COS 533: Advanced Cryptography — Princeton University
Lecture 8 (February 25, 2021)
Lecturer: Mark Zhandry — Scribe: Sacheth Sathyanarayanan

Notes for Lecture 8

1 Introduction

In this lecture, we will continue talking about various algebraic tools that are used in cryptography. In particular, we will talk about lattices, discuss hard problems on lattices and describe why they are useful.

2 Lattices

A lattice is, informally, a regular grid of points in Euclidean space. We usually think of lattices as being high dimensional objects (with dimension greater than 2). Here are two definitions of lattices:

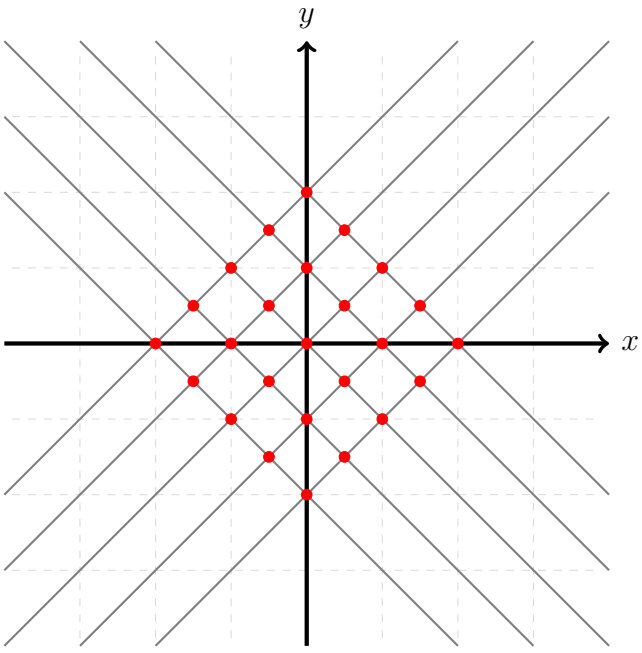


Figure 1: A lattice

1. A discrete (the points aren't too close together) subgroup of $\mathbb{R}^n$

   Note that a regular set of points is indeed a subgroup as long as the origin is a member of the regular set of points.

2. The set of integer linear combinations of a linearly independent basis

   Consider a basis $\mathcal{B} = \{\vec{b_1}, \vec{b_2}, \ldots, \vec{b_{n'}}\}$. The lattice for this basis is $L(\mathcal{B}) = \{\sum_{i=1}^{n'} x_i \vec{b_i} : x_i \in \mathbb{Z}\}$. We usually consider full rank bases i.e. with $n' = n$. If the x_i here were, instead real, then these combinations would just be some vector subspace of $\mathbb{R}^n$.

The two definitions above are equivalent; in fact, one direction is easy to show. The set of integer linear combinations of any set of vectors is always a subgroup of $\mathbb{R}^n$. We need the vectors to be linearly independent to ensure that the points are discrete. If the vectors have linear dependence, we may end up with a non-discrete set of points.

Non-example For $n = 1$, set $\mathcal{B} = \{1, \sqrt{2}\}$. All integer combinations of 1 and $\sqrt{2}$ are not discrete. In particular, based on any rational approximation of $\sqrt{2}$, we could get arbitrarily close to it but never hit it. We can use this to get integer combinations that get arbitrarily close to 0 without ever hitting it.

Examples of Lattices

1. $\mathcal{B} = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$

   The lattice for this basis is $L(\mathcal{B}) = \mathbb{Z}^2$, the set of all points with integer coordinates.

2. $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$

   Here, again, $L(\mathcal{B}) = \mathbb{Z}^2$. To see why notice that $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ are in this lattice $L(\mathcal{B})$. Consequently, the lattice generated by them is also in $L(\mathcal{B})$. We can also show that all the vectors in $\mathcal{B}$ are spanned by the two vectors $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

   Key Takeaway: Different bases can generate the same lattice.

3. $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$

Note that this is a sublattice of the prior two lattices since the points are all integer coordinates. However, it does not contain all integer points — for instance, it does not contain $\begin{pmatrix}0\\1\end{pmatrix}$ since the only way to do this is to have a (signed) half contribution from each, which is not an integer combination.

3 Generating the Same Lattice

In this section, we characterize when two bases generate the same lattice.

Recall Two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ generate the same vector space if and only if there exists some invertible matrix U such that $\mathcal{B}_1 = \mathcal{B}_2 U$. This is because the vectors in $\mathcal{B}_1$ can now be expressed as a real-coefficient linear combination of the vectors in $\mathcal{B}_2$ and vice-versa.

Analogy for Lattices

Definition 1 *A matrix $U \in \mathbb{Z}^{n\times n}$ is unimodular if det$(U) = \pm 1$.*

Theorem 2 *If U is unimodular, then U^{-1} exists and is unimodular. Note that the inverse is defined over $\mathbb{R}^{n\times n}$ though the entries are all integers.*

First, we see that U is invertible since $\det(U) \neq 0$. Recall that $U^{-1} = \frac{1}{\det(U)}\text{adj}(U)$. Since $\text{adj}(U)$ is obtained by taking determinants of submatrices, each of which are integer coefficient polynomials, it has integer entries. This combined with the fact that $\det(U) = \pm 1$ tells us that U^{-1} has integer entries. Since $\det(U^{-1}) = \frac{1}{\det(U)} = \pm 1$, we have that U^{-1} is unimodular.

> Question: Is the unimodular condition sufficient and necessary?
> Are there any other integer matrices that have integer inverses?

Yes, it is sufficient and necessary. Since $\det(U^{-1}) = \frac{1}{\det(U)}$ and the determinants are integers, we must have that $\det(U) = \pm 1$.

Theorem 3 *If $\mathcal{B}_1, \mathcal{B}_2 \in \mathbb{R}^{n\times n}$ are full rank then $L(\mathcal{B}_1) = L(\mathcal{B}_2)$ if and only if there exists some unimodular matrix U such that $\mathcal{B}_2 = \mathcal{B}_1 U$.*

$\implies$ If $L(\mathcal{B}_1) = L(\mathcal{B}_2)$ and $\mathcal{B}_2 = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}$ then b_i must lie in $L(\mathcal{B}_1)$. Thus, there must exist some integer matrix U such that $\mathcal{B}_2 = \mathcal{B}_1 U$ since the columns of $\mathcal{B}_2$ are linear combinations of the columns of $\mathcal{B}_1$. By the same argument as above, there exists some integer matrix U' such that $\mathcal{B}_1 = \mathcal{B}_2 U'$. Combining these two equations, we have $\mathcal{B}_2 = \mathcal{B}_2 U' U$. Using the fact that $\mathcal{B}_2$ is full rank, we have that $U'U = I$. Since these two matrices have integer determinants that multiply to 1, we have that $\det(U) = \pm 1$, which tells us that it is unimodular.

$\impliedby$ Suppose $y \in L(\mathcal{B}_2)$. This tells us that there exists some integer vector x such that $y = \mathcal{B}_2 x = \mathcal{B}_1 U x$. Since U is unimodular, Ux has integer entries. Thus, y also lies in $L(\mathcal{B}_1)$ and so $L(\mathcal{B}_2) \subseteq L(\mathcal{B}_1)$. An identical argument (using the fact that U^{-1} is unimodular) shows that $L(\mathcal{B}_1) \subseteq L(\mathcal{B}_2)$ and we are done.

4 Hard Problems on Lattices

Definition 4 *(Shortest Vector Problem (SVP)). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$, find $x \in \mathbb{Z}^n$ such that*

1. *$x \in L(\mathcal{B}) \backslash \{0\}$*
2. *$|x|_2$ is minimized, where $|x|_2$ is the L_2 norm of x*

The shortest vector need not be unique. In fact, if x is a shortest vector, so is $-x$. As another example, for the basis $\mathbb{Z}^n$, all standard bases and their negations will be shortest vectors.

Question: Is the L_2 norm special here or are all norms equivalently hard?

The various $p-$norms are more or less equivalent. We will use a relaxation that is the approximate SVP that tolerates some amount of error. All L_p norms are related by some multiplicative factors and those factors will be absorbed into the approximation. At least for the approximate version the different L_p norms are equivalent. For the exact version they are *believed* to be equivalently hard.

Note All lattices we deal with will have integer coordinates. Though real coordinates are technically allowed, we will not deal with them since we need finite sized inputs. We could have rational inputs, but this is equivalent to the integer case since we can multiply by the lowest common denominator.

Definition 5 *(Closest Vector Problem (CVP)). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$ and a target vector $t \in \mathbb{Z}^n$ find $x \in \mathbb{Z}^n$ such that*

1. $x \in L(\mathcal{B})$
2. $|x - t|_2$ *is minimized*

Unfortunately, we don't know how to build crypto from either of these problems. Thus, we define approximate versions of them.

Definition 6 *(SVP_γ). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$, find $x \in \mathbb{Z}^n$ such that*

1. $x \in L(\mathcal{B}) \backslash \{0\}$
2. $|x|_2 \leq \gamma \lambda_1(\mathcal{B})$

where $\lambda_1(\mathcal{B})$ is the length of the shortest vector.

Definition 7 *(CVP_γ). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$ and a target vector $t \in \mathbb{Z}^n$ find $x \in \mathbb{Z}^n$ such that*

1. $x \in L(\mathcal{B})$
2. $|x - t|_2 \leq \gamma dist(L(\mathcal{B}), t)$

where $dist(L(\mathcal{B}), t)$ is the actual shortest distance between the lattice and t.

The following definitions are decisional variants of the approximate versions:

Definition 8 *(GAP SVP_γ). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$ and a real number $s > 0$, decide whether $\lambda_1(\mathcal{B}) \leq s$ or $\lambda_1(\mathcal{B}) \geq \gamma s$ where $\lambda_1(\mathcal{B})$is the length of the shortest vector.*

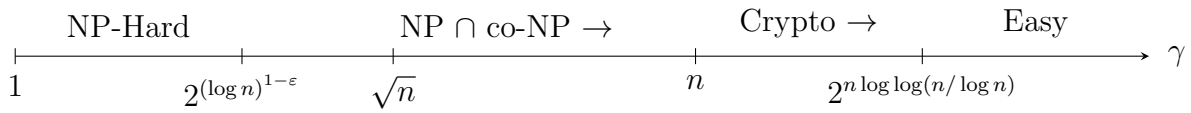
Definition 9 *(GAP CVP_γ). Given a basis $\mathcal{B} \in \mathbb{Z}^{n \times n}$, target vector $t \in \mathbb{Z}^n$ and a real $s > 0$, decide whether $dist(L(\mathcal{B}), t) \leq s$ or $dist(L(\mathcal{B}), t) \geq \gamma s$ where $dist(L(\mathcal{B}), t)$ is the actual shortest distance between the lattice and t.*

5 Complexity Landscape for Gap_γ

We analyze the complexity of Gap_γ as a function of γ. As we increase γ, eventually (for $\gamma > 2^{n \log \log(n/\log n)}$) the problem becomes easy. On the other hand, if $\gamma < 2^{(\log n)^{1-\varepsilon}}$ for $\varepsilon < 0$ (i.e. sub-polynomial in n), the problem is NP-Hard.[1] A complexity result

[1]Note that these problems aren't necessarily in NP since, for the SVP problem, when we get a vector of size s and a lattice, we know that there is a vector of length at most s, but not that it is the minimal vector.

states that once $\gamma > \sqrt{n}$, tthe problem is in NP $\cap$ co-NP. Crypto comes in when $\gamma > n$.



6 Why are Lattices Useful?

In this section, we will give a sketch of lattice-base signatures. Though we will do things a little differently later, here is a little intuition:

Intuition Suppose we have a CVP_γ instance $\mathcal{B}, t$. We can do something called "lattice rounding." If our lattice was all the integers, then solving the closest vector problem is easy — we can just round the coefficients of our target vector to the nearest integer and we are done.

In a more general lattice, we round the coefficients of the target vector so that it is still close to t but now lies in the lattice. To do this, we compute $z = \mathcal{B}^{-1}t$. If $t \in L(\mathbb{B})$, then this is equivalent to $z \in \mathbb{Z}^n$. Thus, if z is all integers we know that t is in the lattice and it is the closest vector.

If $z \notin \mathbb{Z}^n$, we round each coordinate of z to the nearest integer to get $v = \lceil z \rfloor \in \mathbb{Z}^n$. We now output $\mathcal{B}v \in L(\mathcal{B})$. The difference between this and our target vector is

$$\begin{aligned} |\mathcal{B}v - t| &= |\mathcal{B}\lceil \mathcal{B}^{-1}t \rfloor - t|_2 \\ &= |\mathcal{B}\lceil \mathcal{B}^{-1}t \rfloor - \mathcal{B}\mathcal{B}^{-1}t|_2 \\ &= |\mathcal{B}\left(\lceil \mathcal{B}^{-1}t \rfloor - \mathcal{B}^{-1}t\right)|_2 \end{aligned}$$

Each entry in $(\lceil \mathcal{B}^{-1}t \rfloor - \mathcal{B}^{-1}t)$ is between $-1/2$ and $1/2$. Thus the norm of this difference vector is $\mathcal{O}(\sqrt{n})$. Suppose the entries of $\mathcal{B}$ are bounded by δ. Then, $|\mathcal{B}v - t|_2 \leq \mathcal{O}(n^{1.5}\delta)$. [2] Thus having a short basis lets us solve CVP_γ. On the flip side, having a long basis prevents us from solving CVP_γ.

Signature Scheme from Lattices

- Set sk = short basis and pk = long basis. [3]

[2] Since $\mathcal{B}$ is an $n \times n$ matrix, the size of product with a vector can only grow by a factor of n corresponding to the size of the matrix. We get another factor of δ corresponding to the entries of the matrix. We get the $\sqrt{n}$ from the norm of our original vector.

[3] We generate our short basis by sampling random short vectors and hoping they're linearly independent. We can get our long basis by multiplying with a random unimodular matrix.

- $\text{sign}(\mathsf{sk}, m) : H(m) \to \mathbb{Z}^n$ for some hash function H. The signature is a CVP_γ solution σ such that $|\sigma - H(m)|_2$ is small.
- To verify, check whether $\sigma \in L(\mathcal{B})$ and check the norm $|\sigma - H(m)|_2$

Why do we like lattices?

- It is an alternate hard problem with conjectured post-quantum resistance
- The verification is super fast (simple linear algebra). The downside here is that though it is very fast, the parameters are large
- They provide additional functionalities such as fully homomorphic encryption.[4]

[4]Computing on encrypted data.