Dr. Matthias Heizmann
Dominik Klumpp

Hand in until 10:00 on May 31, 2021
Discussion: May 31, 2021

Tutorial for Program Verification
Exercise Sheet 9

In this exercise sheet we work with precondition-postcondition pairs and the Hoare proof system for our Boostan language.

Submit your solution by uploading it as PDF in ILIAS.

Exercise 1: Precondition - Postcondition 4 Points

Consider the following precondition-postcondition pairs. Which of them are satisfied by all program statements *st* and all formulas φ?

(a) $\{\textbf{true}\}\ st\ \{\varphi\}$

(b) $\{\textbf{false}\}\ st\ \{\varphi\}$

(c) $\{\varphi\}\ st\ \{\textbf{true}\}$

(d) $\{\varphi\}\ st\ \{\textbf{false}\}$

If a precondition-postcondition is satisfied by all program statements *st* and all formulas φ, then explain why. If a precondition-postcondition is not satisfied by some program statement *st* and some formulas φ, then give a counterexample.

Exercise 2: Assignment Axiom 1 Point

Find some program P whose code is a single assignment statement of the form `x := expr;` and some formula φ such that P does not satisfy the precondition-postcondition pair $(\{\varphi\}, \{\varphi \land x = \texttt{expr}\})$.

The motivation of this exercise is the following. In the lecture we have seen the assignment axiom of the Hoare proof system.

$$(assig)\frac{}{\{\varphi[x \mapsto \texttt{expr}]\}\ \texttt{x := expr;}\ \{\varphi\}}$$

This rule is not very intuitive because the precondition is obtained as a modification of the postcondition. One may wonder if the following proof rule could be an alternative.

$$(BadAss)\frac{}{\{\varphi\}\ \texttt{x := expr;}\ \{\varphi \land x = \texttt{expr}\}}$$

The result of this exercise should hint that the (BadAss) proof rule cannot be used as an axiom in a proof system whose goal is the derivation of valid Hoare triples.

Exercise 3: Hoare Proof System 4 Points

Is there a program that can swap the values of two variables without using a temporary variable? In this exercise we will consider such a program and prove that the program indeed has this property.

Consider the Boostan program $P_{\mathsf{swap}} = (V, \mu, \mathcal{T})$ with $V = \{a, b, x, y\}$, $\mu(a) = \mu(b) = \mu(x) = \mu(y) = \mathbb{Z}$, and $\mathcal{T}$ a derivation tree for the program code shown below.

```
x := x + y;
y := x - y;
x := x - y;
```

Use the Hoare proof system to show that P satisfies the precondition-postcondition pair $(\{x = a \wedge y = b\}, \{x = b \wedge y = a\})$.

Exercise 4: Programming in Boogie 3 Points

Using the Boogie[1] language, implement a procedure with signature

```
procedure square(x : int) returns (z : int)
```

that takes a (mathematical) integer x and, if it is greater or equal 0, computes and returns the square $z = x^2$. The algorithm may only make use of addition and subtraction, but not use multiplication, division or modulo.

You can use the Boogie interpreter Boogaloo[2] to test your program. A user manual is available online[3].

Exercise 5: Hoare Logic Proof 3 Points

Consider the following Boostan program $P = (V, \mu, \mathcal{T})$ with $V = \{i, j, x, y\}$, $\mu(i) = \mu(j) = \mu(x) = \mu(y) = \mathbb{Z}$, and $\mathcal{T}$ a derivation tree for the program code shown below.

```
x := i;
y := j;
while (x != 0) {
    x := x - 1;
    y := y - 1;
}
```

Give a Hoare logic proof showing that $\{\mathbf{true}\}\, \mathcal{T}\, \{i = j \rightarrow y = 0\}$ is a valid Hoare triple.

[1] https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/krml178.pdf
[2] http://comcom.csail.mit.edu/comcom/#Boogaloo
[3] https://github.com/nadia-polikarpova/boogaloo/wiki/User-Manual