Prof. Friedrich Eisenbrand
Alfonso Cevallos and Yuri Faenza

Discussions from: May 06, 2014

Computer Algebra

Spring 2014

Assignment Sheet 6

Exercises marked with a $\star$ can be handed in for bonus points. Due date is May 20.

Exercise 1

Let $B \in \mathbb{Z}^{n \times n}$ consists of parwise orthogonal vectors. Prove that a shortest non-zero vector of $\Lambda(B)$ is the column of B 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

Let $A \in \mathbb{Z}^{m \times n}$ be a matrix of full row rank. Let $A \cdot U = B$, where $U \in \mathbb{Z}^{n \times n}$ is unimodular and B is the HNF of A, i.e. $B = (H|0)$ where $H \in \mathbb{Z}^{m \times m}$ is a lower-diagonal matrix with nonnegative entries, where each row i has a unique maximum element, and this element is in column i. In class we observed that B can be computed in polynomial time. Show that also U can be computed in polynomial time.

Exercise 4 ($\star$)

Give a polynomial time algorithm for the following problem: given an integer matrix $A \in \mathbb{Z}^{m \times n}$ and a column vector $b \in \mathbb{Z}^{m \times n}$, find an integral solution to the system $Ax = b$, or deduce there exists none. Does the algorithm also work if we replace "=" with "≤"?

Exercise 5

Consider three points $v_1, v_2, v_3 \in \mathbb{Z}^2$ that do not lie on the same line.

a) Show the following: the triangle with vertices v_1, v_2, v_3 does not contain an integer point other than its vertices if and only if the matrix $(v_2 - v_1, v_3 - v_2)$ is unimodular.

b) Show that the previous statement cannot be extended to $\mathbb{R}^3$, providing linearly independent vectors v_1, v_2, v_3, v_4 such that $\text{conv}\{v_1, v_2, v_3, v_4\}$ does not contain an integer different from its vertices but $\det(v_2 - v_1, v_3 - v_1, v_4 - v_1) \neq \pm 1$.

Exercise 6
Let $v_1, \dots, v_n \in \mathbb{Z}^2$ and $P = \mathrm{conv}\{v_1, \dots, v_n\}$. Let A,I, and B be respectively the area, the number of integer points in the interior, and the number of integer points on the boundary of P. Prove that $A = I + B/2 - 1$.

Exercise 7 (⋆)
Implement the algorithm that computes the HNF of a given matrix (the standard one is ok, you do not need to implement the one that keep coefficients bounded).

Exercise 8
Recall that in class we showed that Minkwoski's theorem implies a bound on $2 \cdot \sqrt[n]{\det(\Lambda)/V_n}$ on the size of a shortest non-zero vector in a lattice. Prove that this bound is aymptotically equivalent to $\sqrt{\frac{2n}{\pi e}} \det(\Lambda)^{1/n} (n\pi)^{1/2n}$.

Exercise 9
Let
$$B = (b_1, \dots, b_{i-1}, b_i, b_{i+1}, b_{i+2}, \dots, b_n)$$
and
$$C = (b_1, \dots, b_{i-1}, b_{i+1}, b_i, b_{i+2}, \dots, b_n)$$
be two lattice bases. Notice that C originates from B via swapping the i-th and $i+1$-st column. Prove that B^* and C^* only differ in the i-th and $i+1$-st column. Show further that $\|b_i^*\| \cdot \|b_{i+1}^*\| = \|c_i^*\| \cdot \|c_{i+1}^*\|$ holds. What does this imply for $\det(B)$ and $\det(C)$?
(B^* and C^* are the output of the Gram-Schmidt process with input B and C, respectively.)

Exercise 10
Let p be an odd prime. Prove that $(p-1)! \equiv -1 \pmod{p}$.