Dr. Gennady Shmonin Due Date: March 3, 2009

Integer Points in Polyhedra

Spring 2009

Assignment Sheet 1

Exercise 1 (Euclidean algorithm)
Recall the Euclidean algorithm that computes the greatest common divisor of two integers $a \geq b \geq 0$:

while $b \neq 0$ **do**
  $r := a \bmod b$
  $a := b$; $b := r$
end while
output a

Prove that the Euclidean algorithm runs in time $O\big(\log(|a|+1) \cdot \log(|b|+1)\big)$; particularly, it is polynomial in the binary encoding length of a and b.

Exercise 2 (Hermite normal form)
Let Λ' be a sublattice of a lattice Λ. Given a basis B of Λ, show that there is a basis B' of Λ' such that $B' = BH$ with H being in Hermite normal form. Conversely, show that for any basis B' of Λ', there is a basis B of Λ such that $B = B'H'$, where H' is in Hermite normal form.

Exercise 3 (Hermite normal form)
Let A be an integral matrix of full row rank. Show that one can compute in polynomial time the unimodular matrix U such that $H = AU$, where H is a matrix in Hermite norml form.

Exercise 4 (Linear Diophantine equations)
Consider a system of linear Diophantine equations $Ax = b$, $x \in \mathbb{Z}^n$, where $A \in \mathbb{Z}^{m \times n}$ is a matrix and $b \in \mathbb{Z}^m$ is a vector.

(a) Prove that the system $Ax = b$ has an integral solution if and only if $y^{\mathrm{T}} b$ is an integer for all vectors y such that $y^{\mathrm{T}} A$ is integral.

(b) Show that if a system $Ax = b$ has an integral solution, then

$$\big\{x \in \mathbb{Z}^n : Ax = b\big\} = \Big\{x_0 + \sum_{i=1}^{k} \lambda_i x_i : \lambda_i \in \mathbb{Z},\, i = 1, 2, \ldots, k\Big\} \tag{1}$$

for some linearly independent vectors $x_1, x_2, \ldots, x_k \in \mathbb{Z}^n$, with $k = m - \operatorname{rank}(A)$.

(c) Show that the set of solutions (1) can be found in polynomial time.