Manuel Leda

Exercise 3: Magistral classes

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

$$s_3 = s_1 - q_2 s_2 = -q_2 < 0$$

- 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 $q_1 > 0 \Rightarrow t_2 = -q_1 < 0$

$$t_3 = \underset{=1}{t_1} - q_2 t_2 = 1 - q_2(-q_1) = 1 + q_2 q_1 > 0.$$

- General case:

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

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

□

Moreover, recall that from the previous magistral class exercise, that $\gcd(r_i, t_i) = \gcd(f, t_i)$

Therefore, $f = |r_{i-1} t_i - r_i t_{i-1}|$ by the prop above, $= r_{i-1}|t_i| + r_i|t_{i-1}| \geq r_{i-1}|t_i| \to |t_i| \leq f/r_{i-1}$

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

for $1 \leq i \leq l+1$

■