Functional Programming and Verification

Prof. Dr. H. Seidl, N. Hartmann, R. Vogler
WS 2018/19

Exercise Sheet 3
Deadline: 11.11.2018

General Information

Detailed information about the lecture, tutorials and homework assignments can be found on the lecture website[1]. Solutions have to be submitted to Moodle[2]. Make sure your uploaded documents are readable. Blurred images will be rejected. Use Piazza[3] to ask questions and discuss with your fellow students.

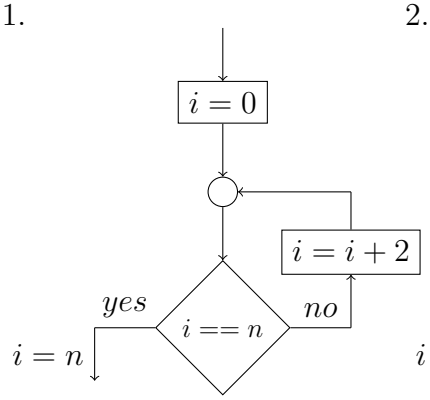
Loop Invariants

In this exercise sheet, you will discuss and practice different strategies to find suitable loop invariants. For additional insight, tips and tricks on how to find a good invariant, we recommend watching the recording of last year's exercise on this particular topic[4].

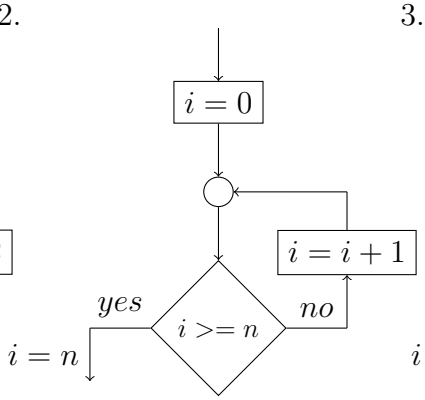
Assignment 3.1 (L) Individual Loops

Inspect the following loops and discuss the preconditions that have to hold, such that the assertion $i = n$ is satisfied. In particular, discuss the results for positive and negative inputs, respectively.

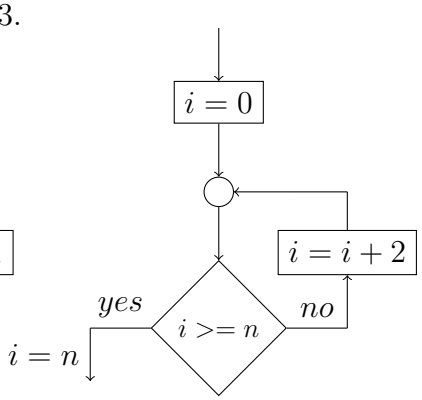
1.



2.



3.



Suggested Solution 3.1

1. In the first case, the assertion follows from the loop condition, immediately. Regardless of what is true before or within the loop, whenever the loop is left, $i = n$ holds. For $n < 0$ the loop does not terminate. However, this does not violate the assertion!

[1] https://www.in.tum.de/i02/lehre/wintersemester-1819/vorlesungen/functional-programming-and-verification/
[2] https://www.moodle.tum.de/course/view.php?id=44932
[3] https://piazza.com/tum.de/fall2018/in0003/home
[4] http://ttt.in.tum.de/recordings/Info2_2017_11_24-1/Info2_2017_11_24-1.mp4

Same holds for $n \not\equiv 0 mod 2$. Thus $true$ is a sufficient precondition:

$$\begin{aligned} & \mathsf{WP}[\![\texttt{i == n}]\!](true, i = n) \\ \equiv\ & (i \neq n \implies true) \wedge (i = n \implies i = n) \\ \equiv\ & true \end{aligned}$$

2. Intuitively, we recognize that the loop terminates when i reaches n and thus $i = n$ holds. However, for $n < 0$, the situation is different. In this case the exit of the loop is reached immediately with $i \neq n$. In order to exclude these runs of the program, we have to make sure that $n \geq 0$ (or more generally $n \geq i$) holds before the loop:

$$\begin{aligned} & \mathsf{WP}[\![\texttt{i = i + 1}]\!](n \geq i) \\ \equiv\ & n \geq i + 1 \end{aligned}$$

$$\begin{aligned} & \mathsf{WP}[\![\texttt{i >= n}]\!](n \geq i + 1, i = n) \\ \equiv\ & (i < n \implies n \geq i + 1) \wedge (i \geq n \implies i = n) \\ \equiv\ & i \geq n \implies i = n \\ \equiv\ & i < n \vee i = n \\ \equiv\ & i \leq n \impliedby n \geq i \end{aligned}$$

3. For $n < 0$, the same problem arises, so we require $n \geq i$ before the loop. Moreover, the loop may be reached with an $i = n-1$. In this case the program would increment i to $i = n + 1$ and reach the exit with $i \neq n$. We show that $n \geq i$ is indeed not sufficient:

$$\begin{aligned} & \mathsf{WP}[\![\texttt{i = i + 2}]\!](n \geq i) \\ \equiv\ & n \geq i + 2 \end{aligned}$$

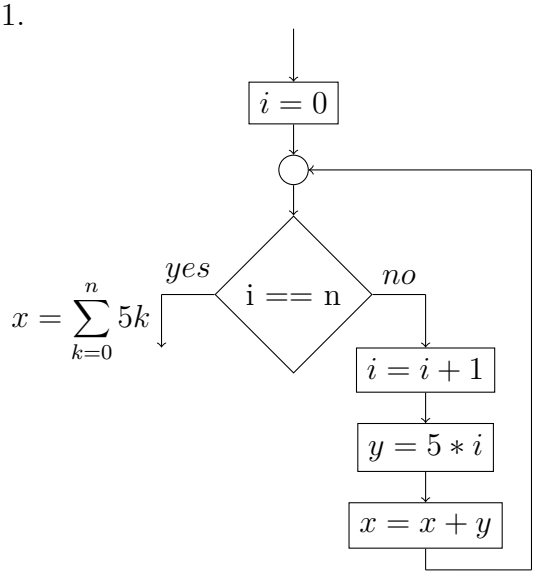
$$\begin{aligned} & \mathsf{WP}[\![\texttt{i >= n}]\!](n \geq i + 2, i = n) \\ \equiv\ & (i < n \implies n \geq i + 2) \wedge (i \geq n \implies i = n) \\ \equiv\ & (i \geq n \vee n \geq i + 2) \wedge (i < n \vee i = n) \\ \equiv\ & i \neq n - 1 \wedge i \leq n \not\impliedby n \geq i \end{aligned}$$

The weakest precondition tells us what we already knew, namely that i must not be equal to $n-1$ or, if we continue the loop $n-(2k+1)$ for any k. A much stronger precondition, that contains information about the divisibility of n and i by 2, is thus required here.

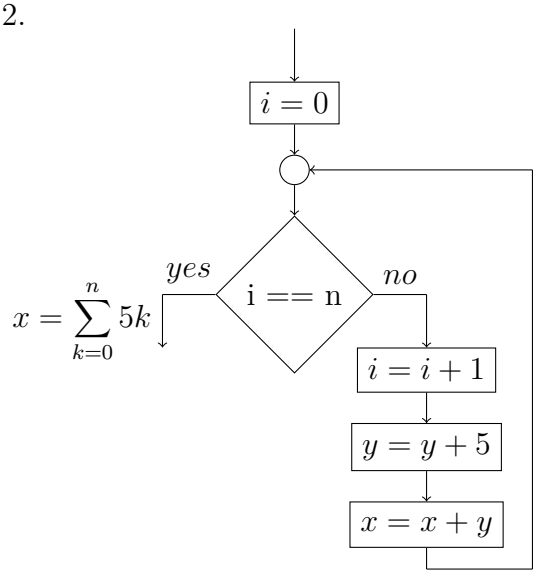
Assignment 3.2 (L) Y?

Consider these control flow graph fragments (assume x and y to be 0 initially):

1.



2.



Find suitable loop invariants and prove them locally consistent. Discuss, why these invariants have to be like that.

Suggested Solution 3.2

1. We show that $I :\equiv x = \sum_{k=0}^{i} 5k$ is sufficient:

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + y}]\!](I) \\
&\equiv \mathsf{WP}[\![\texttt{x = x + y}]\!](x = \sum_{k=0}^{i} 5k) \\
&\equiv x + y = \sum_{k=0}^{i} 5k \\
&\equiv x = -y + \sum_{k=0}^{i} 5k \quad \equiv: A
\end{aligned}$$

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{y = 5 * i}]\!](A) \\
&\equiv \mathsf{WP}[\![\texttt{y = 5 * i}]\!](x = -y + \sum_{k=0}^{i} 5k) \\
&\equiv x = -5i + \sum_{k=0}^{i} 5k \\
&\equiv x = \sum_{k=0}^{i-1} 5k \quad \equiv: B
\end{aligned}$$

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](B) \\
&\equiv \mathsf{WP}[\![\texttt{i = i + 1}]\!](x = \sum_{k=0}^{i-1} 5k) \\
&\equiv x = \sum_{k=0}^{i} 5k \quad \equiv: C
\end{aligned}$$

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](C, x = \sum_{k=0}^{n} 5k) \\
&\equiv \mathsf{WP}[\![\texttt{i == n}]\!](x = \sum_{k=0}^{i} 5k, x = \sum_{k=0}^{n} 5k) \\
&\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k) \vee (i = n \wedge x = \sum_{k=0}^{n} 5k) \\
&\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k) \vee (i = n \wedge x = \sum_{k=0}^{i} 5k) \\
&\equiv x = \sum_{k=0}^{i} 5k \quad \equiv I
\end{aligned}$$

2. We show that $I :\equiv x = \sum_{k=0}^{i} 5k$ is **not** sufficient:

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + y}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + y}]\!](x = \sum_{k=0}^{i} 5k) \\
\equiv\ &x + y = \sum_{k=0}^{i} 5k \\
\equiv\ &x = -y + \sum_{k=0}^{i} 5k \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = y + 5}]\!](A) \\
\equiv\ &\mathsf{WP}[\![\texttt{y = y + 5}]\!](x = -y + \sum_{k=0}^{i} 5k) \\
\equiv\ &x = -(y+5) + \sum_{k=0}^{i} 5k \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](B) \\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](x = -(y+5) + \sum_{k=0}^{i} 5k) \\
\equiv\ &x = -(y+5) + \sum_{k=0}^{i+1} 5k \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](C, x = \sum_{k=0}^{n} 5k) \\
\equiv\ &\mathsf{WP}[\![\texttt{i == n}]\!](x = -(y+5) + \sum_{k=0}^{i+1} 5k) \\
\equiv\ &(i \neq n \wedge x = -(y+5) + \sum_{k=0}^{i+1} 5k) \\
&\vee (i = n \wedge x = \sum_{k=0}^{n} 5k) \quad \not\Leftarrow A
\end{aligned}
$$

This invariant is not strong enough, because we do not have any information about y, so we cannot simplify anything. Adding $y = 5i$ renders the invariant sufficient:

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{x = x + y}]\!](I) \\
\equiv\ & \mathsf{WP}[\![\texttt{x = x + y}]\!](x = \sum_{k=0}^{i} 5k \wedge y = 5i) \\
\equiv\ & x + y = \sum_{k=0}^{i} 5k \wedge y = 5i \\
\equiv\ & x = -5i + \sum_{k=0}^{i} 5k \wedge y = 5i \\
\equiv\ & x = \sum_{k=0}^{i-1} 5k \wedge y = 5i \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{y = y + 5}]\!](A) \\
\equiv\ & \mathsf{WP}[\![\texttt{y = y + 5}]\!](x = \sum_{k=0}^{i-1} 5k \wedge y = 5i) \\
\equiv\ & x = \sum_{k=0}^{i-1} 5k \wedge y + 5 = 5i \\
\equiv\ & x = \sum_{k=0}^{i-1} 5k \wedge y = 5(i-1) \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{i = i + 1}]\!](B) \\
\equiv\ & \mathsf{WP}[\![\texttt{i = i + 1}]\!](x = \sum_{k=0}^{i-1} 5k \wedge y = 5(i-1)) \\
\equiv\ & x = \sum_{k=0}^{i} 5k \wedge y = 5i \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{i == n}]\!](C, x = \sum_{k=0}^{n} 5k) \\
\equiv\ & \mathsf{WP}[\![\texttt{i == n}]\!](x = \sum_{k=0}^{i} 5k \wedge y = 5i, x = \sum_{k=0}^{n} 5k) \\
\equiv\ & (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{n} 5k) \\
\Longleftarrow\ & (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \\
\equiv\ & x = \sum_{k=0}^{i} 5k \wedge y = 5i \quad \equiv I
\end{aligned}
$$

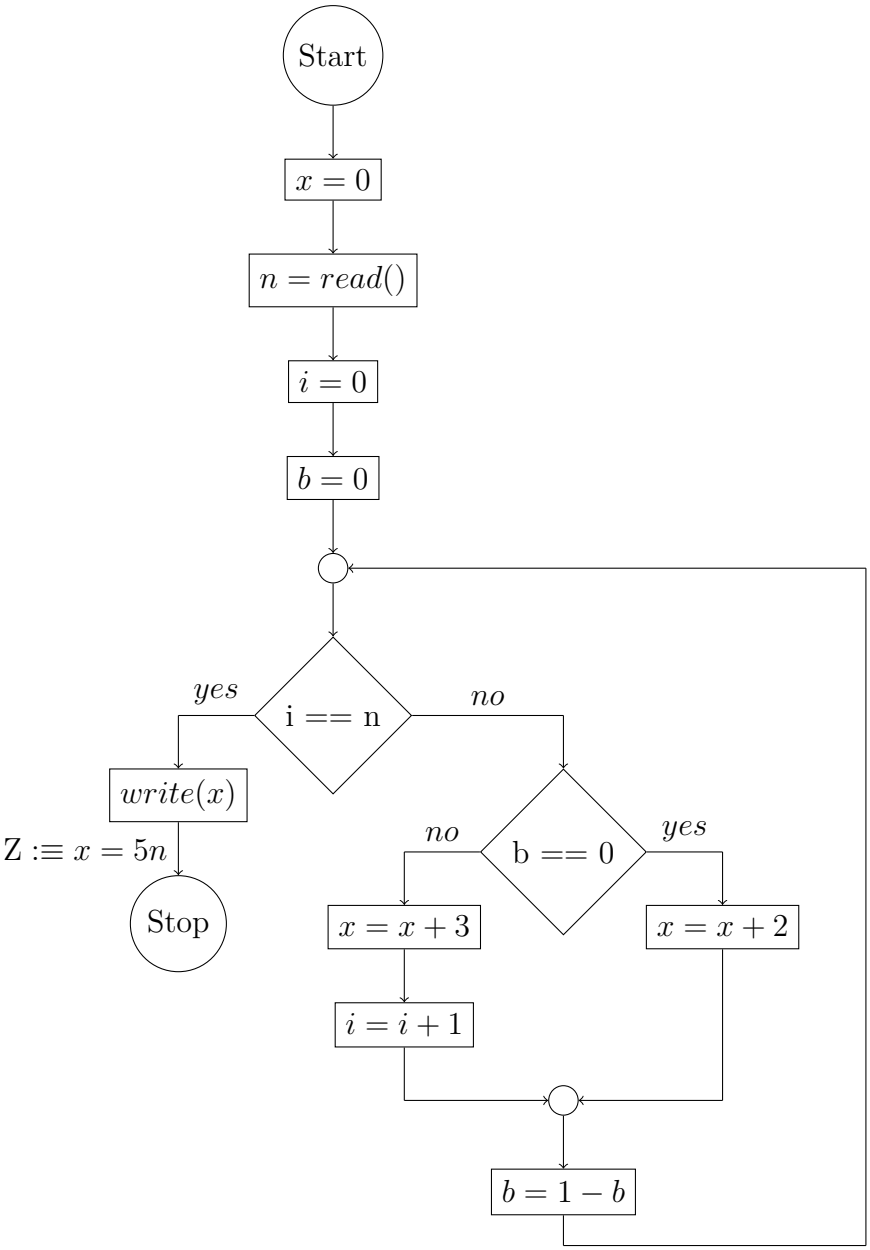
In general, two questions arise:

- Why is information about y required at all? The simple answer is, because y is used to compute x and x is the variable we want to prove something about.

- Why is information about y required in the second invariant, but not in the first? In the first cfg, the value of y is computed inside the loop independently of any value other than i, so it is not necessary to know anything about the previous value of y. This becomes much clearer when looking at the weakest preconditions. The third statement in the loop introduces the variable y into the assertion, but this y is removed (replaced by $5i$) by the next statement, such that the WP is again y-independant. In other words: Since the value of y is irrelevant when entering a loop iteration, we do not need it in the invariant. In the second case, however, y is computed from the previous value of y, so the value of y when entering a loop iteration is indeed important, so we have to make a statement about it inside the invariant. This is often referred to as *loop-carried dependency*.

Assignment 3.3 (L) Two b, or not two b

Prove Z using weakest preconditions.



Suggested Solution 3.3

An intuitive loop invariant is $I :\equiv x = 5i + 2b \wedge b \in \{0, 1\}$.

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b = 1 - b}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{b = 1 - b}]\!](x = 5i + 2b \land b \in \{0,1\})\\
\equiv\ &x = 5i + 2(1-b) \land (1-b) \in \{0,1\}\\
\equiv\ &x = 5i - 2b + 2 \land b \in \{0,1\} \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](x = 5i - 2b + 2 \land b \in \{0,1\})\\
\equiv\ &x = 5(i+1) - 2b + 2 \land b \in \{0,1\}\\
\equiv;\ &x = 5i - 2b + 7 \land b \in \{0,1\} \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + 3}]\!](B)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + 3}]\!](x = 5i - 2b + 7 \land b \in \{0,1\})\\
\equiv\ &x + 3 = 5i - 2b + 7 \land b \in \{0,1\}\\
\equiv\ &x = 5i - 2b + 4 \land b \in \{0,1\} \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + 2}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + 2}]\!](x = 5i - 2b + 2 \land b \in \{0,1\})\\
\equiv\ &x + 2 = 5i - 2b + 2 \land b \in \{0,1\}\\
\equiv\ &x = 5i - 2b \land b \in \{0,1\} \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b == 0}]\!](C, D)\\
\equiv\ &\mathsf{WP}[\![\texttt{b == 0}]\!](x = 5i - 2b + 4 \land b \in \{0,1\}, x = 5i - 2b \land b \in \{0,1\})\\
\equiv\ &(b \neq 0 \land x = 5i - 2b + 4 \land b \in \{0,1\}) \lor (b = 0 \land x = 5i - 2b \land b \in \{0,1\})\\
\equiv\ &(b = 1 \land x = 5i + 2) \lor (b = 0 \land x = 5i)\\
\equiv\ &(b = 1 \land x = 5i + 2b) \lor (b = 0 \land x = 5i + 2b)\\
\equiv\ &x = 5i + 2b \land b \in \{0,1\} \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](E, Z)\\
\equiv\ &\mathsf{WP}[\![\texttt{i == n}]\!](x = 5i + 2b \land b \in \{0,1\}, x = 5n)\\
\equiv\ &(i \neq n \land x = 5i + 2b \land b \in \{0,1\}) \lor (i = n \land x = 5n)\\
\equiv\ &(i \neq n \land x = 5i + 2b \land b \in \{0,1\}) \lor (i = n \land x = 5n + 2b \land b = 0)\\
\equiv\ &x = 5i + 2b \land ((i \neq n \land b \in \{0,1\}) \lor (i = n \land b = 0)) \quad \not\Longleftarrow\ I
\end{aligned}
$$

The proof of local consistency fails, because the invariant does not imply that $b = 0$ when leaving the loop ($i = n$), so we have to add this to the invariant:

$$I :\equiv x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0)$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b = 1 - b}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{b = 1 - b}]\!](x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0))\\
\equiv\ &x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1) \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1))\\
\equiv\ &x = 5i - 2b + 7 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1) \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + 3}]\!](B)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + 3}]\!](x = 5i - 2b + 7 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1))\\
\equiv\ &x = 5i - 2b + 4 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1) \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + 2}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + 2}]\!](x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1))\\
\equiv\ &x = 5i - 2b \land b \in \{0,1\} \land (i = n \implies b = 1) \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b == 0}]\!](C, D)\\
\equiv\ &\mathsf{WP}[\![\texttt{b == 0}]\!](x = 5i - 2b + 4 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1),\\
&\qquad x = 5i - 2b \land b \in \{0,1\} \land (i = n \implies b = 1))\\
\equiv\ &(b = 1 \land x = 5i - 2b + 4 \land (i + 1 = n \implies b = 1))\\
&\qquad \lor (b = 0 \land x = 5i - 2b \land (i = n \implies b = 1))\\
\equiv\ &(b = 1 \land x = 5i + 2) \lor (b = 0 \land x = 5i \land i \neq n)\\
\impliedby\ &(b = 1 \land x = 5i + 2b \land i \neq n) \lor (b = 0 \land x = 5i + 2b \land i \neq n)\\
\equiv\ &x = 5i + 2b \land i \neq n \land b \in \{0,1\} \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](E, Z)\\
\equiv\ &\mathsf{WP}[\![\texttt{i == n}]\!](x = 5i + 2b \land i \neq n \land b \in \{0,1\}, x = 5n)\\
\equiv\ &(i \neq n \land x = 5i + 2b \land b \in \{0,1\}) \lor (i = n \land x = 5n)\\
\impliedby\ &(i \neq n \land x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0))\\
&\qquad \lor (i = n \land x = 5n \land (i = n \implies b = 0) \land b \in \{0,1\})\\
\equiv\ &(i \neq n \land x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0))\\
&\qquad \lor (i = n \land x = 5i + 2b \land (i = n \implies b = 0) \land b \in \{0,1\})\\
\equiv\ &x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0) \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b = 0}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{b = 0}]\!](x = 5i + 2b \wedge b \in \{0, 1\} \wedge (i = n \implies b = 0)) \\
\equiv\ &x = 5i \quad \equiv\text{: } F
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = 0}]\!](F) \\
\equiv\ &\mathsf{WP}[\![\texttt{i = 0}]\!](x = 5i) \\
\equiv\ &x = 0 \quad \equiv\text{: } G
\end{aligned}
$$

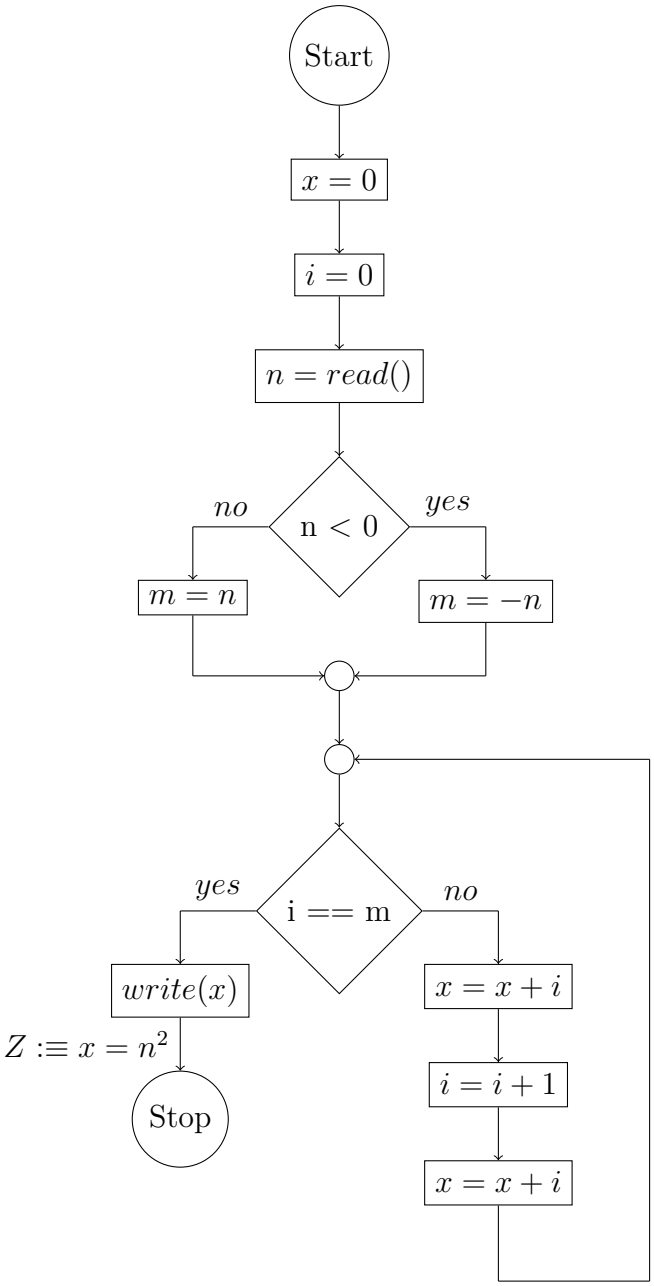
$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n = read()}]\!](G) \\
\equiv\ &\mathsf{WP}[\![\texttt{n = read()}]\!](x = 0) \\
\equiv\ &x = 0 \quad H
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = 0}]\!](H) \\
\equiv\ &\mathsf{WP}[\![\texttt{x = 0}]\!](x = 0) \\
\equiv\ &\mathit{true}
\end{aligned}
$$

□

Assignment 3.4 (L) Squared

Given is the following control flow graph:



Prove that Z holds.

Suggested Solution 3.4

First of all, we find a suitable loop invariant:

- At the point before the loop it holds for every iteration that $x = i^2$.
- Now we have a relation between x and i, as well as i and m (due to the loop's condition), but to prove Z, we need an additional relation (of one of them) with n. We know that $m = |n|$.

We combine these into the loop invariant $I :\equiv x = i^2 \wedge m = |n|$. Then, we compute weakest preconditions:

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + i}]\!](I)\\
&\equiv \mathsf{WP}[\![\texttt{x = x + i}]\!](x = i^2 \wedge m = |n|)\\
&\equiv x + i = i^2 \wedge m = |n|\\
&\equiv x = i^2 - i \wedge m = |n| \quad \equiv: A
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](A)\\
&\equiv \mathsf{WP}[\![\texttt{i = i + 1}]\!](x = i^2 - i \wedge m = |n|)\\
&\equiv x = (i+1)^2 - i - 1 \wedge m = |n|\\
&\equiv x = i^2 + i \wedge m = |n| \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + i}]\!](B)\\
&\equiv \mathsf{WP}[\![\texttt{x = x + i}]\!](x = i^2 + i \wedge m = |n|)\\
&\equiv x + i = i^2 + i \wedge m = |n|\\
&\equiv x = i^2 \wedge m = |n| \quad \equiv I \quad \equiv: C
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(x)}]\!](Z)\\
&\equiv \mathsf{WP}[\![\texttt{write(x)}]\!](x = n^2)\\
&\equiv x = n^2 \quad \equiv Z \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == m}]\!](C, D)\\
&\equiv \mathsf{WP}[\![\texttt{i == m}]\!](x = i^2 \wedge m = |n|, x = n^2)\\
&\equiv (i \neq m \wedge x = i^2 \wedge m = |n|) \vee (i = m \wedge x = n^2)\\
&\Longleftarrow (i \neq m \wedge x = i^2 \wedge m = |n|) \vee (i = m \wedge x = n^2 \wedge m = |n|)\\
&\equiv (i \neq m \wedge x = i^2 \wedge m = |n|) \vee (i = m \wedge x = i^2 \wedge m = |n|)\\
&\equiv x = i^2 \wedge m = |n| \wedge (i \neq m \vee i = m)\\
&\equiv x = i^2 \wedge m = |n| \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{m = n}]\!](I)\\
&\equiv \mathsf{WP}[\![\texttt{m = n}]\!](x = i^2 \wedge m = |n|)\\
&\equiv x = i^2 \wedge n = |n| \quad \equiv: E
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{m = -n}]\!](I)\\
&\equiv \mathsf{WP}[\![\texttt{m = -n}]\!](x = i^2 \wedge m = |n|)\\
&\equiv x = i^2 \wedge -n = |n| \quad \equiv: F
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n < 0}]\!](E, F)\\
&\equiv \mathsf{WP}[\![\texttt{n < 0}]\!](x = i^2 \wedge n = |n|, x = i^2 \wedge -n = |n|)\\
&\equiv (n \geq 0 \implies x = i^2 \wedge n = |n|) \wedge (n < 0 \implies x = i^2 \wedge -n = |n|)\\
&\equiv (n \geq 0 \implies x = i^2) \wedge (n < 0 \implies x = i^2)\\
&\equiv x = i^2 \vee (n < 0 \wedge n \geq 0)\\
&\equiv x = i^2 \quad \equiv: G
\end{aligned}
$$

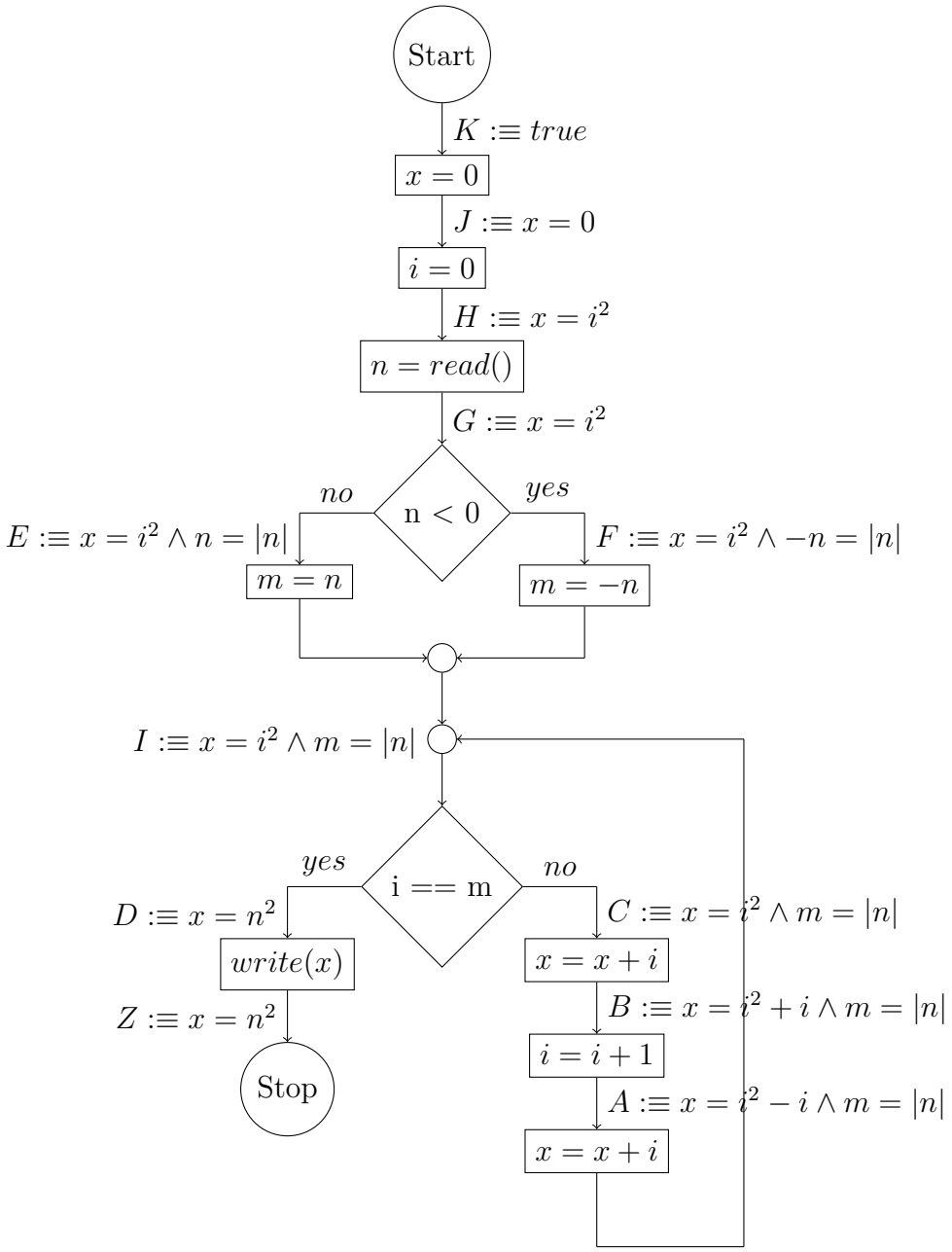
$$
\mathsf{WP}[\![\texttt{n = read()}]\!](G) \equiv G \quad \equiv: H
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = 0}]\!](H)\\
&\equiv \mathsf{WP}[\![\texttt{i = 0}]\!](x = i^2)\\
&\equiv x = 0 \quad \equiv: J
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = 0}]\!](J)\\
&\equiv \mathsf{WP}[\![\texttt{x = 0}]\!](x = 0)\\
&\equiv 0 = 0\\
&\equiv \mathit{true} \quad \equiv: K
\end{aligned}
$$

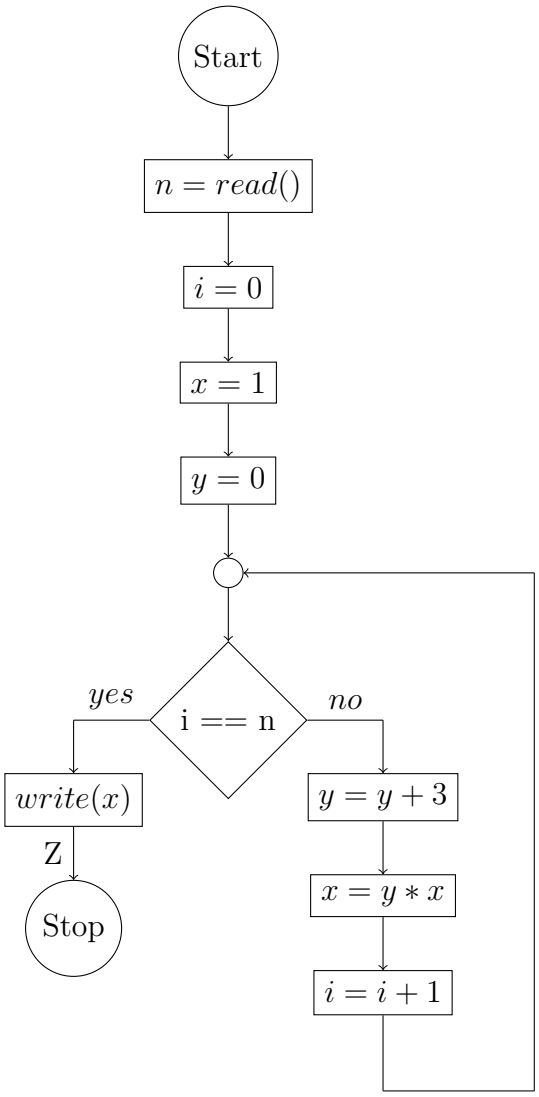
We did prove all assertions locally consistent and for *true* at the start node, thus Z holds for all runs of the program.

This is the annotated control flow graph:



Assignment 3.5 (H) Ready, Z, go! [6 Points]

Find a formula Z to express the exact value x the program computes. Then prove this Z using weakest preconditions.



Suggested Solution 3.5

The program computes: $Z :\equiv x = 3^n * n!$

We use the loop invariant $I :\equiv x = 3^i * i! \wedge y = 3i \wedge i \geq 0$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(x)}]\!](Z)\\
\equiv\ &\mathsf{WP}[\![\texttt{write(x)}]\!](x = 3^n * n!)\\
\equiv\ &x = 3^n * n! \quad \equiv: H
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](x = 3^i * i! \land y = 3i \land i \geq 0)\\
\equiv\ &x = 3^{i+1} * (i+1)! \land y = 3(i+1) \land i + 1 \geq 0 \quad \equiv: G
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = y * x}]\!](G)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = y * x}]\!](x = 3^{i+1} * (i+1)! \land y = 3(i+1) \land i + 1 \geq 0)\\
\equiv\ &y * x = 3^{i+1} * (i+1)! \land y = 3(i+1) \land i + 1 \geq 0\\
\Longleftarrow\ &x = \frac{3^{i+1} * (i+1)!}{y} \land y = 3(i+1) \land i \geq 0\\
\equiv\ &x = \frac{3^{i+1} * (i+1)!}{3(i+1)} \land y = 3(i+1) \land i \geq 0\\
\equiv\ &x = 3^i * i! \land y = 3(i+1) \land i \geq 0 \quad \equiv: F
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = y + 3}]\!](F)\\
\equiv\ &\mathsf{WP}[\![\texttt{y = y + 3}]\!](x = 3^i * i! \land y = 3(i+1) \land i \geq 0)\\
\equiv\ &x = 3^i * i! \land y + 3 = 3(i+1) \land i \geq 0\\
\equiv\ &x = 3^i * i! \land y = 3i \land i \geq 0 \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](E, H)\\
\equiv\ &\mathsf{WP}[\![\texttt{i == n}]\!](x = 3^i * i! \land y = 3i \land i \geq 0, x = 3^n * n!)\\
\equiv\ &(i \neq n\ \land\ x = 3^i * i! \land y = 3i \land i \geq 0) \lor (i = n\ \land\ x = 3^n * n!)\\
\equiv\ &(i \neq n \land x = 3^i * i! \land y = 3i \land i \geq 0) \lor (i = n \land x = 3^i * i!)\\
\Longleftarrow\ &(i \neq n \land x = 3^i * i! \land y = 3i \land i \geq 0) \lor (i = n \land x = 3^i * i! \land y = 3i \land i \geq 0)\\
\equiv\ &x = 3^i * i! \land y = 3i \land i \geq 0 \land (i \neq n \lor i = n)\\
\equiv\ &x = 3^i * i! \land y = 3i \land i \geq 0 \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = 0}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{y = 0}]\!](x = 3^i * i! \land y = 3i \land i \geq 0)\\
\equiv\ &x = 3^i * i! \land 0 = 3i \land i \geq 0 \quad \equiv: D
\end{aligned}
$$

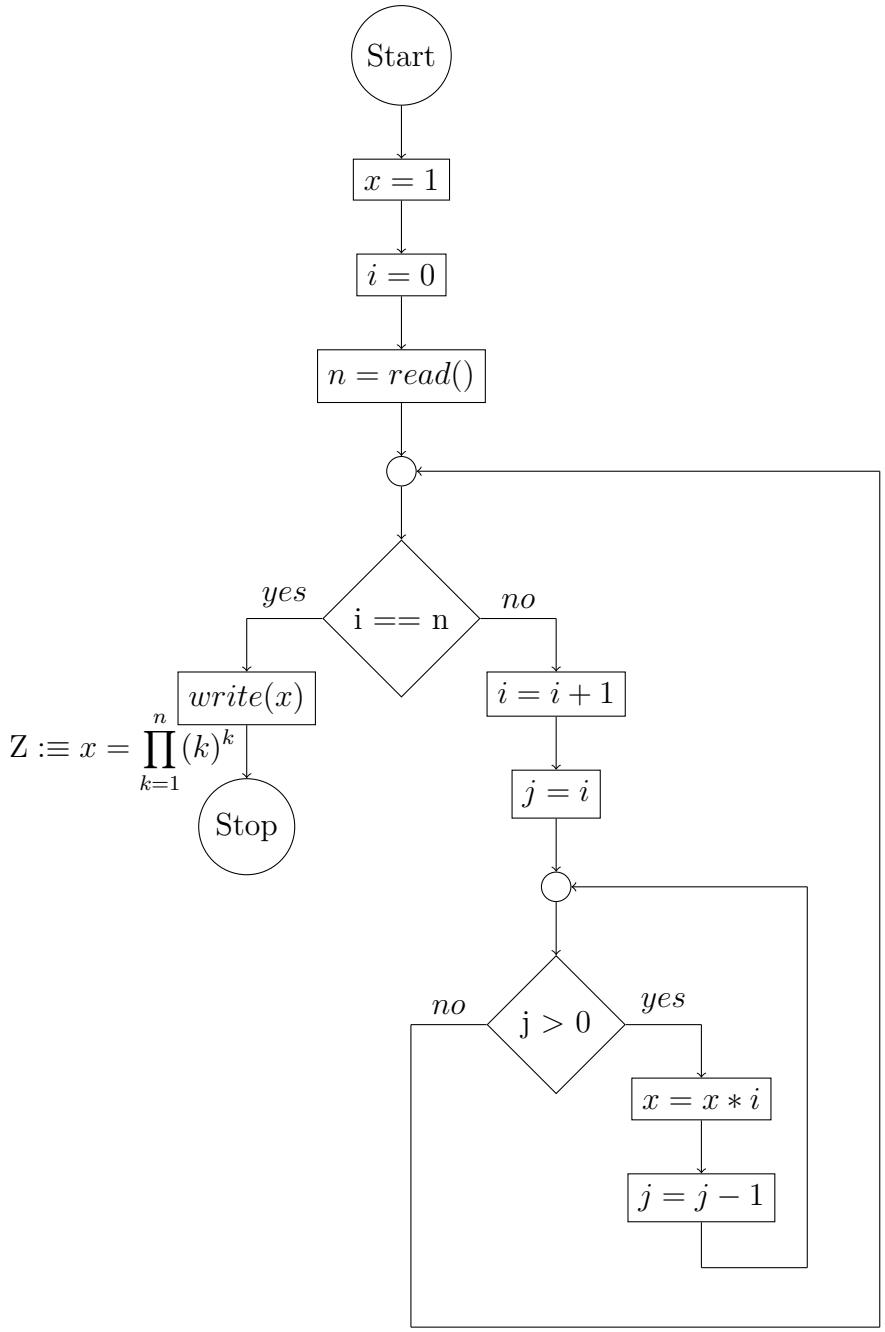
$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = 1}]\!](D)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = 1}]\!](x = 3^i * i! \land 0 = 3i \land i \geq 0)\\
\equiv\ &1 = 3^i * i! \land 0 = 3i \land i \geq 0 \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{i = 0}]\!](C) \\
\equiv\ & \mathsf{WP}[\![\texttt{i = 0}]\!](1 = 3^i * i! \wedge 0 = 3i \wedge i \geq 0) \\
\equiv\ & 1 = 3^0 * 0! \wedge 0 = 3 * 0 \wedge 0 \geq 0 \\
\equiv\ & \mathit{true} \quad \equiv\!: B
\end{aligned}
$$

$$
\begin{aligned}
& \mathsf{WP}[\![\texttt{n = read()}]\!](B) \\
\equiv\ & \mathsf{WP}[\![\texttt{n = read()}]\!](\mathit{true}) \\
\equiv\ & \mathit{true} \quad \equiv\!: A
\end{aligned}
$$

Assignment 3.6 (H) Loloopop [8 Points]

Prove Z using weakest preconditions:



Hint: If you have to find invariants for nested loops, it is usually easiest to work from outermost loop to innermost loop.

Suggested Solution 3.6

For the outer loop, we find the invariant $I :\equiv x = \prod_{k=1}^{i} k^k \wedge i \geq 0$ and for the inner loop $J :\equiv x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j \geq 0$.

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{j = j - 1}]\!](J)\\
\equiv\ &\mathsf{WP}[\![\texttt{j = j - 1}]\!](x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j \geq 0)\\
\equiv\ &x = i^{i-j+1} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j > 0 \quad \equiv\!: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x * i}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x * i}]\!](x = i^{i-j+1} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j > 0)\\
\equiv\ &x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j > 0 \quad \equiv\!: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{j > 0}]\!](I, B)\\
\equiv\ &\mathsf{WP}[\![\texttt{j > 0}]\!](x = \prod_{k=1}^{i} k^k \wedge i \geq 0, x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j > 0)\\
\equiv\ &(j \leq 0 \wedge x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \vee (j > 0 \wedge x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0)\\
\Longleftarrow\ &(j = 0 \wedge x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0) \vee (j > 0 \wedge x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0)\\
\equiv\ &x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j \geq 0 \quad \equiv J
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{j = i}]\!](J)\\
\equiv\ &\mathsf{WP}[\![\texttt{j = i}]\!](x = i^{i-j} * \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \wedge j \geq 0)\\
\equiv\ &x = \prod_{k=1}^{i-1} k^k \wedge i \geq 0 \quad \equiv\!: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](C)\\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](x = \prod_{k=1}^{i-1} k^k \wedge i \geq 0)\\
\equiv\ &x = \prod_{k=1}^{i} k^k \wedge i + 1 \geq 0 \quad \equiv\!: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(x)}]\!](Z)\\
\equiv\ &\mathsf{WP}[\![\texttt{write(x)}]\!](x = \prod_{k=1}^{n} k^k)\\
\equiv\ &x = \prod_{k=1}^{n} k^k \quad \equiv\!: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i == n}]\!](D, E) \\
\equiv\ &\mathsf{WP}[\![\texttt{i == n}]\!](x = \prod_{k=1}^{i} k^k \wedge i + 1 \geq 0, x = \prod_{k=1}^{n} k^k) \\
\equiv\ &(i \neq n \wedge x = \prod_{k=1}^{i} k^k \wedge i + 1 \geq 0) \vee (i = n \wedge x = \prod_{k=1}^{n} k^k) \\
\equiv\ &(i \neq n \wedge x = \prod_{k=1}^{i} k^k \wedge i + 1 \geq 0) \vee (i = n \wedge x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \\
\Longleftarrow\ &(i \neq n \wedge x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \vee (i = n \wedge x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \\
\equiv\ &x = \prod_{k=1}^{i} k^k \wedge i \geq 0 \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n = read()}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{n = read()}]\!](x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \\
\equiv\ &x = \prod_{k=1}^{i} k^k \wedge i \geq 0 \quad \equiv\!: F
\end{aligned}
$$

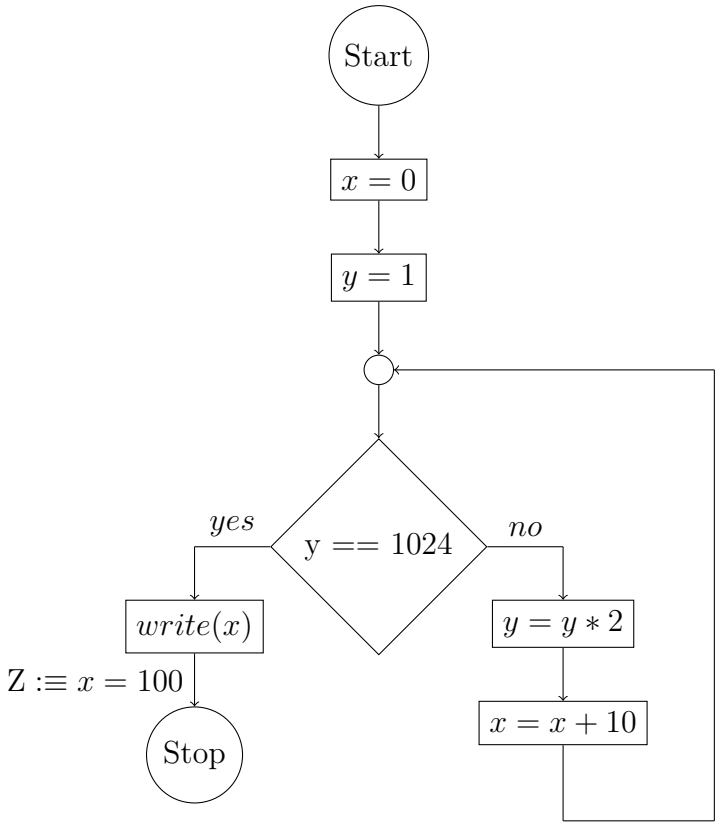
$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = 0}]\!](F) \\
\equiv\ &\mathsf{WP}[\![\texttt{i = 0}]\!](x = \prod_{k=1}^{i} k^k \wedge i \geq 0) \\
\equiv\ &x = 1 \quad \equiv\!: G
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = 1}]\!](G) \\
\equiv\ &\mathsf{WP}[\![\texttt{x = 1}]\!](x = 1) \\
\equiv\ &\mathit{true}
\end{aligned}
$$

□

Assignment 3.7 (H) Somethng s wrong wth ths program... [3 Points]

Prove Z using weakest preconditions.



Suggested Solution 3.7

We notice, that there is no classical loop counter i, so we use a little trick to find a correlation between variables. By # we denote the number of loop iterations the program has performed already. At the loop's join point, the variables can then be expressed like this:

- $y = 2^{\#}$
- $x = 10\#$

Now, we can resolve the second equation by # and replace it in the first one, leading to the following relation between x and y: $I :\equiv x = 10 \log_2 y$.

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x + 10}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{x = x + 10}]\!](x = 10 \log_2 y) \\
\equiv\ &x + 10 = 10 \log_2 y \\
\equiv\ &x = 10 \log_2 y - 10 \\
\equiv\ &x = 10(\log_2 y - 1) \\
\equiv\ &x = 10(\log_2 y - \log_2 2) \\
\equiv\ &x = 10 \log_2 \frac{y}{2} \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = y * 2}]\!](A) \\
\equiv\ &\mathsf{WP}[\![\texttt{y = y * 2}]\!](x = 10 \log_2 \frac{y}{2}) \\
\equiv\ &x = 10 \log_2 y \quad \equiv: B
\end{aligned}
$$

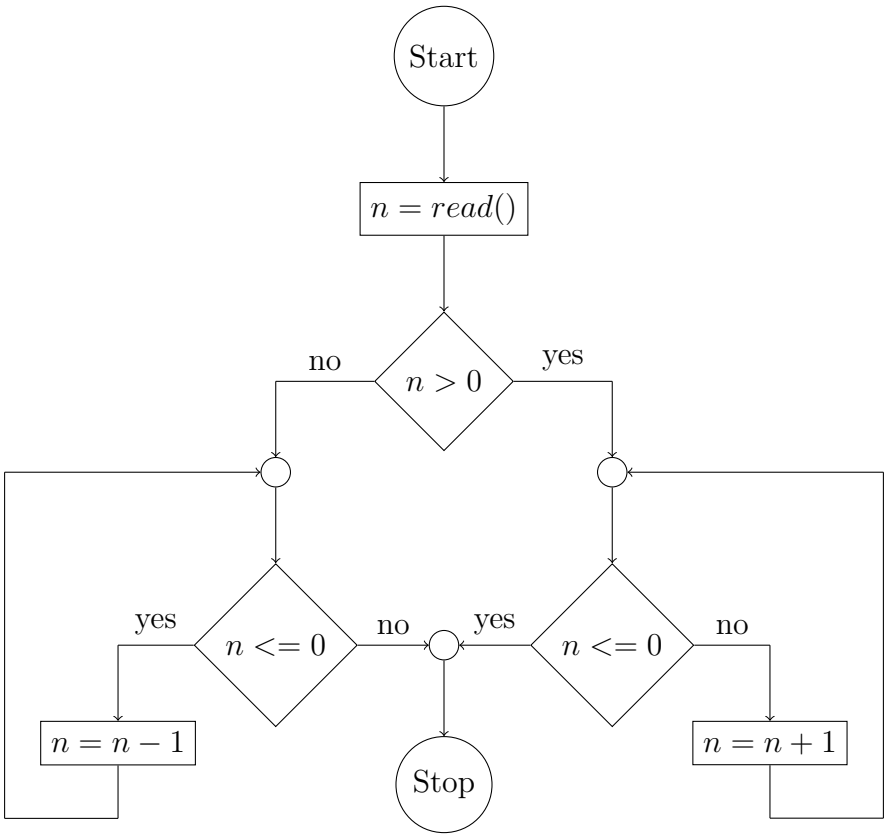
$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(x)}]\!](Z) \\
\equiv\ &\mathsf{WP}[\![\texttt{write(x)}]\!](x = 100) \\
\equiv\ &x = 100 \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y == 1024}]\!](B, C)\\
\equiv\ &\mathsf{WP}[\![\texttt{y == 1024}]\!](x = 10\log_2 y, x = 100)\\
\equiv\ &(y \neq 1024 \wedge x = 10\log_2 y) \vee (y = 1024 \wedge x = 100)\\
\equiv\ &(y \neq 1024 \wedge x = 10\log_2 y) \vee (y = 1024 \wedge x = 10\log_2 1024)\\
\equiv\ &(y \neq 1024 \wedge x = 10\log_2 y) \vee (y = 1024 \wedge x = 10\log_2 y)\\
\equiv\ &x = 10\log_2 y \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = 1}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{y = 1}]\!](x = 10\log_2 y)\\
\equiv\ &x = 10\log_2 1\\
\equiv\ &x = 0 \quad \equiv: D
\end{aligned}
\qquad\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = 0}]\!](D)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = 0}]\!](x = 0)\\
\equiv\ &\mathit{true}
\end{aligned}
$$

Assignment 3.8 (H) A Neverending Story [3 Points]

Prove that the following program cannot terminate using weakest preconditions.



Suggested Solution 3.8

In order to show that the program does not terminate, we have to prove that $false$ holds before the stop node for all executions. We use invariants $I :\equiv n \leq 0$ and $J :\equiv n > 0$ as

invariants for the left and right loop, respectively.

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n = n - 1}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{n = n - 1}]\!](n \leq 0)\\
\equiv\ &n - 1 \leq 0\\
\equiv\ &n \leq 1 \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n = n + 1}]\!](J)\\
\equiv\ &\mathsf{WP}[\![\texttt{n = n + 1}]\!](n > 0)\\
\equiv\ &n + 1 > 0\\
\equiv\ &n \geq 0 \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n <= 0}]\!](\mathit{false}, A)\\
\equiv\ &\mathsf{WP}[\![\texttt{n <= 0}]\!](\mathit{false}, n \leq 1)\\
\equiv\ &(n > 0 \wedge \mathit{false}) \vee (n \leq 0 \wedge n \leq 1)\\
\equiv\ &n \leq 0 \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n <= 0}]\!](B, \mathit{false})\\
\equiv\ &\mathsf{WP}[\![\texttt{n <= 0}]\!](n \geq 0, \mathit{false})\\
\equiv\ &(n > 0 \wedge n \geq 0) \vee (n \leq 0 \wedge \mathit{false})\\
\equiv\ &n > 0 \quad \equiv J
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n > 0}]\!](I, J)\\
\equiv\ &\mathsf{WP}[\![\texttt{n > 0}]\!](n \leq 0, n > 0)\\
\equiv\ &(n \leq 0 \implies n \leq 0) \wedge (n > 0 \implies n > 0)\\
\equiv\ &\mathit{true} \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{n = read()}]\!](C)\\
\equiv\ &\mathsf{WP}[\![\texttt{n = read()}]\!](\mathit{true})\\
\equiv\ &\forall n.\mathit{true}\\
\equiv\ &\mathit{true} \quad \equiv: D
\end{aligned}
$$

□