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.

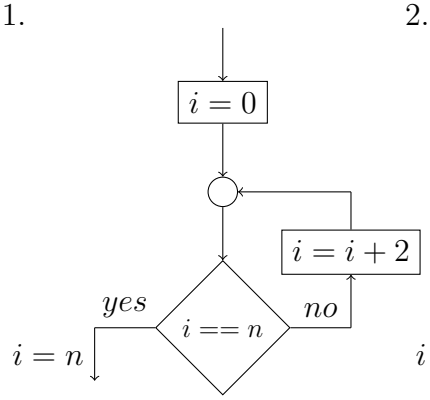
Loop Invariants

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].

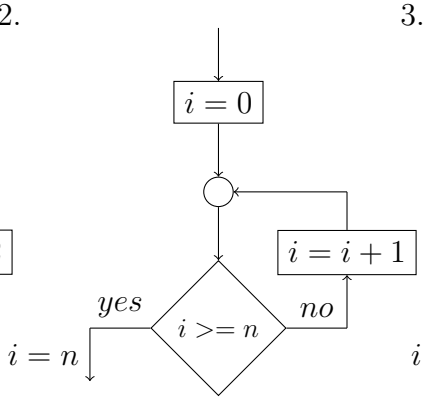
Assignment 3.1 (L) Individual Loops

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.

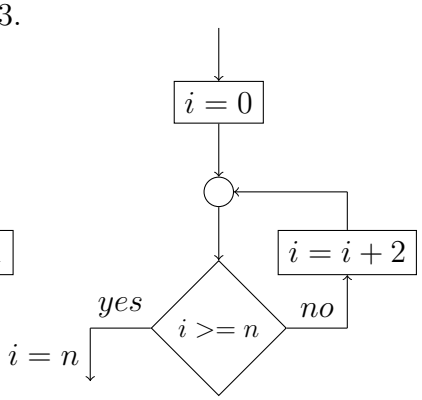
1.



2.



3.



[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

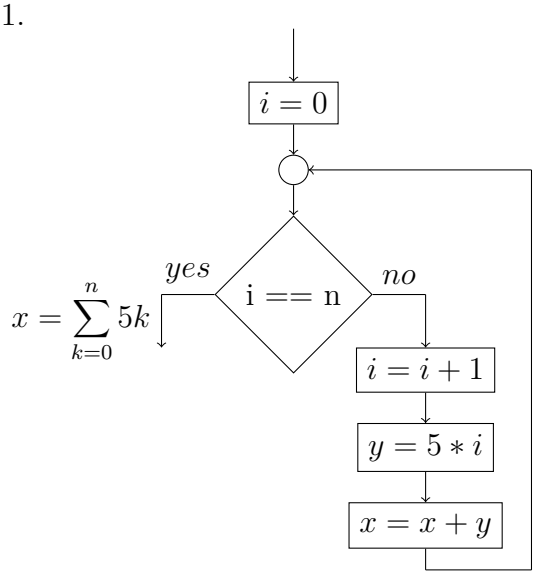
[3] https://piazza.com/tum.de/fall2018/in0003/home

[4] http://ttt.in.tum.de/recordings/Info2_2017_11_24-1/Info2_2017_11_24-1.mp4

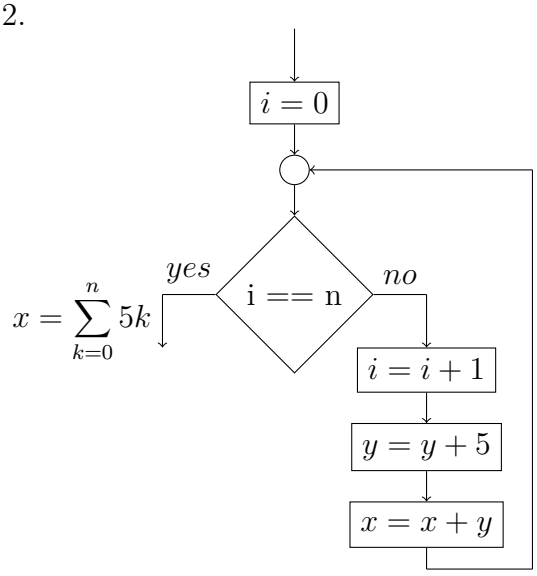
Assignment 3.2 (L) Y?

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

1.



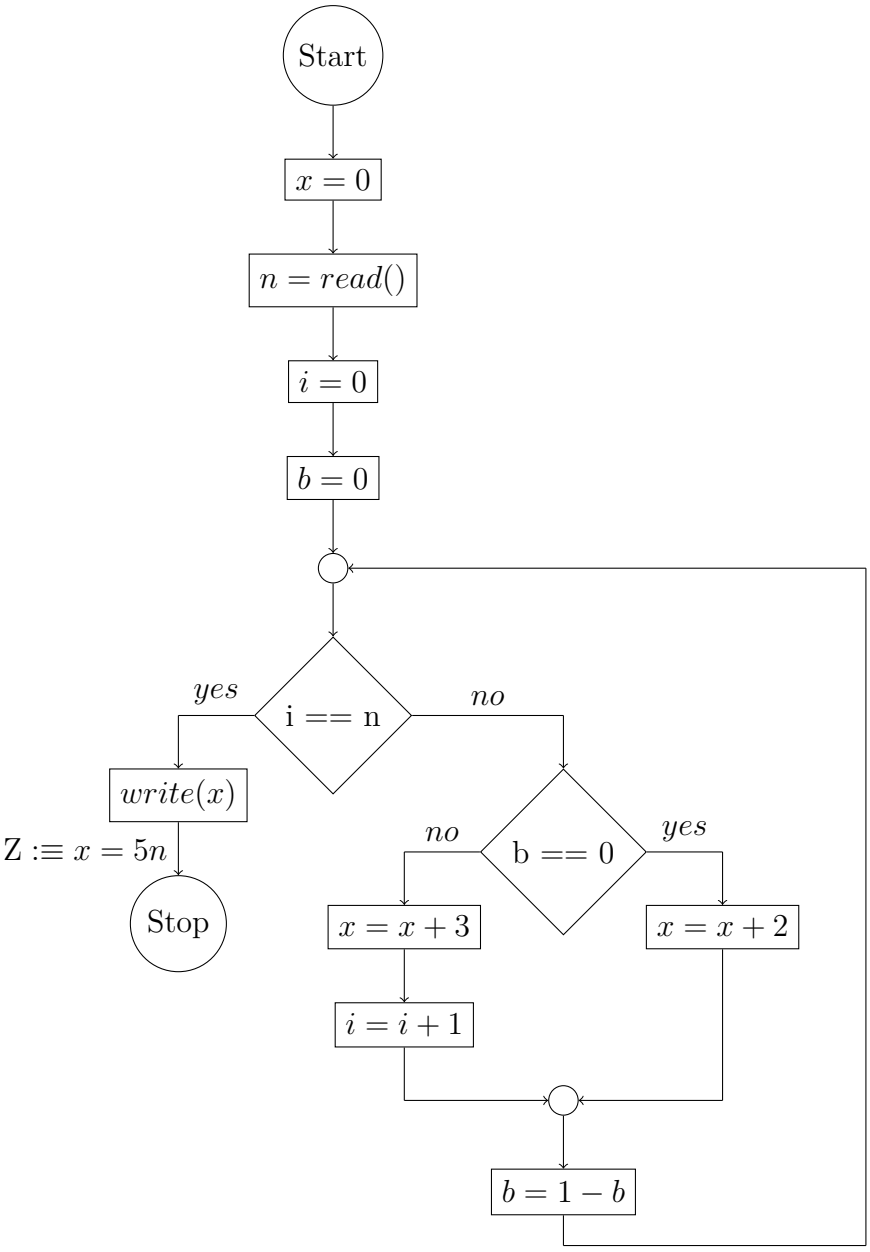
2.



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

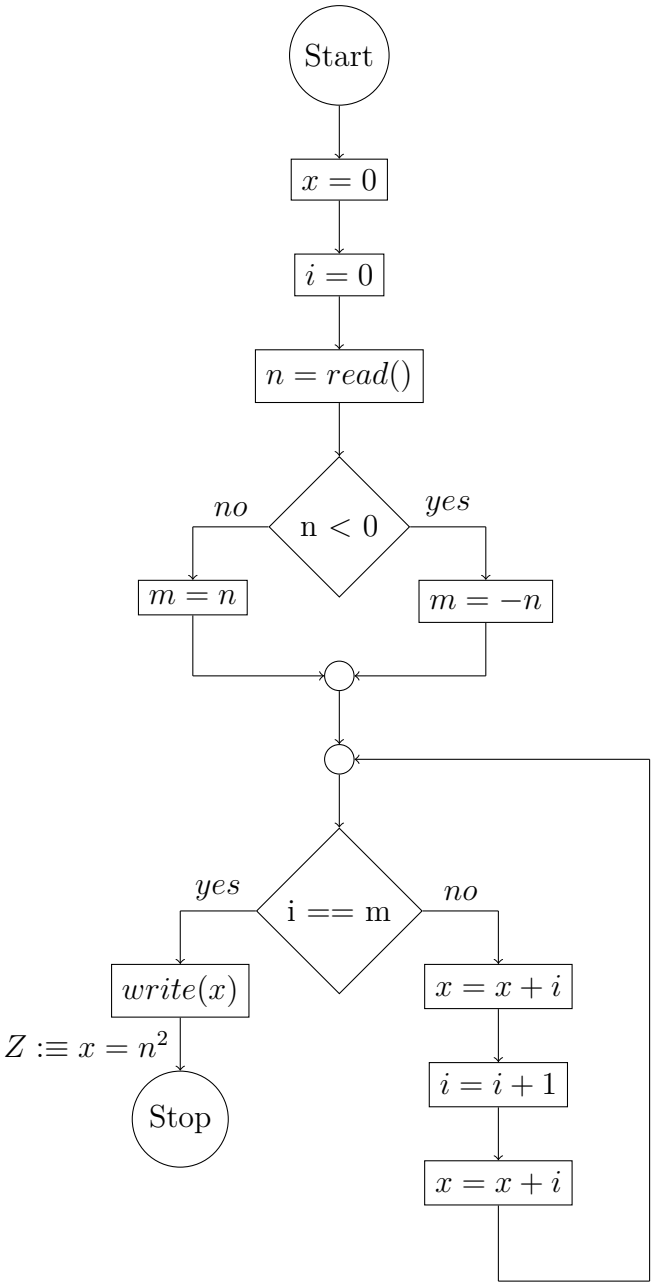
Assignment 3.3 (L) Two b, or not two b

Prove Z using weakest preconditions.



Assignment 3.4 (L) Squared

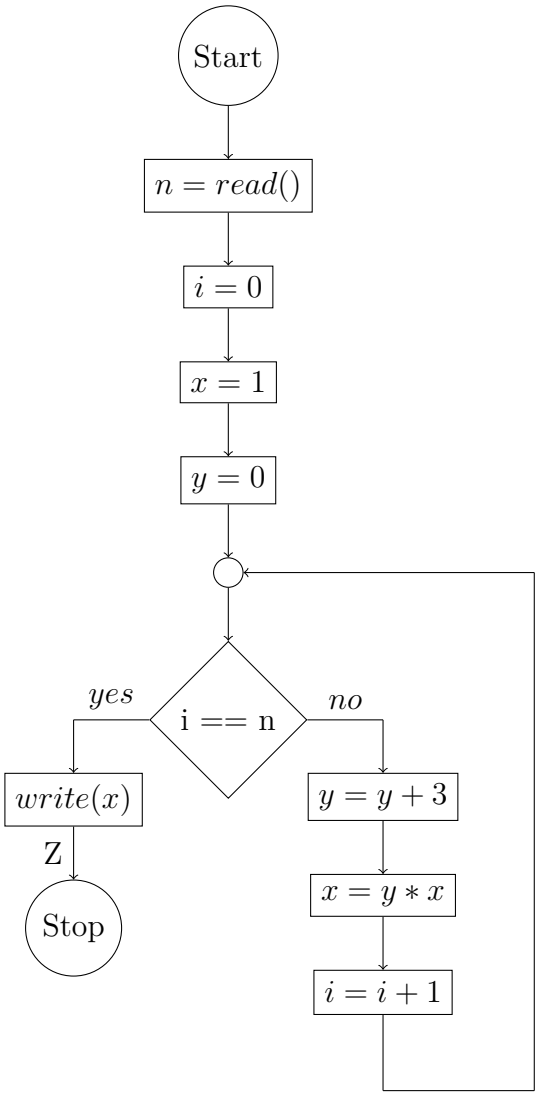
Given is the following control flow graph:



Prove that Z holds.

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.



Das Programm liest den Input n ein. Dieser entspricht der Anzahl der Schleifendurchläufe. Innerhalb der Schleife wird x dann immer wieder mit y multipliziert. y wird dabei bei jedem Durchlauf um 3 inkrementiert. Das bedeutet, dass $x = \prod_{i=1}^{n} 3i$ berechnet wird. Dieses Produkt wählen wir als Schleifeninvariante I. Wenn wir uns dieses Produkt genauer anschauen, sehen wir, dass es 3^n ($\prod_{i=1}^{n} 3$) sowie $n!$ ($\prod_{i=1}^{n} i$) berechnet,das Produkt also $n! \cdot 3^n$ entspricht. $\rightarrow Z :\equiv x = n! \cdot 3^n$

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

$$\begin{aligned} \mathsf{WP}[\![\texttt{i = i + 1}]\!](I) &\equiv \mathsf{WP}[\![\texttt{i = i + 1}]\!](x = i! \cdot 3^i \wedge y = 3i) \\ &\equiv x = (i+1)! \cdot 3^{(i+1)} \wedge y = 3(i+1) \\ &:\equiv B \end{aligned}$$

$$
\begin{aligned}
\mathsf{WP}[\![\texttt{x = y * x}]\!](B) &\equiv \mathsf{WP}[\![\texttt{x = y * x}]\!](x = (i+1)! \cdot 3^{(i+1)} \wedge y = 3(i+1)) \\
&\equiv y * x = (i+1)! \cdot 3^{(i+1)} \wedge y = 3(i+1) \\
&\equiv 3(i+1) * x = (i+1)! \cdot 3^{(i+1)} \wedge y = 3(i+1) \\
&\equiv x = \frac{(i+1)! \cdot 3^{(i+1)}}{3(i+1)} \wedge y = 3(i+1) \\
&\equiv x = \frac{i! \cdot 3^{(i+1)}}{3} \wedge y = 3(i+1) \\
&\equiv x = i! \cdot 3^i \wedge y = 3(i+1) \\
&:\equiv C
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{WP}[\![\texttt{y = y + 3}]\!](C) &\equiv \mathsf{WP}[\![\texttt{y = y + 3}]\!](x = i! \cdot 3^i \wedge y = 3(i+1)) \\
&\equiv x = i! \cdot 3^i \wedge y + 3 = 3(i+1) \\
&\equiv x = i! \cdot 3^i \wedge y + 3 = 3i + 3 \\
&\equiv x = i! \cdot 3^i \wedge y = 3i \\
&:\equiv D
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{WP}[\![\texttt{i == n}]\!](D, A) &\equiv \mathsf{WP}[\![\texttt{i == n}]\!](x = i! \cdot 3^i \wedge y = 3i, x = n! \cdot 3^n) \\
&\equiv (i \neq n \wedge x = i! \cdot 3^i \wedge y = 3i) \vee (i = n \wedge x = n! \cdot 3^n) \\
&\Leftarrow (i \neq n \wedge x = i! \cdot 3^i \wedge y = 3i) \vee (i = n \wedge x = n! \cdot 3^n \wedge y = 3n) \\
&\equiv (i \neq n \wedge x = i! \cdot 3^i \wedge y = 3i) \vee (i = n \wedge x = i! \cdot 3^i \wedge y = 3i) \\
&\equiv x = i! \cdot 3^i \wedge y = 3i \\
&\equiv I
\end{aligned}
$$

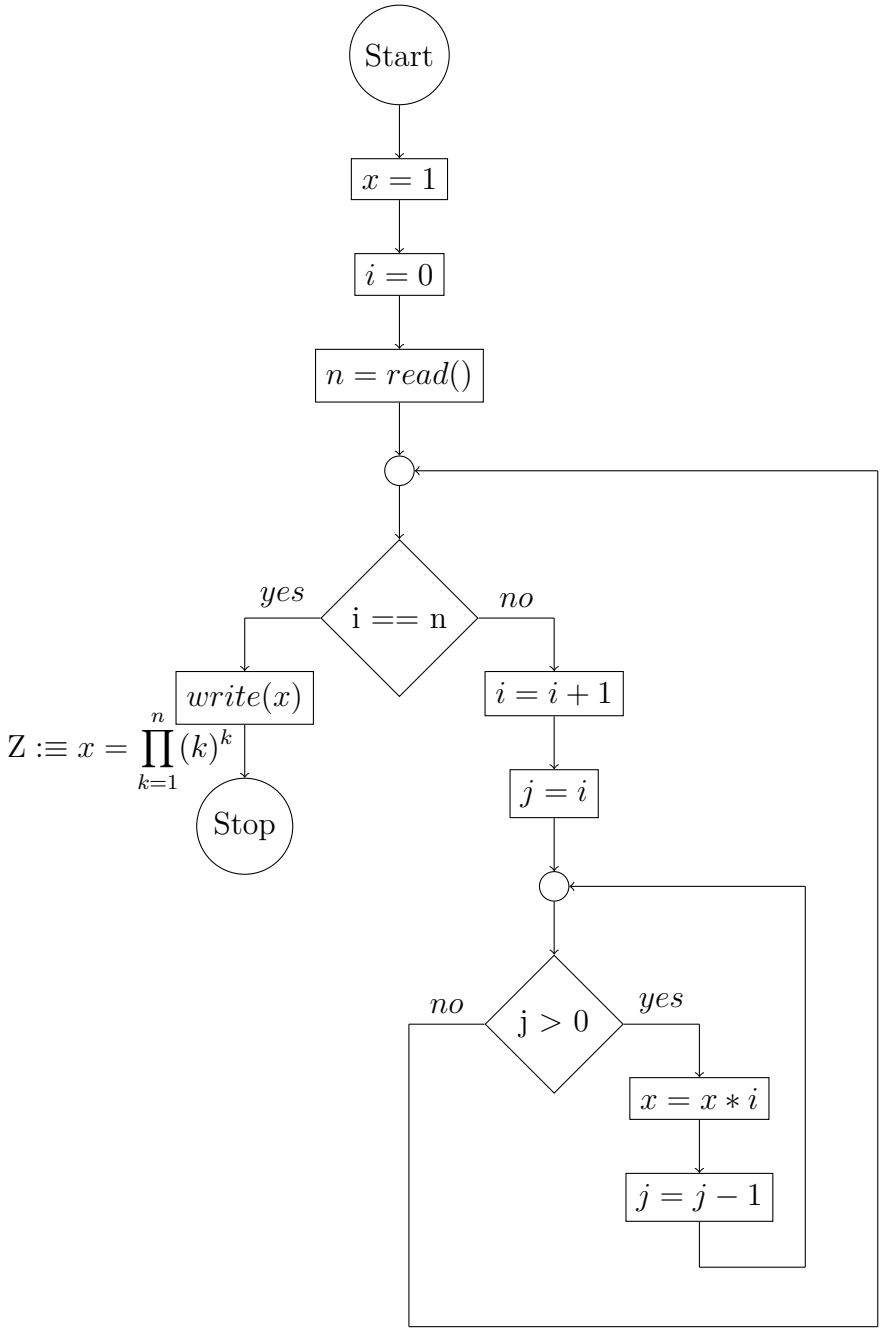
$$
\begin{aligned}
\mathsf{WP}[\![\texttt{y = 0}]\!](I) &\equiv \mathsf{WP}[\![\texttt{y = 0}]\!](x = i! \cdot 3^i \wedge y = 3i) \\
&\equiv x = i! \cdot 3^i \wedge 0 = 3i \\
&\equiv x = i! \cdot 3^i \wedge i = 0 \\
&\equiv x = 0! \cdot 3^0 \wedge i = 0 \\
&\equiv x = 1 \cdot 1 \wedge i = 0 \\
&\equiv x = 1 \wedge i = 0 \\
&:\equiv E
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{WP}[\![\texttt{x = 1}]\!](E) &\equiv \mathsf{WP}[\![\texttt{x = 1}]\!](x = 1 \wedge i = 0) \\
&\equiv 1 = 1 \wedge i = 0 \\
&\equiv \mathit{true} \wedge i = 0 \\
&\equiv i = 0 \\
&:\equiv F
\end{aligned}
$$

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

Assignment 3.6 (H) Loloopop [8 Points]

Prove Z using weakest preconditions:



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

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

$$\mathsf{WP}[\![\texttt{j = i}]\!](J) \equiv \mathsf{WP}[\![\texttt{j = i}]\!](x = i^{j-i} \cdot \prod_{k=1}^{i-1} (k)^k)$$

$$\equiv x = i^0 \cdot \prod_{k=1}^{i-1}(k)^k$$
$$\equiv x = \prod_{k=1}^{i-1}(k)^k$$
$$:\equiv B$$

$$\mathsf{WP}[\![\texttt{i = i + 1}]\!](B) \equiv \mathsf{WP}[\![\texttt{i = i + 1}]\!](x = \prod_{k=1}^{i-1}(k)^k)$$
$$\equiv x = \prod_{k=1}^{i}(k)^k$$
$$:\equiv C$$

$$\mathsf{WP}[\![\texttt{i == n}]\!](C, A) \equiv \mathsf{WP}[\![\texttt{i == n}]\!](x = \prod_{k=1}^{i}(k)^k, x = \prod_{k=1}^{n}(k)^k)$$
$$\equiv (i \neq n \land x = \prod_{k=1}^{i}(k)^k) \lor (i = n \land x = \prod_{k=1}^{n}(k)^k)$$
$$\equiv (i \neq n \land x = \prod_{k=1}^{i}(k)^k) \lor (i = n \land x = \prod_{k=1}^{i}(k)^k)$$
$$\equiv x = \prod_{k=1}^{i}(k)^k$$
$$\equiv I$$

$$\mathsf{WP}[\![\texttt{j = j - 1}]\!](J) \equiv \mathsf{WP}[\![\texttt{j = j - 1}]\!](x = i^{j-i} \cdot \prod_{k=1}^{i-1}(k)^k)$$
$$\equiv x = i^{j-1-i} \cdot \prod_{k=1}^{i-1}(k)^k$$
$$:\equiv D$$

$$\mathsf{WP}[\![\texttt{x = x · i}]\!](D) \equiv \mathsf{WP}[\![\texttt{x = x · i}]\!](x = i^{j-1-i} \cdot \prod_{k=1}^{i-1}(k)^k)$$
$$\equiv x \cdot i = i^{j-1-i} \cdot \prod_{k=1}^{i-1}(k)^k$$
$$\equiv x = i^{j-i} \cdot \prod_{k=1}^{i-1}(k)^k$$
$$\equiv J$$

$$\mathsf{WP}[\![\texttt{n = read()}]\!](I) \equiv \mathsf{WP}[\![\texttt{n = read()}]\!](x = \prod_{k=1}^{i}(k)^k)$$
$$\equiv \forall n.x = \prod_{k=1}^{i}(k)^k$$

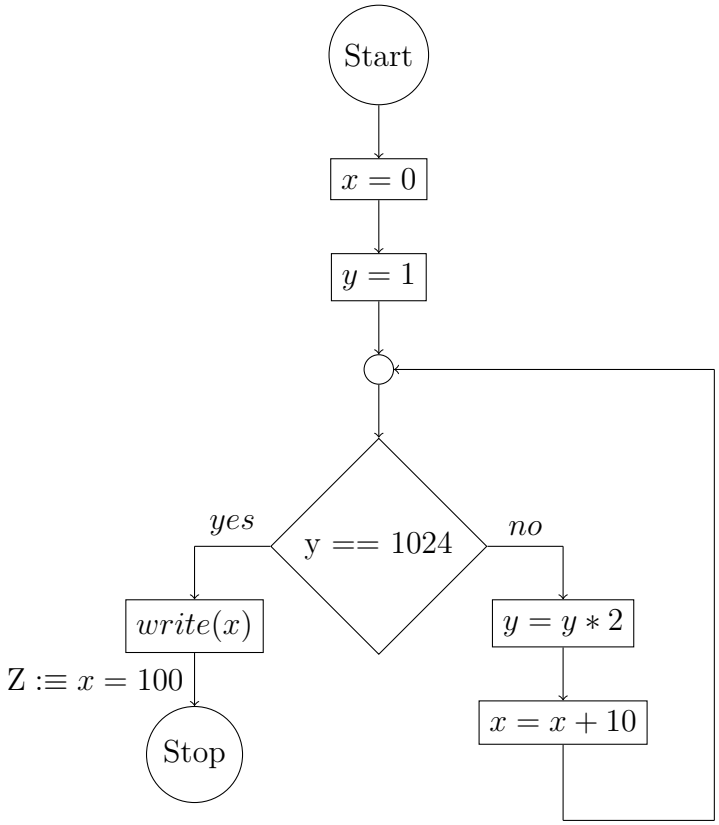
$$\equiv x = \prod_{k=1}^{i} (k)^k$$
$$:\equiv E$$

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

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

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

Prove Z using weakest preconditions.



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

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

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

$$\begin{aligned}
\mathsf{WP}[\![\texttt{y == 1024}]\!](C, A) &\equiv \mathsf{WP}[\![\texttt{y == 1024}]\!](x = 10 \cdot log_2 y, x = 100) \\
&\equiv (y \neq 1024 \land x = 10 \cdot log_2 y) \lor (y = 1024 \land x = 100) \\
&\equiv (y \neq 1024 \land x = 10 \cdot log_2 y) \lor (y = 1024 \land x = 10 \cdot 10) \\
&\equiv (y \neq 1024 \land x = 10 \cdot log_2 y) \lor (y = 1024 \land x = 10 \cdot log_2 1024) \\
&\equiv (y \neq 1024 \land x = 10 \cdot log_2 y) \lor (y = 1024 \land x = 10 \cdot log_2 y)
\end{aligned}$$

$$\equiv x = 10 \cdot log_2 y$$
$$\equiv I$$

$$\mathsf{WP}[\![\texttt{y = 1}]\!](I) \equiv \mathsf{WP}[\![\texttt{y = 1}]\!](x = 10 \cdot log_2 y)$$
$$\equiv x = 10 \cdot log_2 1$$
$$\equiv x = 10 \cdot 0$$
$$\equiv x = 0$$
$$:\equiv D$$

$$\mathsf{WP}[\![\texttt{x = 0}]\!](D) \equiv \mathsf{WP}[\![\texttt{x = 0}]\!](x = 0)$$
$$\equiv 0 = 0$$
$$\equiv true$$

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

Prove that the following program cannot terminate using weakest preconditions.