The LLL Algorithm

1 Motivation

The rows of the following matrix form a basis for a lattice L in $\mathbb{R}^4$:

$$X = \begin{bmatrix} -2 & 7 & 7 & -5 \\ 3 & -2 & 6 & -1 \\ 2 & -8 & -9 & -7 \\ 8 & -9 & 6 & -4 \end{bmatrix}.$$

One can check that the rows of the following matrix also form a basis for the same lattice:

$$Y = \begin{bmatrix} -13071 & -5406 & -9282 & -2303 \\ -20726 & -8571 & -14772 & -3651 \\ -2867 & -1186 & -2043 & -505 \\ -14338 & -5936 & -10216 & -2525 \end{bmatrix}.$$

Intuitively, the rows of Y seem to be a "worse" basis for L than those of X. Here we make precise the notion of a "nice" basis and introduce a polynomial time algorithm that transforms a "bad" basis into a "good" one.

2 Lattices in $\mathbb{R}^n$

Definition 2.1. Let $n \geq 1$ and let $x_1, \ldots, x_n$ be a basis of $\mathbb{R}^n$. The **lattice** with dimension n and basis $x_1, \ldots, x_n$ is the set L of all linear combinations of the basis vectors with integral coefficients:

$$L = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n = \left\{ \sum_{i=1}^{n} a_i x_i : a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

Let X be the matrix whose rows are the basis vectors $x_1, \ldots, x_n$. The **determinant** of the lattice L is

$$\det(L) = |\det(X)|.$$

Lemma 2.1. *Let $x_1, \ldots, x_n$ be a basis for the lattice $L \subset \mathbb{R}^n$ and let $y_1, \ldots, y_n$ be a collection of n vectors in L. Let X and Y be the $n \times n$ matrices with rows $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, respectively. Then $y_1, \ldots, y_n$ is a basis for L if and only if there is an $n \times n$ matrix C with integer entries and $\det(C) = \pm 1$ such that $Y = CX$.*