Ramya Krishnan
A20506653

1. Minimal and Full Proof outlines

Task 1.1

$\{n \geq 0\}$

$i := 0;$ $\quad\{n \geq 0 \wedge i = 0\}$ — ①

$\{inv\ i \leq n \wedge n = i!\}$

while $i < n$ do $\quad\{i \leq n \wedge n = i! \wedge i < n\}$ — ②

$n := n * i$ $\quad\{(i+1) \leq (n * i) \wedge (n * i) = (i+1)!\}$

$i := i + 1$ $\quad\{(i+1) \leq n \wedge n = (i+1)!\}$

od $\quad\{i \leq n \wedge n = i!\}$

$\{i \leq n \wedge n = i! \wedge i \geq n\}$ — ③

$\{\exists k.\ n = k!\}$

With this, when we apply the algorithm, we have proof obligation at three places where we can proof one.

1. $i = 0 \wedge n \geq 0 \Rightarrow i \leq n \wedge n = i!$ ⇒ (Not provable)

The assumption $n \geq 0$ does not directly imply $i!$ or the relationship b/n i & n. we need additional info to prove that.

2. $i \leq n \wedge n = i! \wedge i < n \Rightarrow (i+1) \leq (n * i) \wedge (n * i) = (i+1)!$

(Not provable)

Here again, the transition from $i!$ to $(i+1)!$ which could be less than $(n * i)$ can not be ~~proved~~ proved without more information on i & n.

3. $i \le n \wedge n = i! \wedge i \ge n \Rightarrow \exists_k . n = k! \Rightarrow$ (Provable)

Here based on first conditions n is 1 since it satisfies all and there exists k where $k!$ is equal to n (1). Hence it is provable.

Task 1.2

$\{n \ge 0\}$

i := 0; $\{n \ge 0 \wedge i = 0\}$

r := 1; $\{n \ge 0 \wedge i = 0 \wedge r = 1\}$

while i < n do

$\{i \le n \wedge r = i! \wedge i < n\}$

i := i+1; $\{(i+1) \le n \wedge (r * (i+1)) = (i+1)!\}$

r := r * i $\{i \le n \wedge (r * i) = i!\}$

od $\{i \le n \wedge r = i!\}$

$\{i \le n \wedge r = i! \wedge i \ge n\}$

$\{r = n!\}$

With this we have proof obligation in three places where we can prove all.

1. $n \geq 0 \wedge i = 0 \wedge r = 1 \Rightarrow i \leq n \wedge r = i!$ $\Rightarrow$ (Provable)

The assumption $n \geq 0$, $i = 0$ and $r = 1$ directly imply $i \leq n$ and $r = i!$. Hence it is provable.

2. $i \leq n \wedge r = i! \wedge i < n \Rightarrow (i+1) \leq n \wedge (r * (i+1) = (i+1)!)$

(Provable)

The assumption $i \leq n$, $r = i!$ and $i < n$ imply the conclusion $(i+1) \leq n \wedge (r * (i+1) = (i+1)!)$ based on proof obligation $i \leq n \wedge r = i! \wedge i \geq n \Rightarrow r = n!$

3. $i \leq n \wedge r = i! \wedge i \geq n \Rightarrow r = n!$ $\Rightarrow$ (Provable)

when i is less than or equal to n and the factor of $i = r$ and $i \geq n$ that directly implies $r = x!$

Hence it is provable.

And the program calculates $n!$ and satisfies the given pre and post condition.

2. Proofs with loops.

Task 2.1, 2.2

Attached the dfy program.

3. It took me 4-5 hours excluding the lecture.