Lattices

Lukas Helminger

Mathematical Foundations of Cryptography – WT 2019/20

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Outline

Lattice Reduction Algorithms

- The Two-Dimensional Case
- Lenstra-Lenstra-Lováz Algorithm (LLL)

Literature

The slides are based on the following sources

- **An Introduction to Mathematical Cryptography**, Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H.
- **The LLL Algorithm**, Phong Q. Nguyen, Brigitte Vallée (Eds.)

Lattice Reduction Algorithms

Recap from Last Lecture

Lattice: Basis, Fundamental Domain, Volume

Recap from Last Lecture

Lattice: Basis, Fundamental Domain, Volume

SVP: Minkowski's and Hermite's Theorem

Recap from Last Lecture

Lattice: Basis, Fundamental Domain, Volume

SVP: Minkowski's and Hermite's Theorem

Reduction: Babai's Algorithm

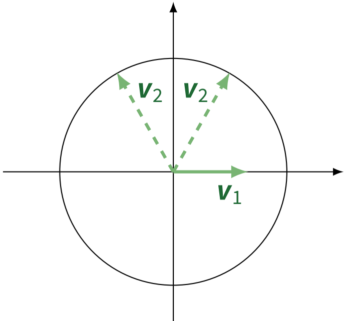
Lagrange-Reduced

Definition

Lagrange-reduced Let L be a two-dimensional lattice. A basis (v_1, v_2) of L is said to be Lagrange-reduced if and only if

$$\|v_1\| \leq \|v_2\| \quad \text{and} \quad |v_1 \cdot v_2| \leq \frac{\|v_1\|^2}{2}.$$

Optimal: $\lambda_1(L) = \|v_1\|$



Lagrange's Reduction Algorithm

Input: A basis (u, v) of a 2-dimensional lattice L.
Ouput: A Lagrange-reduced basis of L.

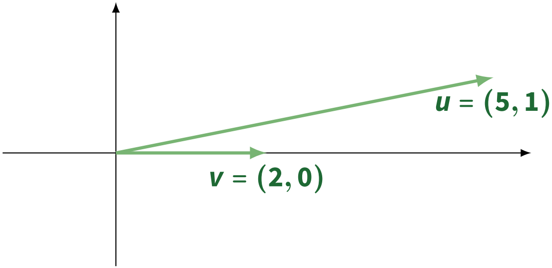
Lagrange's Reduction Algorithm

Input: A basis (u, v) of a 2-dimensional lattice L.
Ouput: A Lagrange-reduced basis of L.

if $\|u\| < \|v\|$ **then**
    sawp u and v
while $\|v\| > \|u\|$ **do**
    $r \leftarrow u - qv$ where $q = \left\lfloor \dfrac{u \cdot v}{\|v\|^2} \right\rceil$
    $u \leftarrow v$
    $v \leftarrow r$
return (u, v)

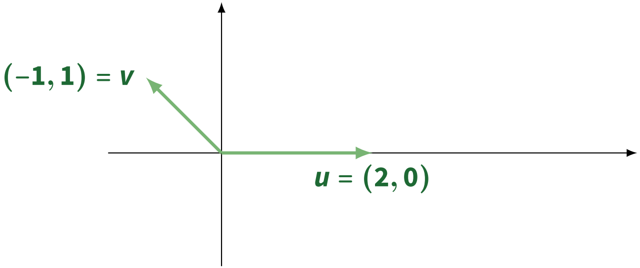
Lagrange Reduction: Example

Input: $v = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, u = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$



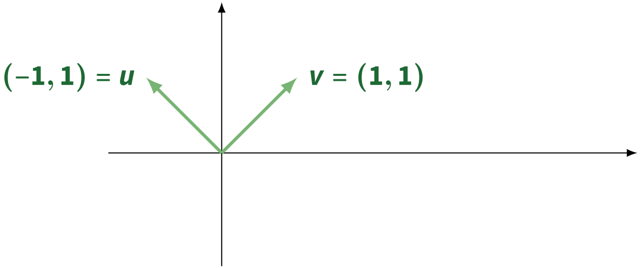
Lagrange Reduction: Example

Input: $v = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, u = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$



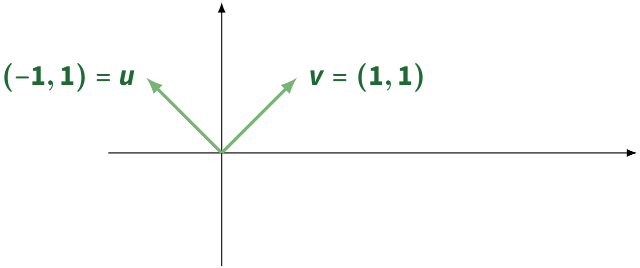
Lagrange Reduction: Example

Input: $v = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, u = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$



Lagrange Reduction: Example

Input: $v = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, u = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$



Task: Solve SVP for the lattice generated by

$$v_1 = (66586820, 65354729)^T, v_2 = (6513996, 6393464)^T.$$

Size-Reduction

Definition (Size-Reduced)

A basis $v_1, \dots, v_n$ of a lattice is size-reduced if its Gram-Schmidt orthogonalization satisfies

$$|\mu_{i,j}| \leq \frac{1}{2}.$$

Size-Reduction

Definition (Size-Reduced)

A basis $v_1, \ldots, v_n$ of a lattice is size-reduced if its Gram-Schmidt orthogonalization satisfies

$$|\mu_{i,j}| \leq \frac{1}{2}.$$

Input: A basis $(v_1, \ldots v_n)$ of a lattice L.
Ouput: A size-reduced basis of L.

Size-Reduction

Definition (Size-Reduced)

A basis $v_1, \ldots, v_n$ of a lattice is size-reduced if its Gram-Schmidt orthogonalization satisfies

$$|\mu_{i,j}| \leq \frac{1}{2}.$$

Input: A basis $(v_1, \ldots v_n)$ of a lattice L.
Ouput: A size-reduced basis of L.

```
Compute all the Gram-Schmidt coefficients μ_{i,j}
for i = 2..n do
    for j = (i − 1)..1 do
        v_i ← v_i − ⌊μ_{i,j}⌉ v_j
        for k = 1..j do
            μ_{i,k} ← μ_{i,k} − ⌊μ_{i,j}⌉ μ_{j,k}
```

LLL Algorithm

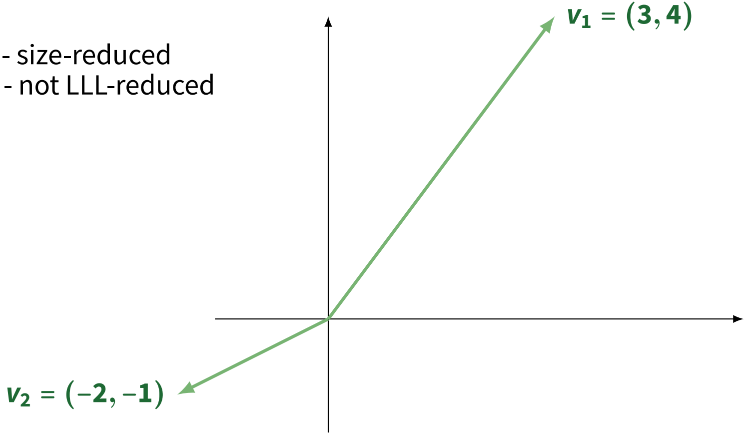
Definition (LLL-Reduced)

Let $B = \{v_1, \ldots, v_n\}$ be a basis for a lattice L and denote its associated Gram-Schmidt orthogonal basis as $v_1^*, \ldots, v_n^*$. The basis is said to be LLL-reduced if it is size-reduced and satisfies for all $1 < i \leq n$.

$$\|v_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|v_{i-1}^*\|^2. \qquad \text{(Lovász Condition).}$$

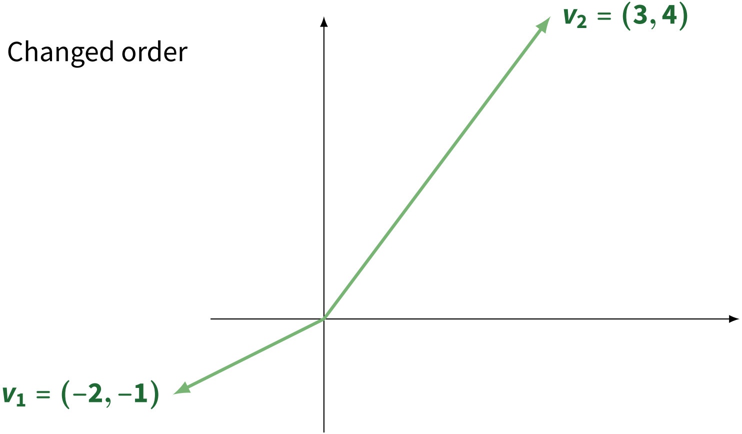
Why Lovász Condition?

- size-reduced
- not LLL-reduced



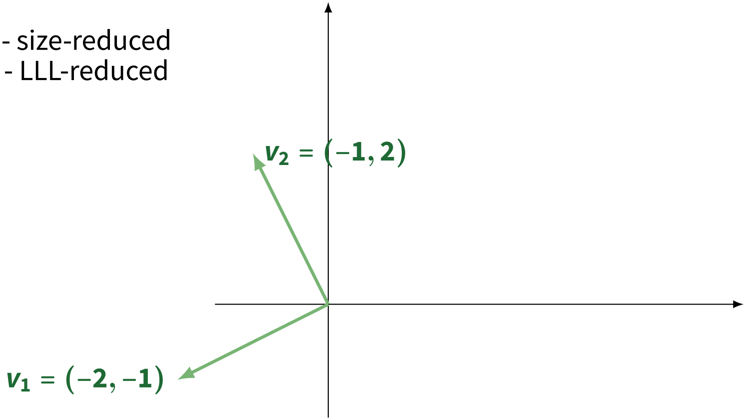
Why Lovász Condition?

Changed order



Why Lovász Condition?

- size-reduced
- LLL-reduced



LLL-reduced Basis is Good Basis

Theorem

Let L be a lattice of dimension n. Any LLL reduced basis $v_1, \ldots, v_n$ for L has the following property:

$$\prod_{i=1}^{n} \|v_i\| \leq 2^{\frac{n(n-1)}{4}} \operatorname{vol}(L).$$

In particular,

$$\|v_1\| \leq 2^{\frac{n-1}{2}} \lambda_1(L).$$

Thus an *LLL* reduced basis solves apprSVP within a factor of $2^{(n-1)/2}$.

LLL Algorithm

Input: A basis $(v_1, \ldots v_n)$ of a lattice L.
Ouput: A LLL-reduced basis of L.

LLL Algorithm

Input: A basis $(v_1, \ldots v_n)$ of a lattice L.
Ouput: A LLL-reduced basis of L.

Size-reduce $(v_1, \ldots v_n)$
if $\exists\, j \in \{2, \ldots, n\}$: Lovász Condition violated **then**
swap v_j and v_{j-1}
$LLL(v_1, \ldots, v_n)$

LLL Algorithm

Input: A basis $(v_1, \dots v_n)$ of a lattice L.
Ouput: A LLL-reduced basis of L.

Size-reduce $(v_1, \dots v_n)$
if $\exists j \in \{2, \dots, n\}$: Lovász Condition violated **then**
  swap v_j and v_{j-1}
  $LLL(v_1, \dots, v_n)$

Theorem

Given a basis $v_1, \dots, v_n$ of a Lattice L the LLL algorithm calculates an LLL-reduced basis in time

$$\mathcal{O}\left(n^6 \log^3 B\right), \qquad \text{where } B = \max_i \|v_i\|.$$

Proof sketch

It is clear that the output is LLL-reduced. So we only have to show finite number of steps.

- L_l = lattice spanned by $v_1, \ldots v_l$.

Proof sketch

It is clear that the output is LLL-reduced. So we only have to show finite number of steps.

- L_l = lattice spanned by $v_1, \ldots v_l$.
- $d_l = \prod_{i=1}^{l} \|v_i^*\|^2$ and $D = \prod_{i=1}^{l} d_l \Rightarrow \det(L_l)^2 = d_l$.

Proof sketch

It is clear that the output is LLL-reduced. So we only have to show finite number of steps.

- L_l = lattice spanned by $v_1, \ldots v_l$.
- $d_l = \prod_{i=1}^{l} \|v_i^*\|^2$ and $D = \prod_{i=1}^{l} d_l \Rightarrow \det(L_l)^2 = d_l$.
- D changes only when swapping. More precisely, D is reduced by a factor of at least $(3/4)^N$ (argumentation with fact that Lovász condition is violated).

Proof sketch

It is clear that the output is LLL-reduced. So we only have to show finite number of steps.

- L_l = lattice spanned by $v_1, \ldots v_l$.
- $d_l = \prod_{i=1}^{l} \|v_i^*\|^2$ and $D = \prod_{i=1}^{l} d_l \Rightarrow \det(L_l)^2 = d_l$.
- D changes only when swapping. More precisely, D is reduced by a factor of at least $(3/4)^N$ (argumentation with fact that Lovász condition is violated).
- Bound D from above with Hermite's Theorem.

LLL Example

Task: Compute an LLL-reduced basis of the 6-dimensional lattice L with basis given by the rows of the matrix

$$\begin{pmatrix} 19 & 2 & 32 & 46 & 3 & 33 \\ 15 & 42 & 11 & 0 & 3 & 24 \\ 43 & 15 & 0 & 24 & 4 & 16 \\ 20 & 44 & 44 & 0 & 18 & 15 \\ 0 & 48 & 35 & 16 & 31 & 31 \\ 48 & 33 & 32 & 9 & 1 & 29 \end{pmatrix}$$

Also, compute the Hadamard ratio of both basis.