Lecture1-2019/20

Lecture 1: Euclidean lattices.

(1) Definition ~ intro: basic maths about lattices

Def: $(b_i)_{i \le d} \in \mathbb{R}^n$ lin. indep.
The spanned lattice is $L((b_i)_i) := \sum_{i \le d} \mathbb{Z} \cdot b_i$
If the b_i's are in $\mathbb{Z}^n$, $L((b_i)_i)$ is called an integral lattice.

Ex.: $\mathbb{Z}^n$, not $\mathbb{Z} + \sqrt{2} \cdot \mathbb{Z}$

Alternative def: A lattice is a discrete subgroup of $(\mathbb{R}^n, +)$.

Ex.: Every subgroup of $\mathbb{Z}^n$.

Def [lattice bases]: Let $L = L[(b_i)_i]$ for lin. indep. b_i's. Then the b_i's are called a basis of L.

Lemma: Let $(b_i)_{i \le d}$ and $(b'_i)_{i \le d'}$ be 2 families of lin. indep. vectors in $\mathbb{R}^n$. Then $L((b_i)_i) = L((b'_i)_i)$ iff $d = d'$ and $B' = B \cdot U$ for some $U \in GL_d(\mathbb{Z})$ and $B = (b_1 | \cdots | b_d)$, $B' = (b'_1 | \cdots | b'_d)$.

unimodular (ie det $= \pm 1$). basis matrices.

Proof: • $d = \dim \mathrm{Span}_{\mathbb{R}} L = d'$.
• $b'_1 \in L((b_i)_i)$, $b'_2 \in L((b_i)_i), \ldots \Rightarrow \exists U \in \mathbb{Z}^{d \times d}$ s.t. $B' = B \cdot U$
$b_1 \in L((b'_i)_i)$, $b_2 \in L((b'_i)_i), \ldots \Rightarrow \exists U' \in \mathbb{Z}^{d \times d}$ s.t. $B = B' \cdot U'$.
$\Rightarrow B \cdot (I_d - UU') = 0 \Rightarrow U \cdot U' = I_d$ (cols of B are lin. indep.) etc ■

(R) → Examples of unimodular transforms: * sign-permute vectors.
* $b_i \leftarrow b_i + x \cdot b_j$ for $i \neq j$ unique and $x \in \mathbb{Z}$.

$\Rightarrow d \geq 2 \Rightarrow$ infinitely many bases for any fixed lattice.

Easy tasks: - decide whether a point belongs to $L((b_i)_i)$.
- decide if B and B' span the same lattice.

Unless stated otherwise, we now assume that $d = n$.

2.- Lattice minimum

PICTURE

Def. [Minimum]: $\lambda_1(L) := \min(r : \exists b \in L \setminus 0, \|b\| \leq r)$.

Ⓡ→ Here $\|\cdot\|$ refers to the ℓ_2-norm. (Euclidean norm)
I may use the ℓ_∞-norm sometimes, and then I will write $\lambda_1^\infty(L)$.
$\lambda_1(L)$ is an invariant of L because it does not dpd on the basis choice.

Lemma: The minimum is never unique, but cannot be reached $\geq 3^d$ times.

Proof: $\pm b$; for every vector $b \in L$ w. $\|b\| = \lambda_1(L)$, put a ball of radius $\lambda_1/2$ centered on b. They are disjoint, and all contained in $B(0, 3\lambda_1/2) \Rightarrow$ At most $\frac{\mathrm{vol}(B(0, 3\lambda_1/2))}{\mathrm{vol}(B(0, \lambda_1/2))} \leq 3^d$ of these.

SVP$_\gamma$: Given as input a basis $(b_1, \dots, b_n)$ of a lattice L, find $b \in L \setminus 0$ s.t. $\|b\| \leq \gamma \cdot \lambda_1(L)$.

Remarks:
- $\gamma = 1$: find a shortest $\neq 0$ vector.
- no harder when γ increases.
- the associated decision problem is NP-hard under randomized reductions [Ajtai98] for $\gamma = 1$, and even for $\gamma = \exp[(\lg n)^{1-\varepsilon}]$ for every $\varepsilon > 0$. [HaRe07]
- in NP $\cap$ coNP for $\gamma = \sqrt{n}$
- used as a cryptographic hardness assumption for $\gamma = \mathrm{poly}(n)$ ⟶ [Regev05], NIST competition for post-q. crypto

3 - The List Sieve algorithm for SVP

Input: basis $B \in \mathbb{Z}^{m \times m}$

// assume all $\|b_i\|$'s $\leq 2^{2m} \cdot \lambda_1(L)$.

// LLL-reduce, remove $b_j \ldots b_m$ if $\|b_j^*\| \geq 2^m \cdot \lambda_1$
(none of these vectors can be used in a combination leading to λ_1.)

$T := \emptyset$. For $i = 1$ to N (to be determined)
- create $t_i \in L$ not much longer than B.
- reduce t_i against all previous $t_j \in T$
(i.e., $t_i \leftarrow t_i - t_j$ if $\|t_i - t_j\| \leq (1-\varepsilon)\|t_i\|$ for some j until not possible).

add t_i to T unless it is already in T.

Return a shortest non-zero vector in T.

Run-time: Subdivide the space into coronas
$$\mathcal{C}_k := \mathcal{B}(0,(1+\varepsilon)^{k+1}) \setminus \mathcal{B}(0,(1+\varepsilon)^k).$$
By choice of B and t_i's, T is covered by $O\left(\frac{\lg\|B\|}{\lg(1+\varepsilon)}\right)$ coronas.

In each $t_i, t_j \in \mathcal{C}_k$ with $i > j$:
$$\|t_i\| \simeq \|t_j\| \text{ and } \|t_i - t_j\| \gtrsim \|t_i\|$$
$\Rightarrow$ all vectors in $T \cap \mathcal{C}_k$ have angles $\geq \frac{\pi}{3} - O(\varepsilon)$

Kabatiansky-Levenshtein 78: at most $2^{[0.42 + O(\varepsilon)]m}$ vectors
heuristically: $2^{0.21m} = \sqrt{\frac{4}{3}}^m$

fraction of n-sphere at angle $\leq \pi/3$ from a given point is $\simeq (\sin \pi/3)^{n}$.

This gives the estimate $\sqrt{\frac{4}{3}}^m$ if the caps don't intersect much.