Prof. Friedrich Eisenbrand
Alfonso Cevallos

Discussions from: May 5, 2015

# Computer Algebra

Spring 2015

Assignment Sheet 6

Note: These are just notes and not necessarily full solutions to each exercise. Please report any mistakes you may find.

**Exercise 1**

Suppose that $A = [a_1, \cdots, a_n] \leq \mathbb{Z}^{n\times n}$ consists of pairwise orthogonal where, without loss of generality, $a_1$ has the smallest norm. Then, any non-zero vector in $\Lambda(A)$ is of the form $v = \sum_i k_i a_i$, for integers $k_1, \cdots, k_n$ not all zero. So if $k_j \neq 0$, then $|k_j| \geq 1$, and using Pithagoras we get $\|v\|^2 = \sum_i \|k_i a_i\|^2 \geq |k_j|^2 \|a_j\|^2 \geq \|a_1\|^2$, and the result follows.

**Exercise 2**

We will prove that, given real numbers $\alpha_1, \cdots, \alpha_n$, and $Q > 1$, there are integers $p_1, \cdots, p_n, q$, with $1 \leq q \leq Q^n$, such that $|q\alpha_i - p_i| < \frac{1}{Q}$ for each $1 \leq i \leq n$.[1] Recall that the *fractional part* of a real number $x$ is $x - \lfloor x \rfloor$, and is always contained in the half-closed interval $[0, 1)$.

We first deal with the case $n = 1$. Divide the half-closed interval $[0, 1)$ into sub-intervals $[0, \frac{1}{Q}), [\frac{1}{Q}, \frac{2}{Q}), \cdots, [\frac{Q-1}{Q}, 1)$. Note that any two points within the same interval have a distance $< \frac{1}{Q}$. For $j = 0, \cdots, Q$, consider the $Q+1$ fractional parts of $j\alpha$. Using the pigeon-hole principle, at least two of them (say those corresponding to $j' < j''$) lie in the same sub-interval. This implies that $|(j'' - j')\alpha - p| < \frac{1}{Q}$, for an appropiate integer $p$, as required.

We now consider the general case. Divide the cube $C = [0, 1)^n$ into $Q^n$ sub-cubes, where each sub-cube corresponds to $\frac{1}{Q}C = [0, \frac{1}{Q})^n$, shifted by a lattice point $v \in \Lambda(\frac{1}{Q} I_n) \cap C$. Now, for each $j = 0, \cdots, Q^n$, consider the $n$-dimensional vector whose $i$-th component is the fractional part of $j\alpha_i$. As we have $Q^n + 1$ such vectors, again by the pigeon-hole principle at least two of them (say those corresponding to $j' < j''$) lie in the same sub-cube. This implies that, for each $i = 1, \cdots, n$, $|(j'' - j')\alpha_i - p_i| < \frac{1}{Q}$, for some appropiate integers $p_i$, as required.

[1] We proved in class the same result (Dirichlet's theorem) but without strict inequalities, using Minkowski's convex body theorem.

**Exercise 3**

We assume without loss of generality that the given matrix $A \in \mathbb{Z}^{m\times n}$ has full row rank (if not, we can start by applying an appropiate linear transformation, to embed $A$ in a lower-dimensional space). We can compute in polynomial time the HNF: $AU = (H|0)$, where the matrix $H \in \mathbb{Z}^{m\times m}$ is invertible because $A$ has full row rank. Since $U$ is an invertible, integer matrix with $\det U = \pm 1$, clearly $U^{-1}$ is also an integer matrix, and the equation $Ux' = x$ has a (unique) integer solution $x'$ if and only if $x$ is an integer vector. Hence:

$$\begin{aligned} & \exists x \in \mathbb{Z}^n : \ v = Ax \\ \Leftrightarrow\ & \exists x' = \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} \in \mathbb{Z}^n : \ v = A(Ux') = (AU)x' = (H|0)\begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = Hx'_1 \\ & x'_1 := H^{-1}v \in \mathbb{Z}^m \end{aligned}$$

Where $x'_1$ is the projection of $x'$ over the first $m$ coordinates. So $Ax = v$ has an integer solution iff $x'_1 = H^{-1}v$ is integer; however $x'_1$ corresponds to several possible solutions $x$, depending on what $x'_2$ we choose to extend $x'_1$ into $x'$. This corresponds to the fact that in general there are several ways to write $v$ as an integer combination of columns of $A$.

The algorithm is: Compute the matrices $H$ and $U$ defined above, matrix $H^{-1}$, and vector $x'_1 = H^{-1}v$. If this vector is not integer, output 'No integer solution'. Else, pick an arbitrary vector $x'_2 \in \mathbb{Z}^{n-m}$, and output $x = U\binom{x'_1}{x'_2}$.

The related problem $Ax \leq v$ (where the inequality must hold in every row) is a classic problem in discrete optimization, known as Integer Programming, as is known to be NP-complete. Thus, we do not expect to find a general algorithm that solves it in polynomial time. And in particular, the present algorithm does not extend to this case.

**Exercise 4**

Backward implication: Suppose that there is a real vector $y$ such that $y^T A$ is integer, but $y^T v$ is not. If $Ax = v$ had an integer solution, we would have that $y^T v = (y^T A)x$ is the product of two integer vectors, so it is integer, and we get a contradiction.

Forward implication. Again we assume that $A \in \mathbb{Z}^{m\times n}$ has full row rank. Let its HNF be $AU = (H|0)$, where $A$ is invertible. Following the same arguments as in the previous exercise, we conclude that $Ax = v$ has no integer solution iff $H^{-1}v$ is not integer. Thus, there is a row in $H^{-1}$ (that we call $y$) such that $y^T v$ is not integer. On the other hand, from the equation $AU = (H|0)$ we get $H^{-1}A = (I|0)U^{-1}$. Since both matrices on the right-hand side are integer, then the product on the left-hand side must be integer. And in particular $y^T$ is integer.

**Exercise 5**

Part 1. Let $T$ be the triangle with vertices $v_1, v_2, v_3$, and let $A = [v_2 - v_1, v_3 - v_1]$. We can assume wlog that $v_1 = 0$, since this corresponds to an integer translation of $T$, and clearly this changes neither the number of integer points in its interior, nor $A$. A key remark is that for any point $x$ on the plane, there are unique numbers $\alpha, \beta$ such that $x = \alpha v_2 + \beta v_3$. This implies that $x$ is in $\Lambda(A)$ iff $\alpha, \beta \in \mathbb{Z}$, and $x$ is in $T$ iff $\alpha, \beta \geq 0$ and $\alpha + \beta \leq 1$.

We first prove the reverse implication, so we suppose $A$ is unimodular. We saw in class that if an integer matrix is right-multiplied by a unimodular matrix, it still generates the same lattice. Hence $\mathbb{Z}^2 = \Lambda(I) = \Lambda(IA) = \Lambda(A)$. So any point $x$ on the plane that is both integer and inside $T$, must be of the form $x = \alpha v_2 + \beta v_3$ with $(\alpha, \beta) \in \{(0,0), (0,1), (1,0)\}$, and thus it corresponds to one of the 3 vertices of $T$.

For the forward implication, we prove the contrapositive. So we start by assuming that $A$ is not unimodular. We know that two bases of the same lattice always have the same determinant in absolute value. So, since $\Lambda(I) = \mathbb{Z}^2$, any basis of $\mathbb{Z}^2$ must be unimodular, and in particular $\Lambda(A) \neq \mathbb{Z}^2$. This means that there is an integer vector $x = \alpha v_2 + \beta v_3 \in \mathbb{Z}^2 \setminus \Lambda(A)$, with $\alpha$ and $\beta$ not both integer. Now we consider two cases:

- If $\alpha - \lfloor \alpha \rfloor + \beta - \lfloor \beta \rfloor \leq 1$. Define $x' = x - \lfloor \alpha \rfloor v_2 - \lfloor \beta \rfloor v_3 = (\alpha - \lfloor \alpha \rfloor) v_2 + (\beta - \lfloor \beta \rfloor) v_3$. Clearly, this is an integer point, and it is in $T$, but its coefficients are not both integer, so it is not one of the 3 vertices of $T$.

- Else, it must be the case that $(1 + \lfloor \alpha \rfloor - \alpha) + (1 + \lfloor \beta \rfloor - \beta) \leq 1$. Define $x' = (1 + \lfloor \alpha \rfloor) v_2 + (1 + \lfloor \beta \rfloor) v_3 - x = (1 + \lfloor \alpha \rfloor - \alpha) v_2 + (1 + \lfloor \beta \rfloor - \beta) v_3$. Again, this is an integer point in $T$, but its coefficients are not both integer, so it is not one the of the 3 vertices of $T$, and we are done.

Part 2. Example: $v_1 = 0,\ v_2 = (1,-1,0)^T,\ v_3 = (2,1,1)^T,\ v_4 = (0,0,1)^T$.

**Exercise 6**

Proof 1: A triangle in $\mathbb{Z}^2$ is called *elementary* if its vertices are integer, but it contains no other integer point besides its vertices. Notice that an easy corollary of exercise 5.1 is that an elementary triangle always has an area of $1/2$. Another remark is that any lattice polygon can be triangulated by elementary triangles (it can be done by progressively joining with straight segments any two points that are on a common face and not yet adjacent).

We triangulate $P$ into $N$ triangles. We now sum up the internal angles of all these triangles in two different ways. On the one hand, the angle sum of any triangle is $\pi$, so the sum of all the angles is $\pi N$. On the other hand, for each interior point, the angles touching it sum up to $2\pi$, so the sum over the interior points is $2\pi I$. At each boundary point that is not a vertex, the angles touching it sum to $\pi$; and at a vertex, the angles do not add up to $\pi$, but if we add the interior angles at all the vertices, we get $n\pi - 2\pi$, where $n$ is the number of vertices, because

the sum of the exterior angles is $2\pi$. Thus, the sum over the boundary points is $\pi B - 2\pi$, and the overall sum is $2\pi I + \pi B - 2\pi$. We put things together, and notice that $N = 2A$, to get $\pi N = 2\pi A = 2\pi I + \pi B - 2\pi$, thus $A = I + \frac{1}{2}B - 1$.

Proof 2: Recall Euler's formula for planar graphs: If a connected planar graph has $f$ faces, $e$ edges and $v$ vertices, then $v - e + f = 2$. As before, we triangulate $P$ into $N$ elementary triangles. This defines a connected planar graph with $f = N + 1$ faces (including the unbounded external face) and $v = I + B$ vertices. Let $e_i$ and $e_b$ be respectively the number of edges on the interior and on the border, so $e = e_i + e_b$, and notice also that $e_b = B$. Since internal edges belong to 2 triangles, and border edges belong to 1 triangle, counting edges in two different ways gives us $3N = 2e_i + e_b$; and this implies $e = e_i + e_b = \frac{3}{2}N + \frac{1}{2}B$.

Finally, we apply Euler's formula: $2 = v - e + f = (I + B) - (\frac{3}{2}N + \frac{1}{2}B) + (N + 1) = I + \frac{1}{2}B - \frac{1}{2}N + 1$. After rearranging, we get $A = \frac{1}{2}N = I + \frac{1}{2}B - 1$.

**Exercise 7**

See the code.

**Exercise 8**

Just use the formula for the volume of an $n$-dimensional ball, and Stirling's approximation of the factorial.