Problem Set 4

XUANQI WEI
10093533209

Q1

(a). Assume the precondition is true, which $x_0 \in \mathbb{R}$, $y_0 \in \mathbb{N}$. where x_0, y_0 are the inputs.

I'll set the loop invariant be $z_k \cdot x_k^{y_k} = x_0^{y_0} \wedge y_k \in \mathbb{N}$ where $y_0, k \in \mathbb{N}$. k represents the number of iterations of the loop and z is a variable in program.

Assume L.I. holds; Assume the loop terminates

I'll prove the partial correctness.

WTS: Post (x, y), which the function will return $x_0^{y_0}$ and return 1 if $x_0 = y_0 = 0$.

Since the loop stops, gives $y \leq 0$.

Since $y \in \mathbb{N}$. gives $y \geq 0$. which $y = 0$.

From Loop Invariant, gives. $z_k x_k^{\,0} = x_0^{y_0}$. (Since $x_k^{\,0} = 1$.).

$$\Rightarrow \quad z_k = x_0^{y_0}$$

I've shown that the function returns z_k which equals $x_0^{y_0}$ as needed.

I've shown the function is partially correct. ■

(b). Assume the precondition is true, which $x_0 \in \mathbb{R}$, $y_0 \in \mathbb{N}$. where x_0, y_0 are the inputs.

I'll set the loop invariant be $z_k \cdot x_k^{y_k} = x_0^{y_0} \wedge y_k \in \mathbb{N}$ where $k \in \mathbb{N}$. k represents the number of iterations of the loop and z is a variable in program. same as (a).

I'll prove by simple induction on k. where $k \in \mathbb{N}$.

Base Case: $k = 0$.

When $k = 0$, we haven't entered the loop. which $z_k = z_0 = 1$.

Thus $z_k x_k^{y_k} = z_0 \cdot x_0^{y_0} = 1 \cdot x_0^{y_0} = x_0^{y_0}$.

I've shown L.I is true when $k=0$.

Inductive Step: Let $k \in \mathbb{N}$. $k > 0$.

Inductive Assumption: Assume L.I.$_k$ holds and there are at least $(k+1)$ iterations, which $z_k x_k^{y_k} = x_0^{y_0} \wedge y_k \in \mathbb{N}$.

WTS: L.I.$_{k+1}$ holds, which $z_{k+1} x_{k+1}^{y_{k+1}} = x_0^{y_0} \wedge y_{k+1} \in \mathbb{N}$.

① When y_k is odd.

Since y_k is odd, gives $y_k \% 2 == 1$. which, from line 5. $z_{k+1} = z_k \cdot x_k$.

From line 6. $x_{k+1} = x_k^2$.

Since y_k is odd. $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor = \frac{y_k - 1}{2}$.

Thus, $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = z_k \cdot x_k \cdot (x_k^2)^{\frac{y_k - 1}{2}} = z_k \cdot x_k \cdot (x_k)^{y_k - 1} = z_k \cdot x_k^{y_k} = x_0^{y_0}$, by I.H.

② When y_k is even

Since y_k is even, gives $y_k \% 2 == 0$. which, it doesn't go into 'if' branch, we obtain that $z_{k+1} = z_k$

From line 6. $x_{k+1} = x_k^2$.

Since y_k is even, $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor = \frac{y_k}{2}$.

Thus, $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = z_k \cdot (x_k^2)^{\frac{y_k}{2}} = z_k \cdot x_k^{y_k} = x_0^{y_0}$ (by I.H.)

From Line 7, gives $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor$, as $k+1$-th iteration executes.

Since $y_k \in \mathbb{N}$, gives $\frac{y_k}{2} \geq 0$, from definition of floor operation. $\lfloor \frac{y_k}{2} \rfloor \geq 0$, $\lfloor \frac{y_k}{2} \rfloor \in \mathbb{Z}$, gives $y_{k+1} \in \mathbb{N}$.

Therefore, I've shown $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = x_0^{y_0}$, which L.I.$_{k+1}$ holds.

■

(c). Loop Variant for Pow is y, which $v = y$.

WTS: L.V. is correct and function terminates.

① L.V. is correct.

WTS: $v \in \mathbb{N}$ at the beginning of each iteration

From (b). I've shown that $y_0 \in \mathbb{N}$ and if there're at least $k+1$ iterations, $\forall k \in \mathbb{N}$. $y_k \in \mathbb{N}$. which $v = y$ is always a natural number at the start of

each iteration, which is correct.

② Function Terminates.

WTS: If there're at least $k+1$ iterations, $v_{k+1} < v_k$.

Let $k \in \mathbb{N}$.

Assume there're at least $k+1$ iterations.

From (b), Since $\forall k \in \mathbb{N}$. $y_k \in \mathbb{N}$, $v_k \in \mathbb{N}$;

Since $y_k \geq 0$ as $k+1$-th iteration exists. $y_k > \frac{y_k}{2} \geq \lfloor \frac{y_k}{2} \rfloor = y_{k+1}$. which.

$\forall k \in \mathbb{N}$. $v_k = y_k > y_{k+1} = v_{k+1}$.

Take set $S = \{ v_k \in \mathbb{N} : v_k = y_k \wedge y_{k+1} = \lfloor \frac{y_k}{2} \rfloor \}$, we obtain that $S \neq \emptyset$.

Since $S \subseteq \mathbb{N}$, from WOP, there exist a minimum value v_k' in the set which the function terminates

■

(d). The Precondition: $x \in \mathbb{R}$. $y \in \mathbb{N}$.

The Postcondition: return x^y (return 1 if $x = y = 0$).

The Loop Invariant: $z_k \cdot x_k^{y_k} = x_0^{y_0} \wedge y_k \in \mathbb{N}$ where $k \in \mathbb{N}$, k represents the number of iterations of the loop and z is a variable in program. same as (a).

WTS: If Precondition holds, L.I. holds, Function terminates. then postcondition holds.

① L. V. holds.

Will prove by simple induction on k. where $k \in \mathbb{N}$.

Base Case: $k = 0$.

When $k = 0$, we haven't entered the loop. which $z_k = z_0 = 1$.

Thus $z_k x_k^{y_k} = z_0 \cdot x_0^{y_0} = 1 \cdot x_0^{y_0} = x_0^{y_0}$.

I've shown L.I is true when $k = 0$.

Inductive Step: Let $k \in \mathbb{N}$. $k > 0$.

Inductive Assumption: Assume L.I. k holds and there are at least $(k+1)$ iterations, which $z_k x_k^{y_k} = x_0^{y_0} \wedge y_k \in \mathbb{N}$.

WTS: L.I. $k+1$ holds, which $z_{k+1} x_{k+1}^{y_{k+1}} = x_0^{y_0} \wedge y_{k+1} \in \mathbb{N}$.

① When y_k is odd.

Since y_k is odd, gives $y_k \% 2 == 1$. which, from line 5, $z_{k+1} = z_k \cdot x_k$.

From line 6, $x_{k+1} = x_k^2$.

Since y_k is odd, $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor = \frac{y_k - 1}{2}$.

Thus, $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = z_k \cdot x_k \cdot (x_k^2)^{\frac{y_k - 1}{2}} = z_k \cdot x_k \cdot (x_k)^{y_k - 1} = z_k \cdot x_k^{y_k} = x_0^{y_0}$, by l.H.

② When y_k is even

Since y_k is even, gives $y_k \% 2 == 0$. which, it doesn't go into 'if' branch, we obtain that $z_{k+1} = z_k$

From line 6, $x_{k+1} = x_k^2$.

Since y_k is even, $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor = \frac{y_k}{2}$.

Thus, $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = z_k \cdot (x_k^2)^{\frac{y_k}{2}} = z_k \cdot x_k^{y_k} = x_0^{y_0}$ (by l.H.)

From Line 7, gives $y_{k+1} = \lfloor \frac{y_k}{2} \rfloor$, as $k+1$-th iteration executes.

Since $y_k \in \mathbb{N}$, gives $\frac{y_k}{2} \geq 0$, from definition of floor operation. $\lfloor \frac{y_k}{2} \rfloor \geq 0$, $\lfloor \frac{y_k}{2} \rfloor \in \mathbb{Z}$, gives $y_{k+1} \in \mathbb{N}$.

Therefore, I've shown $z_{k+1} \cdot x_{k+1}^{y_{k+1}} = x_0^{y_0}$, which L.I.$_{k+1}$ holds.

Therefore. I've shown L.V. holds.

② Loop variant is correct and function terminates.

Loop Variant for Pow is y, which $v = y$.

WTS: L.V. is correct and function terminates.

① L.V. is correct.

WTS: $v \in \mathbb{N}$ at the beginning of each iteration

From (b). I've shown that $y_0 \in \mathbb{N}$ and if there're at least $k+1$ iterations, $\forall k \in \mathbb{N}$. $y_k \in \mathbb{N}$. which $v = y$ is always a natural number at the start of each iteration, which is correct.

② Function Terminates.

WTS: If there're at least $k+1$ iterations, $v_{k+1} < v_k$.

Let $k \in \mathbb{N}$.

Assume there're at least $k+1$ iterations.

From (b), Since $\forall k \in \mathbb{N}$. $y_k \in \mathbb{N}$, $v_k \in \mathbb{N}$;

Since $y_k \geq 0$ as $k+1$-th iteration exists. $y_k > \frac{y_k}{5} \geq \lfloor \frac{y_k}{5} \rfloor = y_{k+1}$. which.

$\forall k \in \mathbb{N}$. $v_k = y_k > y_{k+1} = v_{k+1}$.

Take set $S = \{ v_k \in \mathbb{N} : v_k = y_k \wedge y_{k+1} = \lfloor \frac{y_k}{5} \rfloor \}$, we obtain that $S \neq \emptyset$.

Since $S \subseteq \mathbb{N}$. from WOP. there exist a minimum value $v_{k'}$ in the set which the function terminates

Therefore, the function is correct. ■