Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: May 24, 2011

Computer Algebra

Spring 2011

Assignment Sheet 7

Warning: These are just notes and not necessarily full solutions for each exercise. Full solutions may require some additional details to be fleshed out. Please report any mistakes you may find.

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 $(\Lambda^\star)^\star = \Lambda$.

   Let us first use the definition that a lattice is a discrete subgroup of $\mathbb{R}^n$. It is easy to see that $\Lambda^\star$ is a group: clearly $0 \in \Lambda^\star$, and when $y, y' \in \Lambda^\star$, then for all $x \in \Lambda$ one has

   $$(y - y')^T x = \underbrace{y^T x}_{\in\mathbb{Z}} - \underbrace{y'^T x}_{\in\mathbb{Z}} \in \mathbb{Z}$$

   so $y - y' \in \Lambda^\star$ by definition. These two facts together show that $\Lambda^\star$ is a group. We also have to show that $\Lambda^\star$ is discrete, i.e. there exists an $\varepsilon > 0$ such that the distance between any two different lattice points is at least ε. Since $\Lambda^\star$ is a group, this is equivalent to saying that there is an $\varepsilon > 0$ such that no non-zero lattice point has norm less than ε. Observe that for such a short lattice vector $y \in \Lambda^\star$ we get

   $$|y^T x| \leq \|y\| \cdot \|x\| < \varepsilon \cdot \|x\|.$$

   On the other hand, $|y^T x|$ must be an integer. We can combine these observations to prove the result as follows. Let $x_1, \ldots, x_n \in \Lambda$ be linearly independent lattice vectors.[1] Then for every $y \in \Lambda^\star \setminus \{0\}$, there is a j such that

   $$y^T x_j \neq 0.$$

   On the other hand,

   $$1 \leq |y^T x_j| \leq \|y\| \cdot \|x_j\|,$$

   so we must have

   $$\|y\| \geq \frac{1}{\|x_j\|}$$

[1] Such a set exists because Λ is full-dimensional, e.g. take a basis.

Since $y \in \Lambda^\star \setminus \{0\}$ was arbitrary, we can conclude that for all such y, one has

$$\|y\| \geq \min\{\frac{1}{\|x_1\|}, \ldots, \frac{1}{\|x_n\|}\}.$$

This completes the proof that $\Lambda^\star$ is discrete.[2]

The easiest way to show $\Lambda = (\Lambda^\star)^\star$ is probably by first showing the next part of this exercise.

2. Let B be a basis of Λ. Prove that B^{-T} is a basis of $\Lambda^\star$.

   Let Λ' be the lattice generated by B^{-T}. Let us show that $\Lambda' = \Lambda^\star$. Let $y \in \Lambda'$, that is $y = B^{-T} \cdot z$ for some $z \in \mathbb{Z}^n$. Then for any $x = B \cdot w \in \Lambda$ one has

   $$y^T x = z^T B^{-1} B w = z^T w \in \mathbb{Z},$$

   which shows $y \in \Lambda^\star$.

   Now let $y \in \Lambda^\star$. We know that $y^T B = w^T$ with $w \in \mathbb{Z}^n$. Transposing this equation gives $B^T y = w$, from which $y = B^{-T} w \in \Lambda'$ follows.

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 $\Lambda \subset \bigcup_{k \in \mathbb{Z}} H_k$.

   This follows directly from the definitions.

4. Let U be an $(n-1)$-dimensional subspace of $\mathbb{R}^n$ so that $\Lambda' := \Lambda \cap U$ is an $(n-1)$-dimensional lattice with basis $b_1, \ldots, b_{n-1}$.

   a) Prove that there exists $y \in \Lambda^\star$ such that $U = \{x \in \mathbb{R}^n \mid y^T x = 0\}$ and $\frac{1}{k} \cdot y \notin \Lambda^\star$ for all integers $k \geq 2$.

      By linear algebra, it suffices to find $y \in \Lambda^\star$ such that $y^T b_j = 0$ for all $j = 1 \ldots n-1$. Using a basis B of Λ, we can rewrite these equations as $0 = y^T b_j = w^T B^{-1} B x_j = w^T x$. Again by linear algebra, this set of linear equations has a one-dimensional space of solutions, and since the coefficients are rational, there exists a non-zero rational solution, and, by scaling, an integer solution $w \in \mathbb{Z}^n \setminus \{0\}$. Then $y = B^{-T} w$ satisfies $y \in \Lambda^\star$ and $U = \{x \in \mathbb{R}^n \mid y^T x = 0\}$. The final condition can be achieved by replacing y by the shortest dual lattice vector on the line through the origin and y.

   b) Consider the affine lattice hyperplane $H = \{x \in \mathbb{R}^n \mid y^T x = 1\}$. Prove that $H \cap \Lambda$ is non-empty.

      Let $H_k = \{x \in \mathbb{R}^n \mid y^T x = k\}$. Since Λ is full-dimensional, there must be *some* $k \in \mathbb{N}$ such that $H_k \neq \emptyset$, so let k be the *smallest* natural number so that $H_k \neq \emptyset$. Then whenever $H_m \neq \emptyset$ one has $k | m$, because if $m = dk + r$ with $0 < r < k$, we

[2] In fact, by using shortest independent vectors $x_1, \ldots, x_n$, we can say that $\|y\| \geq \frac{1}{\lambda_n(\Lambda)}$, where $\lambda_n(\Lambda)$ is the n-th successive minimum of the lattice, as in Exercise 2. This shows the simple *transference bound* $\lambda_1(\Lambda^\star) \cdot \lambda_n(\Lambda) \geq 1$.

can subtract a representative lattice vector $x \in H_k$ d times from a representative lattice vector $x' \in H_m$ to show that H_r is non-empty, which is a contradiction.[3]

But then it follows that $y/k \in \Lambda^\star$, so $k = 1$ and $H = H_1 \neq \emptyset$.

c) Let $w \in H \cap \Lambda$ be arbitrary. Prove that $b_1, \ldots, b_{n-1}, w$ is a basis of Λ.

We have to show that the lattice L generated by $b_1, \ldots, b_{n-1}, w$ is equal to Λ. Since $b_1, \ldots, b_{n-1}, w \in \Lambda$, $L \subseteq \Lambda$ is clear.

Let $x \in \Lambda$ and let $k := y^T x$. Then $x - kw \in \Lambda'$ and can be written as

$$x - kw = \mu_1 b_1 + \cdots + \mu_{n-1} b_{n-1}$$

for integers μ_j. Therefore, $x \in L$.

Exercise 2

For a full-dimensional lattice $\Lambda \subset \mathbb{R}^n$, we say that $v_1, \ldots, v_n$ is a sequence of shortest independent vectors if v_j is a shortest vector in $\Lambda \setminus \langle v_1, \ldots, v_{j-1} \rangle$. In particular, v_1 is a shortest non-zero lattice vector.

1. Prove that a sequence of shortest independent vectors always exists, and that $v_1, \ldots, v_n$ span all of $\mathbb{R}^n$, i.e., they are linearly independent.

   Linear algebra.

2. Prove that the sequence $\lambda_1 := \|v_1\|, \ldots, \lambda_n := \|v_n\|$ is independent of the choice of shortest independent vectors. In other words, the λ_j are a property of the lattice.

   The sequence of vectors $v_1, \ldots, v_n$ is not unique. There is always at least the choice of replacing v_j by $-v_j$, but even greater choice may be possible, and a priori it seems conceivable that an early choice may affect the length of choices that are available later. The goal is to show that this is not the case.

   For this purpose, take two sequences of shortest independent vectors, $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$. Our goal is to show $\|v_j\| = \|w_j\|$ for all $j = 1 \ldots n$.

   By definition, v_j is a shortest vector in $\Lambda \setminus \langle v_1, \ldots, v_{j-1} \rangle$. Since $\langle v_1, \ldots, v_{j-1} \rangle$ is $(j-1)$-dimensional and the vectors $w_1, \ldots, w_j$ are linearly independent, there is some $1 \leq i \leq j$ such that $w_i \notin \langle v_1, \ldots, v_{j-1} \rangle$. It follows that[4]

   $$\|v_j\| \leq \|w_i\| \leq \max\{\|w_1\|, \ldots, \|w_j\|\} = \|w_j\|$$

   The argument is symmetric, i.e. $\|w_j\| \leq \|v_j\|$ follows simply by exchanging the roles of the two sequences, and so we have $\|w_j\| = \|v_j\|$.

[3] At a high level, this is because the quotient group Λ/Λ' has a natural embedding into the group of hyperplanes H_k (which is naturally isomorphic to $\mathbb{Z}$ via $k \mapsto H_k$).

The group Λ/Λ' is also naturally isomorphic to a one-dimensional lattice that is obtained by the orthogonal projection of Λ onto the orthogonal complement of U.

[4] Strictly speaking, we first need to prove that $\|w_1\| \leq \|w_2\| \leq \cdots \leq \|w_n\|$. Why is that?

3. Let $n = 2$. Prove that a sequence of shortest independent vectors is a basis of the lattice.

   Let v_1, v_2 be shortest independent vectors and let $U = \langle v_1 \rangle$. Since v_1 is a shortest vector, it is easy to see that v_1 is a basis for $U \cap \Lambda$. Let y be a primitive[5] dual lattice vector such that $y^T v_1 = 0$. If we can show $|y^T v_2| = 1$, then the result follows from the last part of Exercise 1. We can perform the Gram-Schmidt orthogonalization

   $$v_2 = v_2^\star + \lambda v_1$$

   It is easy to see that $|\lambda| \leq 1/2$.[6] Suppose $|y^T v_2| = k \geq 2$. Then by Exercise 1, there exists a lattice vector $w \in \Lambda$ with $y^T w = 1$ and Gram-Schmidt orthogonalization

   $$w = \frac{1}{k} \cdot v_2^\star + \mu v_1$$

   with $|\mu| \leq 1/2$. By the theorem of Pythagoras we have:

   $$\begin{aligned} \|v_1\|^2 \leq \|w\|^2 &= \frac{1}{k^2} \cdot \|v_2^\star\|^2 + \mu^2 \|v_1\|^2 \\ &\leq \frac{1}{4} \cdot \|v_2^\star\|^2 + \frac{1}{4} \|v_1\|^2 \end{aligned}$$

   This implies $\|v_2^\star\|^2 \geq 3\|v_1\|^2$. We can use this to compute:

   $$\begin{aligned} \|w\|^2 &\leq \frac{1}{4} \cdot \|v_2^\star\|^2 + \frac{1}{12} \|v_2^\star\|^2 < \|v_2^\star\|^2 \\ \|v_2\|^2 &= \|v_2^\star\|^2 + \lambda^2 \|v_1\|^2 \geq \|v_2\|^\star > \|w\|^2 \end{aligned}$$

   This contradicts the fact that v_2 is a shortest lattice vector outside of U. Therefore, $|y^T v_2| = 1$ which, by Exercise 1, shows that v_1, v_2 is a basis of Λ.

4. Prove that, for $n \geq 4$, a sequence of shortest independent vectors is not necessarily a lattice basis.

   Hint: Consider the *parity lattice* $\Lambda = \{x \in \mathbb{Z}^n \mid x_1 \equiv \cdots \equiv x_n \pmod 2\}$. Prove that it is a lattice. Then find a sequence of shortest independent vectors that is not a basis. It probably helps to first find a basis of the lattice.

   Lattice vectors in the parity lattice have components that are either all even or all odd. Non-zero vectors that are all even have length at least 2, and so do odd vectors, because if $x \in \Lambda$ has odd components, then

   $$\|x\| = \sqrt{x_1^2 + \cdots + x_n^2} \geq \sqrt{1 + \cdots + 1} = \sqrt{n} \geq \sqrt{4} = 2$$

   Therefore, the vectors $2e_1, \ldots, 2e_n$ are shortest independent vectors. However, they do not generate the entire parity lattice, since they generate only even vectors. A "nice" basis of the lattice is given by

   $$2e_1, \ldots, 2e_{n-1}, e_1 + e_2 + \cdots + e_n$$

[5] Meaning that $y/k \notin \Lambda^\star$ for all $k \geq 2$.

[6] Otherwise, we can find a shorter independent vector v_2 by subtracting an appropriate multiple of v_1.

Observe that this proof shows even more: for $n \geq 5$, there are lattices for which no basis consists of shortest independent vectors.