Dr. Matthias Heizmann
Tanja Schindler
Dominik Klumpp

Hand in until 10:00 on June 3, 2019
Discussion: June 3, 2019

Tutorial for Program Verification
Exercise Sheet 10

Exercise 1: Soundness of the Weakening Postcondition Rule 1 Point

Prove that the weakening postcondition rule of the Hoare proof system displayed below is sound.

$$(weakpos)\frac{\{\varphi\}st\{\psi\}}{\{\varphi\}st\{\psi'\}} \text{ if } \psi \models \psi'$$

More precisely, prove the following lemma from the lecture:

> If the Hoare triple $\{\varphi\}st\{\psi\}$ is valid and the side condition $\psi \models \psi'$ is valid, then the Hoare triple $\{\varphi\}st\{\psi'\}$ is valid.

Exercise 2: Soundness of the Composition Rule 2 Bonus Points

Prove that the composition rule of the Hoare proof system displayed below is sound.

$$(compo)\frac{\{\varphi_1\}st_1\{\varphi_2\} \quad \{\varphi_2\}st_2\{\varphi_3\}}{\{\varphi_1\}st_1 st_2\{\varphi_3\}}$$

More precisely, prove the following lemma from the lecture:

> If the Hoare triple $\{\varphi_1\}st_1\{\varphi_2\}$ is valid and the Hoare triple $\{\varphi_2\}st_2\{\varphi_3\}$ is valid, then the Hoare triple $\{\varphi_1\}st_1 st_2\{\varphi_3\}$ is valid.

Exercise 3: Soundness of the Conditional Rule 2 Points

Prove that the conditional rule of the Hoare proof system displayed below is sound.

$$(condi)\frac{\{\varphi \land expr\}\ st_1\ \{\psi\} \quad \{\varphi \land \neg expr\}\ st_2\ \{\psi\}}{\{\varphi\}\ \texttt{if}(expr)\{st1\}\texttt{else}\{st2\}\ \{\psi\}}$$

More precisely, prove the following lemma from the lecture:

> If the Hoare triple $\{\varphi \land expr\}\ st_1\ \{\psi\}$ is valid and the Hoare triple $\{\varphi \land \neg expr\}\ st_2\ \{\psi\}$ is valid, then the Hoare triple $\{\varphi\}\ \texttt{if}(expr)\{st1\}\texttt{else}\{st2\}\ \{\psi\}$ is valid.

Exercise 4: Hoare Logic Proof 3 Points

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

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

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

Exercise 5: Satisfiability in the Theory of Arrays 2 Points

Determine which of the following FOL formulas is satisfiable in the theory of arrays. If a formula is satisfiable, give a satisfying assignment. You may assume that the arrays have integer indices and values.

(a) $\mathit{select}(a, i) = i \wedge \mathit{store}(a, i, k) = a \wedge i \neq k$

(b) $a = \mathit{store}(b, k, v) \wedge \mathit{select}(a, i) \neq \mathit{select}(b, i) \wedge \mathit{select}(a, j) \neq \mathit{select}(b, j)$

(c) $b = \mathit{store}(a, k, v) \wedge \forall i.\ i \neq j \rightarrow \mathit{select}(a, i) = \mathit{select}(b, i)$

You may use an SMT solver to solve this task. To declare an array constant `a`, you can use the SMT-LIB command `(declare-fun a () (Array Int Int))`. The function applications for the *select* function and the *store* function are written as usual, e.g. `(select a i)` and `(store a i v)`.

Exercise 6: Theory of Arrays 2 Points

Formalize the following statements as first order logic formulas.

(a) The array a has the value 0 at every index except at index 5, where the value is 23.

(b) The array a contains no duplicate values between the indices 0 and 10 inclusive.