

# FPV Tutorübung

Woche 1

## Implications, Assertions and Conditions

Manuel Lerchner

20.04.2023

# Organisatorisches

## Grade Bonus

- Successful participation ( $\geq 70\%$ ) in quizzes and programming tasks will lead to a bonus of 0.3 in the final exam, provided that you passed the exam.
- Programming homework and quizzes are to be submitted individually.
- Discussing solutions before the end of the week is considered plagiarism.
- Plagiarism will not be tolerated and will (at the very least) lead to exclusion from the bonus system

## Changes

- Manual correction of homework not possible. However, non-programming exercises remain crucial for the exam
- 20% of the exam will be Single-Choice
- To receive points in the exam, your code needs to compile
- We currently anticipate an in-person exam using Artemis

# Materialien

The screenshot displays the GitHub repository page for `ManuelLerchner/fpv-tutorial-SS23`. The repository is public and has 334 commits. The main branch is `master`, with 1 branch and 0 tags. The repository was last updated 2 weeks ago.

The repository structure includes the following files and folders:

- `.github/workflows`: fix (2 weeks ago)
- `docs`: Update PDFs (2 weeks ago)
- `md`: add slide template (2 weeks ago)
- `ocaml`: clean up project (2 weeks ago)
- `slides`: clean up project (2 weeks ago)
- `.gitignore`: improve rendering (2 weeks ago)
- `README.md`: add slide template (2 weeks ago)
- `render.sh`: initial commit (last month)

The README content is titled "FPV Tutorial - SS23" and includes the following sections:

- Renderers**: Rerender PDFs (passing), Deploy static content to Pages (passing)
- About**: Materialien für Manuel's FPV-Tutorium im Sommersemester 2023. Die Materialien sind privat erstellt und können Fehler enthalten. Im Zweifelsfall haben immer die offiziellen

The right sidebar shows the repository's "About" section, which includes the repository's description, a link to the repository's website, and the repository's statistics (0 stars, 1 watching, 0 forks). The "Environments" section shows the repository is active, and the "Languages" section shows the repository is primarily composed of OCaml (61.5%) and Shell (38.5%).

# Quiz



Artemis 6.1.3

Courses > Funktionale Programmierung und Verifikation (Sommersemester 2023) > Exercises > Week 02 Quiz

✓ Week 02 Quiz **Quiz**

Points: 20

[Open quiz](#)

The quiz is not active.

**Communication**

Search for a post

☐ Unresolved ☐ Own ☐ Reacted

Date: →

No posts found.

[+](#)

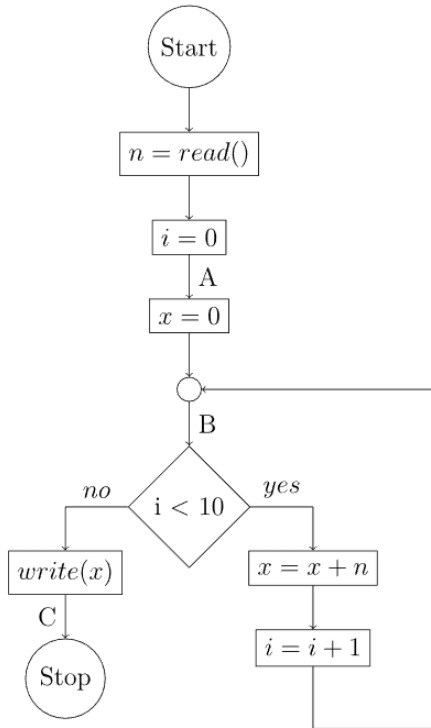
Password:

---

# T01: Recap Implications

1.  $x = 1 \implies 0 < x$
2.  $x < 6 \implies x = 3$
3.  $x > 0 \implies x \geq 0$
4.  $x = -2 \implies x < -1 \vee x > 1$
5.  $x = 0 \vee x = 7 \implies 4 \neq x$
6.  $x = 1 \implies x \leq 3 \wedge y > 0$
7.  $x < 8 \wedge y = x \implies y \neq 12$
8.  $x = 1 \vee y = 1 \implies x > 0$
9.  $x \neq 5 \implies \text{false}$
10.  $\text{true} \implies x \neq y$
11.  $\text{false} \implies x = 1$
12.  $x \geq 1 \implies 2x + 3 = 5$
13.  $A \wedge x = y \implies A$
14.  $B \implies A \vee B$
15.  $A \implies (B \implies A)$
16.  $(A \implies B) \implies A$

# T02: Assertions



1. Which of the following assertions hold at point *A*?

- a)  $i \geq 0$
- b)  $x = 0$
- c)  $i \leq 10 \wedge x \neq 0$
- d) *true*
- e)  $i = 0$
- f)  $x = i$

2. Which of the following assertions hold at point *B*?

- a)  $x = 0 \wedge i = 0$
- b)  $x = i$
- c)  $i < x$
- d)  $0 \leq i \leq 10$
- e)  $i \geq 0 \wedge x \geq 0$
- f)  $n = 1 \implies x = i$

3. Which of the following assertions hold at point *C*?

- a)  $i \geq 0$
- b)  $i = 10$
- c)  $i > 0$
- d)  $x \neq n$
- e)  $x = 10n$
- f)  $x = i * n \wedge i = 10$

# T03: The Strong and the Weak

3. Which of the following assertions hold at point  $C$ ?

- a)  $i \geq 0$  ✓
- b)  $i = 10$  ✓
- c)  $i > 0$  ✓
- d)  $x \neq n$  ✗
- e)  $x = 10n$  ✓
- f)  $x = i * n \wedge i = 10$  ✓

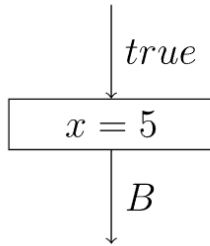
Again consider the assertions that hold at point  $C$  of assignment 2. Discuss the following questions:

1. When annotating the control flow graph, can you say that one of the given assertions is "better" than the others?
2. Can you arrange the given assertions in a meaningful order?
3. How can you define a *stronger than* relation formally?
4. How do *true* and *false* fit in and what is their meaning as an assertion?
5. What are the strongest assertions that still hold at  $A$ ,  $B$  and  $C$ ?



# T04: Strongest Postconditions 1

1.



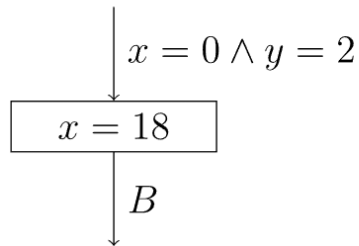
3.



5.



2.



4.



6.



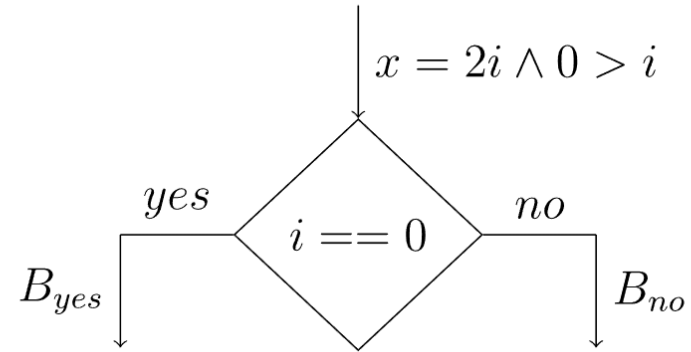


## T04: Strongest Postconditions 2

7.



8.



## T04: Strongest Postconditions 3

9.



# FPV Tutorübung

Woche 2

## Preconditions, Postconditions and Local Consistency

Manuel Lerchner

03.05.2023

# Quiz



Artemis 6.1.3

Courses > Funktionale Programmierung und Verifikation (Sommersemester 2023) > Exercises > Week 02 Quiz

✓ Week 02 Quiz **Quiz**

Points: 20

[Open quiz](#) The quiz is not active.

**Communication**

Search for a post

☐ Unresolved ☐ Own ☐ Reacted

Date: →

No posts found.

Password:

---

# T01: From Post- to Preconditions

1.



2.



3.



1. For each of these graphs show whether the assertion  $Z$  holds...
  - (a) ...using strongest postconditions and
  - (b) ...using weakest preconditions.
2. Discuss advantages and disadvantages of either approach.

# T01: From Post- to Preconditions 1

Post-Condition:

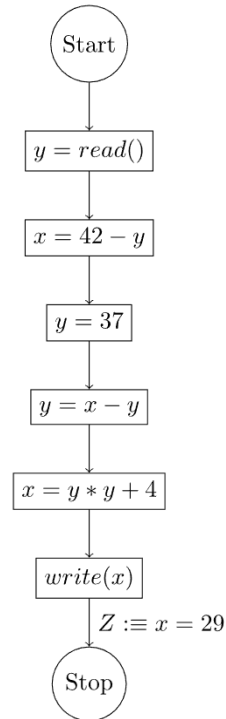


Pre-Condition:

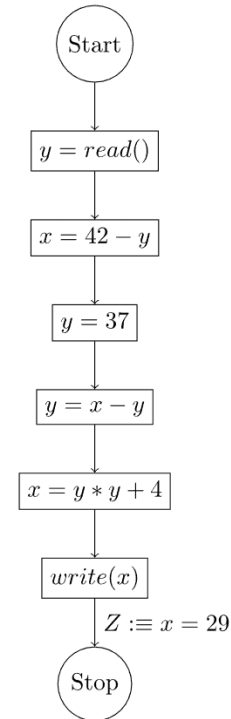


# T01: From Post- to Preconditions 2

Post-Condition:

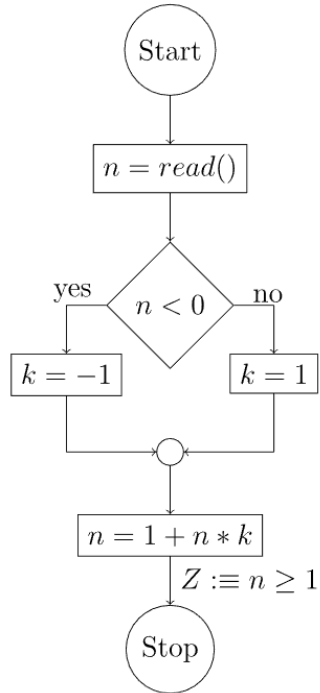


Pre-Condition:



# T01: From Post- to Preconditions 3

Post-Condition:

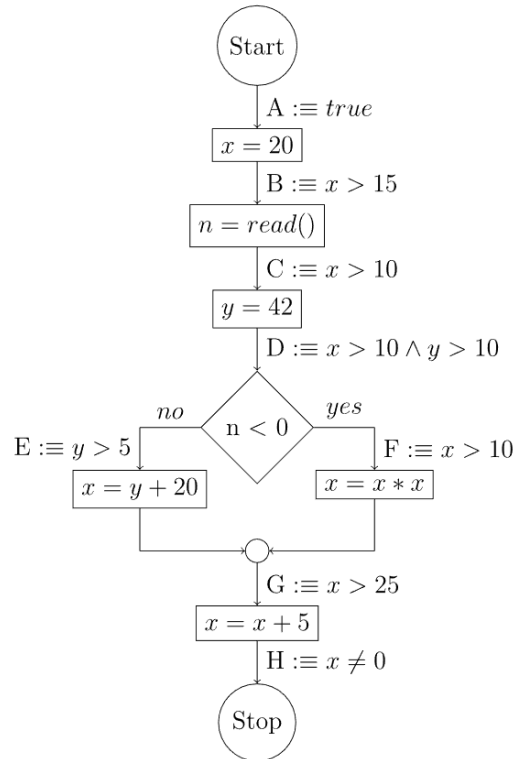


Pre-Condition:



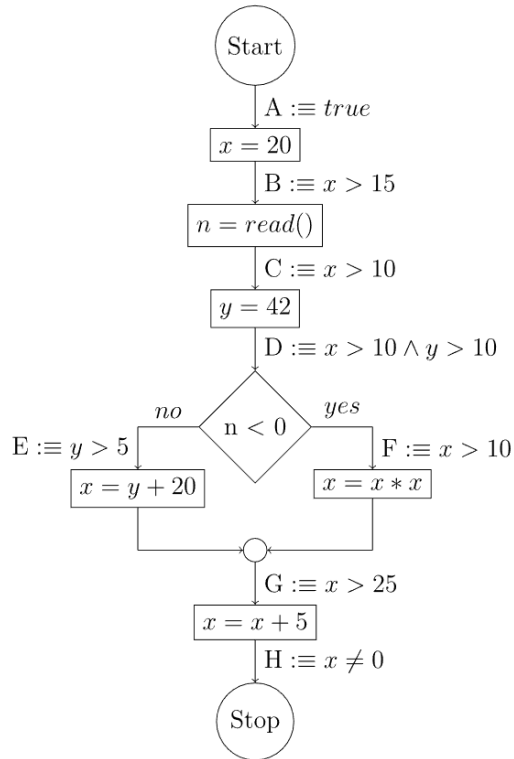


# T02: Local Consistency

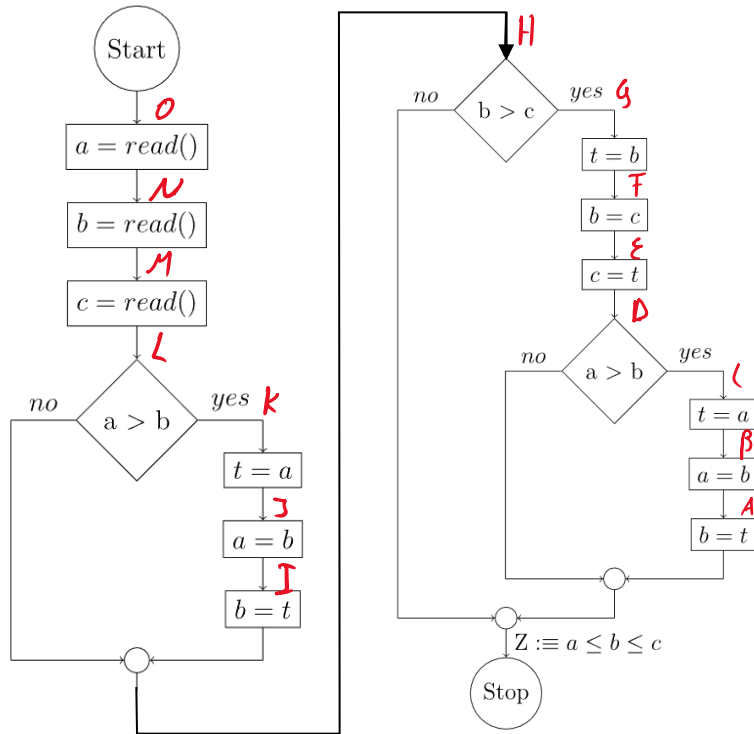


Check whether the annotated assertions prove that the program computes an  $x \neq 0$  and discuss why this is the case.

# T02: Local Consistency (Extra Space)



# T03: Trouble Sort



1. Annotate each program point in the following control flow diagram with a suitable assertion, then show that your annotations are locally consistent and prove that  $Z$  holds at the given program point.
2. Discuss the drawbacks of annotating each program point with an assertion before applying weakest preconditions, and discuss how you could optimize the approach to proving that  $Z$  holds.

# T03: Trouble Sort (Extra Space)



# FPV Tutorübung


Woche 3

## MiniJava 2.0, Loop Invariants

Manuel Lerchner

09.05.2023

# Quiz



**Artemis** 6.1.6

Courses > Funktionale Programmierung und Verifikation (Sommersemester 2023) >

✓ Week 03 Quiz **Quiz**

Points: 20

▶ Open quiz

Password:

---

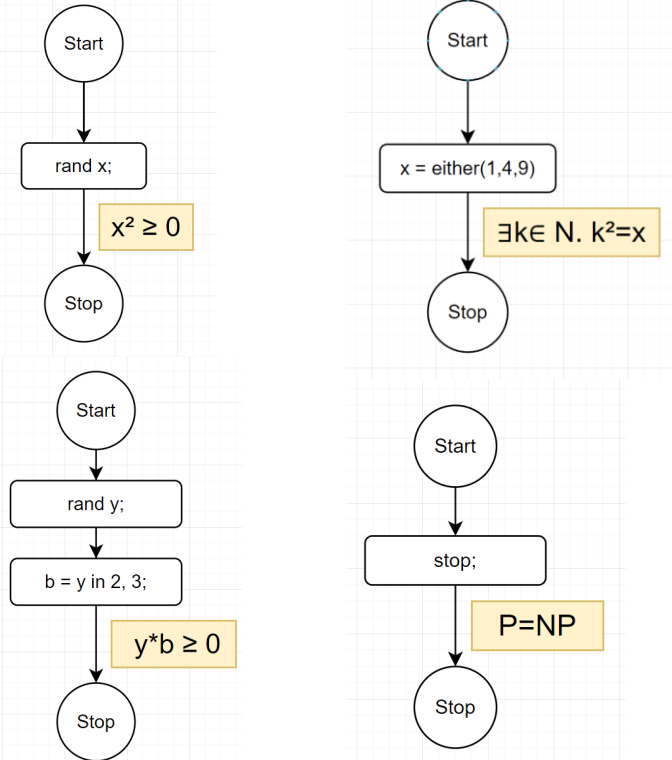
# T01: MiniJava 2.0

In the lecture, the weakest precondition operator has been defined for all statements of MiniJava. In this assignment, we consider an extension of the MiniJava language, which provides four new statements:

1. **rand x**:  
Assigns a random value to variable  $x$ ,
2. **x = either  $e_0, \dots, e_k$** :  
Assigns one of the values of the expressions  $e_0, \dots, e_k$  to variable  $x$  non-deterministically,
3. **x = e in a, b**:  
Assigns the value 1 to variable  $x$ , if the value of expression  $e$  is in the range  $[a, b]$  and 0 if  $e$  is not in the range or the range is empty ( $a > b$ ),
4. **stop**:  
Immediately stops the program.

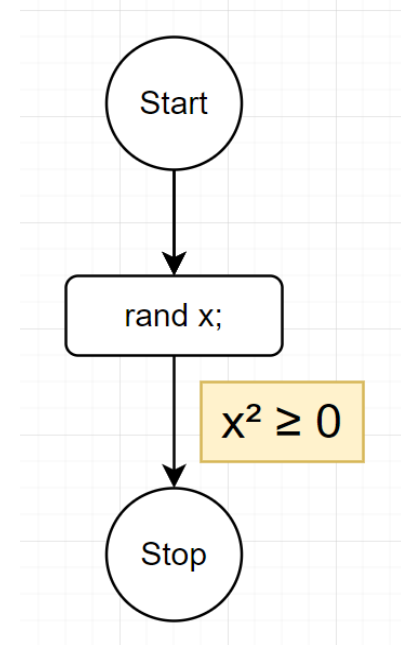
Define the weakest precondition operator  $\mathbf{WP}[\cdot](B)$  for each of these statements. (In terms of  $B$ )

## Beispiele zum Testen:



# T01: MiniJava 2.0

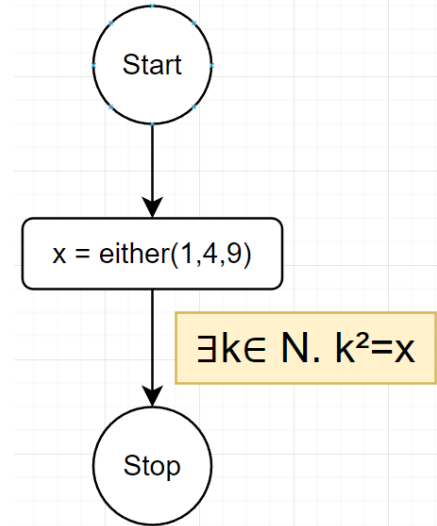
WP[rand x;](B) =





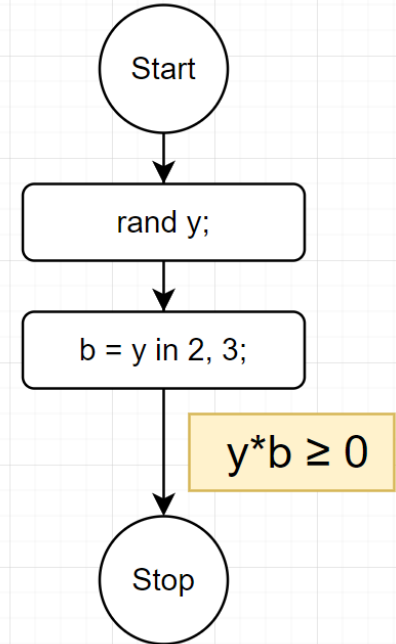
# T01: MiniJava 2.0

$WP[x = \text{either } e_0, e_1 \dots e_k](B) =$



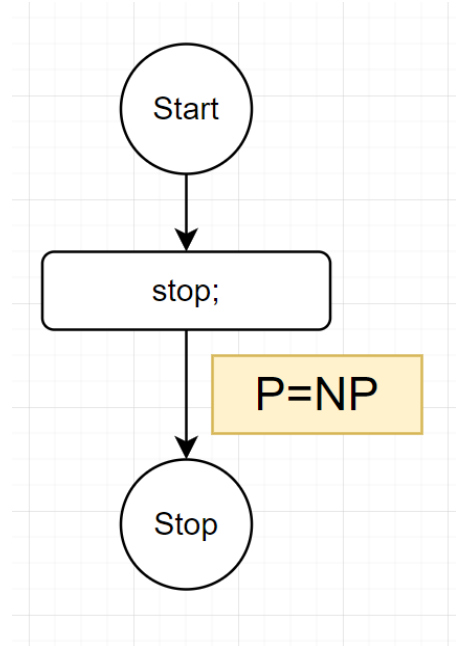
# T01: MiniJava 2.0

$WP[x \text{ e in } a, b](B) =$



# T01: MiniJava 2.0

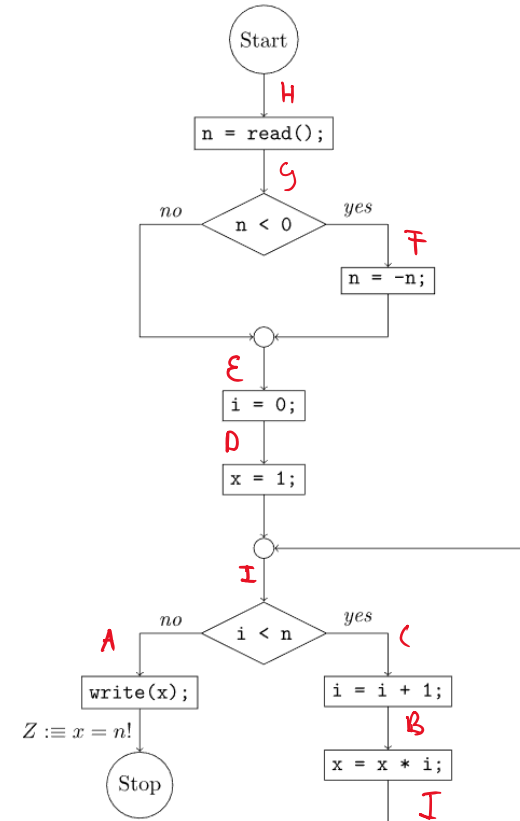
$WP[\text{stop}](B) =$



# T02: Loop Invariants

1. Discuss the problem that arises when computing weakest preconditions to prove  $Z$ .
2. How can you use weakest preconditions to prove  $Z$  anyway?
3. Try proving  $Z$  using the the loop invariants  $x \geq 0$  and  $i = 0 \wedge x = 1 \wedge n = 0$  at the end of the loop body and in particular discuss these questions:
  - a) How has a useful loop invariant be related to  $Z$ ?
  - b) What happens if the loop invariant is chosen too strong?
  - c) What happens if the loop invariant is chosen too weak?
  - d) Can you give a meaningful lower and upper bound for useful loop invariants?
4. Retry proving  $Z$  using the loop invariant  $x = i!$  (again at the end of the loop body) and improve this invariant until the proof succeeds.

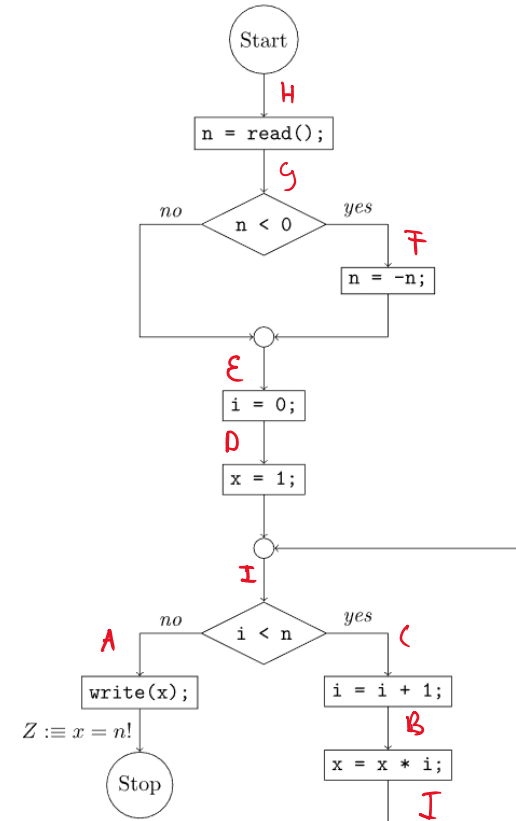
A program computes the factorial of its input:



# T02: Loop Invariants 1

3. Try proving  $Z$  using the the loop invariants  $x \geq 0$  and  $i = 0 \wedge x = 1 \wedge n = 0$  at the end of the loop body and in particular discuss these questions:

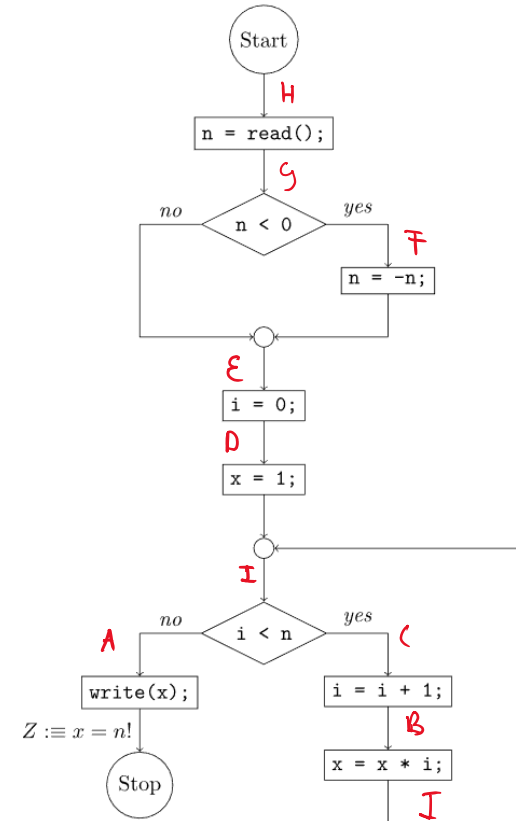
A program computes the factorial of its input:



# T02: Loop Invariants 2

3. Try proving  $Z$  using the the loop invariants  $x \geq 0$  and  $i = 0 \wedge x = 1 \wedge n = 0$  at the end of the loop body and in particular discuss these questions:

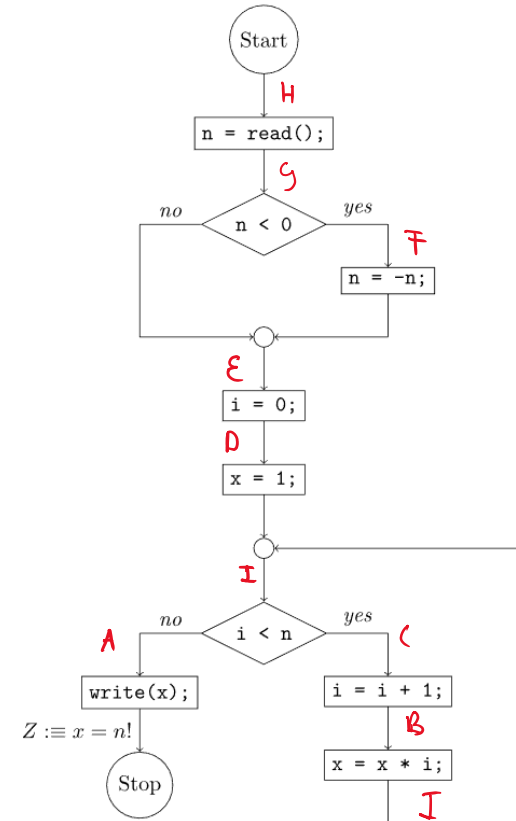
A program computes the factorial of its input:



# T02: Loop Invariants 3

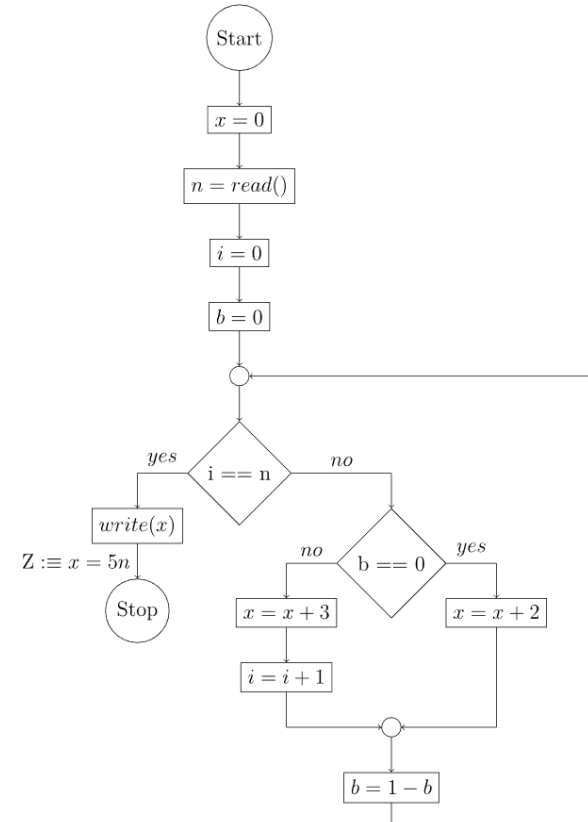
4. Retry proving  $Z$  using the loop invariant  $x = i!$  (again at the end of the loop body) and improve this invariant until the proof succeeds.

A program computes the factorial of its input:



# T03: Two b, or Not Two b

Prove  $Z$  using weakest preconditions.





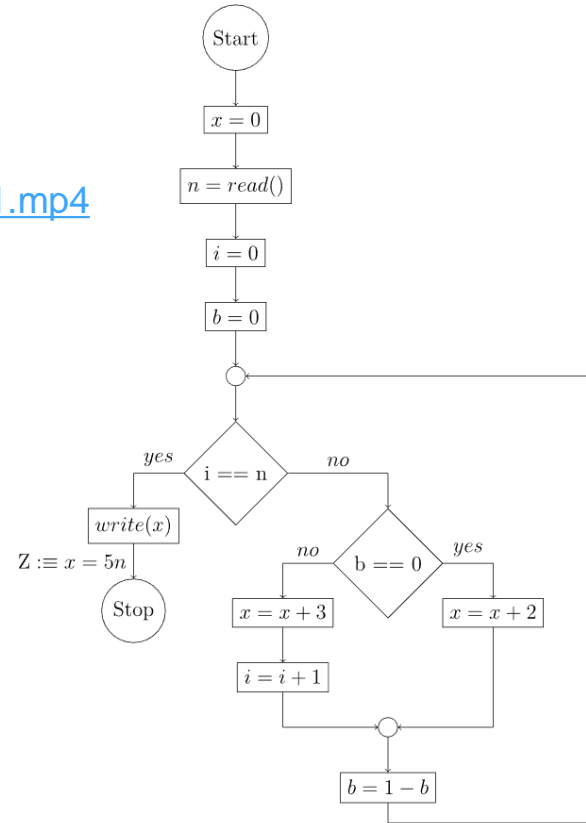
# T03: Two b, or Not Two b

Tipps zum finden von Loop Invarianten:

[https://ttt.in.tum.de/recordings/Info2\\_2017\\_11\\_24-1/Info2\\_2017\\_11\\_24-1.mp4](https://ttt.in.tum.de/recordings/Info2_2017_11_24-1/Info2_2017_11_24-1.mp4)

Beispieltrace:  $n=3$

Variable \ Schleifendurchgang	0	1	2	3	4	5	6
<b>x</b>	0	2	5	7	10	12	15
<b>i</b>	0	0	1	1	2	2	3
<b>b</b>	0	1	0	1	0	1	0



# Tipps für Loop Invarianten

[https://tut.in.tum.de/recordings/Info2\\_2017\\_11\\_24-1/Info2\\_2017\\_11\\_24-1.mp4](https://tut.in.tum.de/recordings/Info2_2017_11_24-1/Info2_2017_11_24-1.mp4)

## Tipps

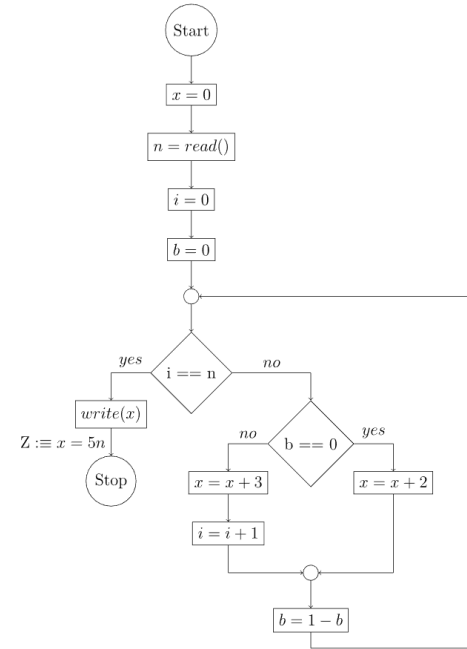
**Tipps**  
Wir benötigen eine Aussage über den Wert der Variablen, über die wir etwas beweisen wollen ( $x$ ) in der Schleifeninvariante. Die Aussage muss dabei mindestens so präzise ( $\neq, \geq, \leq, =$ ) sein, wie die Aussage, die wir beweisen wollen.

## Tipps

**Tipps**  
Variablen, die an der Berechnung von  $x$  beteiligt sind **und** Werte von einer Schleifeniteration in die nächste transportieren ("loop-carried"), müssen in die Schleifeninvariante aufgenommen werden.

## Tipps

**Tipps**  
Die Schleife zu verstehen ist unerlässlich. Eine Tabelle für einige Schleifendurchläufe kann helfen die Zusammenhänge der Variablen (insbesondere mit dem Schleifenzähler  $i$ ) aufzudecken. Oft lassen sich mit einer Tabelle, in der man die einzelnen Berechnungsschritte notiert, diese Zusammenhänge deutlich leichter erkennen, als mit einer Tabelle, die nur konkrete Werte enthält.



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