The LLL Algorithm

1 Motivation

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

$$X = \begin{bmatrix} -168 & 602 & 58 \\ 157 & -564 & -57 \\ 594 & -2134 & -219 \end{bmatrix}.$$

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

$$Y = \begin{bmatrix} -6 & 6 & -4 \\ 9 & 4 & 1 \\ -1 & 8 & 6 \end{bmatrix}.$$

Intuitively, the rows of X seem to be a "worse" basis for L than those of Y. 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 Basis Reduction and the LLL Algorithm

A basis is "nice" if the constituent vectors are short and orthogonal to one another. The Gram-Schmidt process transforms a given basis into an orthogonal basis, but when working in a lattice L, this Gram-Schmidt basis need not live in L.

Definition 2.1. Let $x_1, \ldots, x_n$ be an ordered basis for a lattice L in $\mathbb{R}^n$, and let $x_1^*, \ldots, x_n^*$ be its Gram-Schmidt orthogonalization (GSO). Write $X = MX^*$ where X (respectively X^*) is the matrix with x_i (respectively x_i^*) as row i and $M = (\mu_{ij})$ is the matrix of GSO coefficients. Let α be a real number with $\frac{1}{4} < \alpha < 1$, called the reduction parameter (usually taken to be $\frac{3}{4}$). We say that the basis $x_1, \ldots, x_n$ is **α-reduced** if it satisfies

1. $|\mu_{ij}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$,
2. $|x_i^* + \mu_{i,i-1}x_{i-1}^*|^2 \geq \alpha |x_{i-1}^*|^2$ for $2 \leq i \leq n$.

Condition (1) says that the i-th basis vector is "almost orthogonal" to the span of the previous $i-1$ vectors. The vector $x_i^* + \mu_{i,i-1}x_{i-1}^*$ is the vector one obtains when swapping vectors x_i and x_{i-1} and then computing the $(i-1)$-st vector of the GSO. Condition (2) then says that this new GSO vector, while potentially shorter than x_{i-1}^* isn't "too much" shorter.

Algorithm 1 test

```
if i ≥ maxval then
    i ← 0
else
    if i + k ≤ maxval then
        i ← i + k
    end if
end if
```