The LLL Algorithm

Liam Hardiman

May 27, 2019

1 Motivation

2 Setup

Two Lattices

- Recall that the **lattice**, L, generated by the linearly independent vectors $x_1, x_2, \ldots, x_n \in \mathbb{R}^n$ is the $\mathbb{Z}$-span of these vectors:

$$L = \{c_1 x_1 + c_2 x_2 + \cdots + c_n x_n : c_i \in \mathbb{Z}, 1 \leq i \leq n\}.$$

Two Lattices

- Recall that the **lattice**, L, generated by the linearly independent vectors $x_1, x_2, \ldots, x_n \in \mathbb{R}^n$ is the $\mathbb{Z}$-span of these vectors:

$$L = \{c_1x_1 + c_2x_2 + \cdots + c_nx_n : c_i \in \mathbb{Z}, 1 \leq i \leq n\}.$$

- Consider the lattices, L and M, generated by the rows of the matrices X and Y, respectively.

$$X = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}, \quad Y = \begin{bmatrix} -6 & 6 & -4 \\ 9 & 4 & 1 \\ -1 & 8 & 6 \end{bmatrix}.$$

Two Lattices

- Each row of X is an integer linear combination of the rows of Y, so $L \subseteq M$:

Two Lattices

- Each row of X is an integer linear combination of the rows of Y, so $L \subseteq M$:

$$
\begin{bmatrix} -168 \\ 602 \\ 58 \end{bmatrix}^T = 14 \begin{bmatrix} 4 \\ 2 \\ -9 \end{bmatrix}^T + 50 \begin{bmatrix} -1 \\ 8 \\ 6 \end{bmatrix}^T - 29 \begin{bmatrix} 6 \\ -6 \\ 4 \end{bmatrix}^T,
$$

$$
\begin{bmatrix} 157 \\ -564 \\ -57 \end{bmatrix}^T = -13 \begin{bmatrix} 4 \\ 2 \\ -9 \end{bmatrix}^T - 47 \begin{bmatrix} -1 \\ 8 \\ 6 \end{bmatrix}^T + 26 \begin{bmatrix} 6 \\ -6 \\ 4 \end{bmatrix}^T,
$$

$$
\begin{bmatrix} 594 \\ -2134 \\ -219 \end{bmatrix} = -49 \begin{bmatrix} 4 \\ 2 \\ -9 \end{bmatrix}^T - 178 \begin{bmatrix} -1 \\ 8 \\ 6 \end{bmatrix} + 102 \begin{bmatrix} 6 \\ -6 \\ 4 \end{bmatrix}^T.
$$

Two Lattices

- In particular, we have the matrix equation

$$UY = X,$$

$$\begin{bmatrix} 14 & 50 & -29 \\ -13 & -47 & 27 \\ -49 & -178 & 102 \end{bmatrix} \begin{bmatrix} 4 & 2 & -9 \\ -1 & 8 & -6 \\ 6 & -6 & 4 \end{bmatrix} = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}.$$

Two Lattices

- In particular, we have the matrix equation

$$UY = X,$$

$$\begin{bmatrix} 14 & 50 & -29 \\ -13 & -47 & 27 \\ -49 & -178 & 102 \end{bmatrix} \begin{bmatrix} 4 & 2 & -9 \\ -1 & 8 & -6 \\ 6 & -6 & 4 \end{bmatrix} = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}.$$

- $\det U = -1$, so U^{-1} is an integer matrix as well. This gives us another matrix equation, $Y = U^{-1}X$.

Two Lattices

- In particular, we have the matrix equation

$$UY = X,$$

$$\begin{bmatrix} 14 & 50 & -29 \\ -13 & -47 & 27 \\ -49 & -178 & 102 \end{bmatrix} \begin{bmatrix} 4 & 2 & -9 \\ -1 & 8 & -6 \\ 6 & -6 & 4 \end{bmatrix} = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}.$$

- $\det U = -1$, so U^{-1} is an integer matrix as well. This gives us another matrix equation, $Y = U^{-1}X$.
- Since the entries of U^{-1} are integers, this equation expresses the rows of Y as integer linear combinations of the rows of X, so $M \subseteq L$.

Two Lattices

- Even though the rows of X and Y generate the same lattice, something about the Y-basis "feels" nicer.

$$X = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}, \quad Y = \begin{bmatrix} -6 & 6 & -4 \\ 9 & 4 & 1 \\ -1 & 8 & 6 \end{bmatrix}.$$

Two Lattices

- Even though the rows of X and Y generate the same lattice, something about the Y-basis "feels" nicer.

$$X = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}, \quad Y = \begin{bmatrix} -6 & 6 & -4 \\ 9 & 4 & 1 \\ -1 & 8 & 6 \end{bmatrix}.$$

- Two qualities that make a basis desirable are:
  - Length: how long are the basis vectors?
  - Orthogonality: are the basis vectors nearly orthogonal to each other?

What Makes a Basis "Nice"?

- Suppose $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ are pairwise orthogonal.

What Makes a Basis "Nice"?

- Suppose $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ are pairwise orthogonal.
- If $x = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$, $c_i \in \mathbb{Z}$, is in the lattice L generated by $v_1, \ldots, v_n$ then

$$|x|^2 = c_1^2 |v_1|^2 + c_2^2 |v_2|^2 + \cdots + c_n^2 |v_n|^2.$$

What Makes a Basis "Nice"?

- Suppose $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$ are pairwise orthogonal.
- If $x = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$, $c_i \in \mathbb{Z}$, is in the lattice L generated by $v_1, \ldots, v_n$ then

$$|x|^2 = c_1^2 |v_1|^2 + c_2^2 |v_2|^2 + \cdots + c_n^2 |v_n|^2.$$

- This completely solves the shortest vector problem (SVP) since

$$\arg\min_{x \in L} |x| = \arg\min_{x \in \{\pm v_1, \pm v_2, \ldots, \pm v_n\}} |x|.$$

What Makes a Basis "Nice"?

- Say we want to find a vector in L that is closest to

$$x = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n,$$

where the t_i are *real* numbers.

What Makes a Basis "Nice"?

- Say we want to find a vector in L that is closest to

$$x = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n,$$

where the t_i are *real* numbers.

- If $y = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$, $c_i \in \mathbb{Z}$, is any vector in L then by the orthogonality of the v_i we have

$$|x-y|^2 = (t_1 - c_1)^2 |v_1|^2 + (t_2 - c_2)^2 |v_2|^2 + \cdots + (t_n - c_n)^2 |v_n|^2.$$

What Makes a Basis "Nice"?

- Say we want to find a vector in L that is closest to

$$x = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n,$$

where the t_i are *real* numbers.

- If $y = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$, $c_i \in \mathbb{Z}$, is any vector in L then by the orthogonality of the v_i we have

$$|x - y|^2 = (t_1 - c_1)^2 |v_1|^2 + (t_2 - c_2)^2 |v_2|^2 + \cdots + (t_n - c_n)^2 |v_n|^2.$$

- If we take c_i to be the closest integer to t_i then we solve the closest vector problem (CVP).

1 Motivation

2 Setup

How do we Quantify Orthogonality?

$\emptyset$