Week1 - FPV Week 1 exercise solutions and notes

Funktionale Programmierung (Technische Universität München)

Friday IV - EN - 6/5/2022

Mittwoch, 27. Oktober 2021 11:34

Zulip-Links:

- FPV-Announcements
- FPV-Lecture
- FPV-TechSupport
- FPV-Organization
- **FPV-Memes**
- FPV_T_IX EN

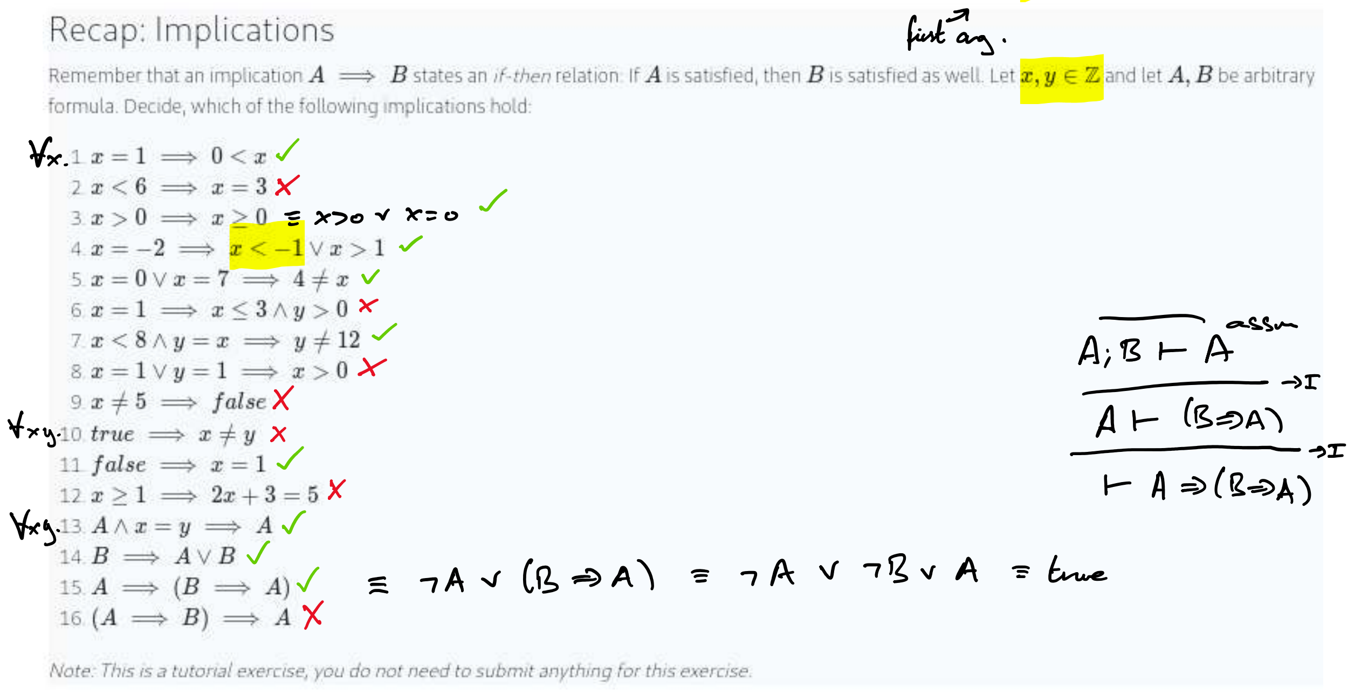
Homework: Always through Artemis

$A \Rightarrow B \equiv \neg A \vee B$

$\Rightarrow$	0	1
0	1	1
1	0	1

← 2nd arg.

first arg.



Recap: Implications

Remember that an implication $A \implies B$ states an *if-then* relation: If A is satisfied, then B is satisfied as well. Let $x, y \in \mathbb{Z}$ and let A, B be arbitrary formula. Decide, which of the following implications hold:

$\forall x.$ 1. $x = 1 \implies 0 < x$ ✓
2. $x < 6 \implies x = 3$ ✗
3. $x > 0 \implies x \geq 0$ $\equiv x>0 \vee x=0$ ✓
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. $x \neq 5 \implies false$ ✗

$\forall xy.$ 10. $true \implies x \neq y$ ✗
11. $false \implies x = 1$ ✓
12. $x \geq 1 \implies 2x + 3 = 5$ ✗

$\forall xy.$ 13. $A \wedge x = y \implies A$ ✓
14. $B \implies A \vee B$ ✓
15. $A \implies (B \implies A)$ ✓ $\equiv \neg A \vee (B \Rightarrow A) \equiv \neg A \vee \neg B \vee A \equiv true$
16. $(A \implies B) \implies A$ ✗

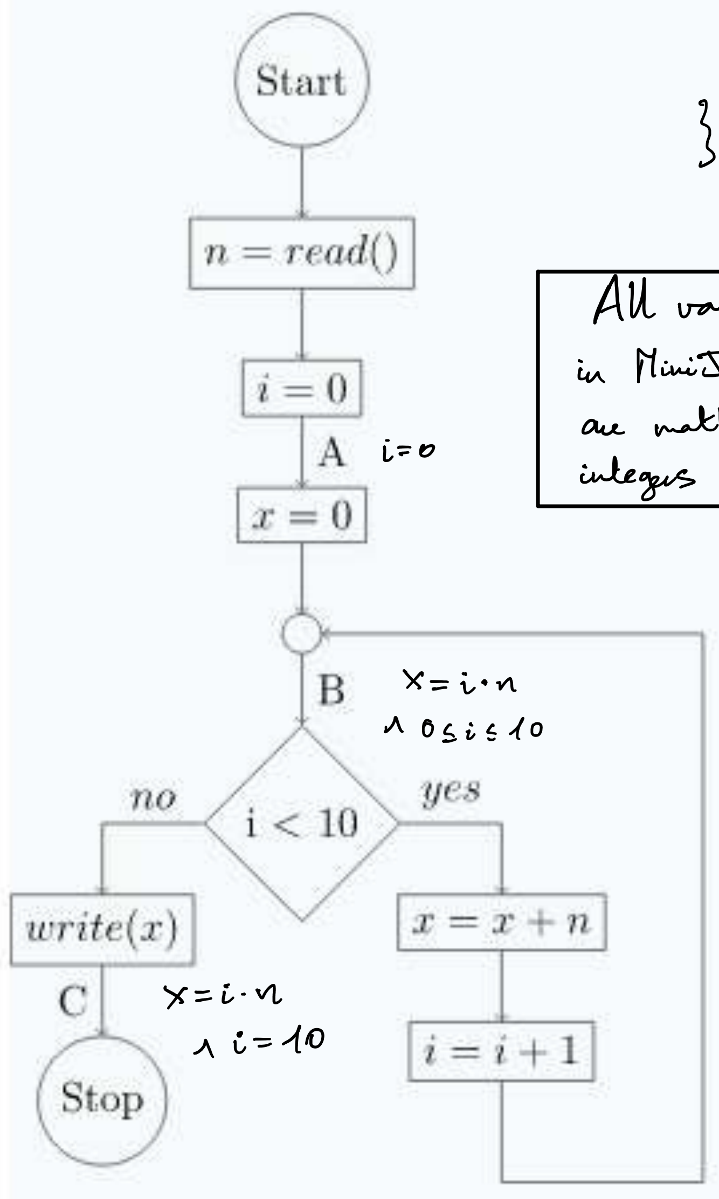
$$\cfrac{\cfrac{\overline{A; B \vdash A}^{\,assm}}{A \vdash (B \Rightarrow A)}\,\rightarrow I}{\vdash A \Rightarrow (B \Rightarrow A)}\,\rightarrow I$$

Note: This is a tutorial exercise, you do not need to submit anything for this exercise.

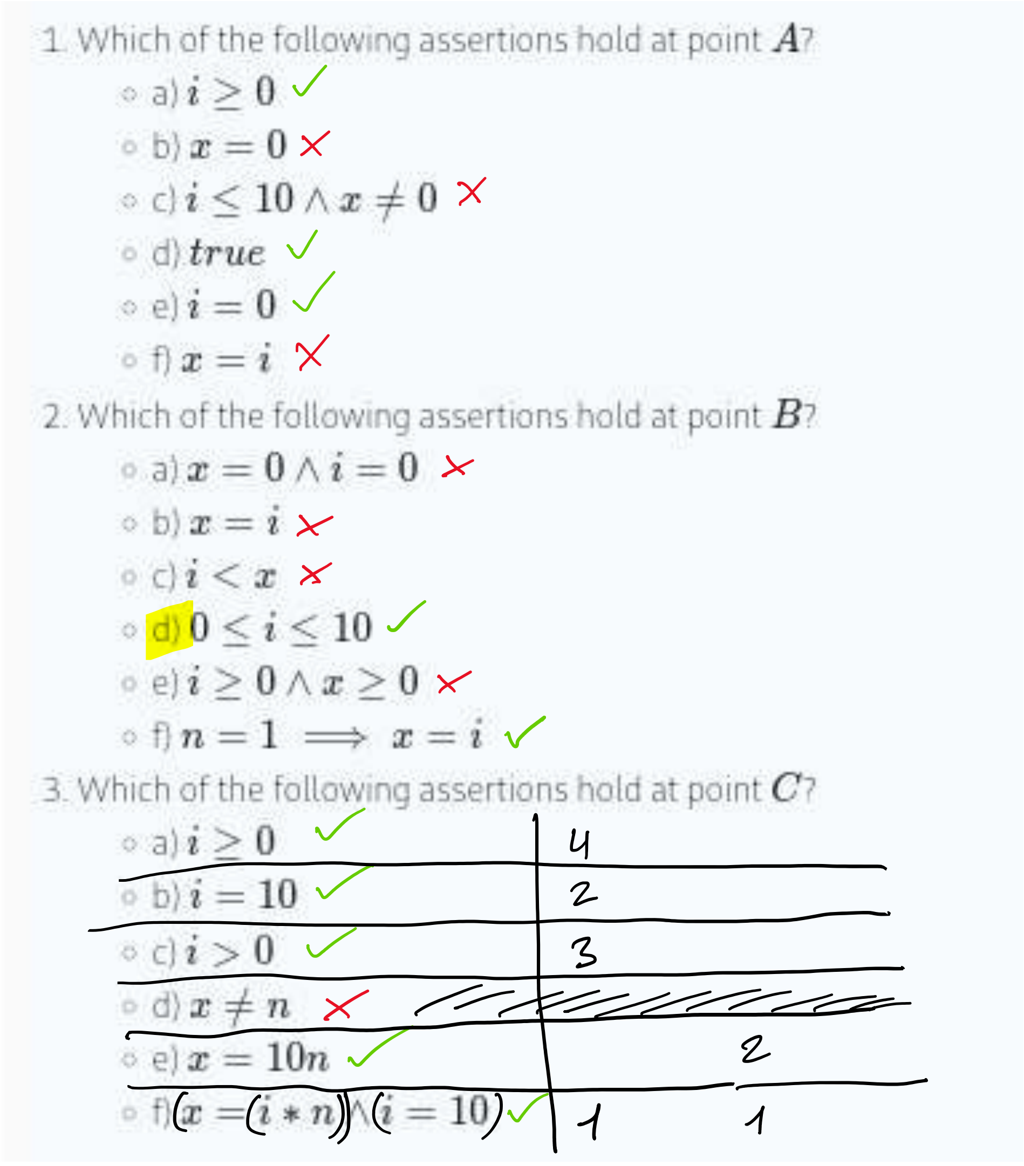
Assertions

Consider the following control flow graph:

```
if(x>0){
  assert(a>=0);
   :
}
```



All variables in MiniJava are mathematical integers ($\mathbb{Z}$)



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?

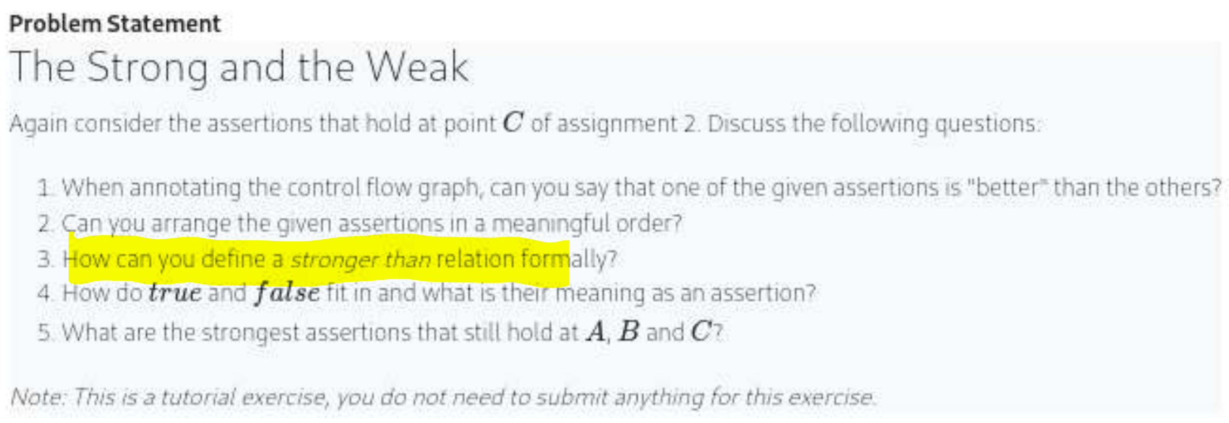
a) $i \geq 0$ ✓	4	
b) $i = 10$ ✓	2	
c) $i > 0$ ✓	3	
d) $x \neq n$ ✗		
e) $x = 10n$ ✓		2
f) $(x = (i * n)) \wedge (i = 10)$ ✓	1	1

f) $\Leftrightarrow (x = 10n) \wedge (i = 10)$

$x = 5 \wedge$
$y = 10 \wedge$
$z = x + y$

$\Leftrightarrow$

$x = 5 \wedge$
$y = 10 \wedge$
$z = 15$



Problem Statement

The Strong and the Weak

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?

Note: This is a tutorial exercise, you do not need to submit anything for this exercise.

1. An assertion is "better" if it is more specific, aka. it gives more information about the program state.
2. We can arrange some of them in a meaningful order. Some are incomparable. (see table).
3. A is stronger than B := $A \Rightarrow B$

   This defines a relation on assertions, which is a partial order

   [Recap: partial order is: reflexive: $\forall A.\ A \Rightarrow A$
   transitive: $\forall ABC. (A \Rightarrow B \wedge B \Rightarrow C) \rightarrow A \Rightarrow C$
   antisymmetric: $\forall AB.\ (A \Rightarrow B \wedge B \Rightarrow A) \rightarrow A = B$

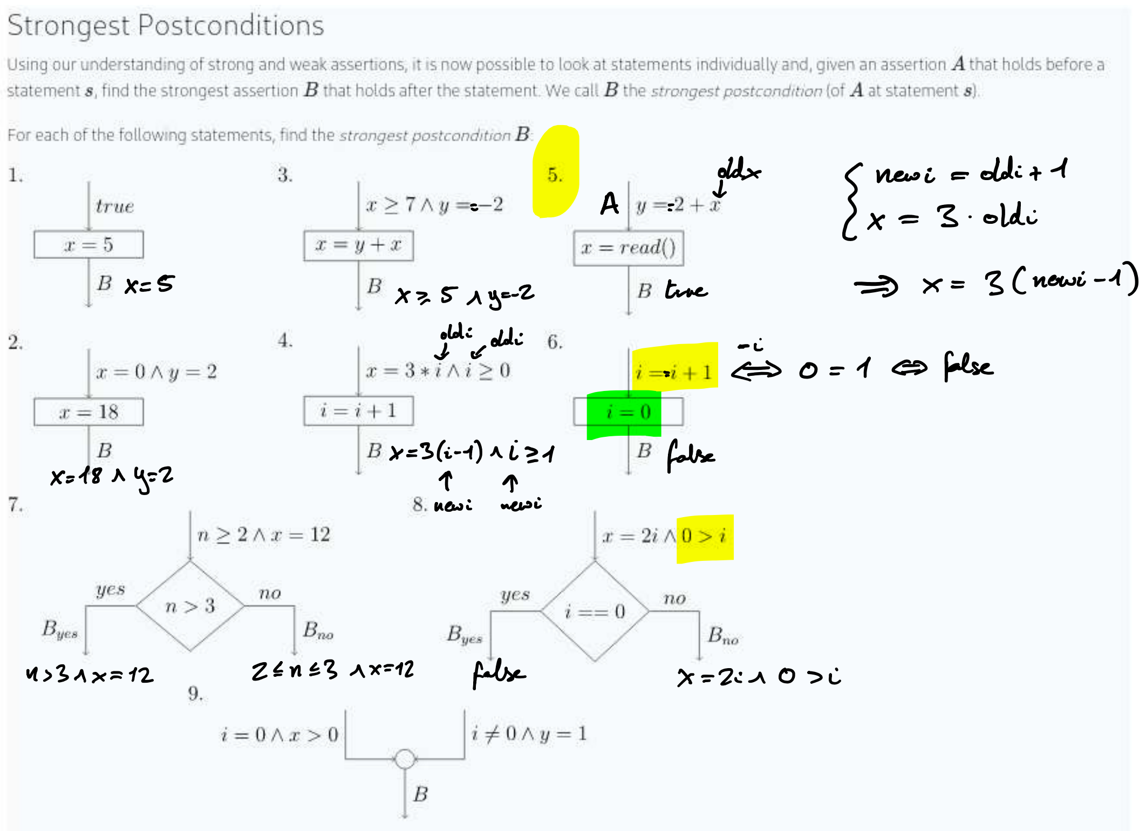
   It is not total, since $i=10 \not\Rightarrow x = 10n$ and $x = 10n \not\Rightarrow i = 10$.
4. - true is the weakest assertion, since it holds at every program point. (in the relation it is the minimum)
   - false is the strongest assertion, since for it to hold the program point needs to be unreachable. (in the relation it is the maximum)

5.:

A

$y = 2 + x$

B x is anything
y is anything



Strongest Postconditions

Using our understanding of strong and weak assertions, it is now possible to look at statements individually and, given an assertion A that holds before a statement s, find the strongest assertion B that holds after the statement. We call B the *strongest postcondition* (of A at statement s).

For each of the following statements, find the *strongest postcondition* B:

$\begin{cases} new\,i = old\,i + 1 \\ x = 3 \cdot old\,i \end{cases}$

$\Rightarrow x = 3(new\,i - 1)$

$\Leftrightarrow 0 = 1 \Leftrightarrow false$

$(i=0 \wedge x>0) \vee (i \neq 0 \wedge y=1)$

$x = x + 1 \quad | -x$

$\Leftrightarrow 0 = 1$

$\Leftrightarrow false$