Lattice in Wonderland: An LLL Optimization Problem

Antonio Gonzalez, Fion Huang, Sara Khattab
Junwen Liao, Abdullah Majmundar

University of California, Riverside

October 21, 2019

Definition

Let $n \geq 1$ and let $x_1, x_2, \ldots, x_n$ be a basis of $\mathbb{R}^n$. The lattice with dimension n and basis $x_1, x_2, \ldots, x_n$ is the set L of all linear combinations of the basis vectors with integral coefficients:

$$L = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_1, a_2, \ldots, a_n \in \mathbb{Z} \right\}.$$

Definition

Let $n \geq 1$ and let $x_1, x_2, \ldots, x_n$ be a basis of $\mathbb{R}^n$. The lattice with dimension n and basis $x_1, x_2, \ldots, x_n$ is the set L of all linear combinations of the basis vectors with integral coefficients:

$$L = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_1, a_2, \ldots, a_n \in \mathbb{Z} \right\}.$$

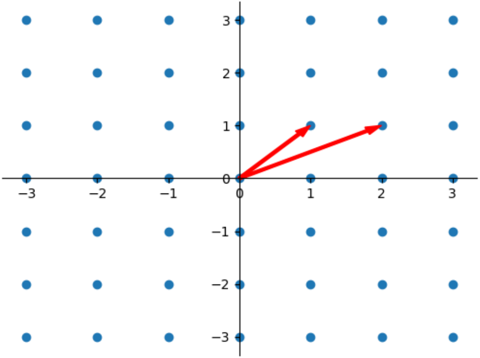
- A single lattice can be represented by more than one basis
- A common problem faced is what is the shortest vector in a given lattice

Shortest Vector Problem

- *Let* $\beta = \{(2,1),(1,1)\}$ and $\mathsf{L} = \mathsf{Span}_{\mathbb{Z}}\ \beta$

Shortest Vector Problem

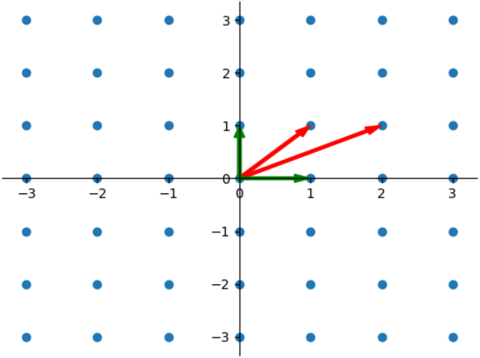
- *Let* $\beta = \{(2,1),(1,1)\}$ and $\mathsf{L} = \mathsf{Span}_{\mathbb{Z}}\ \beta$
- **Question:** What is the shortest vector in this lattice?



Shortest Vector Problem

- *Let* $\beta = \{(2,1),(1,1)\}$ and $\mathsf{L} = \mathsf{Span}_{\mathbb{Z}}\ \beta$
- **Question:** What is the shortest vector in this lattice?

$$(1)(2,1) + (-1)(1,1) = (1,0)$$



Harder Question

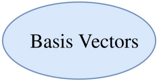
- *Let* $\beta = \{b_1, b_2, ..., b_n\}$ and $\mathsf{L} = \mathrm{Span}_{\mathbb{Z}}\, \beta$
- **Question:** What is the shortest vector in **this** lattice?

Harder Question

- *Let* $\beta = \{b_1, b_2, ..., b_n\}$ and $\mathsf{L} = \mathrm{Span}_{\mathbb{Z}}\, \beta$
- **Question:** What is the shortest vector in **this** lattice?
- **Solution:** LLL Algorithm

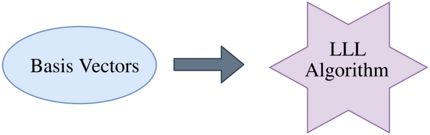
Harder Question

- *Let* $\beta = \{b_1, b_2, ..., b_n\}$ and $\mathsf{L} = \mathrm{Span}_{\mathbb{Z}}\, \beta$
- **Question:** What is the shortest vector in **this** lattice?
- **Solution:** LLL Algorithm



Harder Question

- *Let* $\beta = \{b_1, b_2, ..., b_n\}$ and $\mathsf{L} = \mathrm{Span}_{\mathbb{Z}}\,\beta$
- **Question:** What is the shortest vector in **this** lattice?
- **Solution:** LLL Algorithm



Harder Question

- *Let* $\beta = \{b_1, b_2, ..., b_n\}$ and $\mathrm{L} = \mathrm{Span}_{\mathbb{Z}}\,\beta$
- **Question:** What is the shortest vector in **this** lattice?
- **Solution:** LLL Algorithm

LLL Algorithm

Theorem (1982)

If $x_1, x_2, \ldots, x_n$ is an α-reduced basis of the lattice L in $\mathbb{R}^n$ and $y \in L$ is any nonzero vector, then

$$|\, x_1 \,| \leq \beta^{\frac{n-1}{2}} \,|\, y \,|,\ \beta = \frac{4}{4\alpha - 1}$$

$$\text{brothers} \begin{cases} \text{Arjen Klaas Lenstra} \\ \text{Hendrik Willem Lenstra Jr.} \end{cases}$$
László Lovász

First polynomial time algorithm to factor polynomials with rational coefficients.

Definition

Let $b_1, b_2, \ldots, b_n$ be an ordered basis of the lattice L in R^n, and let $b_1^*, b_2^*, \ldots, b_n^*$ be its Gram-Schmidt orthogonalization.

Definition

Let $b_1, b_2, \ldots, b_n$ be an ordered basis of the lattice L in R^n, and let $b_1^*, b_2^*, \ldots, b_n^*$ be its Gram-Schmidt orthogonalization.
The basis $b_1, b_2, \ldots, b_n$ is called *reduced* if it satisfies

(1) $|\mu_{i,j}| \leq 1/2$, for $1 \leq j < i \leq n$,

(2) $|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq \alpha |b_{i-1}^*|^2$, for $1 < i \leq n$ $\quad (\frac{1}{4} \leq \alpha < 1)$.

Key Question

What is the "best" α?

Does it have a correlation to dimension?

- Different alphas can produce different reduced bases
- We defined the "best" α to be the smallest value that produces the shortest basis vectors
- Larger alphas can be more computationally costly

LLL Algorithm Code

Core functions of LLL:

- Reduce
- Exchange

*based on pseudocode by Murray B. R.

LLL Algorithm Code

Core functions of LLL:

- Reduce
- Exchange

*based on pseudocode by Murray B. R.

Theorem

The total number of passes through Reduce and Exchange is at most

$$-\frac{2\log B}{\log \alpha} n(n-1) + (n-1).$$

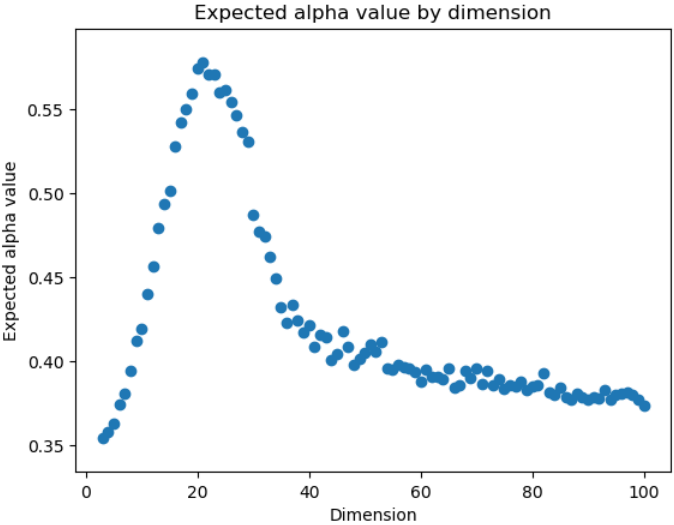
where B is the magnitude of the largest basis vector

LLL Algorithm Code

Program functionality:

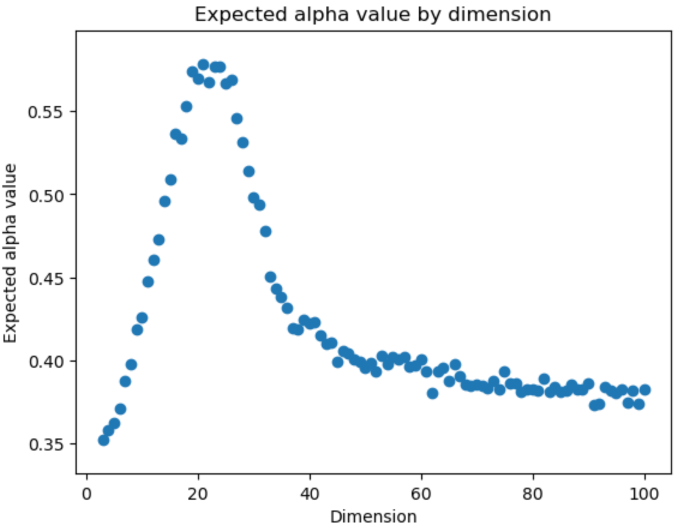
- Generates random lattice bases for a given dimension.
- Runs LLL on each basis in a given dimension using $0.35 \leq \alpha \leq 0.95$ with a step size of 0.05.
- For each basis, the smallest α that produces the reduced basis containing the shortest vector is the best α for that basis.
- Expected α is the average of the best α's for a dimension.

Experimental Observation



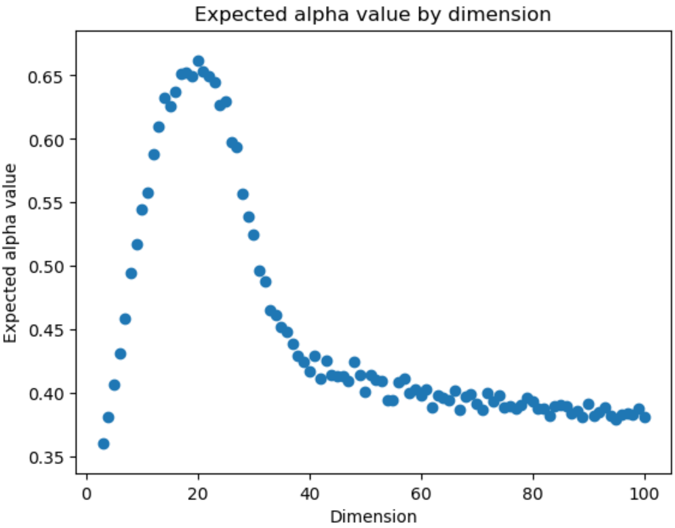
*using integers between [-9, 9]

Experimental Observation



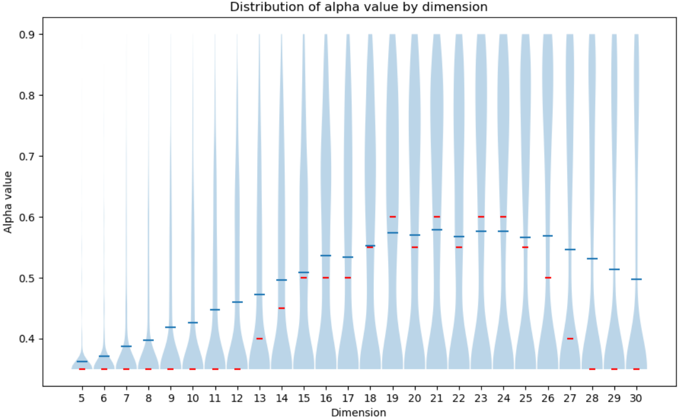
*using integers between [-100,100]

Experimental Observation



*using floats between [-10.0,10.1)

Experimental Observation



Future Work

2 Possible Venues

2 Possible Venues

- α Generation
- Theory

Future Work

α **Generation**

- Create a Machine Learning Model to accurately predict an α value for any given Basis
- Use multiple parameters such as Dimension of the Basis, Average element value, etc.
- Save computational resources when running the LLL - Algorithm

Future Work

Theory

- Why does α peak at $n = 20$?
- Can we prove that as dimension increases to infinity, the best average alpha will stay small?
- Can we prove that the LLL Algorithm terminates in Polynomial time when $\alpha = 1$?

Thank you!

Any Question?

References I

Akhavi A. *Worst-Case Complexity of the Optimal LLL Algorithm*. Lecture Notes in Computer Science, vol 1776. Springer, Berlin, Heidelberg, 2000.

Lenstra A. K., Lenstra H. W., and Lovàsz L. *Factoring Polynomials with Rational Coefficients*. Math. Ann. 261, 515-534, 1982.

Murray B. R., *Lattice Basis Reduction, An Introduction to the LLL Algorithm and its Applications*, CRC Press, 2012.