CS181A 12: Short notes on lattice cryptography

Let $B = \{\vec{u}_i : i \in [m]\}$ be a collection of m linearly independent vectors in $\mathbb{R}^n$. The lattice spanned by these m vectors in B is defined as

$$\mathcal{L}(B) = \{\sum_{i=1}^{m} a_i \vec{u}_i : a_i \in \mathbb{Z}\}.$$

So, $\mathcal{L}(B)$ consists of all integer linear combinations of the vectors in B. The set B is called a **basis** for the lattice $\mathcal{L}$.

Example

The lattice spanned by $|0\rangle$ and $|1\rangle$ is simply the integer grid $\mathbb{Z} \times \mathbb{Z}$. The same lattice is also spanned by $|0\rangle$ and $|0\rangle + |1\rangle$, and also by $|0\rangle$ and $n|0\rangle + |1\rangle$, for any $n \in \mathbb{Z}$. These different bases are represented by

$$B_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, B_3 = \begin{bmatrix} n & n+1 \\ 1 & 1 \end{bmatrix}$$

The vectors of B_0 are orthogonal since $\langle 0|1\rangle = 0$, but the vectors of B_2 and B_3 are nearly parallel. Suppose U is an integer matrix with determinant ± 1:

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad ad - bc = \pm 1.$$

If $B_U = UB_0$ then $\mathcal{L}(B_U) = \mathcal{L}(B_0)$. In fact, if B satisfies $\mathcal{L}(B) = \mathcal{L}(B_0)$, then there is an integer matrix U with $\det U = \pm 1$ so that $B = UB_0$.

Volume

The *fundamental domain* of a lattice $\mathcal{L}$ spanned by the basis $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ is

$$F(\mathcal{L}) = \{\sum_{i=1}^{n} x_i \vec{v}_i : x_i \in [0, 1)\}.$$

The *determinant* of a lattice $\mathcal{L}$ is the volume of its fundamental domain $F(\mathcal{L})$ (viewed as a parallelepiped in $\mathbb{R}^n$). The determinant of $\mathcal{L}$ is simply the determinant of the matrix B whose columns are the basis vectors. An important fact is that $\det(\mathcal{L})$ is an invariant of a lattice (it is basis-independent).

An inequality due to Hadamard states that

$$\det(\mathcal{L}) \leq \prod_{i=1}^{n} ||\vec{v}_i||.$$

The ratio of the determinant $\det(\mathcal{L})$ and the product $\prod_i ||\vec{v}_i||$ measures how close is the basis B to being orthogonal; that is, equality is achieved in the above if the basis is orthogonal.

Hard Problems

We describe two intractable problems associated with lattices.

> **Shortest Vector Problem** (SVP)
> Given a lattice $\mathcal{L}$ spanned by a basis B, find the shortest lattice vector $\vec{u} \in \mathcal{L}$ that satisfies
>
> $$\vec{u} = \text{argmin}\{||\vec{v}|| : \vec{v} \in \mathcal{L}\}.$$

> **Closest Vector Problem** (CVP)
> Given a lattice $\mathcal{L}$ spanned by a basis B and a real vector $\vec{x} \in \mathbb{R}^n$, find the closest lattice vector $\vec{u} \in \mathcal{L}$ to $\vec{x}$ that satisfies
>
> $$\vec{u} = \text{argmin}\{||\vec{v} - \vec{x}|| : \vec{v} \in \mathcal{L}\}.$$

The above problems are tractable if the lattice has an orthogonal basis. To see this, note if $\vec{v} \in \mathcal{L}$ and $\vec{v} = \sum_{i=1}^{n} a_i \vec{v}_i$, then

$$||\vec{v}||^2 = \sum_{i=1}^{n} a_i^2 ||\vec{v}_i||^2.$$

The following natural algorithm for CVP is due to Babai:

1. Write $\vec{x} = \sum_{i=1}^{n} x_i \vec{v}_i$, where $x_i \in \mathbb{R}$.
2. Define $a_i = \lfloor x_i \rceil$, for each i. So a_i is the nearest integer to x_i.
3. Return the lattice vector $\vec{a} = \sum_{i=1}^{n} a_i \vec{v}_i$.

GGH cryptosystem

The following lattice-based system is due to Goldreich, Goldwasser and Halevi.

Alice selects n linearly independent vectors $\vec{v}_1, \ldots, \vec{v}_n \in \mathbb{Z}^n$. She can use Hadamard's inequality to guide her choice so that the basis is nearly orthogonal. For example, Alice can select random vectors $\vec{v}$ with entries from $\{0, \pm 1, \ldots, \pm d\}$ for some fixed integer $d \geq 1$. This set of vectors will be Alice's secret key which is a good basis for $\mathcal{L}$. So, let

$$B_0 = \begin{bmatrix} \vec{v}_1 & \ldots & \vec{v}_n \end{bmatrix}.$$

Next, Alice builds her public key which is a bad basis for $\mathcal{L}$. She selects a random integer matrix $U \in \mathrm{GL}(\mathbb{Z})$ (say, as a product of random elementary matrices) and let

$$B_1 = UB_0.$$

To send a message $\vec{m}$ to Alice, Bob also selects a random perturbation vector $\vec{r}$ (say, whose entries are from $[-\delta, +\delta]$, for some predetermined δ). The ciphertext that Bob sends to Alice is

$$\vec{c} = B_1\vec{m} + \vec{r}.$$

So, $\vec{c}$ is not in $\mathcal{L}$, but it is close to a lattice vector if $\vec{r}$ is small.

Alice decrypts the ciphertext $\vec{c}$ by using her good basis B_0. For example, she can use Babai's algorithm to recover the nearest lattice point.