Week2

IN0003

Jigao

TUM

7. November 2018

What about the last week?

- The video of central Tutorial is linked in this exercise sheet.
- This time we will do more about the **LOOP INVARIANT**
- I hope you also have attended the tutorial from last week.
- My slide would not almost same as the Solution. But I have no graph.

Assignment 3.1 (L) Individual Loops

- Aufgabe 3.1 of last year, if you want to refer to the german solution.
- We have to discuss the results for **positive and negative inputs**
- Maybe some terminate problem!

- The assertion follows immediately from the loop condition.
- So whenever the loop is left, $i = n$ **holds** automatically.
- Here don't think about, if this point is reachable or not. Just look at the **LOOP CONDITON.**.
- What would this program be, if we have a negative n?

- The assertion follows immediately from the loop condition.
- So whenever the loop is left, $i = n$ **holds** automatically.
- Here don't think about, if this point is reachable or not. Just look at the **LOOP CONDITON.**.
- What would this program be, if we have a negative n?
- For $n < 0$ and $n \not\equiv 0 mod 2$ **the loop does not terminate.**
- However, this does not violate the assertion!
- Here the assertion only depends on the **LOOP CONDITON.**

- The assertion follows immediately from the loop condition.
- So whenever the loop is left, $i = n$ **holds** automatically.
- Here don't think about, if this point is reachable or not. Just look at the **LOOP CONDITON.**.
- What would this program be, if we have a negative n?
- For $n < 0$ and $n \not\equiv 0 mod 2$ **the loop does not terminate.**
- However, this does not violate the assertion!
- Here the assertion only depends on the **LOOP CONDITON.**
- What is the WP of the right of the loop?

- The assertion follows immediately from the loop condition.
- So whenever the loop is left, $i = n$ **holds** automatically.
- Here don't think about, if this point is reachable or not. Just look at the **LOOP CONDITON.**.
- What would this program be, if we have a negative n?
- For $n < 0$ and $n \not\equiv 0 mod 2$ **the loop does not terminate.**
- However, this does not violate the assertion!
- Here the assertion only depends on the **LOOP CONDITON.**
- What is the WP of the right of the loop?
- It is *true*. We don't have to care about what i is.

3.1.1

$$
\begin{aligned}
&\mathrm{WP}[\texttt{i == n}](\mathit{true}, i = n) \\
\equiv\ &(i \neq n \implies \mathit{true}) \land (i = n \implies i = n) \\
\equiv\ &\mathit{true}
\end{aligned}
$$

3.1.2

- The loop terminates when i reaches n and thus $i = n$ holds.
- What if $n < 0$?

3.1.2

- The loop terminates when i reaches n and thus $i = n$ holds.
- What if $n < 0$?
- Terminate the loop immediately. – What we don't want.
- It is harder to find the WP of the right side.
- We make sure that $n \geq 0$ (or generally $n \geq i$) holds before the loop

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

$$
\begin{aligned}
&\mathrm{WP}[\texttt{i >= n}](n \geq i + 1, i = n) \\
\equiv\ & (i < n \implies n \geq i + 1) \land (i \geq n \implies i = n) \\
\equiv\ & i \geq n \implies i = n \\
\equiv\ & i < n \lor i = n \\
\equiv\ & i \leq n \impliedby n \geq i
\end{aligned}
$$

3.1.3

- For $n < 0$ so we require $n \geq i$ before the loop. - like 3.1.2
- Moreover, the loop may be reached with an $i = n - 1$.
- In this case the program would increment i to $i = n + 1$ and reach the exit with $i \neq n$.
- So that $n \geq i$ is indeed not sufficient:

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

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

3.1.3

- Intuitively we could see that:
  $I \equiv n \ mod \ 2 = 0 \wedge i \ mod \ 2 = 0 \wedge n \geq i$
- We make it **stronger**

$$
\begin{aligned}
& \mathrm{WP}[\texttt{i = i + 2}](I) \\
\equiv\ & n \ mod \ 2 = 0 \wedge i + 2 \ mod \ 2 = 0 \wedge n \geq i + 2 \\
\equiv\ & I
\end{aligned}
$$

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

So $I \equiv n \ mod \ 2 = 0 \wedge i \ mod \ 2 = 0 \wedge n \geq i$ is sufficient

We show that $I :\equiv x = \sum_{k=0}^{i} 5k$ is sufficient:

$$\begin{aligned}
&\mathrm{WP}[\texttt{x = x + y}](I) \\
\equiv\ &\mathrm{WP}[\texttt{x = x + y}]\left(x = \sum_{k=0}^{i} 5k\right) \\
\equiv\ &x + y = \sum_{k=0}^{i} 5k \\
\equiv\ &x = -y + \sum_{k=0}^{i} 5k \quad \equiv: A
\end{aligned}$$

$$\begin{aligned}
&\mathrm{WP}[\texttt{y = 5 * i}](A) \\
\equiv\ &\mathrm{WP}[\texttt{y = 5 * i}]\left(x = -y + \sum_{k=0}^{i} 5k\right) \\
\equiv\ &x = -5i + \sum_{k=0}^{i} 5k \\
\equiv\ &x = \sum_{k=0}^{i-1} 5k \quad \equiv: B
\end{aligned}$$

The counter i changed to $i - 1$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{i = i + 1}](B) \\
\equiv\ &\mathrm{WP}[\texttt{i = i + 1}]\left(x = \sum_{k=0}^{i-1} 5k\right) \\
\equiv\ &x = \sum_{k=0}^{i} 5k \quad \equiv: C
\end{aligned}
$$

The counter $i-1$ changed to i

$$\mathrm{WP}[\texttt{i == n}](C, x = \sum_{k=0}^{n} 5k)$$

$$\equiv \mathrm{WP}[\texttt{i == n}](x = \sum_{k=0}^{i} 5k, x = \sum_{k=0}^{n} 5k)$$

$$\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k) \vee (i = n \wedge x = \sum_{k=0}^{n} 5k)$$

$$\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k) \vee (i = n \wedge x = \sum_{k=0}^{i} 5k)$$

$$\equiv x = \sum_{k=0}^{i} 5k \quad \equiv I$$

The two logic terms on the line 4 can be merged!

3.2.2

Your turn to exercise.

Your turn to exercise.
We show that $I :\equiv x = \sum_{k=0}^{i} 5k$ is **not** sufficient:

$$\mathrm{WP}[\texttt{x = x + y}](I)$$
$$\equiv \mathrm{WP}[\texttt{x = x + y}](x = \sum_{k=0}^{i} 5k)$$
$$\equiv x + y = \sum_{k=0}^{i} 5k$$
$$\equiv x = -y + \sum_{k=0}^{i} 5k \quad \equiv: A$$

$$\mathrm{WP}[\texttt{y = y + 5}](A)$$
$$\equiv \mathrm{WP}[\texttt{y = y + 5}](x = -y + \sum_{k=0}^{i} 5k)$$
$$\equiv x = -(y + 5) + \sum_{k=0}^{i} 5k$$
$$\equiv: B$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{i = i + 1}](B) \\
\equiv\ & \mathrm{WP}[\texttt{i = i + 1}]\Big(x = -(y+5) + \sum_{k=0}^{i} 5k\Big) \\
\equiv\ & x = -(y+5) + \sum_{k=0}^{i+1} 5k \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{i == n}](C, x = \sum_{k=0}^{n} 5k) \\
\equiv\ &\mathrm{WP}[\texttt{i == n}](x = -(y+5) + \sum_{k=0}^{i+1} 5k) \\
\equiv\ &(i \neq n \wedge x = -(y+5) + \sum_{k=0}^{i+1} 5k) \\
&\vee (i = n \wedge x = \sum_{k=0}^{n} 5k) \quad {\color{red}\not\Leftarrow A}
\end{aligned}
$$

This invariant is not strong enough, because we do not have any information about y, so we cannot simplify anything.

The one before is too weak to guarantee the loop invariant. Adding $y = 5i$ renders the invariant sufficient, which becomes stronger:

$$
\begin{aligned}
&\mathrm{WP}[\texttt{x = x + y}](I) \\
\equiv\ &\mathrm{WP}[\texttt{x = x + y}]\left(x = \sum_{k=0}^{i} 5k \wedge y = 5i\right) \\
\equiv\ &x + y = \sum_{k=0}^{i} 5k \wedge y = 5i \\
\equiv\ &x = -5i + \sum_{k=0}^{i} 5k \wedge y = 5i \\
\equiv\ &x = \sum_{k=0}^{i-1} 5k \wedge y = 5i \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{y = y + 5}](A) \\
\equiv\ & \mathrm{WP}[\texttt{y = y + 5}]\left(x = \sum_{k=0}^{i-1} 5k \land y = 5i\right) \\
\equiv\ & x = \sum_{k=0}^{i-1} 5k \land y + 5 = 5i \\
\equiv\ & x = \sum_{k=0}^{i-1} 5k \land y = 5(i-1) \qquad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{i = i + 1}](B) \\
\equiv\ & \mathrm{WP}[\texttt{i = i + 1}]\left(x = \sum_{k=0}^{i-1} 5k \wedge y = 5(i-1)\right) \\
\equiv\ & x = \sum_{k=0}^{i} 5k \wedge y = 5i \quad \equiv: C
\end{aligned}
$$

$$\mathrm{WP}[\texttt{i == n}](C, x = \sum_{k=0}^{n} 5k)$$

$$\equiv \mathrm{WP}[\texttt{i == n}](x = \sum_{k=0}^{i} 5k \wedge y = 5i, x = \sum_{k=0}^{n} 5k)$$

$$\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{n} 5k)$$

$$\Longleftarrow \ (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i)$$

$$\equiv x = \sum_{k=0}^{i} 5k \wedge y = 5i \quad \equiv I$$

Why to use a $\Longleftarrow$?

$$\mathrm{WP}[\texttt{i == n}](C, x = \sum_{k=0}^{n} 5k)$$

$$\equiv \mathrm{WP}[\texttt{i == n}](x = \sum_{k=0}^{i} 5k \wedge y = 5i, x = \sum_{k=0}^{n} 5k)$$

$$\equiv (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{n} 5k)$$

$$\Longleftarrow \quad (i \neq n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i) \vee (i = n \wedge x = \sum_{k=0}^{i} 5k \wedge y = 5i)$$

$$\equiv x = \sum_{k=0}^{i} 5k \wedge y = 5i \quad \equiv I$$

Why to use a $\Longleftarrow$?
The loop invariant should be able to imply the WP.

Loop-Carrier

- In the 3.2.1 the y is üseless”. It can be replace directly by $5 * i$.
- But in the 3.2.1 the y contains the information, that i can not describe.
- y is computed from the previous value of y, so the value of y when entering a loop iteration is indeed important, so we have to make a statement about it inside the invariant.
- This is often referred to as loop-carried dependency.

3.3 Two b, or not two b

Var	Time0	Time1	Time2	Time3	Time4	Time5	Time6
i	0	0	1	1	2	2	3
x	0	2	5	7	10	12	15
b	0	1	0	1	0	1	0

- From the tabular $x = 5i + 2b \wedge b \in \{0, 1\}$.
- When I leave the outer loop, I am with the $b = 0$, that is the last time with the inner loop.
- Try to get more information about the last time with the loops.
- Can you find a loop invariant?
- Can you prove, that your loop invar is correct?

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

$$
\begin{aligned}
& \mathrm{WP}[\texttt{b = 1 - b}](I) \\
\equiv\; & \mathrm{WP}[\texttt{b = 1 - b}](x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0)) \\
\equiv\; & x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1) \quad \equiv: A
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{i = i + 1}](A) \\
\equiv\; & \mathrm{WP}[\texttt{i = i + 1}](x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1)) \\
\equiv\; & x = 5i - 2b + 7 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1) \quad \equiv: B
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{x = x + 3}](B) \\
\equiv\; & \mathrm{WP}[\texttt{x = x + 3}](x = 5i - 2b + 7 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1)) \\
\equiv\; & x = 5i - 2b + 4 \land b \in \{0,1\} \land (i + 1 = n \implies b = 1) \quad \equiv: C
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{x = x + 2}](A) \\
\equiv\; & \mathrm{WP}[\texttt{x = x + 2}](x = 5i - 2b + 2 \land b \in \{0,1\} \land (i = n \implies b = 1)) \\
\equiv\; & x = 5i - 2b \land b \in \{0,1\} \land (i = n \implies b = 1) \quad \equiv: D
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{b == 0}](C, D) \\
\equiv\ & \mathrm{WP}[\texttt{b == 0}](x = 5i - 2b + 4 \wedge b \in \{0,1\} \wedge (i + 1 = n \implies b = 1), \\
& \qquad x = 5i - 2b \wedge b \in \{0,1\} \wedge (i = n \implies b = 1)) \\
\equiv\ & (b = 1 \wedge x = 5i - 2b + 4 \wedge (i + 1 = n \implies b = 1)) \\
& \qquad \vee (b = 0 \wedge x = 5i - 2b \wedge (i = n \implies b = 1)) \\
\equiv\ & (b = 1 \wedge x = 5i + 2) \vee (b = 0 \wedge x = 5i \wedge i \neq n) \\
\Longleftarrow\ & (b = 1 \wedge x = 5i + 2b \wedge i \neq n) \vee (b = 0 \wedge x = 5i + 2b \wedge i \neq n) \\
\equiv\ & x = 5i + 2b \wedge i \neq n \wedge b \in \{0,1\} \quad \equiv: E
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{WP}[\texttt{i == n}](E, Z) \\
\equiv\ & \mathrm{WP}[\texttt{i == n}](x = 5i + 2b \wedge i \neq n \wedge b \in \{0,1\}, x = 5n) \\
\equiv\ & (i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\}) \vee (i = n \wedge x = 5n) \\
\Longleftarrow\ & (i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\} \wedge (i = n \implies b = 0)) \\
& \qquad \vee (i = n \wedge x = 5n \wedge (i = n \implies b = 0) \wedge b \in \{0,1\}) \\
\equiv\ & (i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\} \wedge (i = n \implies b = 0)) \\
& \qquad \vee (i = n \wedge x = 5i + 2b \wedge (i = n \implies b = 0) \wedge b \in \{0,1\}) \\
\equiv\ & x = 5i + 2b \wedge b \in \{0,1\} \wedge (i = n \implies b = 0) \quad \equiv I
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{b = 0}](I) \\
\equiv\ &\mathrm{WP}[\texttt{b = 0}](x = 5i + 2b \land b \in \{0,1\} \land (i = n \implies b = 0)) \\
\equiv\ &x = 5i \quad \equiv: F
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{i = 0}](F) \\
\equiv\ &\mathrm{WP}[\texttt{i = 0}](x = 5i) \\
\equiv\ &x = 0 \quad \equiv: G
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{n = read()}](G) \\
\equiv\ &\mathrm{WP}[\texttt{n = read()}](x = 0) \\
\equiv\ &x = 0 \quad H
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{WP}[\texttt{x = 0}](H) \\
\equiv\ &\mathrm{WP}[\texttt{x = 0}](x = 0) \\
\equiv\ &\mathit{true}
\end{aligned}
$$

Summary

- The $L3.4$ is very simliar as the $H1.6$. Even easier. And I would not do that here.
- In this time we must know **How to find a Loop Invariant**, and **How to calulate the WPs**
- $3.2 and 3.3$ are about **how to find a sufficient Loop Invariant.**
- When the loop invariant not so sufficient, what happens? – Look at the solution 3.2.2 and 3.3
- Recommand the recording of last year's exercise.