Math 240: Homework 6

Daniel Ko

Spring 2020

§1 1

a. Prove that the above algorithm satisfies partial correctness.

Proof. Let p be the proposition $a = dq + r \wedge r \geq 0$.
Let's prove that p is the loop invarient by induction.

i. Base case: When the loop condition is tested for the first time, p holds

$r = a$ and $q = 0$ before the loop is run. When the loop condition is first tested $a = dq + r$ holds because $q = 0$, so $a = 0 + r = r$.
$r \geq 0$ also holds because $a \in \mathbb{N}$.

ii. Inductive step: If p and the loop condition both hold at the beginning of an iteration of the loop, then p holds right after said iteration

Let $a = dq + r \wedge r \geq 0$ at some $n - 1$ iteration of the loop (inductive hypothesis). Let r_n and q_n be the value of r and q at the nth iteration respectively.
So at the nth iteration, $a = dq_n + r_n$. We know $q_n = q + 1$ and $r_n = r - d$.

$$\begin{aligned} a &= dq_n + r_n \\ &= d(q + 1) + r - d \\ &= dq + d + r - d \\ &= dq + r \end{aligned}$$

We know that $r_n = r - d$. Our loop condition is $r \geq d$, thus $r_n \geq 0$.

Therefore, p is a loop invarient.
Now we must show that loop invariant holds and the loop condition fails, then the output is correct. Suppose the loop halts at the nth iteration, which is when $r < d$. By our loop invarient, we have that $r \geq 0$. Combining the two statements above, we get $0 \leq r < d$. Also by our loop invariant, we have $a = dq + r$. Therefore, this algorithm satisfies partial correctness. □

b. Prove that the above algorithm satisfies termination.

Proof. Our termination condition is $r < d$. r is set to a then decreases by d after each iteration. Since $d \in \mathbb{N}$, the sequence of the values of r is strictly decreasing. We also know that $r \geq 0$ by our loop invarient. Therefore, by the well-ordering principle, the algorithm satisfies termination. □

§2 2

Prove that for all $n \in \mathbb{N}$, SQ(n) halts and returns n^2.

Proof. We proceed by strong induction on n. Let P(n) be the predicate "SQ(n) halts and returns n^2". Domain: $\mathbb{N}$.

a. Base case:
   We prove P(0). Observe that P(0) halts and returns 0, which is equal to 0^2.

b. Inductive step:
   Suppose $n \in \mathbb{N}$ and P holds for all integers between 0 and n, inclusive. We show that P($n+1$) holds.

$$\begin{aligned} \mathrm{SQ}(n+1) &= \mathrm{SQ}(n-1) + 2n - 1 \\ &= (n-1)^2 + 2n - 1 && \text{(Strong inductive hypothesis)} \\ &= n^2 - 2n + 1 + 2n - 1 \\ &= n^2 \end{aligned}$$

   By the strong inductive hypothesis P($n-1$), SQ($n-1$) halts. Thus, SQ($n+1$) halts.

Therefore, by strong induction we have proved that for all $n \in \mathbb{N}$, SQ(n) halts and returns n^2. □

§3 3

Prove that POW is correct.

Proof. We proceed by strong induction on $b \in \mathbb{N}$. Let $P(b)$ be the following predicate "$POW(a, b)$ halts and returns a^b, where a is a fixed nonzero integer".

a. Base case:
   We prove $P(0)$. $POW(a, 0) = 1$. Observe that P(0) halts and returns 1, which is equal to a^0.

b. Inductive step:
   Suppose $n \in \mathbb{N}$ and P holds for all integers between 0 and n, inclusive. We show that P($n+1$) holds.
   Case 1: $n+1$ is odd

$$\begin{aligned} POW(a, n+1) &= a \cdot (POW(a, \lfloor (n+1)/2 \rfloor))^2 \\ &= a \cdot (a^{\lfloor (n+1)/2 \rfloor})^2 && \text{(Strong inductive hypothesis)} \\ &= a \cdot (a^{n/2})^2 && \text{(n is even)} \\ &= a \cdot a^n \\ &= a^{n+1} \end{aligned}$$

   We know that ($POW(a, \lfloor (n+1)/2 \rfloor)$) halts by our strong induction hypothesis so $POW(a, n+1)$ halts as well.

Case 2: if $n+1>0$ and $n+1$ is even

$$\begin{aligned}
POW(a, n+1) &= (POW(a, \lfloor (n+1)/2 \rfloor))^2 \\
&= (a^{\lfloor (n+1)/2 \rfloor})^2 && \text{(Strong inductive hypothesis)} \\
&= (a^{(n+1)/2})^2 && \text{(n + 1 is even)} \\
&= a^{n+1}
\end{aligned}$$

We know that $(POW(a, \lfloor (n+1)/2 \rfloor))$ halts by our strong induction hypothesis so $POW(a, n+1)$ halts as well.
Therefore, by strong induction we have proved that POW is correct.

$\square$