# Math 240: Midterm 2 Q6bc

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 6b

Assume, in addition to (a), that $gcd(a, b) = gcd(c, d)$ is a loop invariant for the while loop in LIN_COMB. Prove that LIN_COMB satisfies partial correctness.

*Proof.* Suppose that LIN_COMB halts. Fix $n \in \mathbb{N}$ such that exactly $n$ iterations of the while loop are executed. Consider the values of $c, d, s_0, t_0$ after the $n$th iteration. Since the $(n + 1)$th iteration is not executed, the loop condition fails, which means $c = d$. This must mean that $gcd(c, d) = c = d$. Moreover, $gcd(a, b) = c$ by the given loop invariant. From (a), we know $(c = s_0 a + t_0 b) \wedge (d = s_1 a + t_1 b)$ is a loop invarient. Since $\gcd(a, b) = c = s_0 a + t_0 b$, we get the correct output. □

## §2 6c

Prove that $(c > 0) \wedge (d > 0)$ is a loop invariant for the while loop in LIN_COMB.

*Proof. Proof.* Let $P(n)$ be the predicate asserting that if the while loop has run for $n$ iterations, then $(c > 0) \wedge (d > 0)$ . Domain: $\mathbb{N}$. We prove by induction that for all $k$, $P(k)$ holds.
**Base case:** Before any iteration of the loop: $c = a$ and $d = b$. $a$ and $b$ are positive integers by definition. Hence, $P(0)$ holds as desired.
**Inductive step:** Suppose that $n \in \mathbb{N}$ 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: $c' < d'$

$$c = c'$$
$$d = d' - c'$$

By our induction hypothesis, we know that $c' > 0$, so $c > 0$ holds. Since $c' < d'$ and $c' > 0$, so $d' - c' > 0$. Because $d = d' - c'$, this means that $d > 0$ holds. Thus, $P(n+1)$ holds for when $c' < d'$.

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

$$c = c' - d'$$
$$d = d'$$

By our induction hypothesis, we know that $d' > 0$, so $d > 0$ holds. Since $c' > d'$ and $d' > 0$, so $c' - d' > 0$. Because $c = c' - d'$, this means that $c > 0$ holds. Thus, $P(n+1)$ 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.

$\square$

$\square$