Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Polyhedral Computation, Spring 2015
Solutions to Assignment 1

March 09, 2016

Problem 1 (Rational Numbers): Let $r = r_1/r_2$ and $s = s_1/s_2$ be two rational numbers.

1. Note that $r \times s = \frac{r_1 s_1}{r_2 s_2}$. Then,

$$\begin{aligned}
\text{size}(r \times s) &\leq 1 + \lceil \log(|r_1 s_1| + 1) \rceil + \lceil \log(|r_2 s_2| + 1) \rceil \\
&\leq 1 + \lceil \log((|r_1| + 1)(|s_1| + 1)) \rceil + \lceil \log((|r_2| + 1)(|s_2| + 1)) \rceil \\
&\leq 1 + \lceil \log(|r_1| + 1) \rceil + \lceil \log(|s_1| + 1) \rceil + \lceil \log(|r_2| + 1) \rceil + \lceil \log(|s_2| + 1) \rceil \\
&< \text{size}(r) + \text{size}(s)
\end{aligned}$$

2. Note that $r + s = \frac{r_1 s_2 + s_1 r_2}{r_2 s_2}$. Then,

$$\begin{aligned}
\text{size}(r + s) &\leq 1 + \lceil \log(|r_1 s_2 + s_1 r_2| + 1) \rceil + \lceil \log(|r_2 s_2| + 1) \rceil \\
&\leq 1 + \lceil \log(|r_1 s_2| + |s_1 r_2| + 1) \rceil + \lceil \log(|r_2| + 1) \rceil + \lceil \log(|s_2| + 1) \rceil \\
&\leq 1 + \lceil \log((|r_1 s_2| + 1)(|s_1 r_2| + 1)) \rceil + \lceil \log(|r_2| + 1) \rceil + \lceil \log(|s_2| + 1) \\
&\leq 1 + \lceil \log(|r_1| + 1) \rceil + 2\lceil \log(|s_2| + 1) \rceil + \lceil \log(|s_1| + 1) \rceil + 2\lceil \log(|r_2| + 1) \rceil \\
&< 2(\text{size}(r) + \text{size}(s))
\end{aligned}$$

   Note that the constant 2, can not be replaced by one. Consider for example the case where $r_1 = s_1 = s_2 = 1$ and r_2 arbitrary. Then one can check that

$$\begin{aligned}
\text{size}(r) &= \lceil \log(|r_2| + 1) \rceil + 2 \\
\text{size}(s) &= 3 \\
\text{size}(r + s) &= \text{size}\left(\frac{1 + r_2}{r_2}\right) \geq 2\,\text{size}(r) - 1
\end{aligned}$$

Problem 2 (Matrix Size): Let $s > k$ and $r \leq k$. We want to bound the size of $\hat{a}_{rs}$. We observe that

$$\begin{aligned}
\det \hat{A}_{K,K} &= \hat{a}_{rr} \det \hat{A}_{K \setminus \{r\}, K \setminus \{r\}}, \\
\det \hat{A}_{K, K \setminus \{r\} \cup \{s\}} &= \hat{a}_{rs} \det \hat{A}_{K \setminus \{r\}, K \setminus \{r\}}.
\end{aligned}$$

Therefore

$$\begin{aligned}\hat{a}_{rs} &= \frac{\det \hat{A}_{K,K\setminus\{r\}\cup\{s\}}}{\det \hat{A}_{K,K}} \cdot \hat{a}_{r,r} \\ &= \frac{\det A_{K,K\setminus\{r\}\cup\{s\}}}{\det A_{K,K}} \cdot \hat{a}_{r,r}.\end{aligned}$$

It follows from the proof of Theorem 2.4 in the lecture notes that

$$\text{size}(\hat{a}_{rs}) \leq \underbrace{\text{size}\left(\frac{\det A_{K,K\setminus\{r\}\cup\{s\}}}{\det A_{K,K}}\right)}_{<4\Delta} + \underbrace{\text{size}(\hat{a}_{r,r})}_{<4\Delta} < 8\Delta.$$

Problem 3 (Euclidean Algorithm): Let $a_i > b_i$ be the two positive integers arising in the i'th iteration. Note that $a_{i+1} = b_i$ and $b_{i+1} = a_i - \lfloor a_i/b_i \rfloor b_i$.

1. For each iteration i, the set of common divisor of (a_i, b_i) and (a_{i+1}, b_{i+1}) are the same. Secondly, we have $a_{i+1} = b_i < a_i$ and $b_{i+1} < b_i$, therefore the $\max\{a_i, b_i\}$ decreases with every iteration. Furthermore, the a_i and b_i stay non-negative. Thus, for some iteration k, we have to arrive at $a_k \geq 1$ while $b_k = 0$. By the fact that the set of common divisors is preserved, the a_k is the greatest common divisor of (a, b).

2. Observe that $b_{i+1} < a_i/2$ and $a_{i+1} = b_i$. In other words, $\text{size}(a_{i+1}) + \text{size}(b_{i+1})$ is strictly less than $\text{size}(a_i) + \text{size}(b_i)$ since

$$\begin{aligned}\text{size}(b_{i+1}) &= \lceil \log(b_{i+1} + 1) \rceil + 1 \\ &\leq \lceil \log\left(\frac{a_i}{2} - 1 + 1\right) \rceil + 1 \\ &\leq \lceil \log(a_i) - 1 \rceil + 1 \leq \text{size}(a_i).\end{aligned}$$

   Hence, the number of arithmetic operations of the Euclidean algorithm is in $O(\text{size}(a))$ which is asymptotically the same as $O(\log a)$. As the largest size of generated numbers is linear in the input size, the Euclidean algorithm runs in polynomial time.

Problem 4 (Hermite Normal Form): We are given the matrix

$$A = \begin{pmatrix} -4 & 6 & -6 & -6 \\ 6 & -3 & -9 & -3 \\ 4 & -3 & 9 & -3 \end{pmatrix}.$$

1. When applying the procedure from the script, one starts operating on the first row:

$$A_1 := AT_1 = A \begin{pmatrix} 1 & -3 & 3 & 3 \\ 1 & -2 & 3 & 3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & -12 & 0 & 6 \\ 1 & -6 & 12 & 0 \end{pmatrix}.$$

The procedure continues with the second row:

$$A_2 := A_1T_2 = A_1 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 6 & 0 & 0 \\ 1 & 0 & 12 & -6 \end{pmatrix}.$$

Finally, the result is:

$$\begin{bmatrix} B & \mathbf{0} \end{bmatrix} := A_2T_3 = A_2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 6 & 0 & 0 \\ 1 & 0 & 6 & 0 \end{pmatrix}.$$

The Hermite normal form $\begin{bmatrix} B & \mathbf{0} \end{bmatrix}$ is unique. The matrix B is a nonsingular and nonnegative lower triangular matrix with $b_{ii} > 0$ and $b_{ij} < b_{ii}$ for all rows i and columns $j < i$.

2. As the inverse of a lower triangular matrix is also lower triangular, the inverse of B

$$B^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{4} & \frac{1}{6} & 0 \\ -\frac{1}{12} & 0 & \frac{1}{6} \end{pmatrix}$$

can be computed by hand. To check feasibility of the given equation systems we compute

$$B^{-1}b = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{4} & \frac{1}{6} & 0 \\ -\frac{1}{12} & 0 & \frac{1}{6} \end{pmatrix} \begin{pmatrix} 0 \\ 12 \\ 18 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix} \text{ and } B^{-1}b' = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{4} & \frac{1}{6} & 0 \\ -\frac{1}{12} & 0 & \frac{1}{6} \end{pmatrix} \begin{pmatrix} 4 \\ 6 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ \frac{1}{6} \end{pmatrix}.$$

The only equation system allowing an integral solution is $Ax = b$. For the other, the vector

$$z = \begin{pmatrix} -\frac{1}{12} \\ 0 \\ \frac{1}{6} \end{pmatrix}$$

is a certificate proving infeasibility. According to Corollary 2.6, any rational vector z for which $z^T A =$ is integral and $z^T b$ is fractional proves infeasibility.

3. The transformation matrix is

$$T := T_1 T_2 T_3 = \begin{pmatrix} 1 & 3 & -3 & 9 \\ 1 & 3 & -4 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -2 & 4 \end{pmatrix}.$$

4. Every vector

$$x = T \begin{bmatrix} B^{-1}b \\ z \end{bmatrix} = \begin{pmatrix} -3+9z \\ -6+11z \\ z \\ -4+4z \end{pmatrix}$$

where z is an integral vector in $\mathbb{Z}^{n-m}$ is a solution to the equation system $Ax = b$.

Problem 5 (Lattice Basis):

1. Since the columns of B build a basis of $L(A)$, we can write each column of B' as an integer linear combination of columns in B, that is, $B' = BT$ for some integer matrix $T \in \mathbb{R}^{m\times m}$. Then $|\det(B')|$ equals $|\det(B)| \cdot |\det(T)|$, and as both B and B' are non-singular, the absolute value $|\det(T)|$ is non-zero. As T is integral, the determinant $\det(T)$ is also integral and $|\det(T)| \geq 1$ accordingly. The inequality $|\det(B)| \leq |\det(B')|$ immediately follows.

2. Once the statement in a) is proved, the "only if" direction immediately follows. Suppose B' is a basis, and observe that the columns of both B and B' represent points in the lattice. Applying a) twice implies $|\det(B)| \leq |\det(B')|$ and $|\det(B')| \leq |\det(B)|$. For the "if" direction, we assume that $|\det(B)| = |\det(B')|$ and recall $B' = BT$ for some integer matrix T. Therefore $|\det(T)| = 1$, that is, the matrix T is unimodular. The inverse of a unimodular matrix is again unimodular, therefore T^{-1} is integral with $|\det(T^{-1})| = 1$. Since $B = B'T^{-1}$, the basis B can be expressed as a integer linear combination of columns in B', that is, B' is a basis, too.