Exercise 3: Magistral classes

Manuel Leiva

While proving the cost of the extended euclids algorithm when our ring of domain $R = \mathbb{Z}$. it remained to prove that $|s_i| \leq g/r_{i-1}$ and $|t_i| \leq f/r_{i-1}$.

Proof:

First of all, let us prove the following:

Proposition 1 Let $f, g \in \mathbb{Z}$ $f > g > 0$ inputs for the extended euclidean algorithm, then s_i and t_i alternate in sign such that $s_{2i}, t_{2i-1} > 0$ and $s_{2i+1}, t_{2i} < 0$ $\forall i \geq 1$.

Proof: Induction on i.

- Base case ($i = 1$): $s_2 = s_0 - q_1 s_1 = 1 > 0$

$$s_3 = s_1 - q_2 s_2 = -q_2 < 0 \quad ✓$$

- General case: Assume that holds for $i-1$. Therefore, $s_{2(i-1)} > 0$, $s_{2(i-1)+1} < 0$. and since all quotients are positive,

$$s_{2i} = s_{2(i-1)} - q_{2i-1} s_{2i-1} = \overset{>0}{s_{2(i-1)}} - \overset{>0}{q_{2(i-1)+1}} \overset{<0}{s_{2(i-1)+1}} > 0$$

$$s_{2i+1} = \underset{<0}{s_{2(i-1)+1}} - \overset{>0}{q_{2i}} \overset{>0}{s_{2i}} < 0$$

An analogous procedure can be used to prove that $t_{2i} < 0$ and $t_{2i-1} > 0$.

- Base case ($i=1$) $t_2 = \overset{=0}{t_0} - q_1 \overset{=1}{t_1}$ since $q_1 > 0 \Rightarrow t_2 = -q_1 < 0$

$$t_3 = t_1 - q_2 t_2$$
$$= 1 - q_2(-q_1) = 1 + q_2 q_1 > 0.$$

- General case

$$t_{2i} = \underset{<0 \text{ hypoth.}}{t_{2(i-1)}} - \underset{>0}{q_{2(i-1)+1}} \underset{>0 \text{ hypoth.}}{t_{2(i-1)+1}} < 0$$

$$t_{2i+1} = \underset{>0 \text{ hypoth}}{t_{2(i-1)+1}} - q_{2i} \underset{<0 \text{ hypoth}}{t_{2i}} > 0$$

□

Secondly, let us prove the following

Prop2 $f = (-1)^i (t_{i+1} r_i - t_i r_{i+1})$, $g = (-1)^{i+1} (s_{i+1} r_i - s_i r_{i+1})$

From vi) of the previous magistral class exercise we got that $\det R_i = (-1)^i$ and in particular, then R_i was invertible.

Therefore, since $R_i \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$, $\Rightarrow \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = R_i^{-1} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = (-1)^i \begin{pmatrix} t_{i+1} & -t_i \\ -s_{i+1} & s_i \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$

by ii) and v) of the same exercise.

Thus
$$\left.\begin{aligned} f &= (-1)^i \cdot (t_{i+1} r_i - t_i r_{i+1}) \\ g &= (-1)^{i+1} (s_{i+1} r_i - s_i r_{i+1}) \end{aligned}\right\}$$ observe using prop 1 that f and $g > 0$ as expected

At this point, we are able to state the following.

$$\underset{\substack{\uparrow \\ \text{by prop 2} \\ \text{and prop 1}}}{f} = |t_i r_{i-1} - t_{i-1} r_i| \underset{\substack{\uparrow \\ \text{by prop 1} \\ \text{sign}(t_{i-1}) = -\text{sign}(t_i)}}{=} |t_i| r_{i-1} + |t_{i-1}| r_i \geq |t_i| r_{i-1}. \rightarrow |t_i| \leq f/r_{i-1}.$$

Same for g.

$$g = |r_{i-1} s_i - r_i s_{i-1}| = r_{i-1}|s_i| + r_i|s_{i-1}| \geq r_{i-1}|s_i|. \rightarrow |s_i| \leq g/r_{i-1}$$