

# 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 interface for the repository `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 by `github-actions[bot]`.

The file list shows the following structure:

- `.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.md` file is selected, showing the title **FPV Tutorial - SS23**. Below the title, there are two status indicators: `Rerender PDFs` (passing) and `Deploy static content to Pages` (passing). The **About** section states: "Materialien für Manuel's FPV-Tutorium im Sommersemester 2023." and "Die Materialien sind privat erstellt und können Fehler enthalten. Im Zweifelsfall haben immer die offiziellen".

The right sidebar shows the repository's **About** section, including the link `manuellernher.github.io/fpv-tutorial-SS...`, 0 stars, 1 watching, and 0 forks. The **Environments** section shows `github-pages` as **Active**. The **Languages** section shows a progress bar for `OCaml` (61.5%) and `Shell` (38.5%).

# Quiz

The screenshot shows the Artemis 6.1.3 interface. At the top, the navigation bar includes the Artemis logo, version 6.1.3, a notification bell, a sun icon, a user profile 'ge47wer', and a menu icon. Below this, the breadcrumb trail reads: 'Courses > Funktionale Programmierung und Verifikation (Sommersemester 2023) > Exercises > Week 02 Quiz'. The main header area displays 'Week 02 Quiz' with a green 'Quiz' tag and 'Points: 20'. A blue button labeled 'Open quiz' is visible. To the right, a message states 'The quiz is not active.' with three small icons (a calendar, a play button, and a refresh button). Below this is a 'Communication' section with a search bar, filters for 'Unresolved', 'Own', and 'Reacted', and a 'Date' dropdown. The search results show 'No posts found.' and a blue button with a plus sign.

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.



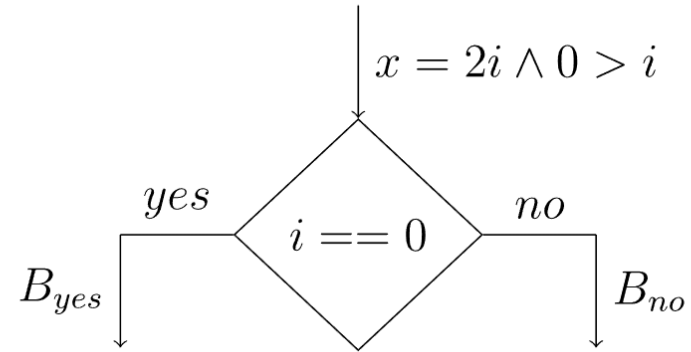


## T04: Strongest Postconditions 2

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:

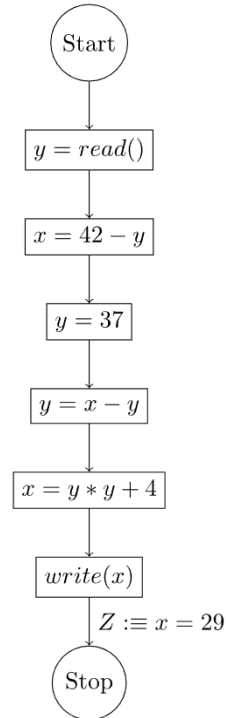


Pre-Condition:

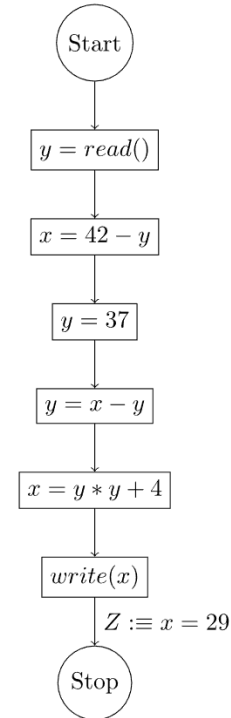


# T01: From Post- to Preconditions 2

Post-Condition:

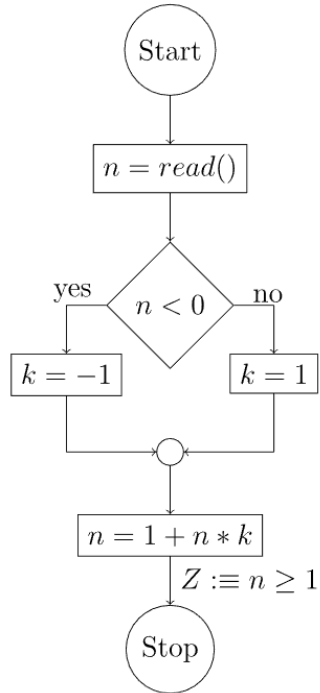


Pre-Condition:

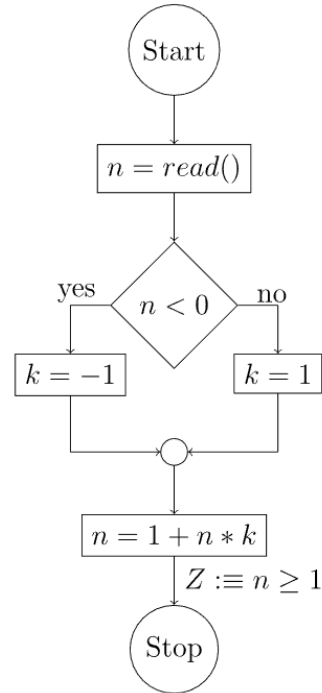


# T01: From Post- to Preconditions 3

Post-Condition:



Pre-Condition:



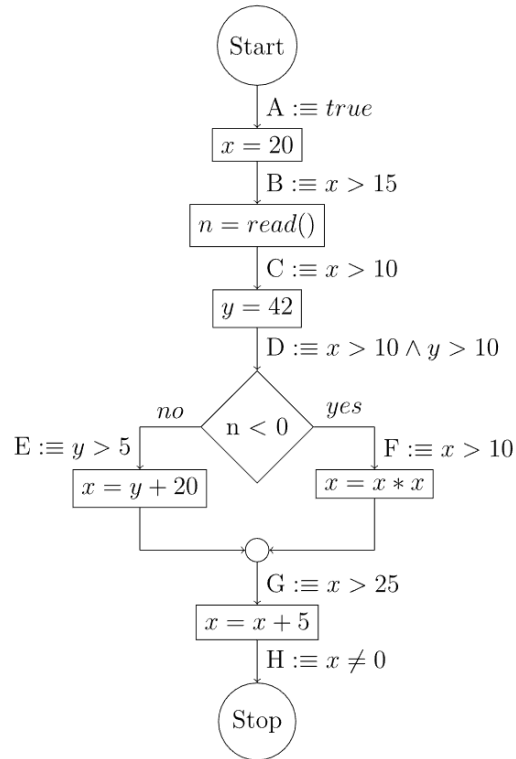


# T02: Local Consistency

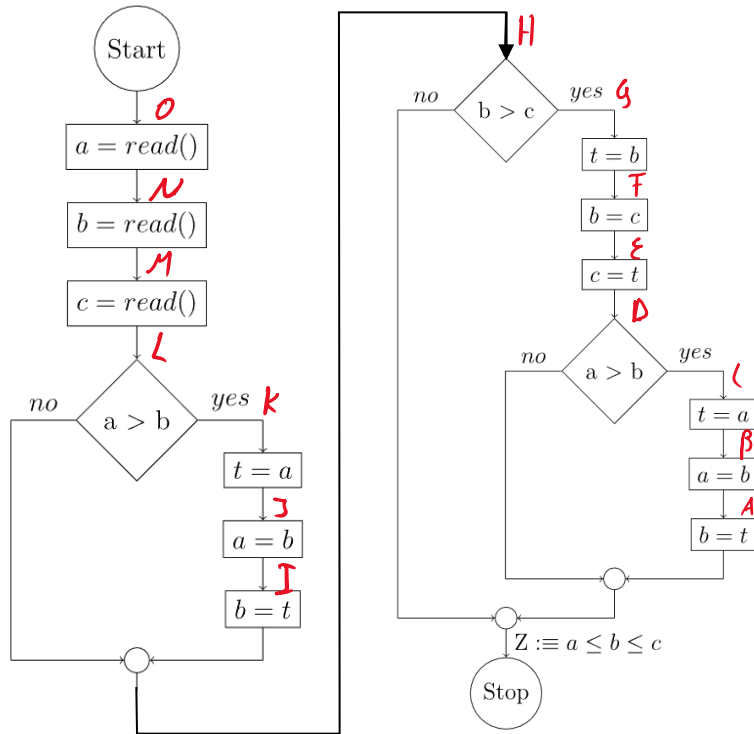


Check whether the annotated assertions prove that the program computes an  $x \neq 0$  and discuss why this is the case.

# 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:

---

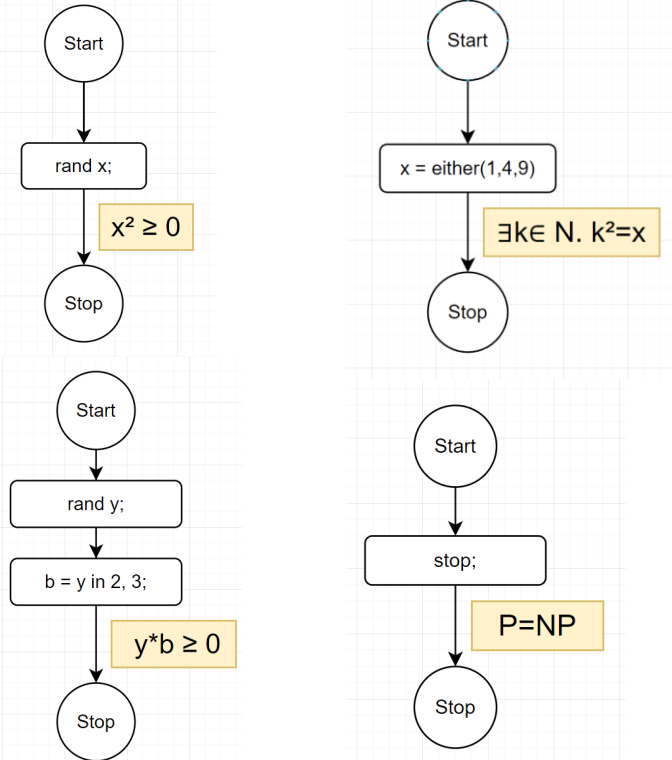
# T01: MiniJava 2.0

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.

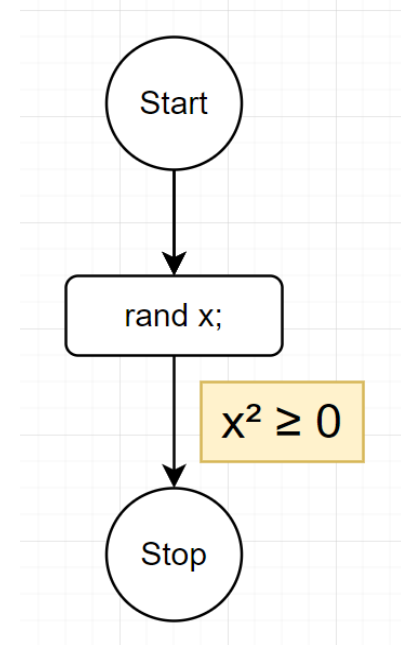
Define the weakest precondition operator  $\mathbf{WP}[\cdot](B)$  for each of these statements. (In terms of  $B$ )

## Beispiele zum Testen:



# T01: MiniJava 2.0

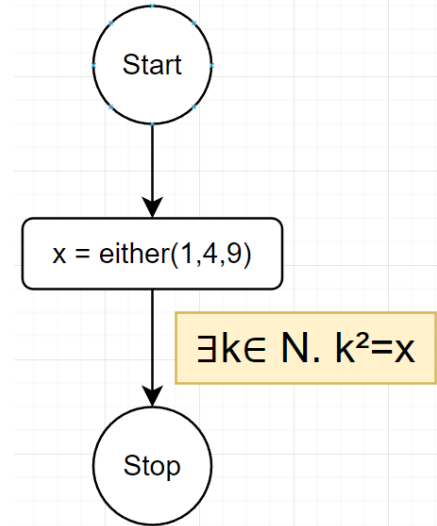
$WP[\text{rand } x;](B) =$





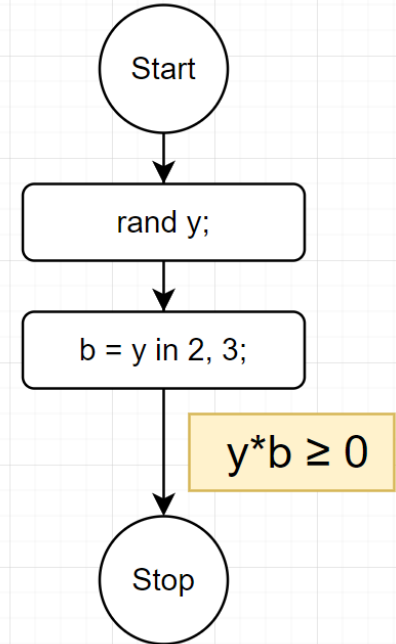
# T01: MiniJava 2.0

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



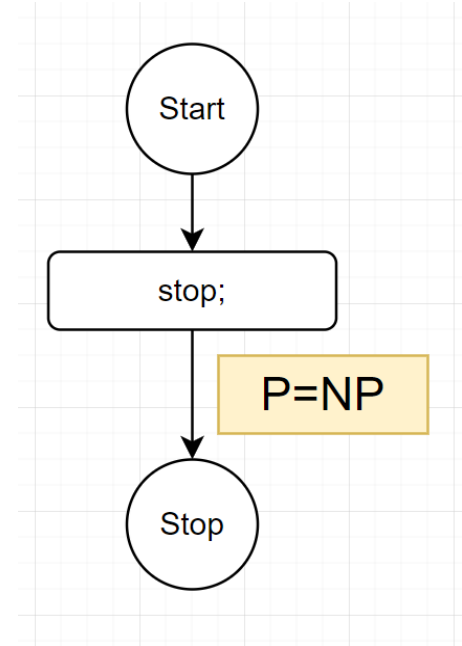
# T01: MiniJava 2.0

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



# T01: MiniJava 2.0

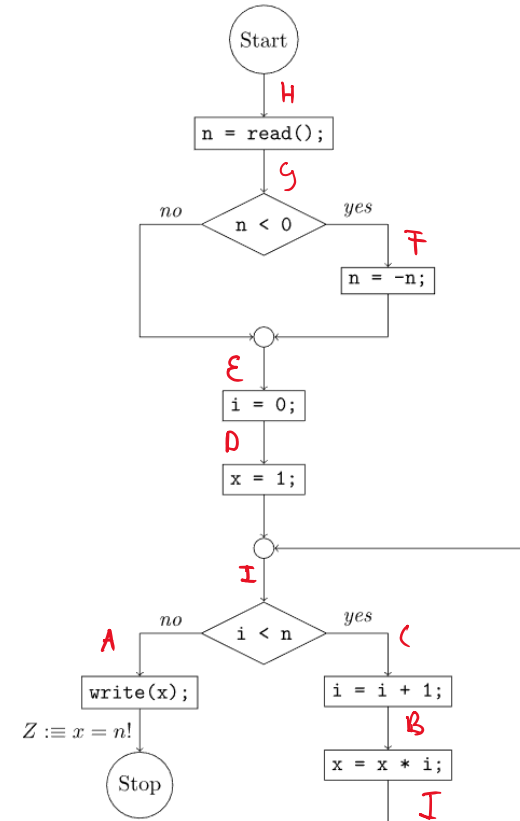
$WP[\text{stop}](B) =$



# 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:
  - o a) How has a useful loop invariant be related to  $Z$ ?
  - o b) What happens if the loop invariant is chosen too strong?
  - o c) What happens if the loop invariant is chosen too weak?
  - o 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.

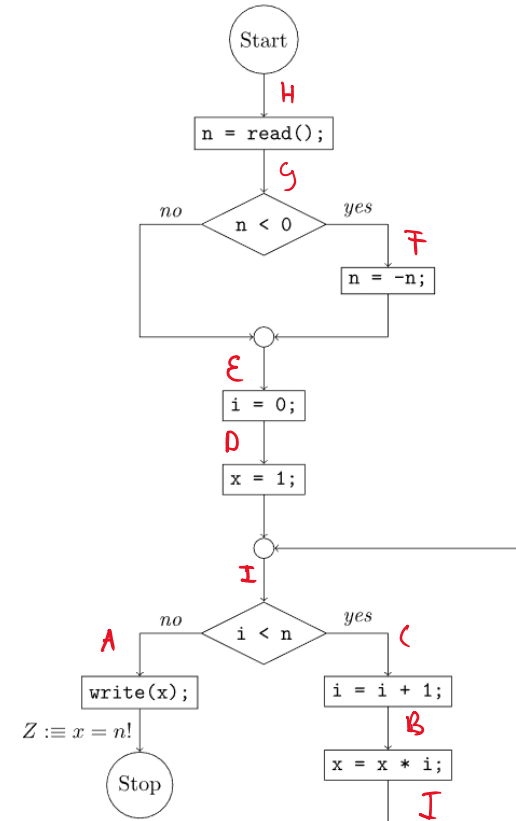
A program computes the factorial of its input:



# 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:

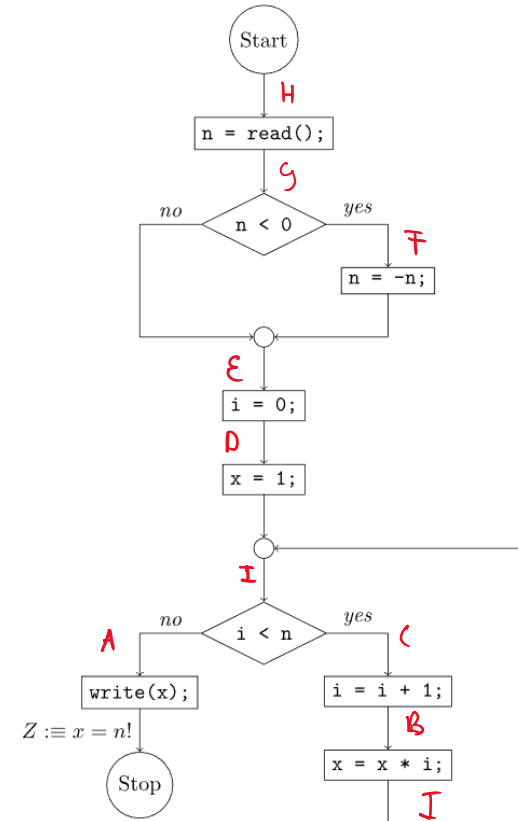
A program computes the factorial of its input:



# 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:

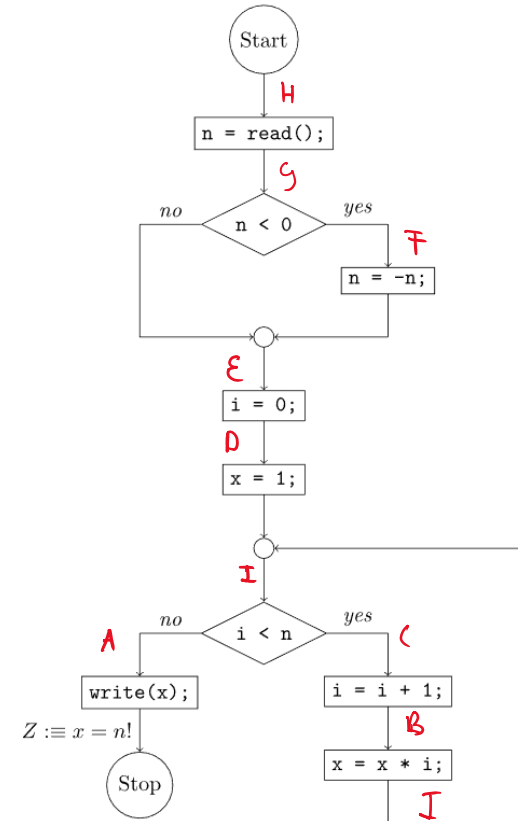
A program computes the factorial of its input:



# T02: Loop Invariants 3

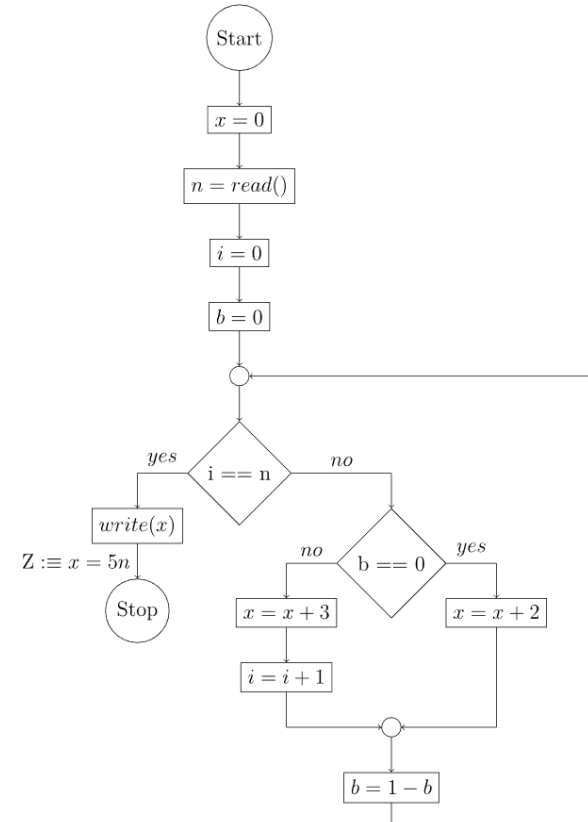
4. Retry proving  $Z$  using the loop invariant  $x = i!$  (again at the end of the loop body) and improve this invariant until the proof succeeds.

A program computes the factorial of its input:



# T03: Two b, or Not Two b

Prove  $Z$  using weakest preconditions.





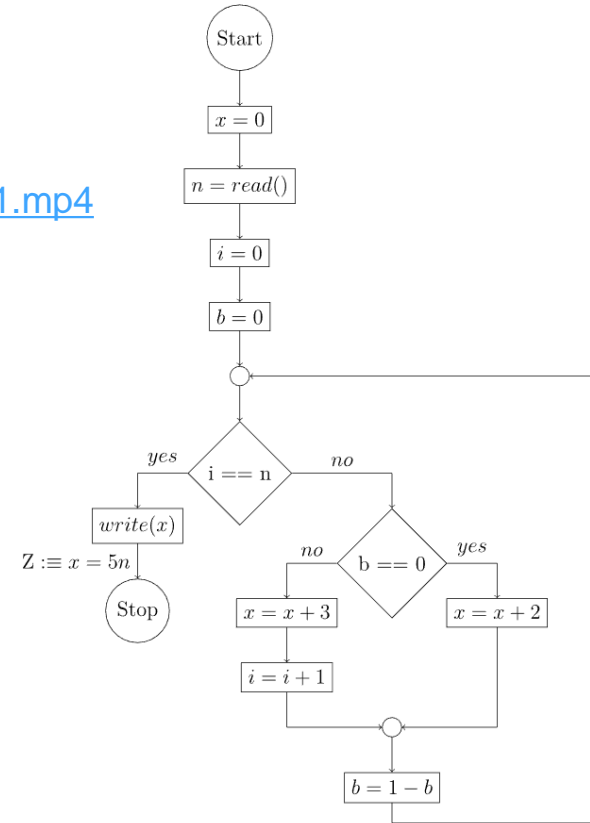
# T03: Two b, or Not Two b

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

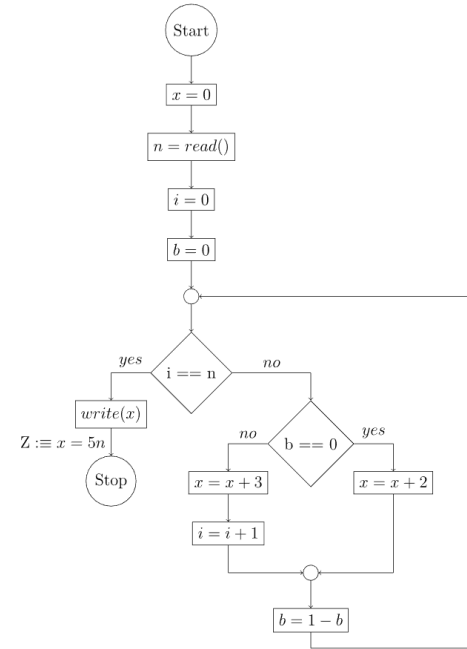
**Tipps**  
Wir benötigen eine Aussage über den Wert der Variablen, über die wir etwas beweisen wollen ( $x$ ) in der Schleifeninvariante. Die Aussage muss dabei mindestens so präzise ( $\neq, \geq, \leq, =$ ) sein, wie die Aussage, die wir beweisen wollen.

## 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.



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

# FPV Tutorübung

Woche 4

## Loop Invariants and Termination proofs

Manuel Lerchner

15.05.2023

# Quiz



Artemis 6.1.7

Courses > Funktionale Programmierung und Verifikation (Sommersemester 2

✓ Week 04 Quiz

Quiz

Points: 23



Open quiz

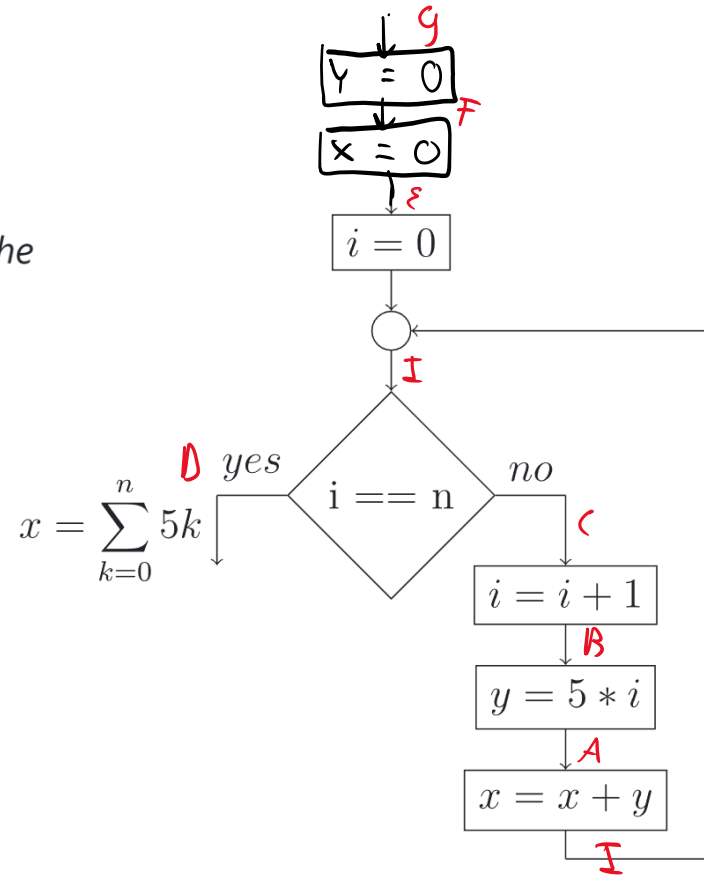
Password:

---

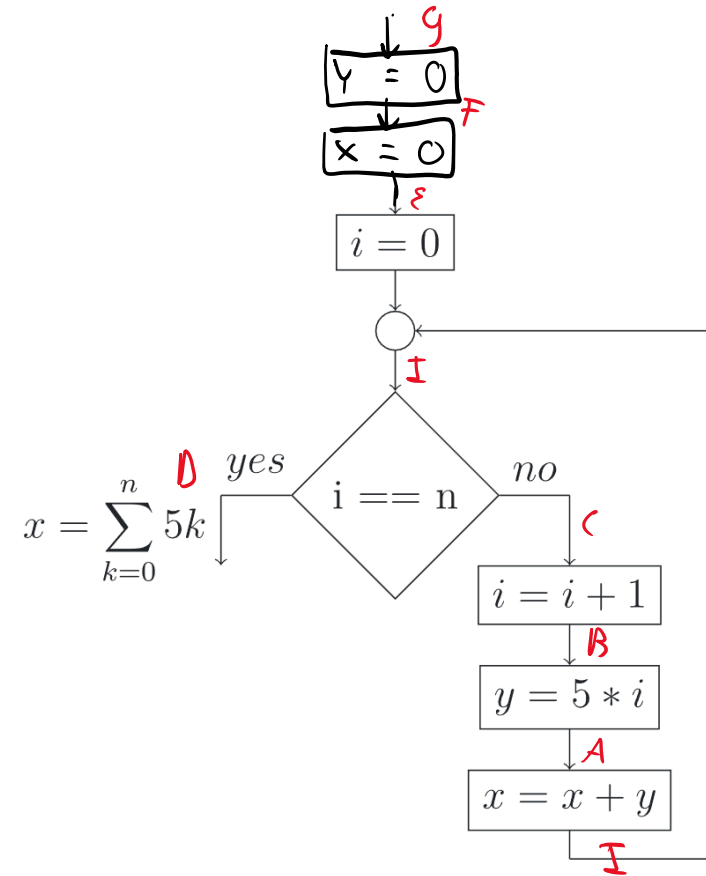
# T01: Loop Invariants

Find a suitable loop invariant and prove it locally consistent.

*Note: We follow the standard practice that the empty sum, where the number of terms is zero, is 0, e.g.:  $\sum_{k=0}^{-1} (\dots) = 0$ .*



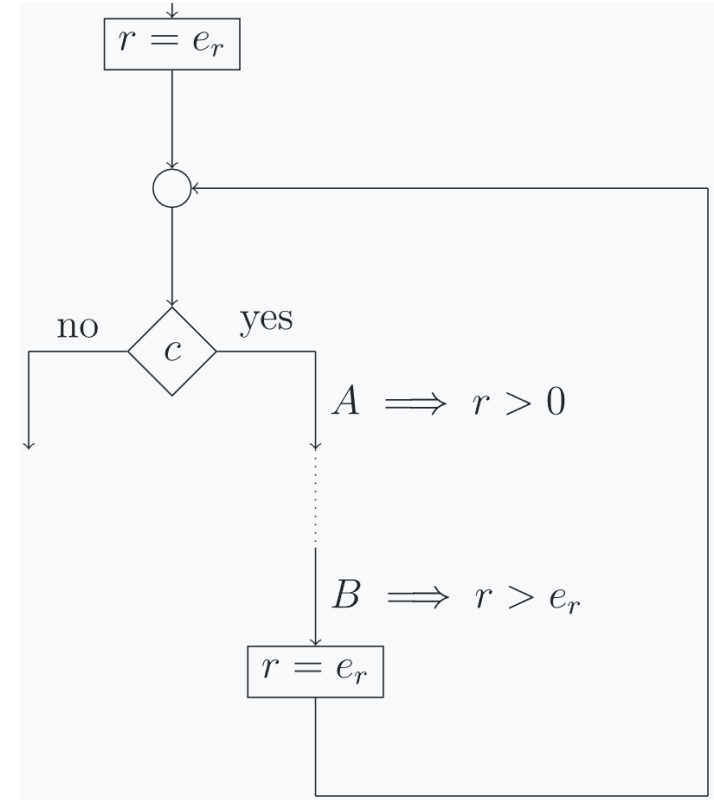
# T01: Loop Invariants



# T02: Termination

In the lecture, you have learned how to prove termination of a MiniJava program. Discuss these questions:

1. How can you decide whether a termination proof is required at all?
2. What is the basic idea of the termination proof?
3. How is the program to be modified?
4. What has to be proven?
5. How is the loop invariant influenced?

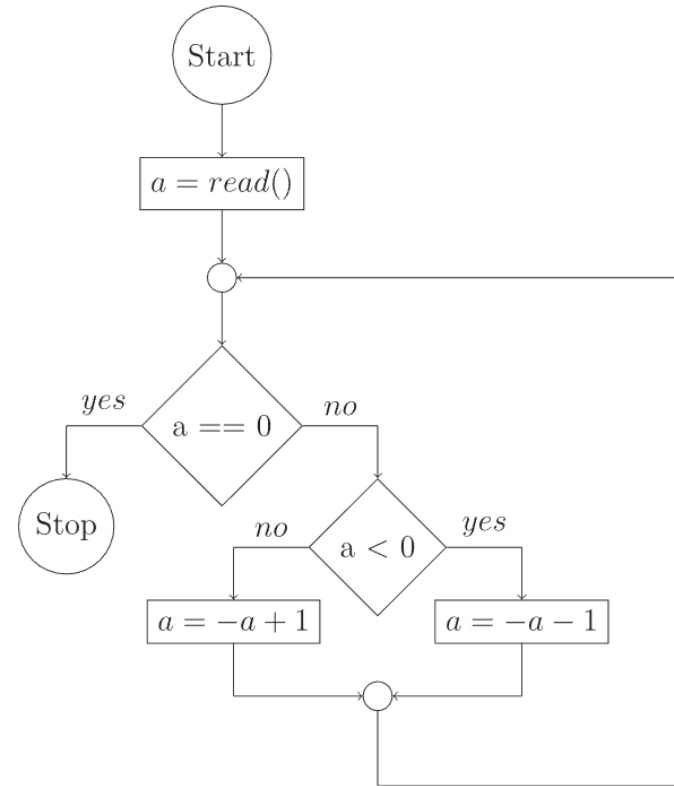


# T03: A Wavy Approach

Prove termination of the following program:

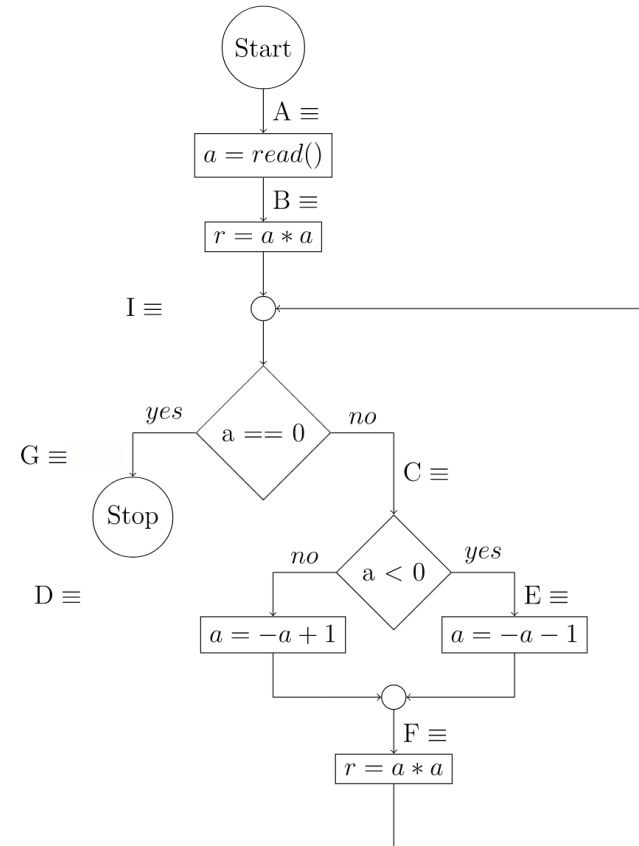
## Todos:

1. Schleife verstehen
2. Variable  $r$  definieren / finden
  - $r \geq 0$  in jedem Durchgang
  - $r$  wird strikt kleiner
3. Neue Variable und Assertions einfügen
  - Am Ende „true“ Assertion!
4. Local-Consistency zeigen





# T03: A Wavy Approach



# 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

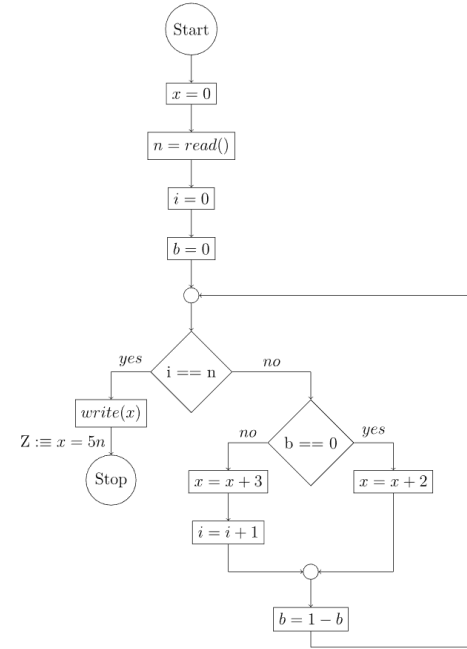
**Tipps**  
Wir benötigen eine Aussage über den Wert der Variablen, über die wir etwas beweisen wollen ( $x$ ) in der Schleifeninvariante. Die Aussage muss dabei mindestens so präzise ( $\neq, \geq, \leq, =$ ) sein, wie die Aussage, die wir beweisen wollen.

## 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.



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

# FPV Tutorübung

Woche 5

Ocaml

Manuel Lerchner

22.05.2023

# T01: Expressions

So far, you learned about the following types of expressions:

- Constants
- Variables
- Unary operators
- Binary operators
- Tuples
- Records
- Lists
- If-then-else
- Pattern matching
- Function definition
- Function application
- Variable binding

1. For each of the aforementioned types of expressions, give the general structure and two concrete examples with different subexpressions.

# T01: Expressions

- Constants:
- Variables:
- Unary Operator:
- Binary Operator:
- Tuples:

# T01: Expressions

- Records (definition):
- Records (access):
- Lists:
- if-then-else:

# T01: Expressions

- Pattern Matching:
- Function Definition :
- Function Application :
- Variable Binding:

# T01: Expressions

2. For the following expressions, list all contained subexpressions and give their corresponding types. Then evaluate the expressions:

(\* a \*) `let a = fun x y -> x + 2 in a 3 8 :: []`

(\* a \*) `let a = fun x y -> x + 2 in a 3 8 :: []`

(\* b \*) `((fun x -> x :: []) (9 - 5), true, ('a', 7))`



# T01: Expressions

```
(* a *) let a = fun x y -> x + 2 in a 3 8 :: []
```

# T01: Expressions

```
(* b *) ((fun x -> x::[]) (9 - 5), true, ('a', 7))
```

# T02: What's the Point

Using what you learned about tuple types in the lecture, implement functionality for computing with three-dimensional vectors.

1.  **Define a suitable data type for your point.** 0 of 1 tests passing

The type `vector3` should be a tuple of 3 float values.

2.  **Define three points** 0 of 1 tests passing

The points `p1`, `p2` and `p3` should all be different, but their exact values don't matter. Use them, along with other points, to test your functions.

3.  **string\_of\_vector3** 0 of 1 tests passing

Implement a function `string_of_vector3 : vector3 -> string` to convert a vector into a human-readable representation.

For example, the string for the zero vector should be: `(0.,0.,0.)`.

**Hint:** use `string_of_float` to convert components.

4.  **vector3\_add** 0 of 1 tests passing

Write a function `vector3_add : vector3 -> vector3 -> vector3` that adds two vectors component-wise.

5.  **vector3\_max** 0 of 1 tests passing

Write a function `vector3_max : vector3 -> vector3 -> vector3` that returns the larger argument vector (the vector with the greater magnitude).

6.  **combine** 0 of 1 tests passing

Write a function `combine : vector3 -> vector3 -> vector3 -> string` that adds its first argument to the larger of the other two arguments and returns the result as a string.

# T03: Student Database

In this assignment, you have to manage the students of a university.

1. **? Type** No results

First you need to define some types.

- Define a data type for a `student`.

A student should be represented as a record of the students `first_name`, `last_name`, identification number `id`, number of the current `semester` as well as the list of `grades` received in different courses.

The grades should be a pair of the course number and the grade value, a floating point number.

- To actually manage student you need a `database` which shall be represented as a list of students.

2. **? insert** No results

Write a function `insert : student -> database -> database` that inserts a student into the database.

3. **? find\_by\_id** No results

Write a function `find_by_id : int -> database -> student list` that returns a list with the (first) student with the given id (either a single student or an empty list, if no such student exists).

4. **? find\_by\_last\_name** No results

Implement a function `find_by_last_name : string -> database -> student list` to find all students with a given last name.

# FPV Tutorübung

Woche 6

## Ocaml: List-Module, Binary Search Trees

Manuel Lerchner

31.05.2023

# T01: Explicit Type Annotation

In OCaml, types are inferred automatically, so there is no need to write them down explicitly. However, types can be annotated by the programmer. Discuss:

1. In the following expression, annotate the types of all subexpressions:

```
let f = fun x y -> x, [y]
```

2. When can explicitly annotated types be helpful?

# T02: The List Module

Check the documentation of the OCaml [List](#) module [here](#) and find out what the following functions do. Then implement them yourself. Make sure your implementations have the same type. In cases where the standard functions throw exceptions, you may just `failwith "invalid"`.

1. ☒ **hd** [0 of 1 tests passing](#)

Implement the function `hd`

2. ☒ **tl** [0 of 1 tests passing](#)

Implement the function `tl`

3. ☒ **length** [0 of 1 tests passing](#)

Implement the function `length`

4. ☒ **append** [0 of 1 tests passing](#)

Implement the function `append`

5. ☒ **rev** [0 of 1 tests passing](#)

Implement the function `rev`

6. ☒ **nth** [0 of 1 tests passing](#)

Implement the function `nth`



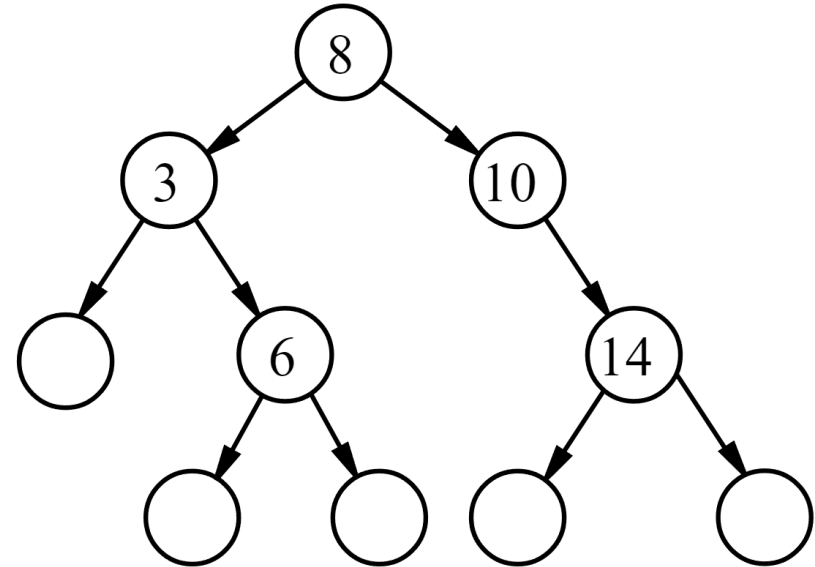
# T03: Binary Search Tree 1

In this assignment, a collection to organize integers shall be implemented via binary search trees.

1. Define a suitable data type `tree` for binary trees that store integers. Each node in the binary tree should either be
  - an inner node which stores a value of type `int` and has a left and a right child of type `tree`, or
  - a leaf node and contain no value.

Since you are free to define your `tree` type however you wish (the type `tree` is said to be *abstract*), we need to define functions for creating trees.

2. Define functions `node` and `leaf`, which should create inner nodes and leaves, respectively:
  - `node v l r` should create an inner node with the value `v`, left child `l` and right child `r`,
  - `leaf ()` should create a leaf node of your `tree` type.

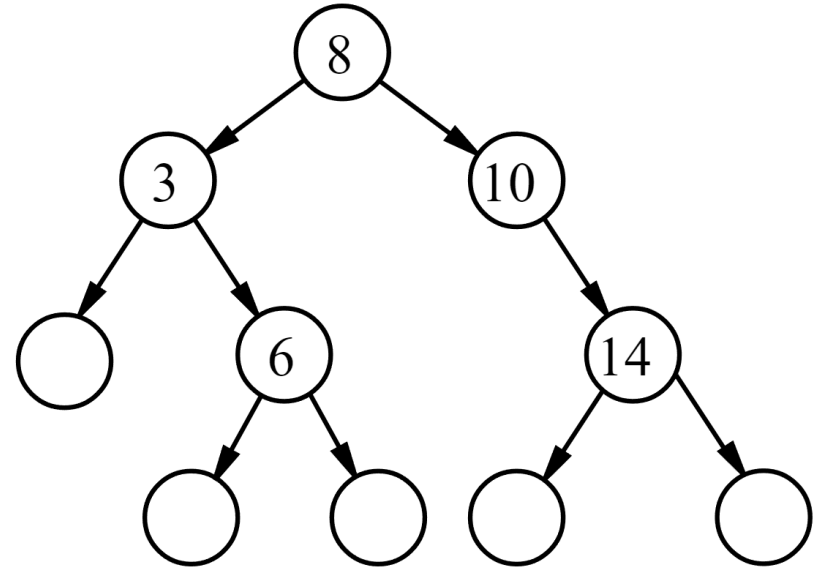




## T03: Binary Search Tree 2

Similarly, we need a function that allows us to inspect the structure of your tree, specifically to access the children of a node. The OCaml `Option` type ([API documentation for Option](#)) allows us to cleanly distinguish between the presence of absence of a value. Here, we will use it to distinguish between inner nodes, which have children, and leaf nodes, which do not. Using the `Option` type and returning `None` instead of raising an exception is (often) good functional programming style!

3. Define the function `inspect`, which allows us to access the children of a node:
  - `inspect n`, where `n` is an inner node of your `tree` type with the value `v` and children `l` and `r`, should return `Some (v, l, r)`. Here, `Some` is used to indicate the *presence* of a value and children.
  - `inspect l`, where `l` is a leaf of your `tree` type (with no children), should return `None`. Here, `None` is used to indicate the *absence* of a value and children.

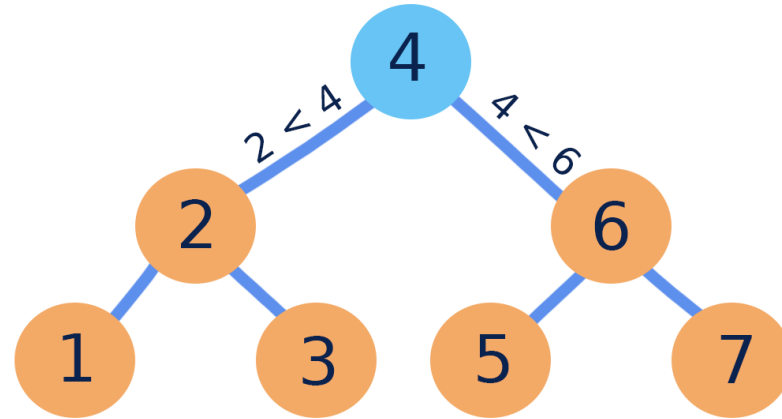


# T03: Binary Search Tree 3

4. Define a binary tree `t1` which contains the values 8, 12, 42, 1, 6, 9, 8. To construct the tree, start with an empty tree, then insert the given values in order.

## T03: Binary Search Tree 4

5. Implement a function `to_list : tree -> int list` that returns an ordered list of all values in the tree.

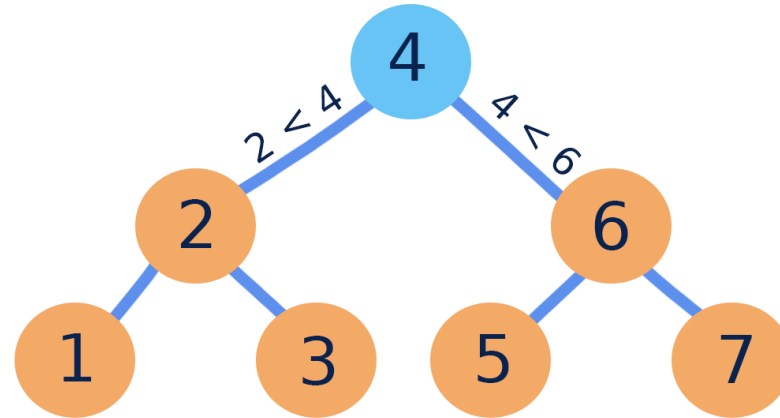


In Order Traversal:  $[1\ 2\ 3\ 4\ 5\ 6\ 7]$

# T03: Binary Search Tree 5

6. Implement a function `insert : int -> tree -> tree` which inserts a value into the tree. If the value exists already, the tree is not modified.

8



## T03: Binary Search Tree 6

7. Implement a function `remove : int -> tree -> tree` to remove a value (if it exists) from the tree. Upon removing a value from an inner node:

- if either child of the inner node is empty, replace the entire inner node with the other child, otherwise
- if neither child of the inner node is empty, the value should be replaced with the largest value from the *left* subtree.

