



## Tutorial for Program Verification

### Exercise Sheet 8

#### Exercise 1: Precondition function

1 Point

We use  $pre(\varphi, \rho)$  to denote the predecessor states from a set of states  $\varphi$  under a transition relation  $\rho$ . In other words,  $pre(\varphi, \rho)$  is the biggest set of states such that after executing  $\rho$  we *can* arrive at a state in  $\varphi$ .

- (a) Write down a formula that describes  $pre(\varphi, \rho)$ .
- (b) In Exercise 4 on Exercise Sheet 7 we used the following formula to describe  $pre(\varphi, \rho)$ :

$$\neg wp(\neg\varphi, \rho)$$

Substitute the definition of  $wp$  and simplify the formula by eliminating negations. You should obtain the same formula as in part (a).

- (c) What is, intuitively speaking, the difference between  $pre$  and  $wp$ ?
- (d) Give formulas  $\varphi_1, \varphi_2, \varphi_3, \rho_1, \rho_2, \rho_3$  such that the claims below hold. (We write  $\subseteq$  for  $\implies$  here.)

$$wp(\varphi_1, \rho_1) \not\subseteq pre(\varphi_1, \rho_1)$$

$$wp(\varphi_2, \rho_2) \not\supseteq pre(\varphi_2, \rho_2)$$

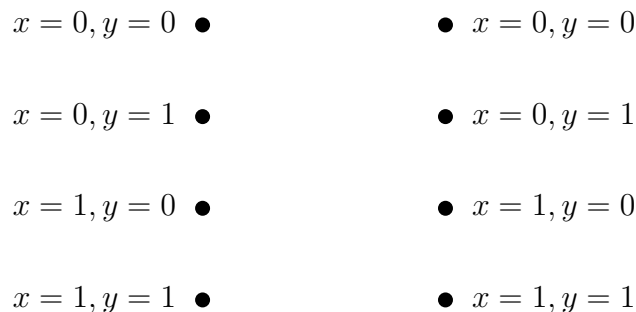
$$wp(\varphi_3, \rho_3) = pre(\varphi_3, \rho_3)$$

#### Exercise 2: Predicate transformers

1 Point

We consider two variables  $x, y$  over the binary domain  $\{0, 1\}$ .

- (a) The following diagram shows the four possible states on the left and on the right.



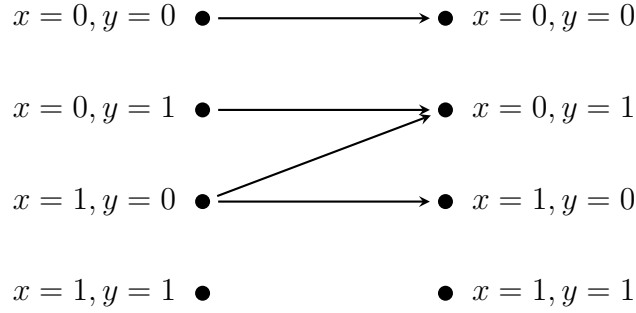
Draw the transitions that correspond to the following statements.

(i)  $x := 1$

(ii)  $havoc(x)$

(iii)  $assume(x = 0)$

(b) Consider the transition relation  $\rho$  that is given by the following diagram.



Find a formula for  $\rho$ .

Furthermore, compute the following sets.

- |                        |                         |                         |
|------------------------|-------------------------|-------------------------|
| (i) $wp(true, \rho)$   | (iii) $wp(y = 1, \rho)$ | (v) $wp(y = 0, \rho)$   |
| (ii) $pre(true, \rho)$ | (iv) $pre(y = 1, \rho)$ | (vi) $pre(y = 0, \rho)$ |

**Exercise 3: Relational composition**

1 Point

Find a formula that denotes the relational composition  $\rho_1 \circ \rho_2$  of the two relations denoted by the formulas  $\rho_1$  and  $\rho_2$ . Here  $\rho_1$  and  $\rho_2$  are formulas in the variables  $V \cup V'$ , where  $V'$  consists of the primed versions of the variables in  $V$ .

Careful: The algebraic definition may be counterintuitive because one first applies  $\rho_2$ :

$$\rho_1 \circ \rho_2 = \{(s_1, s_3) \mid \exists s_2. (s_1, s_2) \in \rho_2 \wedge (s_2, s_3) \in \rho_1\}$$

**Exercise 4: Properties of  $post^\#$**

1 Point

Give a counterexample for those of the following propositions that are wrong.

- (a)  $post^\#(\varphi, \rho_1 \circ \rho_2) \subseteq post^\#(post^\#(\varphi, \rho_2), \rho_1)$
- (b)  $post^\#(\varphi, \rho_1 \circ \rho_2) \supseteq post^\#(post^\#(\varphi, \rho_2), \rho_1)$
- (c)  $post^\#(\varphi, \rho_1 \vee \rho_2) \subseteq post^\#(\varphi, \rho_1) \vee post^\#(\varphi, \rho_2)$
- (d)  $post^\#(\varphi, \rho_1 \vee \rho_2) \supseteq post^\#(\varphi, \rho_1) \vee post^\#(\varphi, \rho_2)$
- (e)  $post^\#(\varphi_1 \vee \varphi_2, \rho) \subseteq post^\#(\varphi_1, \rho_1) \vee post^\#(\varphi_2, \rho)$
- (f)  $post^\#(\varphi_1 \vee \varphi_2, \rho) \supseteq post^\#(\varphi_1, \rho_1) \vee post^\#(\varphi_2, \rho)$