Recursive Lattice Reduction

Thomas Plantard
Willy Susilo

Centre for Computer and Information Security Research
Universiy of Wollongong

http://www.uow.edu.au/~thomaspl
thomaspl@uow.edu.au

Cryptography concerned by Lattice Reduction

Problem

- Shortest Vector Problem (SVP): Ajtai-Dwork, Regev, ...
- Closet Vector Problem (CVP): GGH, NTRU, ...
- Knapsack Problem
- Coding based cryptosystem
- RSA, Factorization.
- Learing With Error (LWE)
- Short Integer Solution (SIS): SWIFFT, SWIFFTX, ...

Lattice Reduction

- Heuristic BUT successful
- Weeks, Month of Computation: Good Estimation.
- 2^{80}, 2^{100}: Unknown.

Outline

Lattice Theory

Lattice

Definition of a Lattice

- All the integral conbinations of $d \leq n$ linearly independant vectors over $\mathbb{R}$

$$\mathcal{L} = \mathbb{Z}\,\mathbf{b}_1 + \cdots + \mathbb{Z}\,\mathbf{b}_d = \{\lambda_1 \mathbf{b}_1 + \cdots + \lambda_d \mathbf{b}_d \ : \ \lambda_i \in \mathbb{Z}\}$$

- d dimension.
- $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a *basis*.

An Example

$$\mathbf{B} = \begin{pmatrix} 5 & \frac{1}{2} & \sqrt{3} \\ \frac{3}{5} & \sqrt{2} & 1 \end{pmatrix} \tag{1}$$

$d = 2 \leq n = 3$

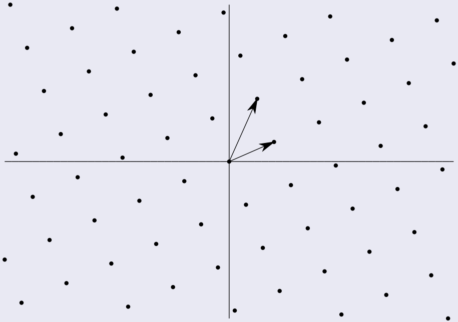
In this work, integer Basis: $B \in \mathbb{Z}^{d,n}$.

Example

A lattice $\mathcal{L}$

$$\mathbf{B} = \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} \tag{2}$$

An infinity of basis

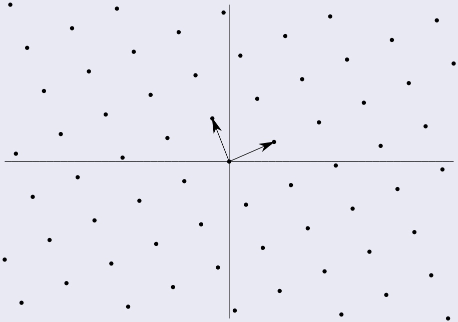


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ -3 & 11 \end{pmatrix} \quad (3)$$

An infinity of basis

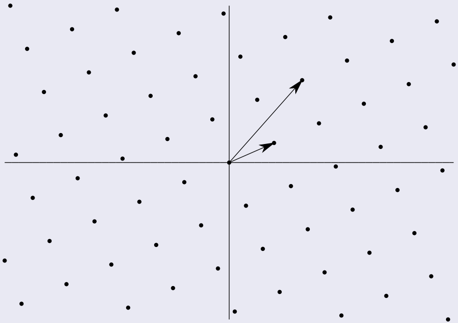


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ 13 & 21 \end{pmatrix} \tag{4}$$

An infinity of basis

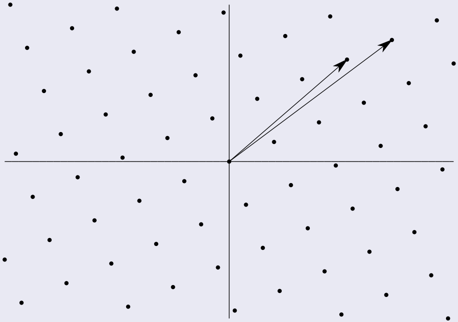


Example

A lattice $\mathcal{L}$

$$\mathbf{UB} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 8 & 5 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 29 & 31 \\ 21 & 26 \end{pmatrix} \quad (5)$$

An infinity of basis

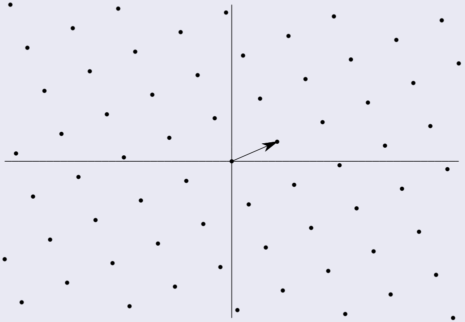


Example

The Shortest Vector and The First Minima

$$\mathbf{v} = \begin{pmatrix} 8 & 5 \end{pmatrix}, \text{ with } \lambda_1 = \sqrt{8^2 + 5^2} = 9.434 \quad (6)$$

The Shortest Vector

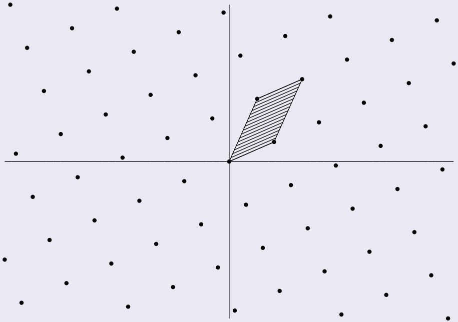


Example

The Determinant

$$\det \mathcal{L} = \sqrt{\det \left(\mathbf{B}\mathbf{B}^T\right)} = 103 \tag{7}$$

The Determinant



Hermite Invariant,Constant and Factor.

Hermite invariant

$$\gamma(\mathcal{L}) = \left(\frac{\lambda_1(\mathcal{L})}{\det(\mathcal{L})^{1/dim(\mathcal{L})}}\right)^2 = (\frac{9.434}{103^{1/2}})^2 = 0.86408$$

Random Lattice: $\gamma(\mathcal{L}) \sim \frac{dim(\mathcal{L})}{2\pi e}$.

Minkowski Theorem 1896

$$\forall \mathcal{L}, \gamma(\mathcal{L}) \leq \gamma_d \leq 1 + \frac{dim(\mathcal{L})}{4} = 1.5$$

γ_d is called Hermite Constant.

Hermite Factor of a basis

$$\gamma(\mathbf{B}) = \frac{\|b_1\|}{\det(\mathcal{L})^{1/dim(\mathcal{L})}}.$$

Capital for Lattice Reduction Quality.

Lattice Reduction Algorithm

Find $v \in \mathcal{L}$ smallest

- SVP is NP-Hard under randomized reduction.
- Deterministic $O(d^{\frac{d}{2e}})$: Kannan 1986, Hanrot and Sthele 2007.
- Probabilistic $O(2^d)$: AKS 2001.

Find $v \in \mathcal{L}$ small

- LLL: Lenstra, Lenstra and Lovasz $O(n^5)$.
- DEEP-k: LLL with Deep Insertion (Exponential time in k).
- BKZ-k: Block Korkine Zolotaref (Exponential time in k).
- ...

Lattice Reduction in Average

Gama-Nguyen Estimation

Model

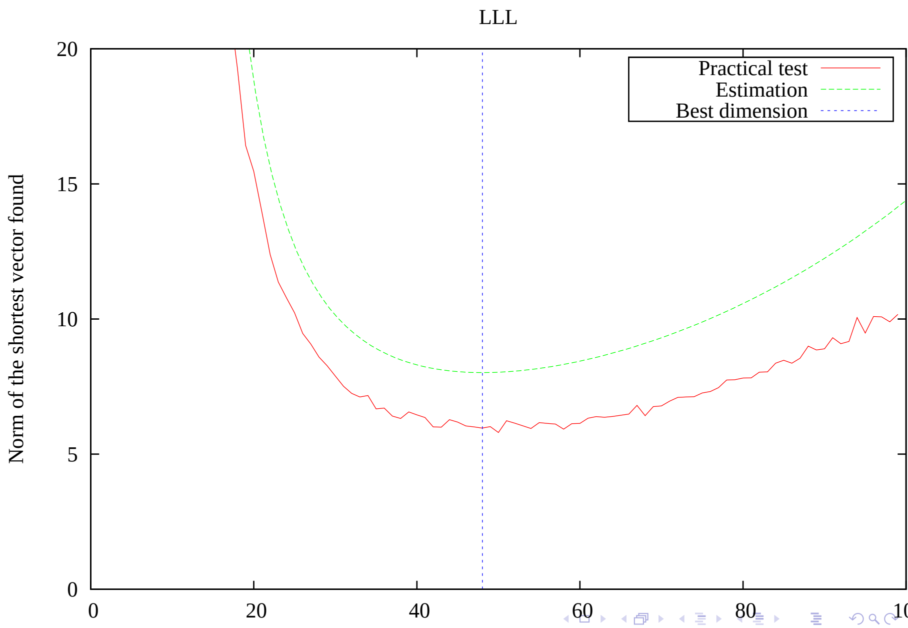
An Lattice Reduction Algorithm is able to find a vector $v \in \mathcal{L}$ such that

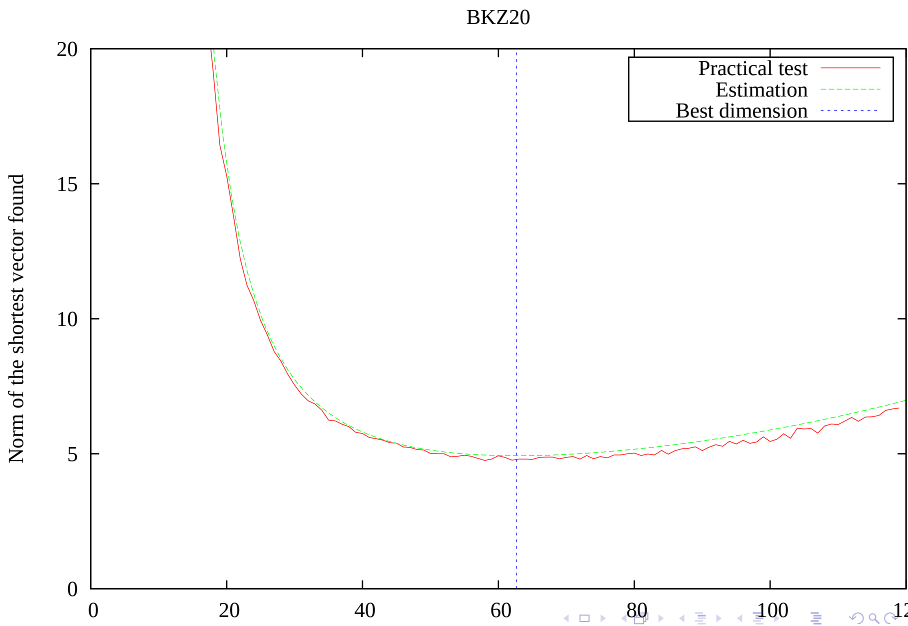
$$\|v\| = c^{dim} \det(\mathcal{L})^{1/dim}$$

where c depends of algorithm quality.

Average beaviour $\neq$ Upper Bound

Algorithm	Average	Upper Bound
LLL	1.0219	1.0754
BKZ-20	1.0128	1.0337
BKZ-28	1.0109	1.0282
DEEP-50	1.011	1.0754
None	1.01	-


LLL
Practical test
Estimation
Best dimension
Norm of the shortest vector found
20
15
10
5
0
0
20
40
60
80


BKZ20
Norm of the shortest vector found
Practical test
Estimation
Best dimension
0
5
10
15
20
0
20
40
60
80
100

Recursive Lattice Reduction

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

Advantage

- Find $\mathcal{L}_{d'}$ where d' is optimal without any extra timing cost.
- Using time computation whenever appropriate only.

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B} = \begin{pmatrix} 1031 & 0 & 0 & 0 & 0 \\ 354 & 1 & 0 & 0 & 0 \\ 322 & 0 & 1 & 0 & 0 \\ 916 & 0 & 0 & 1 & 0 \\ 426 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (8)$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_1} = \begin{pmatrix} 1031 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{9}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_2} = \begin{pmatrix} 1031 & 0 & 0 & 0 & 0 \\ 354 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{10}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_2} = \begin{pmatrix} -31 & -3 & 0 & 0 & 0 \\ 13 & -32 & 0 & 0 & 0 \end{pmatrix} \tag{11}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_3} = \begin{pmatrix} -31 & -3 & 0 & 0 & 0 \\ 13 & -32 & 0 & 0 & 0 \\ 322 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{12}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_3} = \begin{pmatrix} -1 & 2 & 1 & 0 & 0 \\ 0 & -6 & 13 & 0 & 0 \\ -27 & -11 & -4 & 0 & 0 \end{pmatrix} \tag{13}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_4} = \begin{pmatrix} -1 & 2 & 1 & 0 & 0 \\ 0 & -6 & 13 & 0 & 0 \\ -27 & -11 & -4 & 0 & 0 \\ 916 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (14)$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_4} = \begin{pmatrix} -1 & 2 & 1 & 0 & 0 \\ -4 & -3 & 4 & 2 & 0 \\ 4 & 0 & 5 & 5 & 0 \\ 0 & -3 & 4 & -7 & 0 \end{pmatrix} \tag{15}$$

Example

Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_5} = \begin{pmatrix} -1 & 2 & 1 & 0 & 0 \\ -4 & -3 & 4 & 2 & 0 \\ 4 & 0 & 5 & 5 & 0 \\ 0 & -3 & 4 & -7 & 0 \\ 426 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{16}$$

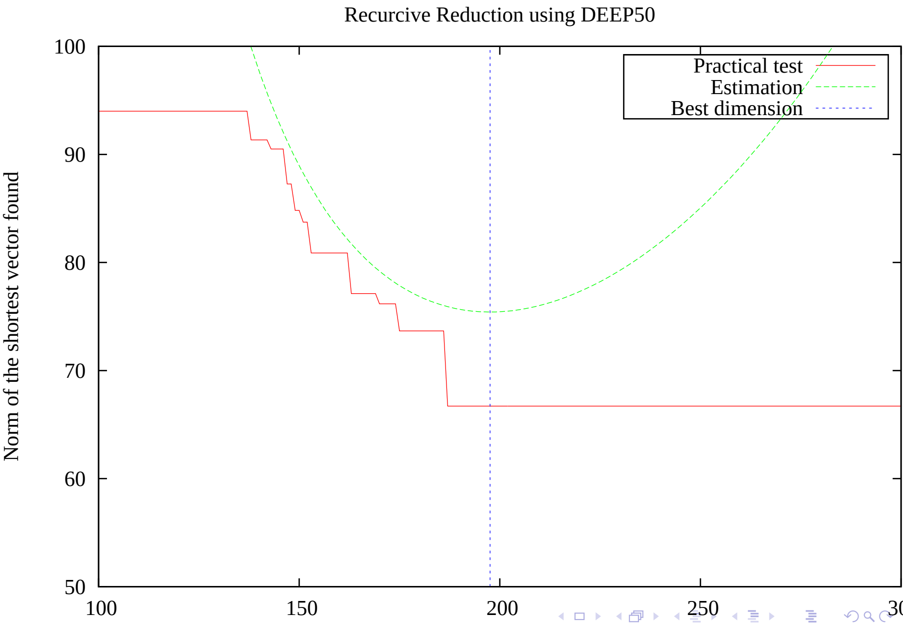
Example

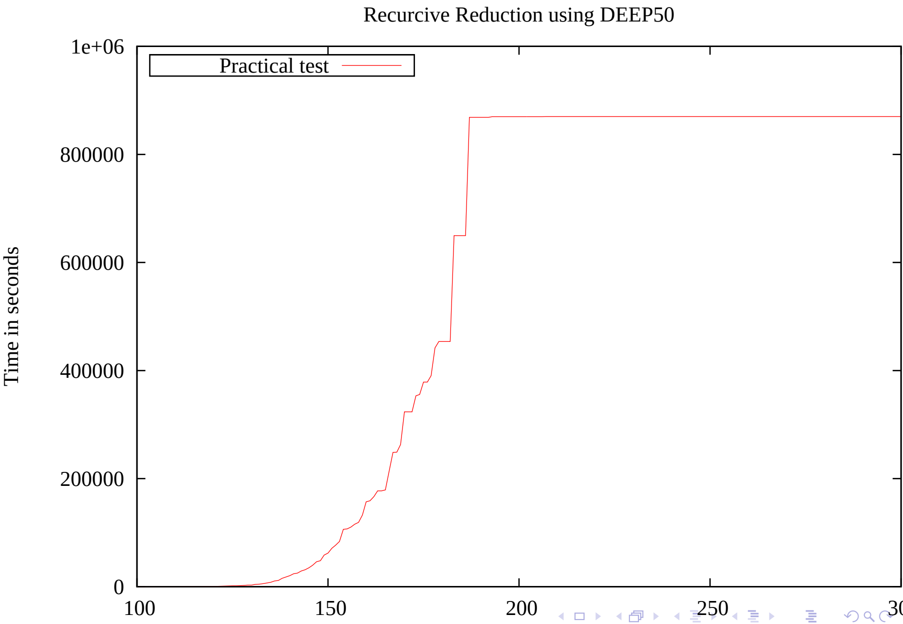
Method

- Choose $\mathcal{L}_1 \subset \cdots \subset \mathcal{L}_i \cdots \subset \mathcal{L}_d = \mathcal{L}$ with $dim(\mathcal{L}_i) = i$.
- $\mathcal{L}_1$ is reduced.
- For each $\mathcal{L}_{i+1}$, apply Lattice Reduction Algorithm on $\mathcal{L}_{i+1} \cup \mathcal{L}_i$

An Example

$$\mathbf{B_5} = \begin{pmatrix} -1 & 2 & 1 & 0 & 0 \\ 0 & -2 & 2 & 1 & -2 \\ -2 & -2 & 3 & -3 & 1 \\ -2 & 1 & -1 & 4 & 1 \\ 3 & 0 & 3 & 0 & 5 \end{pmatrix} \tag{17}$$


Recurcive Reduction using DEEP50
Norm of the shortest vector found
Practical test
Estimation
Best dimension
100
90
80
70
60
50
100
150
200
250


Recurcive Reduction using DEEP50
Practical test
Time in seconds
1e+06
800000
600000
400000
200000
0
100
150
200
250
300

Result

Result on the Darmstadt Challenge

Challenge	Previous Best Result	Recursive Reduction Result
500	25.8457	25.2587
525	35.6651	30.7409
550	39.7995	38.2884
575	50.7149	42.7083
600	57.2975	52.0096
625	61.8061	59.4138
650	69.4478*	66.7158
675	82.6015*	80.0937*
700	89.4315*	89.3924*
725	103.7208*	100.8960
750	—*	—

Future Work

Future Work

- Integrate other Lattice Reduction Algorithm
- Use different sublattice choice.

Question.

What can we do with 2^x operation?