

# 2G1516 Formal Methods – HT05

## CCS - II

**Exercise 1** A communication protocol for transfer of natural numbers can be specified as:

$$Prot \stackrel{\text{def}}{=} in(x).\overline{out}(x).Prot \quad (x \in Nat)$$

- Implement this protocol by splitting it into a sending and a receiving component, so that the two components interact (internally) via a small number of simple (that is, value-free) channels only. (Hint: use for example a unary encoding of the numbers for the internal transmission.)
- Use the transition semantics to derive the transition graphs corresponding to the sender, the receiver, and the entire implementation.
- Are the specification and implementation processes strongly bisimulation equivalent? If so, establish a strong bisimulation relation as evidence. If not, explain why. Are they weakly bisimilar? Again, exhibit a weak bisimulation relation if they are, and explain why they are not, if so is the case.

□

**Exercise 2** Prove formally the law:

$$P \approx P + \tau.P$$

for all  $P$  by directly referring to the definition of weak bisimulation.

□

**Exercise 3** Prove formally the law:

$$\tau.P \mid Q \approx \tau.\tau.Q \mid P$$

for all  $P$  and  $Q$  by exhibiting a suitable weak bisimulation.

□

**Exercise 4** For the processes determined in the previous set, exercise 2, prove that  $Spec \approx Protocol$ .

□

**Exercise 5** Consider an arbitrary process  $P$ . Assume we want to modify  $P$  by adding a new action *exit* to its sort and by adding the possibility of terminating  $P$  in any reachable state (i.e. every process that  $P$  can evolve into) by

communicating through *exit*. Redefining  $P$  accordingly might be a cumbersome enterprise. A more elegant solution would be to define, for arbitrary  $Q$  and  $R$ , a new binary combinator  $Q \mid R$  so that the modified process could simply be specified as:

$$P \mid \text{exit}.0$$

1. Define the semantics of this new combinator by giving suitable transition rules for it. (Hint: the rules are not symmetric!)
2. Prove or disprove the equality:

$$(P \mid Q) \mid R = (P \mid R) \mid Q$$

□

**Exercise 6** Show that  $\approx$  is preserved by prefixing, parallel, restriction and relabelling. □

**Exercise 7** Prove that  $P = P'$  iff for all  $Q$ ,  $P + Q \approx P' + Q$ . □

**Exercise 8** Prove that observational congruence  $=$  is the largest congruence contained in  $\approx$ . □