Lecture 18

Lecturer: Jonathan Kelner *Scribe: Colin Jia Zheng*

1 Lattice

Definition. (Lattice) Given n linearly independent vectors $b_1, \cdots, b_n \in \mathbb{R}^m$, the *lattice* generated by them is defined as $L(b_1, b_2, \cdots b_n) = \{\sum x_i b_i | x_i \in \mathbb{Z}\}$. We refer to $b_1, \cdots, b_n$ as a *basis* of the lattice. Equivalently, if we define B as the $m \times n$ matrix whose columns are $b_1, \cdots, b_n$, then the lattice generated by B is $L(B) = L(b_1, b_2, \cdots, b_n) = \{Bx | x \in \mathbb{Z}^n\}$. We say that the *rank* of the lattice is n and its *dimension* is m. If $n = m$, the lattice is called a *full-rank* lattice.

It is easy to see that, L is a lattice if and only if L is a discrete subgroup of $(\mathbb{R}^n, +)$.

Remark. We will mostly consider full-rank lattices, as the more general case is not substantially different.

Example. The lattice generated by $(1,0)^T$ and $(0,1)^T$ is $\mathbb{Z}^2$, the lattice of all integers points (see Figure 1(a)). This basis is not unique: for example, $(1,1)^T$ and $(2,1)^T$ also generate $\mathbb{Z}^2$ (see Figure 1 (b)). Yet another basis of $\mathbb{Z}^2$ is given by $(2005,1)^T$; $(2006,1)^T$. On the other hand, $(1,1)^T$, $(2,0)^T$ is not a basis of $\mathbb{Z}^2$: instead, it generates the lattice of all integer points whose coordinates sum to an even number (see Figure 1 (c)). All the examples so far were of full-rank lattices. An example of a lattice that is not full is $L((2,1)^T)$ (see Figure 1(d)). It is of dimension 2 and of rank 1. Finally, the lattice $\mathbb{Z} = L((1))$ is a one-dimensional full-rank lattice.

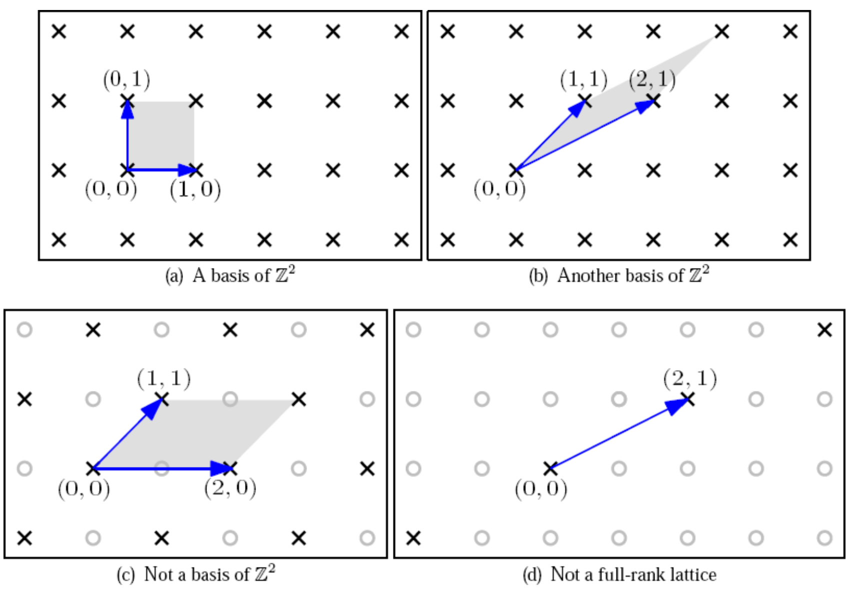

Figure 1: Lattices of $\mathbb{R}^2$

Definition. For matrix B, $P(B) = \{Bx | x \in [0,1)^n\}$ is the *fundamental parallelepiped* of B.

Examples of fundamental parallelepipeds are the gray areas in Figure 1. For a full rank lattice $L(B)$, $P(B)$ tiles $\mathbb{R}^n$ in the pattern $L(B)$, in the sense that $\mathbb{R}^n = \{P(B) + x : x \in L(B)\}$; see Figure 2.

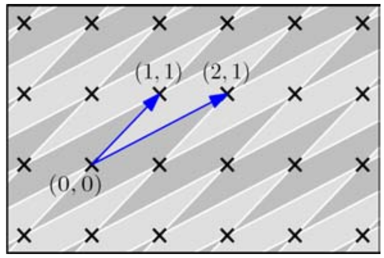

Figure 2: $P(B)$ tiles $\mathbb{R}^n$

Image courtesy of Oded Regev. Used with permission.

In Figure 1, we saw that not every set of n linearly independent vectors B in a rank n full-rank lattice Λ is a basis of Λ. The fundamental parallelepiped characterizes exactly when B is a basis:

Lemma. *Let Λ be a rank n full-rank lattice and B an invertible $n \times n$ matrix. Then B is a basis (of Λ) if and only if $P(B) \cap \Lambda = \{0\}$.*

Proof. " $\Rightarrow$ " is obvious: Λ only contains elements with integer coordinates under B, and 0 is the only element of $P(B)$ with integer coordinates.

For " $\Leftarrow$ ", need to show that any lattice point $x = By$ satisfies $y_i \in \mathbb{Z}$. Note that By' with $y'_i = y_i - \lfloor y_i \rfloor$ is a lattice point in $P(B)$. By our assumption $By' = 0$, ie $y_i \in \mathbb{Z}$. □

It is natural to ask when are two invertible matices A, B *equivalent bases,* ie bases of the same lattice. It turns out that this happens if and only if A, B are related by a *unimodular* matrix.

Definition. A square matrix U is *unimodular* if all entries are integer and $det(U) = \pm 1$.

Lemma. *U is unimodular iff U^{-1} is unimodular.*

Proof. Suppose U is unimodular. Clearly U^{-1} has ± 1 determinant. To see that U^{-1} has integer entries, note that they are simply signed minors of U divided by $det(U)$. □

Lemma. *Nonsingular matrices B_1, B_2 are equivalent bases if and only if $B_2 = B_1 U$ for some unimodular matrix U.*

Proof. "$\Rightarrow$": Since each column of B_1 has integer coordinates under B_2, $B_1 = B_2 U$ for some integer matrix U. Similarly $B_2 = B_1 V$ for some integer matrix V. Hence $B_1 = B_1 V U$, ie $VU = I$. Since V, U are both integer matrices, this means that $det(U) = \pm 1$, as required.

"$\Leftarrow$": Note that each column of B_2 is contained in $L(B_1)$ and vice versa. □

Corollary. *Nonsingular matrices B_1, B_2 are equivalent if and only if one can be obtained from the other by the following operations on columns:*

1. $b_i \leftrightarrow b_i + k b_j$ for some $k \in \mathbb{Z}$
2. $b_i \leftrightarrow b_j$
3. $b_i \leftarrow -b_i$

Now that it is clear that bases of a lattice have the same absolute determinant, we can proceed to define the determinant of lattice:

Definition. (Determinant of lattice) Let $L = L(B)$ be a lattice of rank n. We define the *determinant* of L, denoted $det(L)$, as the n-dimensional volume of $P(B)$, ie $det(L) = \sqrt{det(B^T B)}$. In particular if L is a full rank lattice, $det(L) = |det(B)|$.

1.1 Dual lattices

Definition. The *dual* Λ^* of lattice Λ is $\{x \in \mathbb{R}^n : \forall v \in \Lambda, x \cdot v \in \mathbb{Z}\}$.

Equivalently, the dual can be viewed as the set of linear functionals from Λ to $\mathbb{Z}$.

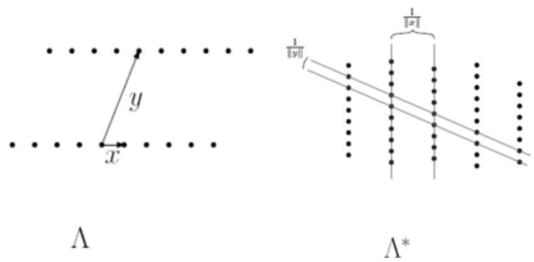

Figure 3: Dual lattice
Image courtesy of Oded Regev. Used with permission.

Definition. For matrix B, its the dual basis B^* is the unique basis that satisfies

1. $span(B) = span(B^*)$
2. $B^T B^* = I$

Fact. $(L(B))^* = L(B^*)$.

Fact. $(\Lambda^*)^* = \Lambda$.

Fact. $det(\Lambda^*) = \frac{1}{det(\Lambda)}$.

2 Shortest vectors and successive minima

One basic parameter of a lattice is the length of the shortest nonzero vector in the lattice, denoted λ_1. How about the second shortest? We are not interested in the second/third/etc shortest vectors which happen to be simply scaler multiples of the shortest vector. Instead, one requires that the next "minimum" increases the dimension of the space spanned:

Definition. The ith *successive minimum* of lattice Λ, $\lambda_i(\Lambda)$, is defined to be $\inf\{r | \dim(span(\Lambda \cap \bar{B}(0, r)) \geq i\}$.

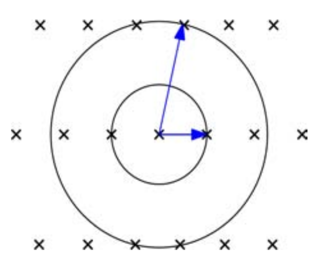

Figure 4: $\lambda_1(\Lambda) = 1$, $\lambda_2\Lambda = 2.3$
Image courtesy of Oded Regev. Used with permission.

The following theorem, due to Blichfield, has various important consequences, and in particular can be used to bound λ_1.

Theorem. *(Blichfield) For any full-rank lattice Λ and (measurable) set $S \subseteq \mathbb{R}^n$ with $vol(S) > det(\Lambda)$, there exist distinct $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.*

Proof. Let B be a basis of Λ. Define $x + P(B)$ to be $\{x + y : y \in P(B)\}$ and S_x to be $= S \cap (x + P(B))$ (see Figure 5). Since $S = \bigcup_{x \in \Lambda} S_x$ we conclude that $vol(S) = \sum_{x \in \Lambda} vol(S_x)$. Let $\hat{S_x}$ denote $\{z - x : z \in S_x\}$. Then $vol(\hat{S_x}) = vol(S_x)$, ie $\sum_{x \in \Lambda} vol(\hat{S_x}) = vol(S) > vol(P(B))$. Therefore, there must exist nondisjoint $\hat{S_x}$ and $\hat{S_y}$ for $x \neq y$. Consider any nonzero $z \in \hat{S_x} \cap \hat{S_y}$, then $z + x, z + y \in S$ and $x - y = (z + x) - (z + y) \in \Lambda$, as required.

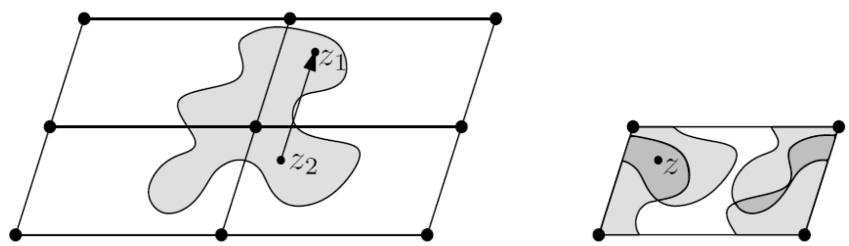

Figure 5: Blichfield's theorem

Image courtesy of Oded Regev. Used with permission.

□

As a corollary of Blichfield's theorem, we obtain the following theorem due to Minkowski, which says that any large enough centrally-symmetric convex set contains a nonzero lattice point. A set S is centrally-symmetric if it is closed under negation. It is easy to see that the theorem is false if we drop either of the central-symmetry or the convexity requirement.

Theorem. *(Minkowski) Let Λ be a full-rank lattice of rank n. Any centrally-symmetric convex set S with $vol(S) > 2^n det(\Lambda)$ contains a nonzero lattice point.*

18.409 Topics in Theoretical Computer Science: An Algorithmist's Toolkit
Fall 2009