Prof. Friedrich Eisenbrand
Alfonso Cevallos and Yuri Faenza

Discussions from: May 20, 2014

Computer Algebra

Spring 2014

Assignment Sheet 7

Exercises marked with a $\star$ can be handed in for bonus points. Because of the upcoming end of the semester, due date is May 27.

You can assume as known the following characterization of lattices: $\Lambda \subseteq \mathbb{R}^n$ is a lattice if and only if it is an *additive subgroup* of $\mathbb{R}^n$, i.e.

- $0 \in \Lambda$;
- $x + y \in \Lambda$ for each $x, y \in \Lambda$;
- $-x \in \Lambda$ for each $x \in \Lambda$;
- $\exists \epsilon > 0$ such that, for each $x \in \Lambda$, the ball centered at x with radius ϵ contains no lattice point other than x.

Exercise 1
Let $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice and define the *dual lattice*

$$\Lambda^\star = \{y \in \mathbb{R}^n \mid y^T x \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

1. Prove that $\Lambda^\star$ is a lattice and that $(\Lambda^\star)^\star = \Lambda$.
2. Let B be a basis of Λ. Prove that ${B^{-1}}^T$ is a basis of $\Lambda^\star$.
3. Let $y \in \Lambda^\star$ be arbitrary and consider the affine hyperplanes $H_k = \{x \in \mathbb{R}^n \mid y^T x = k\}$ for all $k \in \mathbb{Z}$. Prove that $\Lambda \subset \bigcup_{k \in \mathbb{Z}} H_k$.

Exercise 2
Let $K \subseteq \mathbb{R}^n$ be a convex body of volume $\mathrm{vol}(K) \geq k \cdot 2^n$ that is symmetric about the origin. Prove that K contains at least $2k$ nonzero integer points.

Exercise 3
In this exercise we will prove a central result in algorithmic geometry of numbers, known as *Flatness Theorem*. Given a convex body $K \subseteq \mathbb{R}^n$ and a direction $d \in \mathbb{Z}^n$, define the *width of K along d* to be

$$w_d(K) = \max\{d^T x : x \in K\} - \min\{d^T x : x \in K\}.$$

A *flat direction* for K is a nonzero direction that minimizes the quantity above, i.e. a vector $d \in \mathbb{Z}^n$ that realizes

$$w(K) = \min\{w_d(K) : d \in \mathbb{Z}^n \setminus \{0\}\}.$$

Of course, in general, $w(K)$ depends on the specific K. The **Flatness Theorem** states that, when K has no integer point, $w(K)$ can be upper bounded by a function depending only on n (and hence, not on the specific K under analysis):

$\exists \omega : \mathbb{N} \to \mathbb{N}$ such that, for each convex body $K \subseteq \mathbb{R}^n$ with $K \cap \mathbb{Z}^n = \emptyset$, one has $w(K) \leq \omega(n)$.

We will prove the flatness theorem for the special case of K being an ellipsoid, and use an auxiliary result to deduce the more general case. An ellipsoid $E \subseteq \mathbb{R}^n$ is the image of the n−dimensional unit ball $B = \{x \in \mathbb{R}^n : ||x|| \leq 1\}$ under an affine map.

(a) Show that E can be written as $E = \{x \in \mathbb{R}^n : ||A(x-a)|| \leq 1\}$ for some matrix $A \in \mathbb{R}^{n\times n}$ and vector $a \in \mathbb{R}^n$. When $a = 0$ in the representation above, we say that E *is centered at the origin*.

(b) Show that the computation of a flat direction for E can be reduced to the shortest vector problem on the lattice $\Lambda({A^{-1}}^T)$.

(c) Show that $\Lambda({A^{-1}}^T) = \Lambda^*(A)$.

(d) Given a lattice $\Lambda \subseteq \mathbb{R}^n$, we define the *covering radius* to be the smallest α such that the family of balls centered at lattice points and having radius α cover all $\mathbb{R}^n$. The *packing radius* $\rho(\Lambda)$ is the supremum of the β such that no two balls centered at lattice points and having radius β intersect. Show that there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, for each lattice $\Lambda \subseteq \mathbb{R}^n$, $\mu(\Lambda) \cdot \rho(\Lambda^*) \leq f(n)$.

(e) Prove the flatness theorem when K is an ellipsoid.

(f) Assume as known the following result: **John's theorem:** *Let $K \subseteq \mathbb{R}^n$ be a convex body. There exists an ellipsoid E and $a \in \mathbb{R}^n$ such that: E is centered at the origin; $E + a \supseteq K$; and $\frac{1}{n}E + a \subseteq K$.* Use the previous result and the flatness theorem for ellipsoids to prove the flatness theorem for any convex body.

Exercise 4 ($\star$)
Show the following result: For every $k \in \mathbb{N}$ and every convex body $K \subseteq \mathbb{R}^n$ with $|K \cap k\mathbb{Z}^n| = 1$, one has $w(K) \leq 2k\omega(n)$, with ω as in the flatness theorem.[1]

Exercise 5
Recall that we proved in class the following theorem 'almost completely' (LLL algorithm): Given a non-singular matrix $B \in \mathbb{Q}^{n\times n}$, where every entry is bounded in absolute value by some $M \in \mathbb{N}$, we can compute a vector $v \in \Lambda(B)$ in time polynomial in n and $\log M$, such that $\| v\| \leq 2^{\frac{n-1}{2}} \min_{w\in\Lambda(B)\setminus\{0\}} \|w\|$. Complete the proof by showing the following: At any stage of the LLL algorithm, all rational numbers involved have numerators and denominators of binary length at most $O(n \log nM)$.

[1] Being traditional, we exclude the 0 from the set of natural numbers $\mathbb{N}$.