Prof. Friedrich Eisenbrand
Alfonso Cevallos

Discussions from: May 5, 2015

Computer Algebra

Spring 2015

Assignment Sheet 6

Exercises marked with a $\star$ can be handed in for bonus points. Due date is May 19th.
Remarks: If you hand in the homework by e-mail, make sure to type as subject "Computer Algebra HW6".

Exercise 1
Let $A \in \mathbb{Z}^{n \times n}$ consist of pairwise orthogonal column vectors. Prove that a shortest non-zero vector of $\Lambda(A)$ is the column of A of minimum norm.

Exercise 2
Show that, in Dirichlet's theorem on simultaneous approximation of reals, when Q is an integer we can strengthen condition $|\alpha i - p_i/q| \leq 1/Qq$ by replacing it with a strict inequality.

Exercise 3 ($\star$)
Membership problem. Describe a polynomial time algorithm for the following problem: given an integer matrix $A \in \mathbb{Z}^{m \times n}$ and a vector $v \in \mathbb{Z}^m$, find an integral solution $x \in \mathbb{Z}^n$ to the system $Ax = v$, or deduce there exists none. Does the algorithm also work if we replace "$=$" with "$\leq$" (inequality on every row)?

Exercise 4
Certificate of non-membership. Prove that for $A \in \mathbb{Z}^{m \times n}$ and $v \in \mathbb{Z}^m$, the system $Ax = v$ has no integer solution $x \in \mathbb{Z}^n$ if and only if there is a vector $y \in \mathbb{R}^m$ such that $y^T A \in \mathbb{Z}^n$, but $y^T v \notin \mathbb{Z}$; and such a vector y can be found in polynomial time. (Hint: If $AU = [H|0]$ is the HNF of A, look for vector y in the rows of matrix H^{-1}.)

Exercise 5
Consider three points $v_1, v_2, v_3 \in Z^2$ not lying on the same line.

1. Prove that the triangle with vertices v_1, v_2, v_3 does not contain any other integer point besides its vertices, if and only if the matrix $[v_2 - v_1, v_3 - v_1]$ is unimodular.

2. Show that the previous statement cannot be extended to $\mathbb{R}^3$. I.e., provide four non-coplanar vectors v_1, v_2, v_3, v_4 such that the tetrahedron formed by these vectors as vertices does not contain any other integer points, but $\det[v_2 - v_1, v_3 - v_1, v_4 - v_1] \neq \pm 1$.

Exercise 6
Let P be a polygon in the plane with integer vertices (i.e. it is the convex hull of a finite set of point in $\mathbb{Z}^2$). Let A, I, B be respectively its area, the number of integer points in its interior, and the number of integer points in its boundary. Prove that $A = I + B/2 - 1$.

Exercise 7 ($\star$)
Implement the algorithm that computes the HNF of a given matrix (the standard one is fine, you do not need to implement the one that keeps coefficients bounded).

Exercise 8
Recall that Minkwoski's theorem implies an upper bound on $2 \cdot \sqrt[n]{\det(\Lambda)/V_n}$, where V_n is the volume of the unit ball in $\mathbb{R}^n$. Prove that this bound is aymptotically equivalent to $\sqrt{\frac{2n}{\pi e}} \det(\Lambda)^{1/n} (n\pi)^{1/2n}$.