The LLL Algorithm

Motivation

The rows of the following matrices form bases for lattices in $\mathbb{R}^3$:

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

The rows of X and the rows of Y actually span the *same* lattice. 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.

Basis Reduction and the LLL Algorithm [1], [2]

A basis is "nice" if its 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 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 $M = (\mu_{ij} = \frac{x_i \cdot x_j^*}{x_j^* \cdot x_j^*})$ is the matrix of GSO coefficients. Let α be a real number with $\frac{1}{4} < \alpha < 1$. We say that the basis $x_1, \ldots, x_n$ is α**-reduced** if it satisfies

(I) (size condition) $|\mu_{ij}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$,

(II) (Lovász condition) $|x_i^*|^2 \geq (\alpha - \mu_{i,i-1}^2)|x_{i-1}^*|^2$ for $2 \leq i \leq n$.

In the Gram-Schmidt process we build x_i^*, the projection of x_i onto $\text{span}(x_1^*, \ldots, x_{i-1}^*)^\perp$, by subtracting each $\mu_{i,j} x_j^*$ from x_i:

$$x_i^* = x_i - \sum_{j=1}^{i-1} \mu_{i,j} x_j^*.$$

Since $\mu_{i,j}$ need not be an integer, this vector generally won't be an element of L. If we instead subtract off the integer multiple of x_j closest to $\mu_{i,j}$ then we stay in L and end up nearly orthogonal to x_j. Condition (I) then says that the closest integer to $\mu_{i,j}$ is zero: x_i is already nearly orthogonal to x_j for each j.

Condition (II) states that while the GSO vectors may get shorter, they do not decrease in length too quickly. In particular, if $\beta = \frac{1}{\alpha - 1/4}$ then repeatedly applying conditions (I) and (II) gives the estimate

$$|x_1| \leq \beta^{(n-1)/2} \min_{1 \leq i \leq n} |x_i^*|.$$

The LLL algorithm, named after its creators, Arjen Lenstra, Hendrik Lenstra Jr., and László Lovász, takes a basis $x_1, \ldots, x_n$ for a lattice $L \subset \mathbb{R}^n$ and returns an α-reduced basis $y_1, \ldots, y_n$ for L. The algorithm, which runs in time polynomial in n and $\log \max(|x_1|, \ldots, |x_n|)$, proceeds as follows.

1. Copy the basis elements $x_1, \ldots, x_n$ into $y_1, \ldots, y_n$.
2. For each vector y_i, $2 \leq i \leq n$ do the following:
   (a) Reduce y_i with the previous basis vectors, y_j, $j < i$: $y_i \leftarrow y_i - \lceil \mu_{ij} \rfloor y_j$.
   (b) If y_i does not satisfy the Lovász condition, then swap y_i and y_{i-1} and return to step 2(a).
3. Return the reduced basis $y_1, \ldots, y_n$.

An Application: Small Roots of Polynomials mod M [3], [4]

Say we want to find a root x_0 of $f(x) \equiv 0 \pmod{M}$ (e.g., where $f(x) = x^e$ and M is an RSA modulus). Our plan is to use the LLL algorithm to construct an *integer* polynomial with small coefficients that also has x_0 as a root. Since approximating roots of polynomials over $\mathbb{Q}$ is easy, this gives us a solution to $f(x) \equiv 0 \pmod{M}$. Importantly, we do not need to know the factorization of M!

Write $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ with $a_i \in \mathbb{Z}$ and consider the matrix

$$B = \begin{bmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & Mx & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & Mx^{d-1} & 0 \\ a_0 & a_1 x & \cdots & a_{d-1}x^{d-1} & a_d x^d \end{bmatrix}.$$

The rows of B, which we identify with polynomials, span a $d+1$ dimensional lattice of polynomials, each having the solution $x = x_0$ modulo M. Running the LLL algorithm on the rows of B will give a reduced basis for this lattice. Let $G(x)$ be the first element in this reduced basis. If x_0 is small enough (as a function of M and d), then $G(x_0) = 0$ over $\mathbb{Z}$.

References

[1] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261 (1982), pp. 515–534.

[2] J. Hoffstein, J. Pipher, and J. Silverman. *An Introduction to Mathematical Cryptography*. Springer-Verlag New York, 2014.

[3] D. Coppersmith. "Finding a small root of a univariate modular equation". In: *Eurocrypt 1996: Advances in Cryptology*. Lecture Notes in Computer Science, 1070. Springer, 1996, pp. 155–165.

[4] S. Galbraith. *Mathematics of Public Key Cryptography*. 2018. URL: `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`.