MATH 408 Project Proposal

Ben Young

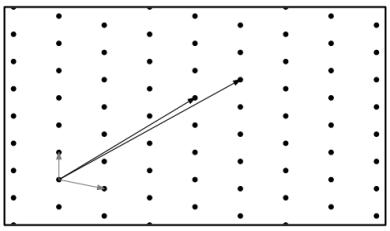
February 24, 2020

For my project I plan to undertake a general exploration of lattice-based cryptography: the math behind it and its applications, especially regarding its potential resistance to quantum-based attacks. I also hope to implement an algorithm to solve a common lattice problem, such as the shortest vector problem.

A *lattice* is essentially the set of all linear combinations of a given set vectors with linear coefficients. More formally, if $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^n$ are n linearly independent basis vectors we can define a lattice $\mathcal{L}$ as

$$\mathcal{L}(\mathbf{b}_1, \cdots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$ [1]

Figure 1: An example of a 2-dimensional lattice with basis vectors [1]



One common lattice-related problem is to find the length of the shortest vector that can be created from the basis. This is the *shortest vector problem*. As with most lattice problems, algorithms aim to find an approximation of the solution within a factor of the actual length of the shortest vector. Several algorithms exist, although none have both polynomial runtime and approximation factor. The *LLL algorithm* runs in polynomial time but achieves only a $O(2^n)$ approximation factor. Every known algorithm that finds an exact solution or a polynomial approximation has running time $O(2^n)$. Furthermore, it is conjectured that there exists no polynomial time algorithm (quantum or classical) that can approximate the shortest vector problem or other lattice problems to within a polynomial factor. Other problems include the *closest vector problem*, which asks for the closest lattice point to a target non-lattice vector, and the *shortest independent vectors problem*, which asks for the set of linearly independent lattice vectors with the smallest maximum length.[1]

The hardness of lattice problems and their resistance to quantum attacks have led to several proposed cryptosystems, although most are too inefficient to be used in practice. One such cryptosystem is the GGH cryptosystem. Public and private keys are two different bases for the same lattice. The public key is a 'good' basis which allows for effeciently solving some cases of the closest vector problem. The public key is a 'bad' basis which is much less efficient for solving the same problem. A different approach is the *learning with errors* (LWE) cryptosystem. The system is based on the lattice problem with the same name. Given a basis for a random lattice and a vector $\mathbf{v} \in \mathbb{Z}_q^m$ (m-length vectors mod q), decide whether $\mathbf{v}$ is chosen randomly and uniformly from $\mathbb{Z}_q^m$ or if it was chosen by randomly perturbing the coordinates of a point in the lattice.[1]

[1] D. Micciancio and O. Regev. "Lattice-based Cryptography". 22 July 2008. cims.nyu.edu/∼ regev/papers/pqc.pdf