Math 240: Midterm 2 Q6d

Daniel Ko

Spring 2020

Given positive integers a and b, we want to compute some integers s and t such that

$$\gcd(a, b) = sa + tb$$

Consider the following iterative program LIN_COMB (a, b) which is supposed to accomplish this:

Initialize variables $c = a$, $d = b$, $s_0 = 1$, $t_0 = 0$, $s_1 = 0$, $t_1 = 1$

While $c \neq d$, do the following:

If $c < d$, then decrement d by c, decrement s_1 by s_0, decrement t_1 by t_0

Else if $c > d$, then decrement c by d, decrement s_0 by s_1, decrement t_0 by t_1

Return s_0 and t_0

§1 6d

Use the well-ordering principle and (c) to prove that LIN_COMB satisfies termination.

Proof. We prove that LIN_COMB terminates. Let c_n and d_n represent the values of c and d after n iterations respectively. Consider the following two cases

1. $a = b$

   The algorithm terminates because $a = b = c = d$.

2. $a \neq b$

   Let c_n and d_n represent the values of c and d after n iterations respectively. Suppose at the nth iteration, $c_n \neq d_n$. Regardless of the values of c_n and d_n, we can observe that $c_{n+1} + d_{n+1} \leq c_n + d_n - 1$. This is because of the following statements. If $c_n > d_n$, then $c_{n+1} = c_n - d_n$. If $c_n < d_n$, then $d_{n+1} = d_n - c_n$. In (c) we have proved that $(c > 0) \wedge (d > 0)$ is a loop invariant. This necessarily implies that $c_{n+1} \leq c_n - 1$ or $d_{n+1} \leq d_n - 1$. So in either case, the sum of c_{n+1} and d_{n+1} will be at least one less the sum of c_n and d_n.

   By the well ordering principle, since $c_n + d_n$ is strictly decreasing, there be an iteration s such that $c_s + d_s$ is the smallest sum which is bounded by $(c > 0) \wedge (d > 0)$. When this is the case, $c_s = d_s$ because if $c_s \neq d_s$, then you can once again decrement c by d_s or d by c_s and this will lead to a contradiction. Thus, the algorithm terminates if $a \neq b$.

Therefore, LIN_COMB satisfies termination.

□