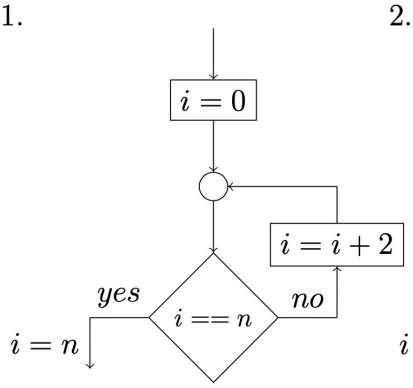
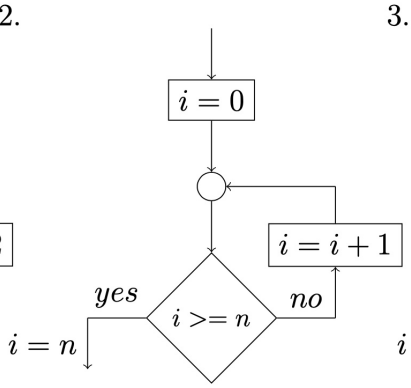
3.1 Frooty Loops (*2017, T3.2*)

For each of the following loops, discuss, which (weakest) preconditions need to hold before the loop for the final assertion $i = n$ to hold. Especially consider what happens if n is positive or negative.

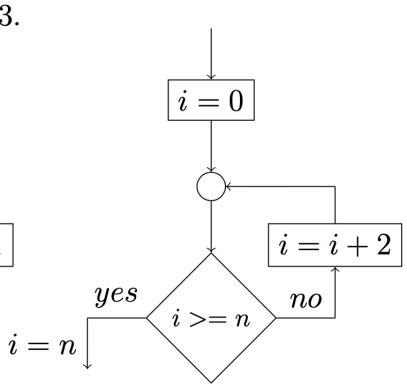
1.



2.



3.



Answer of exercise 3.1

(1) In the first case, the final assertion follows directly from the loop exit condition. Since the loop can only be exited if $i == n$ holds, the assertion can never be violated and therefore holds for arbitrary preconditions. In the case of negative n, or n with $n \ mod \ 2 \neq 0$, the loop never stops, however, this does not violate the final assertion, since the program point of the assertion is never reached. Therefore, the weakest possible precondition is *true*:

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

For this WP calculation, we assumed the assertion *true* to hold at the no-exit of the exit condition. This can be proven to be locally consistent:

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

(2) Intuitively, we can see that the loop is exited when i has reached the value of n, making $i = n$. This changes for negative n: in this case, the loop exits immediately and the final assertion would not hold. Therefore, we need to require $n \geq 0$, or, more generally, $n \geq i$ before the loop. We assume this and show local consistency:

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

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

(3) Here, we can see the same problem as with (2), so we at least need to require $n \geq i$ again. Furthermore, it can be the case that before the last loop iteration, $i = n - 1$. Then, i skips n and assumes the value $n + 1$ in the next iteration, exiting the loop, but not satisfying the condition $i = n$. We can use WP calculations to show that this condition is indeed not strong enough:

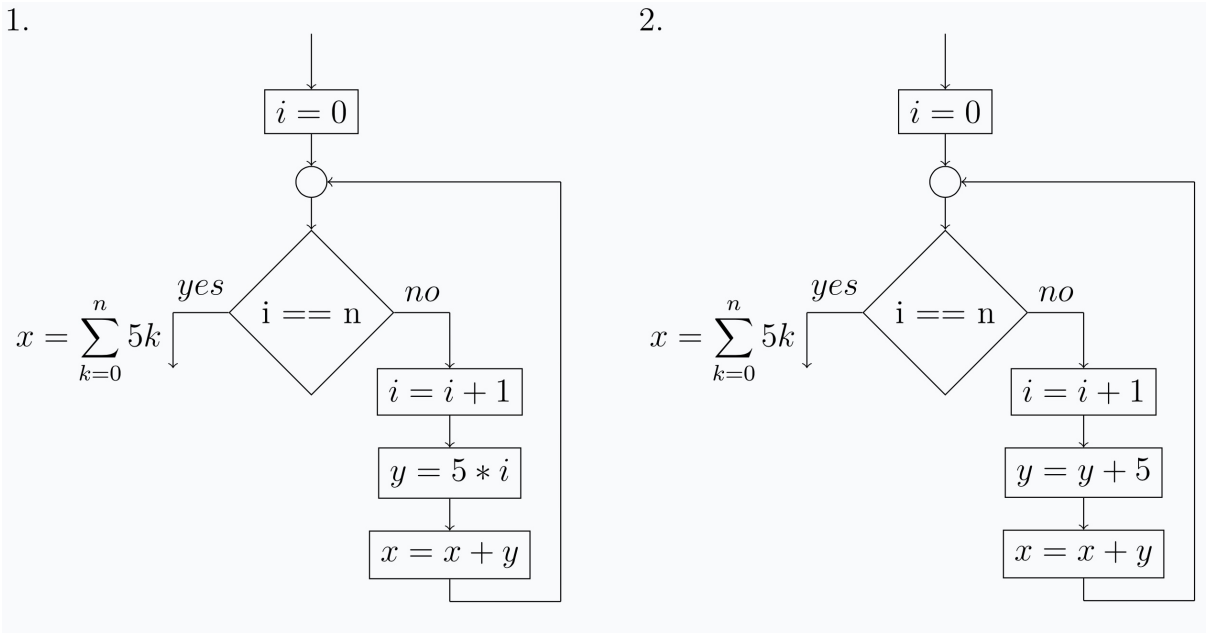
$$\begin{aligned} & \mathsf{WP}[\![\texttt{i = i+2}]\!](n \geq i) \\ \equiv\ & n \geq i + 2 \end{aligned}$$

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

Therefore we need a stronger precondition that requires i and n to have the same remainder *mod* 2.

3.2 More info needed (*2021, T3.2*)

Consider the following two program fragments. Assume x and y to be set to 0 initially:



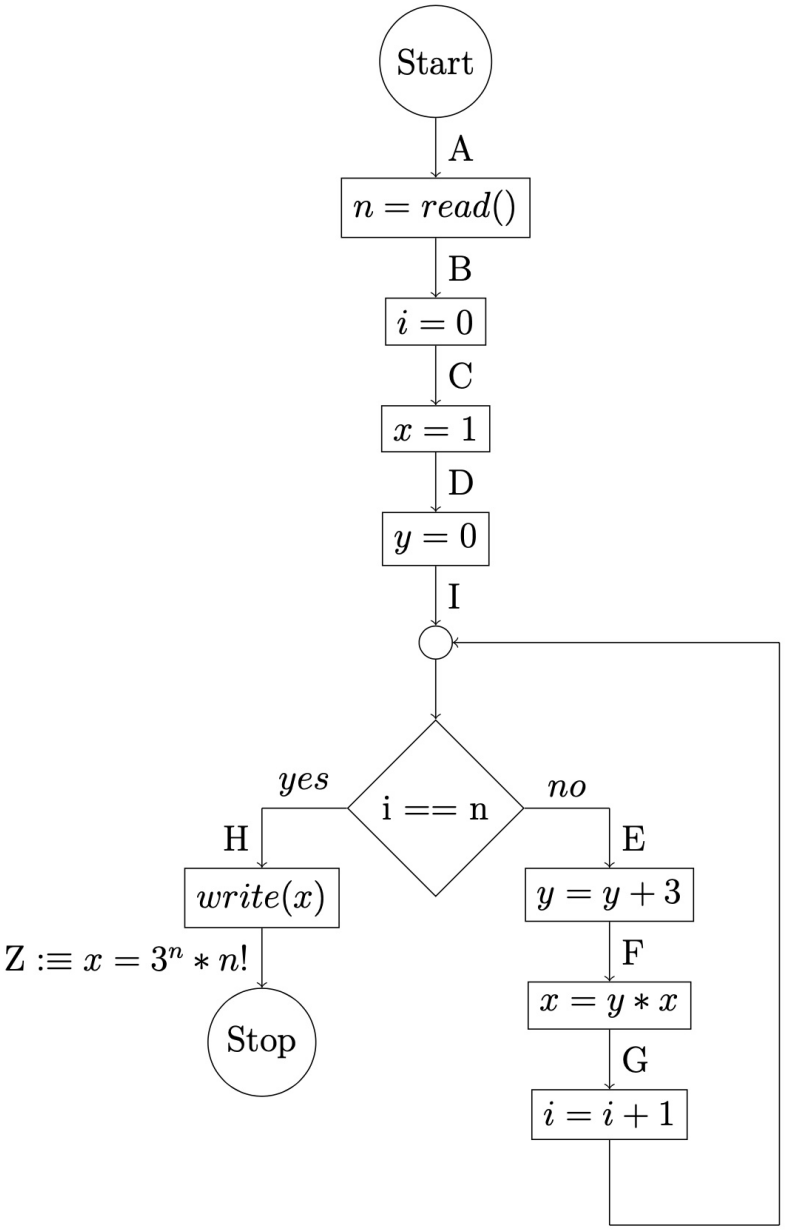
Find suitable loop invariants and prove them locally consistent. Discuss, why one loop invariant needs more information than the other. Try to generalize this observation.

Answer of exercise 3.2

The solution to this exercise can be found on artemis (see `https://artemis.ase.in.tum.de/courses/147/exercises/5418`).

3.3 Threefaculty (*2017, exam*)

Consider the following program:



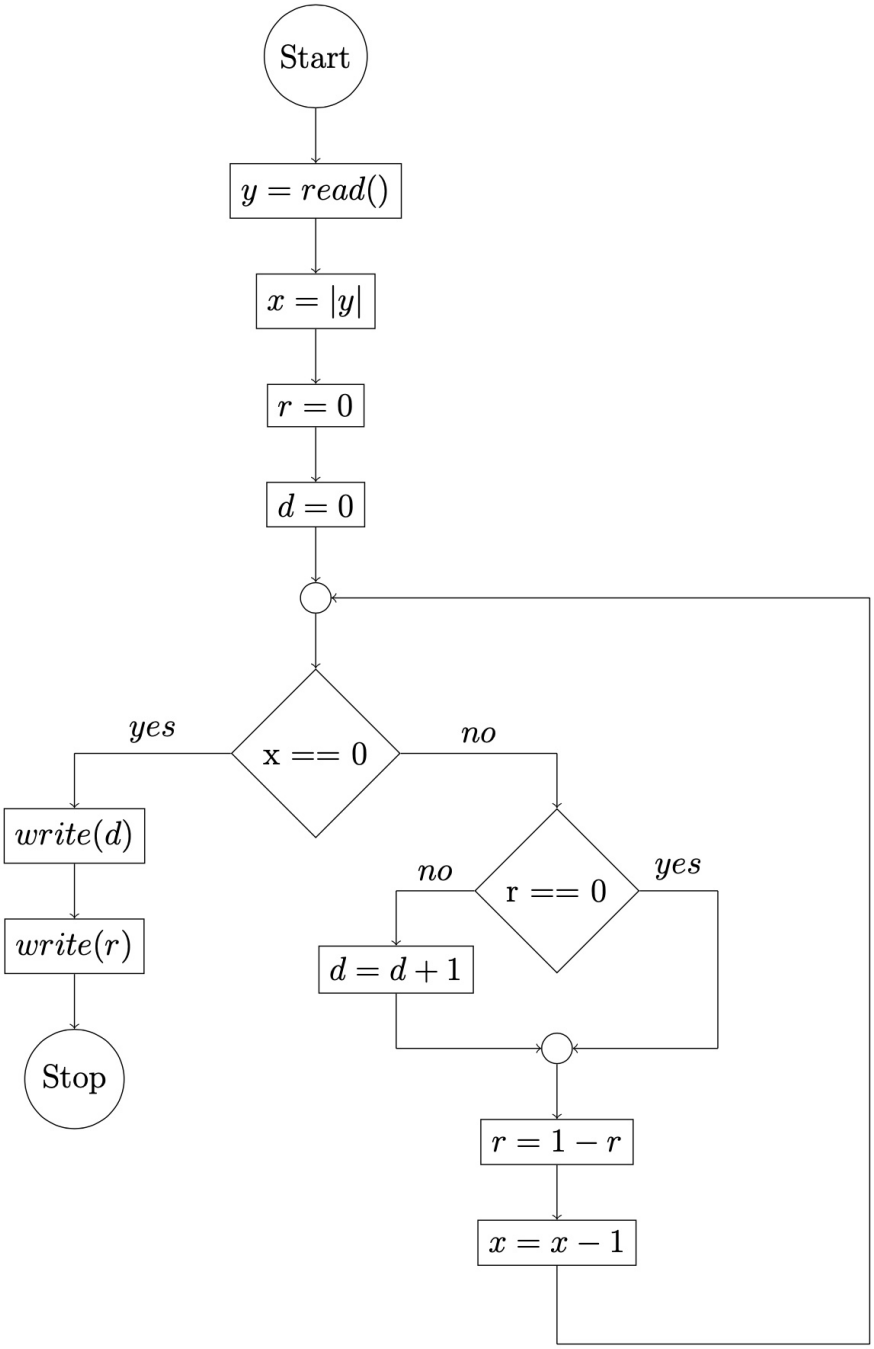
Show that the assertion Z holds for any executions of the program.

Answer of exercise 3.3

The solution to this exercise can be found on artemis (see `https://artemis.ase.in.tum.de/courses/147/exercises/5421`).

3.4 Divide and rest (*2017, H3.7*)

Consider the following program:



Show that the program calculates the result of the integer division $\frac{|y|}{2}$ in d, and the remainder of that division in r. First, formalize this proof goal, then, find a suitable loop invariant, and finally, show the statement using WP calculations.

Answer of exercise 3.4

We formalize the goal: $Z :\equiv |y| = 2d + r \land r \in \{0, 1\}$.
Now we need a suitable loop invariant. By carefully examining the program for a few loop iterations, we arrive at the following invariant: $|y| = x + 2d + r \land r \in \{0, 1\}$.

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(r)}]\!](Z)\\
\equiv\ &\mathsf{WP}[\![\texttt{write(r)}]\!](|y| = 2d + r \land r \in \{0,1\})\\
\equiv\ &|y| = 2d + r \land r \in \{0,1\} \quad \equiv: A
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{write(d)}]\!](A)\\
\equiv\ &\mathsf{WP}[\![\texttt{write(d)}]\!](|y| = 2d + r \land r \in \{0,1\})\\
\equiv\ &|y| = 2d + r \land r \in \{0,1\} \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = x - 1}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = x - 1}]\!](|y| = x + 2d + r \land r \in \{0,1\}\\
\equiv\ &|y| = x - 1 + 2d + r \land r \in \{0,1\} \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{r = 1 - r}]\!](C)\\
\equiv\ &\mathsf{WP}[\![\texttt{r = 1 - r}]\!](|y| = x - 1 + 2d + r \land r \in \{0,1\})\\
\equiv\ &|y| = x - 1 + 2d + 1 - r \land (1 - r) \in \{0,1\}\\
\equiv\ &|y| = x + 2d - r \land r \in \{0,1\} \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{d = d + 1}]\!](D)\\
\equiv\ &\mathsf{WP}[\![\texttt{d = d + 1}]\!](|y| = x + 2d - r \land r \in \{0,1\})\\
\equiv\ &|y| = x + 2d + 2 - r \land r \in \{0,1\} \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{r == 0}]\!](E, D)\\
\equiv\ &\mathsf{WP}[\![\texttt{r == 0}]\!](|y| = x + 2d + 2 - r \land r \in \{0,1\}, |y| = x + 2d - r \land r \in \{0,1\})\\
\equiv\ &(r \neq 0 \land |y| = x + 2d + 2 - r \land r \in \{0,1\}) \lor (r = 0 \land |y| = x + 2d - r \land r \in \{0,1\})\\
&\textit{(Aus } r \neq 0 \textit{ und } r \in \{0,1\} \textit{ folgt } r = 1 \textit{ und somit ist } 2 - r = 2 - 1 = 1 = r\\
&\textit{und wenn } r = 0 \textit{ dann ist } -r = 0 = r\textit{)}\\
\equiv\ &(r \neq 0 \land |y| = x + 2d + r \land r \in \{0,1\}) \lor (r = 0 \land |y| = x + 2d + r \land r \in \{0,1\})\\
&\textit{(Distributivgesetz)}\\
\equiv\ &|y| = x + 2d + r \land r \in \{0,1\} \land (r \neq 0 \lor r = 0)\\
\equiv\ &|y| = x + 2d + r \land r \in \{0,1\} \quad \equiv: F
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x == 0}]\!](F, B)\\
\equiv\ &\mathsf{WP}[\![\texttt{x == 0}]\!](|y| = x + 2d + r \land r \in \{0,1\}, |y| = 2d + r \land r \in \{0,1\})\\
\equiv\ &(x \neq 0 \land |y| = x + 2d + r \land r \in \{0,1\}) \lor (x = 0 \land |y| = 2d + r \land r \in \{0,1\})\\
\equiv\ &(x \neq 0 \land |y| = x + 2d + r \land r \in \{0,1\}) \lor (x = 0 \land |y| = x + 2d + r \land r \in \{0,1\})\\
&\textit{(Distributivgesetz)}\\
\equiv\ &|y| = x + 2d + r \land r \in \{0,1\} \land (x \neq 0 \lor x = 0)\\
\equiv\ &|y| = x + 2d + r \land r \in \{0,1\} \quad \equiv I
\end{aligned}
$$

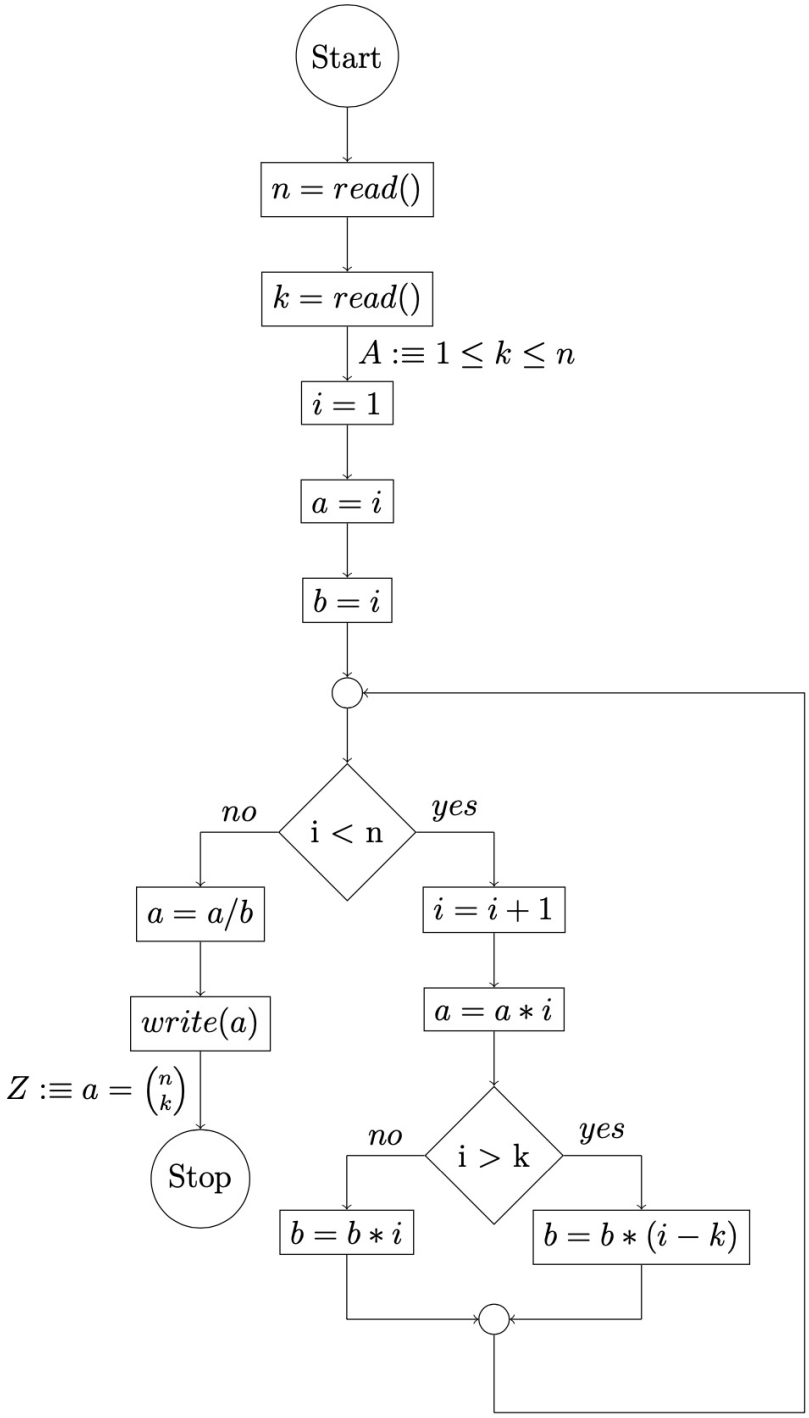
$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{d = 0}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{d = 0}]\!](|y| = x + 2d + r \land r \in \{0,1\})\\
\equiv\ &|y| = x + r \land r \in \{0,1\} \quad \equiv: G
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{r = 0}]\!](G)\\
\equiv\ &\mathsf{WP}[\![\texttt{r = 0}]\!](|y| = x + r \land r \in \{0,1\})\\
\equiv\ &|y| = x \land 0 \in \{0,1\}\\
\equiv\ &|y| = x \quad \equiv: H
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{x = |y|}]\!](H)\\
\equiv\ &\mathsf{WP}[\![\texttt{x = |y|}]\!](|y| = x)\\
\equiv\ &|y| = |y|\\
\equiv\ &\mathit{true} \quad \equiv: J
\end{aligned}
\qquad
\begin{aligned}
&\mathsf{WP}[\![\texttt{y = read}]\!](J)\\
\equiv\ &\mathsf{WP}[\![\texttt{y = read}]\!](\mathit{true}) \equiv \quad \forall y.\, \mathit{true}\\
\equiv\ &\mathit{true} \quad \equiv: K
\end{aligned}
$$

We have now proven local consistency and shown *true* to hold at the start of the program, proving the correctness of Z for all inputs.

3.5 N over K (*2017, H2.6*)

Consider the following program:



Show that the assertion Z annotated at the stop node of the program holds, given the assertion A. Find a suitable loop invariant and show the statement using WP calculations.

Answer of exercise 3.5

To obtain an invariant, we need some pieces of information:

(1) a simply calculates the faculty function, i.e: $a = i!$
(2) $1 \leq k \leq n$
(3) $i \leq n$
(4) As long as $i \leq k$ holds, b is also the faculty function : $i \leq k \implies b = i!$
(5) As soon as i reaches k, $b = k!$ holds, and after that, $(i - k)!$ is multiplied onto b: $i > k \implies b = k!(i - k)!$

The invariant collects this information as follows:

$$I :\equiv a = i! \land 1 \leq k \leq n \land i \leq n \land (i \leq k \implies b = i!) \land (i > k \implies b = k!(i-k)!)$$

For the proof, the following lemmas are useful:

$$A \implies B \land (A \implies C) \land (\neg A \implies D) \equiv B \land C \tag{1}$$

$$(A \implies C) \land (B \implies C) \equiv A \lor B \implies C \tag{2}$$

We begin with the WP calculations:

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{write(a)}]\!](Z) \\
\equiv\ &\mathsf{WP}[\![\texttt{write(a)}]\!](a = \binom{n}{k}) \\
\equiv\ &a = \binom{n}{k} \quad \equiv: A
\end{aligned}$$

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{a = a/b}]\!](A) \\
\equiv\ &\mathsf{WP}[\![\texttt{a = a/b}]\!](a = \binom{n}{k}) \\
\equiv\ &\frac{a}{b} = \binom{n}{k} \\
\equiv\ &a = \frac{n!b}{k!(n-k)!} \quad \equiv: B
\end{aligned}$$

$$\begin{aligned}
&\mathsf{WP}[\![\texttt{b = b * i}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{b = b * i}]\!](a = i! \land 1 \leq k \leq n \land i \leq n \\
&\qquad \land (i \leq k \implies b = i!) \land (i > k \implies b = k!(i-k)!) \\
\equiv\ &a = i! \land 1 \leq k \leq n \land i \leq n \\
&\qquad \land (i \leq k \implies bi = i!) \land (i > k \implies bi = k!(i-k)!) \\
\equiv\ &a = i! \land 1 \leq k \leq n \land i \leq n \\
&\qquad \land (i \leq k \implies b = (i-1)!) \land (i > k \implies b = \frac{k!(i-k)!}{i}) \quad \equiv: C
\end{aligned}$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b = b * (i-k)}]\!](I)\\
\equiv\ &\mathsf{WP}[\![\texttt{b = b * (i-k)}]\!](a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = i!) \land (i > k \implies b = k!(i-k)!)\\
\equiv\ &a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b(i-k) = i!) \land (i > k \implies b(i-k) = k!(i-k)!)\\
\equiv\ &a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = \frac{i!}{i-k}) \land (i > k \implies b = k!(i-k-1)!) \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i > k}]\!](C, D)\\
\equiv\ &\mathsf{WP}[\![\texttt{i > k}]\!](a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = \frac{k!(i-k)!}{i}),\\
&\quad a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = \frac{i!}{i-k}) \land (i > k \implies b = k!(i-k-1)!))\\
\equiv\ &(i \le k \implies a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = \frac{k!(i-k)!}{i}))\\
&\quad \land (i > k \implies a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = \frac{i!}{i-k}) \land (i > k \implies b = k!(i-k-1)!))\\
&\textit{(Wir nutzen Lemma 1 um beide Teile der Konjunktion zu vereinfachen)}\\
\equiv\ &(i \le k \implies a = i! \land 1 \le k \le n \land i \le n \land b = (i-1)!)\\
&\qquad \land (i > k \implies a = i! \land 1 \le k \le n \land i \le n \land b = k!(i-k-1)!)\\
&\textit{(Distributivgesetz)}\\
\equiv\ &a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = k!(i-k-1)!) \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{a = a * i}]\!](E)\\
\equiv\ &\mathsf{WP}[\![\texttt{a = a * i}]\!](a = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = k!(i-k-1)!))\\
\equiv\ &a * i = i! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = k!(i-k-1)!)\\
\equiv\ &a = (i-1)! \land 1 \le k \le n \land i \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = k!(i-k-1)!) \quad \equiv: F
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = i + 1}]\!](F)\\
\equiv\ &\mathsf{WP}[\![\texttt{i = i + 1}]\!](a = (i-1)! \land 1 \le k \le n \land i + 1 \le n\\
&\qquad \land (i \le k \implies b = (i-1)!) \land (i > k \implies b = k!(i-k-1)!))\\
\equiv\ &a = i! \land 1 \le k \le n \land i + 1 \le n\\
&\qquad \land (i + 1 \le k \implies b = i!) \land (i + 1 > k \implies b = k!(i-k)!)\\
\equiv\ &a = i! \land 1 \le k \le n \land i < n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!) \quad \equiv: G
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i < n}]\!](B, G)\\
\equiv\ &\mathsf{WP}[\![\texttt{i < n}]\!](a = \frac{n!b}{k!(n-k)!}, a = i! \land 1 \le k \le n \land i < n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))\\
\equiv\ &(i \ge n \land a = \frac{n!b}{k!(n-k)!}) \lor (i < n \land a = i! \land 1 \le k \le n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))
\end{aligned}
$$

(Nun verstärken wir $i \ge n$ zu $i = n$ und fügen alles was auf der rechten Seite auftaucht auch auf der linken Seite hinzu)

$$
\begin{aligned}
\impliedby\ &(i = n \land a = \frac{n!b}{k!(n-k)!} \land 1 \le k \le n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))\\
&\quad \lor (i < n \land a = i! \land 1 \le k \le n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))
\end{aligned}
$$

(Aus $i = n$ und $k \le n$ folgt nun $k \le i$ und damit gilt $b = k!(i-k)!$)

$$
\begin{aligned}
\equiv\ &(i = n \land a = \frac{i!k!(i-k)!}{k!(i-k)!} \land 1 \le k \le n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))\\
&\quad \lor (i < n \land a = i! \land 1 \le k \le n\\
&\qquad \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!))
\end{aligned}
$$

(Distributivgesetz)

$$
\equiv a = i! \land 1 \le k \le n \land (i < k \implies b = i!) \land (i \ge k \implies b = k!(i-k)!) \land (i = n \lor i < n)
$$

(Wir spalten die vorletzte Klammer mit Lemma 2 auf)

$$
\begin{aligned}
\equiv\ &a = i! \land 1 \le k \le n \land i \le n \land\\
&\quad (i < k \implies b = i!) \land (i = k \implies b = k!(i-k)!) \land (i > k \implies b = k!(i-k)!)\\
\equiv\ &a = i! \land 1 \le k \le n \land i \le n \land\\
&\quad (i < k \implies b = i!) \land (i = k \implies b = i!) \land (i > k \implies b = k!(i-k)!)
\end{aligned}
$$

(Wir nutzen erneut Lemma 2 um zusammenzufassen)

$$
\begin{aligned}
\equiv\ &a = i! \land 1 \le k \le n \land i \le n \land\\
&\quad (i \le k \implies b = i!) \land (i > k \implies b = k!(i-k)!) \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{b = i}]\!](I) \\
\equiv\ &\mathsf{WP}[\![\texttt{b = i}]\!](a = i! \land 1 \leq k \leq n \land i \leq n \land \\
&\qquad (i \leq k \implies b = i!) \land (i > k \implies b = k!(i-k)!)) \\
\equiv\ &a = i! \land 1 \leq k \leq n \land i \leq n \land \\
&\qquad (i \leq k \implies i = i!) \land (i > k \implies i = k!(i-k)!) \quad \equiv: H
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{a = i}]\!](H) \\
\equiv\ &\mathsf{WP}[\![\texttt{a = i}]\!](a = i! \land 1 \leq k \leq n \land i \leq n \land \\
&\qquad (i \leq k \implies i = i!) \land (i > k \implies i = k!(i-k)!)) \\
\equiv\ &i = i! \land 1 \leq k \leq n \land i \leq n \land \\
&\qquad (i \leq k \implies i = i!) \land (i > k \implies i = k!(i-k)!) \quad \equiv: J
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{WP}[\![\texttt{i = 1}]\!](J) \\
\equiv\ &\mathsf{WP}[\![\texttt{i = 1}]\!](i = i! \land 1 \leq k \leq n \land i \leq n \land \\
&\qquad (i \leq k \implies i = i!) \land (i > k \implies i = k!(i-k)!)) \\
\equiv\ &1 = 1! \land 1 \leq k \leq n \land 1 \leq n \land \\
&\qquad (1 \leq k \implies 1 = 1!) \land (1 > k \implies 1 = k!(1-k)!) \\
\equiv\ &1 \leq k \leq n \quad \equiv A
\end{aligned}
$$