vec{b}_i)$

Mathematical Definitions

Projective *local block*

$$L_{[i:j]} \quad := \quad \pi_i(L(\vec{b}_i, \vec{b}_{i+1}, \cdots, \vec{b}_j)) \tag{2}$$

Use $B_i := L_{[i:i+\beta-1]}$ when the blocksize β is clear

Mathematical Definitions

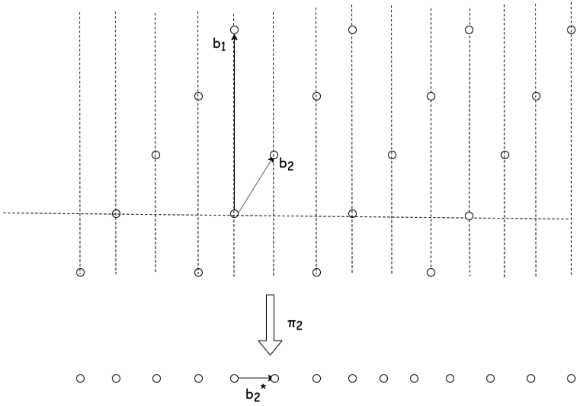

Figure: Projection π_2 on a lattice

Mathematical Definitions

Gaussian Huristic: for convex set S

- $|S \cap L| \approx \mathrm{vol}(S)/\mathrm{vol}(L)$
- $\mathrm{GH}(L) := (\mathrm{vol}(L)/V_n(1))^{1/n}$ approximation of $\lambda_1(L)$

Remark

$V_n(R)$ is the volume of the n-dimensional ball.

$$V_n(R) = R^n \cdot \frac{\pi^{n/2}}{\Gamma(n/2+1)}$$

Mathematical Definitions

Modified Gaussian heuristic for local blocks:

- For local blocks B_i and small blocksize β, $\mathrm{GH}(B_i)$ is often smaller than $\lambda_1(L)$
- Approximates $\lambda_1(L)$ with $\tau_i \mathrm{GH}(B_i)$ instead

where

$$\tau_i := \frac{\|\vec{b}^*_{n-i+1}\|}{V_i(1)^{-1/i} \cdot \prod_{j=n-i+1}^{n} \|\vec{b}^*_j\|^{1/i}}$$

is called modified Gaussian heuristic constant.

Enumeration Algorithm

Given a lattice basis $B = (\vec{b}_1, \cdots, \vec{b}_n)$, finds the shortest vector $\vec{v}^*$

$$\vec{v}^* = a_1\vec{b}_1 + a_2\vec{b}_2 + \cdots + a_n\vec{b}_n \qquad \forall i \in [n]$$

Observation:

- $\|\pi_i(a_i\vec{b}_i + \cdots + a_n\vec{b}_n)\| = \|\pi_i(\vec{v}^*)\| \leq \|\vec{v}^*\| \approx R_i$
- For $i = n$, $|a_n| \leq R_n/\|\vec{b}_n^*\|$
- Fix $a_n, \cdots, a_{i+1}$, then $|a_i|$ is bounded

Enumeration Algorithm

Searching tree:

- Root: zero vector $\vec{0}$
- Children of $\vec{v}$ (at depth k): $\vec{v} + a_{n-k}\vec{b}_{n-k} \quad \forall a_{n-k} \in \mathbb{Z}$ bounded by R_{n-k} projected by $\pi_{n-k+1}(\cdot)$
- Nodes at depth k: $\forall \vec{v} \in \mathbb{R}^n$ with $\|\pi_k(\vec{v})\|$ bounded by R_{n-k+1}

Enumeration Algorithm

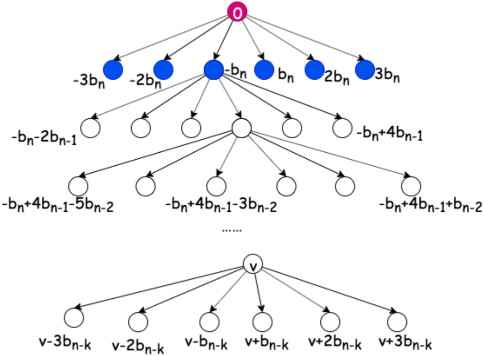

Figure: Searching Tree

LLL Algorithm

Previous BKZ Algorithms

Basic BKZ Algorithm

BKZ 2.0

Progressive BKZ

Improved Progressive BKZ

Optimizing Parameters

Estimating Enumeration Cost

Blocksize Strategy

BKZ Rounds

Pre/Post-Processing

Q/A