Mastermath, Spring 2018 | **Lecturers: D. Dadush, L. Ducas**
Intro to Lattice Algs & Crypto | **Scribe: K. de Boer**

Lecture 3

20/02/18

1 Introduction

In this part of the lecture notes, three topics are treated. First we will look at a concrete application of Minkowski's convex body theorem: the two-squares theorem. Second, we treat projected lattices and the related Gram-Schmidt orthogonalization procedure. We will also consider the so-called Babai fundamental domain. The third and last subject we will cover is the Lagrange reduction algorithm, which finds a short basis for a given two-dimensional lattice. We will consider the running time and correctness of this algorithm rigorously.

2 The two-squares theorem

The two-squares theorem is a number-theoretic result which can be proven fairly elegant by means of lattice theory.

Theorem 1 *Any prime $p \equiv 1$ modulo 4 can be written as the sum of two squares. That is, $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.*

Proof: The group of units $(\mathbb{Z}/p\mathbb{Z})^*$ of the integers mod p has order $p-1$. We have $4 \mid p-1$, and therefore there must exist a primitive fourth root of unity $i \in \mathbb{Z}/p\mathbb{Z}$, i.e., an element i such that $i^4 \equiv 1 \bmod p$ and $i^2 \equiv -1 \bmod p$.

Now, construct the following lattice $\Lambda = \{(x,y) \in \mathbb{Z}^2 \mid x + iy \equiv 0 \bmod p\}$. As it is a additive subgroup of $\mathbb{Z}^2$, it is indeed a lattice.

- Note that the determinant equals p, which follows from the following observation. The lattice Λ equals $\ker(\phi)$, where $\phi : \mathbb{Z}^2 \to \mathbb{Z}/p\mathbb{Z}$ sends $(x,y) \mapsto x + iy \bmod p$ surjectively. Applying an exercise of last week, yields

$$\det(\Lambda) = \det(\ker\phi) = \frac{\det(\ker\phi)}{\det(\mathbb{Z}^2)} = [\mathbb{Z}^2 : \ker\phi] = |\mathbb{Z}^2/\ker\phi| = |\mathrm{im}(\phi)| = p.$$

- For all $\mathbf{v} \in \Lambda$ we have $p \mid \|\mathbf{v}\|^2$. This follows from $\|\mathbf{v}\|^2 = x^2 + y^2 \equiv (x+iy)(x-iy) \equiv 0 \bmod p$, where $\mathbf{v} = (x,y) \in \Lambda$. This holds because $x + iy \equiv 0 \bmod p$ in Λ.
- From Minkowski's convex body theorem one can conclude that $\lambda_1(\Lambda) < \sqrt{2p}$, because $\mathrm{Vol}(\sqrt{2p} \cdot B_2^2) = 2\pi p > 4p = 2^2 \det(\Lambda)$.

Summarizing, there exists a non-zero vector $\mathbf{v} \in \Lambda$ with $\|\mathbf{v}\|^2 < 2p$ and $p \mid \|\mathbf{v}\|^2$. This necessarily implies that this vector has square norm p, i.e., there exists a non-zero vector $\mathbf{v} \in \Lambda$ with $x^2 + y^2 = \|\mathbf{v}\|^2 = p$. $\square$

3 Projected lattices

3.1 Projections and orthogonal complements

Let V be a finite dimensional vector space and $W \subseteq V$ a linear subspace. Then we can define a projection map $\pi_W : V \to W \subseteq V$, as follows. As any basis $(\mathbf{w}_1, \ldots, \mathbf{w}_k)$ of W can be extended to a basis $(\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{v}_1, \ldots, \mathbf{v}_n)$ of V we can let the map π_W act like this:

$$\pi_W \left(\sum_{i=1}^{k} \lambda_i \mathbf{w}_i + \sum_{i=1}^{n} \nu_i \mathbf{v}_i \right) = \sum_{i=1}^{k} \lambda_i \mathbf{w}_i$$

For any $W \subseteq V$ a linear subspace of V, we can define the orthogonal complement $W^\perp$ of W:

$$W^\perp = \{\mathbf{v} \in V \mid \langle \mathbf{v}, \mathbf{w} \rangle = 0 \text{ for all } \mathbf{w} \in W\}$$

When a basis $(\mathbf{w}_1, \ldots, \mathbf{w}_k)$ of W is given, the space $W^\perp$ is sometimes written as $(\mathbf{w}_1, \ldots, \mathbf{w}_k)^\perp$.

3.2 Gram-Schmidt orthogonalization

For the remainder of this section, we fix a basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of the lattice Λ. We define the Gram-Schmidt orthogonalization $\widetilde{\mathbf{B}} = (\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n)$ of $\mathbf{B}$ as follows: $\widetilde{\mathbf{b}}_i = \pi_i(\mathbf{b}_i)$, where $\pi_i = \pi_{(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp}$. In other words, the projection map π_i projects to the orthogonal complement of the space generated by $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$. In a more informal way, this means that $\pi_i(\mathbf{b}_i)$ is $\mathbf{b}_i$ 'orthogonalized against' $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$.

A different way of defining the Gram-Schmidt orthogonalization is by means of matrix decomposition; $\mathbf{B}$ is decomposed as a matrix product $\widetilde{\mathbf{B}} \cdot \mu$, where $\widetilde{\mathbf{B}}$ is orthogonal and μ is upper triangular with ones on the diagonal. One can compute μ and $\widetilde{\mathbf{B}}$ inductively by the following formulae:

$$\mu_{ij} = \frac{\langle \widetilde{\mathbf{b}}_i, \mathbf{b}_j \rangle}{\langle \widetilde{\mathbf{b}}_i, \widetilde{\mathbf{b}}_i \rangle}$$

$$\widetilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \widetilde{\mathbf{b}}_j$$

Lemma 2 $|\det \mathbf{B}| = |\det \widetilde{\mathbf{B}}| = \prod_{i=1}^{n} \|\widetilde{\mathbf{b}}_i\|$

Proof: Since the determinant is a multiplicative map, we have $|\det(\mathbf{B})| = |\det(\widetilde{\mathbf{B}}\mu)| = |\det(\widetilde{\mathbf{B}})\det(\mu)| = |\det(\widetilde{\mathbf{B}})|$, by the fact that μ is upper triangular and has ones on the diagonal. The second equality follows from the fact that $|\det(\widetilde{\mathbf{B}})|$ is known to be volume of the parallelepiped 'generated' by the columns of $\widetilde{\mathbf{B}}$. In the case of $\widetilde{\mathbf{B}}$, the columns are orthogonal, and therefore the parallelepiped generated by $\widetilde{\mathbf{B}}$ is a parallelepiped with sides of length $\|\widetilde{\mathbf{b}}_i\|$. □

Using the maps π_i, we can define the projected lattices Λ_i of Λ. We define:

$$\Lambda_i = \pi_i(\Lambda) \subseteq (\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$$

Exercise 1 Let Λ be a full-rank lattice in V with basis $\mathbf{B}$. Prove that $\Lambda_i = \pi_i(\Lambda)$ is indeed a lattice. More specifically, show that it is a full dimensional lattice in $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$ with basis $(\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n))$.

Exercise 2 Show that, for an arbitrary subspace $W \subseteq V$, $\pi_W(\Lambda)$ doesn't need to be a lattice [Hint: Examples can be as small as dimension 2].

3.3 Babai's fundamental domain

Given a basis $\mathbf{B}$ of the lattice Λ, and let $\widetilde{\mathbf{B}}$ be its Gram-Schmidt orthogonalization. Then we define Babai's fundamental domain as the parallelepiped $\mathcal{P}(\widetilde{\mathbf{B}}) = \widetilde{\mathbf{B}}[0,1)^n$. We didn't yet prove that this is indeed a fundamental domain, for which we need the following lemma.

Lemma 3 *Let $\Lambda = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ a lattice, and let $\Lambda_2 = \pi_2(\Lambda) = \pi_{\mathbf{b}_1^\perp}(\Lambda)$. Then:*

$$\mathcal{F}_2 \text{ is a fundamental domain for } \Lambda_2$$

$$\implies \mathcal{F}_2 + [0,1)\mathbf{b}_1 \text{ is a fundamental domain for } \Lambda$$

Proof: As we leave it to the reader to prove that $\mathcal{F}$ is packing, we will only prove here that $\mathcal{F} = \mathcal{F}_2 + [0,1)\mathbf{b}_1$ is covering. Take an arbitrary $\mathbf{v} \in V = \operatorname{span}(\Lambda)$. Our aim is to show that $\mathbf{v} - \ell \in \mathcal{F}_2 + [0,1)\mathbf{b}_1$ for some $\ell \in \Lambda$.

Compute $\mathbf{v}_2 = \pi_2(\mathbf{v}) \in \Lambda_2$, the projected lattice. As $\mathcal{F}_2$ is a fundamental domain for Λ_2, we can find $\ell_2 \in \Lambda_2$ and $f_2 \in \mathcal{F}_2$ such that $\mathbf{v}_2 = \ell_2 + f_2$. Since $\ell_2 \in \Lambda_2 = \pi_2(\Lambda)$, we can find an $\ell \in \Lambda$ such that $\pi_2(\ell) = \ell_2$. Note that both $\ell_2 - \ell =: \ell_{\mathbf{b}_1}$ and $v - v_2 =: v_{\mathbf{b}_1}$ are in $\operatorname{Span}(\mathbf{b}_1)$.

Rewriting the terms:

$$v = v_2 + (v - v_2) = v_2 + v_{\mathbf{b}_1} = f_2 + \ell_2 + v_{\mathbf{b}_1} = f_2 + \ell + (\ell_2 - \ell) + v_{\mathbf{b}_1}$$

$$= f_2 + \ell + \underbrace{\ell_{\mathbf{b}_1} + v_{\mathbf{b}_1}}_{\in \text{ Span}(\mathbf{b}_1)} = f_2 + \ell + x\mathbf{b}_1 + k\mathbf{b}_1 = \underbrace{f_2 + x\mathbf{b}_1}_{\in \mathcal{F}_2 + [0,1)\mathbf{b}_1} + \underbrace{\ell + k\mathbf{b}_1}_{\in \Lambda}$$

□

Exercise 3 Prove that, in the context of the above lemma, $\mathcal{F}_2 + [0,1)\mathbf{b}_1$ is packing.

Lemma 4 *Babai's fundamental domain $\mathcal{P}(\widetilde{\mathbf{B}})$ is indeed a fundamental domain for $\Lambda = \mathcal{L}(\mathbf{B})$.*

Proof: This is a proof by induction on dimension. Note that for dimension 1, $\widetilde{\mathbf{B}} = \mathbf{B}$, which means $\mathcal{P}(\widetilde{\mathbf{B}}) = \mathcal{P}(\mathbf{B})$.

For dimension n bigger than one, we can proceed as follows. Given a lattice Λ with basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Take $\mathbf{C} = (\pi_2(\mathbf{b}_2), \ldots, \pi_2(\mathbf{b}_n))$, which is a basis for $\Lambda_2 = \pi_2(\Lambda)$. Since Λ_2 has lower dimension, we can apply the induction hypothesis, i.e., $\mathcal{P}(\widetilde{\mathbf{C}})$ is a fundamental domain for Λ_2. By the previous lemma, $[0,1)\mathbf{b}_1 + \mathcal{P}(\widetilde{\mathbf{C}})$ is a fundamental domain for Λ.

But, one can show that $\widetilde{\mathbf{B}} = (\mathbf{b}_1 | \widetilde{\mathbf{C}})$, that is, $\widetilde{\mathbf{b}}_i = \widetilde{\mathbf{c}}_i$ for $i > 1$. Therefore $[0,1)\mathbf{b}_1 + \mathcal{P}(\widetilde{\mathbf{C}}) = \mathcal{P}(\widetilde{\mathbf{B}})$, which proves the claim. □

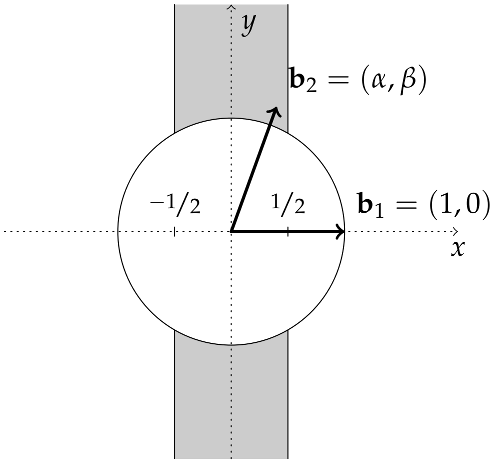

Figure 1: A picture of the wristwatch lemma. The lattice is scaled and rotated such that $\mathbf{b}_1 = (1, 0)$ is of unit length and lies on the x-axis. The second basis vector $\mathbf{b}_2$ must then be in the gray area.

4 Lagrange Reduction Algorithm

In this section, we will explain an algorithm that finds a basis of a two-dimensional lattice consisting of vectors that attain the respective successive minima. Thus, the Lagrange reduction algorithm finds a shortest basis of a two-dimensional lattice.

Theorem 5 (Wristwatch lemma) *Let Λ be a 2-dimensional lattice. Then there exists a basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$ such that*

- $\mathbf{b}_1$ *is a shortest vector of* Λ.
- $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle| \leq \frac{1}{2}\|\mathbf{b}_1\|^2$.

Algorithm 1: Lagrange reduction algorithm

```
Input  : A basis $(\mathbf{b}_1, \mathbf{b}_2)$ of a lattice $\Lambda$.
Output: A basis $(\mathbf{b}_1, \mathbf{b}_2)$ as in the Wristwatch lemma.
repeat
    swap $\mathbf{b}_1 \leftrightarrow \mathbf{b}_2$
    $k \leftarrow \lceil \frac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\|\mathbf{b}_1\|^2} \rfloor$
    $\mathbf{b}_2 \leftarrow \mathbf{b}_2 - k\mathbf{b}_1$
until $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
```

The proof of this theorem is 'by algorithm', which means that we give an algorithm that, given any basis, computes such shortest basis as in the Wristwatch lemma. The proof then consists of showing that the algorithm terminates, and after termination indeed gives the required basis.
Proof:[Proof (of Wristwatch lemma)] We will now show that the output of Algorithm 1 indeed is as in Theorem 5.

- Algorithm 1 terminates. This can be seen by the fact that $\|\mathbf{b}_1\|$ diminishes every iteration in the repeat-loop. As Λ has a minimum non-zero length, and $\mathbf{b}_1$ and $\mathbf{b}_2$ are linear independent, this necessarily means that the algorithm should terminate.

- The resulting $\mathbf{b}_1, \mathbf{b}_2$ indeed form a basis of the lattice Λ. This can be seen by the fact that every operation in the loop (swap, row-addition) is a unimodular transformation on the basis, i.e., multiplication by a matrix in $\mathrm{GL}_2(\mathbb{Z})$. The resulting pair of vectors must then be a basis, too.

- We indeed have $\langle \mathbf{b}_1, \mathbf{b}_2 \rangle \leq \frac{1}{2}\|\mathbf{b}_1\|^2$. To prove this, we assume, without loss of generality (after scaling and rotating) that $\mathbf{b}_1 = (0, 1)$. Write $\mathbf{b}_2 = (\alpha, \beta)$. Then in the last iteration of the algorithm (omitting the swap), we essentially forced that $|\beta| \leq 1/2$. As $\langle \mathbf{b}_1, \mathbf{b}_2 \rangle = \beta$, this proves our claim.

- $\mathbf{b}_1$ is the shortest (non-zero) lattice vector of Λ. As any vector in Λ can be written as $\ell = m\mathbf{b}_1 + n\mathbf{b}_2$ with $m, n \in \mathbb{Z}$, our aim is to prove that $\|\ell\| = \|m\mathbf{b}_1 + n\mathbf{b}_2\| \geq \|\mathbf{b}_1\|$. Again, we write $\mathbf{b}_1 = (0, 1)$ and $\mathbf{b}_2 = (\alpha, \beta)$.

  For $n = 0$, this is clearly true, as then then $\ell = m\mathbf{b}_1$ is a multiple of $\mathbf{b}_1$, which is always at least as long as $\mathbf{b}_1$ itself. The same holds for $m = 0$. For $n, m \neq 0$, we have

  $$\|\ell\| = \|(n\alpha, m + n\beta)\| = n^2\alpha^2 + (m + n\beta)^2 = n^2(\alpha^2 + \beta^2) + m^2 + 2mn\beta$$
  $$\geq n^2 + m^2 - |mn| \geq \min(n^2, m^2) \geq 1$$

  Where the first inequality comes from the fact that $\alpha^2 + \beta^2 = \|\mathbf{b}_2\|^2 \geq 1$ and $|\beta| \leq 1/2$.

□

Lemma 6 *The Lagrange reduction algorithm terminates after* $O\left(\log \frac{\|\mathbf{b}_1\|}{\sqrt{\det\Lambda}}\right)$ *iterations.*

Proof: Without loss of generality, we may assume that the determinant of the lattice is 1, by scaling. Note that this also means that $\|\widetilde{\mathbf{b}}_1\|\|\widetilde{\mathbf{b}}_2\| = 1$. We divide the algorithm into two phases, namely the phase where $\|\mathbf{b}_1\|^2 \geq 2$, and the phase where $\|\mathbf{b}_1\|^2 < 2$.

- (Phase 1) As $\mathbf{b}_1 = \widetilde{\mathbf{b}}_1$, and $\|\mathbf{b}_1\|^2 \geq 2$, we must have that $\|\widetilde{\mathbf{b}}_2\|^2 \leq 1/2 \leq 1/4\|\mathbf{b}_1\|^2$. Denote $\mathbf{c}_1$ as being the 'next iteration' $\mathbf{b}_1$. Note that the $\mathbf{c}_1 = \mathbf{b}_2 - k\mathbf{b}_1$ satisfies $|\langle \mathbf{c}_1, \mathbf{b}_1 \rangle| \leq 1/2\|\mathbf{b}_1\|^2$ and $\langle \mathbf{c}_1, \widetilde{\mathbf{b}}_2 \rangle = \langle \mathbf{b}_2, \widetilde{\mathbf{b}}_2 \rangle = \|\widetilde{\mathbf{b}}_2\|^2$. It follows that

  $$\|\mathbf{c}_1\|^2 \leq \frac{1}{4}\|\mathbf{b}_1\|^2 + \|\widetilde{\mathbf{b}}_2\|^2 \leq \frac{1}{2}\|\mathbf{b}_1\|^2$$

  This means that the square length of $\mathbf{b}_1$ reduces by a factor a half every iteration. Therefore, the number of iterations in phase 1 is at most $\log_2(\|\mathbf{b}_1\|)$.

- (Phase 2) In this phase, $\|\mathbf{b}_1\|^2 < 2$. We distinguish the cases $\lambda_2(\Lambda)^2 \geq 2$ and $\lambda_2(\Lambda)^2 < 2$. In the first case the algorithm is done, because $\|\mathbf{b}_1\|^2 < 2 \leq \lambda_2(\Lambda)^2$. Namely, this means that $\mathbf{b}_1$ is a multiple of a shortest vector in Λ. But, as $(\mathbf{b}_1, \mathbf{b}_2)$ is a basis of Λ, $\mathbf{b}_1$ must be a shortest vector itself.

  In the second case we know that for a basis $(\mathbf{c}_1, \mathbf{c}_2)$ attaining the successive minima, we have $\|\mathbf{c}_2^*\|^2 \leq \|\mathbf{c}_2\|^2 < 2$, and therefore $\lambda_1(\Lambda)^2 = \|\mathbf{c}_1\|^2 > 1/2$. So, we have $\lambda_1(\Lambda) > 1/\sqrt{2}$.

In a circle of radius $\sqrt{2}(1+\frac{1}{4})$ surely fit at most 25 circles of radius $\frac{1}{2\sqrt{2}}$, so, the reduction needs to perform at most 25 iterations in this phase in order to terminate (recall that $\|b_1\|$ is strictly decreasing).

□

Definition 7 *Given a full rank lattice Λ of dimension n. Then we define $\gamma(\Lambda)$ of this lattice as*

$$\gamma(\Lambda) := \frac{\lambda_1(\Lambda)^2}{\det(\Lambda)^{2/n}}$$

Exercise 4 Show that the invariant $\gamma(\Lambda)$ of a lattice Λ is scaling-invariant. That is: $\gamma(c\Lambda) = \gamma(\Lambda)$ for any $c \in \mathbb{R}$.

Definition 8 (Hermite constant) *The hermite constant γ_n is the supremum of γ over n-dimensional full rank lattices:*

$$\gamma_n := \sup_{\Lambda} \gamma(\Lambda)$$

Lemma 9 *The densest sphere packing in dimension 2 is attained by the hexagonal lattice H, which achieves $\gamma(H) = \sqrt{4/3}$.*

Proof: Let $H = \mathcal{L}((0,1), (\sqrt{3/4}, 1/2))$. Verify that this indeed has the required Hermite constant. We now have to show that any 2-dimensional lattice has a Hermite constant at least $\gamma(H)$. Let Λ be any lattice and let $(\mathbf{b}_1, \mathbf{b}_2)$ be a basis as in the Wristwatch lemma. Without loss of generality we may assume $\mathbf{b}_1 = (0,1)$ and $\mathbf{b}_2 = (\alpha, \beta)$. Then $\lambda_1(\Lambda) = 1$, and $\det(\Lambda) = \det(B) = \alpha$. As $|\beta| \le 1/2$ we must have $1 \le \alpha^2 + \beta^2 \le \alpha^2 + \frac{1}{4}$. This directly implies $\alpha \ge \sqrt{3/4}$, which proves the claim. □