Math 240: Midterm 2 Q6a

Daniel Ko

Spring 2020

§1 6a

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

Prove that $(c = s_0a + t_0b) \wedge (d = s_1a + t_1b)$ is a loop invariant for the while loop in LIN_COMB.

Proof. Let $P(n)$ be the predicate asserting that if the while loop has run for n iterations, then $(c = s_0a + t_0b) \wedge (d = s_1a + t_1b)$. Domain: $\mathbb{N}$. We prove by induction that for all k, $P(k)$ holds.

Base case: Before any iteration of the loop: $c = a, d = b, s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$.

$$\begin{aligned} c &= s_0a + t_0b \\ &= 1c + 0d \\ &= c \end{aligned}$$

$$\begin{aligned} d &= s_1a + t_1b \\ &= 0c + 1d \\ &= d \end{aligned}$$

Hence, $P(0)$ holds as desired.

Inductive step: Suppose that $n \in N$ such that $P(n)$ holds. We prove that $P(n + 1)$ holds.

Suppose the loop has run for $n + 1$ iterations. Let $c', d', s_0', t_0', s_1', t_1'$ be the value of the variables after the loop has run for n iterations. Now we consider what happens in the $(n + 1)^{th}$ iteration.

i. Case 1: $c' < d'$

$$\begin{aligned} c &= c' \\ d &= d' - c' \\ s_0 &= s_0' \\ t_0 &= t_0' \\ s_1 &= s_1' - s_0' \\ t_1 &= t_1' - t_0' \end{aligned}$$

By our induction hypothesis, we know that $c' = s_0'a + t_0'b$ and $d' = s_1'a + t_1'b$. Thus,

$$\begin{aligned} c &= c' \\ &= s_0'a + t_0'b \\ &= s_0a + t_0b \end{aligned}$$

$$\begin{aligned} d &= d' - c' \\ &= s_1'a + t_1'b - (s_0'a + t_0'b) \\ &= s_1'a + t_1'b - s_0'a - t_0'b \\ &= (s_1' - s_0')a + (t_1' - t_0')b \\ &= s_1a + t_1b \end{aligned}$$

as desired. So $P(n+1)$ holds for when $c' < d'$.

ii. Case 2: $c' > d'$

$$\begin{aligned} c &= c' - d' \\ d &= d' \\ s_0 &= s_0' - s_1' \\ t_0 &= t_0' - t_1' \\ s_1 &= s_1' \\ t_1 &= t_1' \end{aligned}$$

By our induction hypothesis, we know that $c' = s_0'a + t_0'b$ and $d' = s_1'a + t_1'b$. Thus,

$$\begin{aligned} c &= c' - d' \\ &= s_0'a + t_0'b - (s_1'a + t_1'b) \\ &= s_0'a + t_0'b - s_1'a - t_1'b \\ &= (s_0' - s_1')a + (t_0' - t_1')b \\ &= s_0a + t_0b \end{aligned}$$

$$\begin{aligned} d &= d' \\ &= s_1'a + t_1'b \\ &= s_1a + t_1b \end{aligned}$$

as desired. So $P(n+1)$ holds for when $c' > d'$.

This proves the inductive step. By induction, we conclude that $P(n)$ holds for all $n \in \mathbb{N}$ which makes it an loop invarient for LIN_COMB.

$\square$