

## Examination Program Correctness

6 January 2003, 14:00 - 17:00

---

1. Consider a vending machine with two buttons, B1 and B2, accepting coins of 1 Euro and 2 Euros. If button B1 is pressed the machine output product X, whereas if button B2 is pressed, the machine output product Y. Product X costs 3 Euros and product Y costs only 1 Euro. The machine can give back change (assume that it always has enough coins to give back as change).

- a) Model the behaviour of this vending machine using a labelled transition system with the following labels:

**B1** – button B1 is pressed

**B2** – button B2 is pressed

**I1** – a coin of 1 Euro is inserted

**I2** – a coin of 2 Euro is inserted

**OX** – product X is output

**OY** – product Y is output

**C1** – a coin of 1 Euro is given back as change

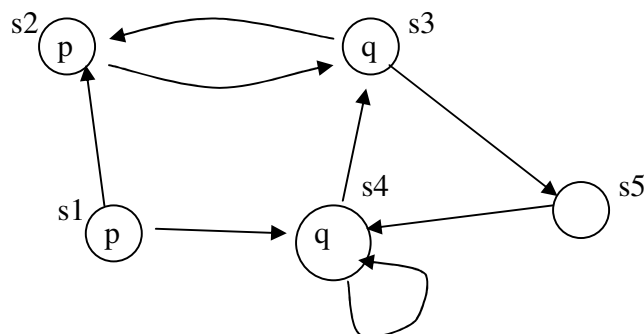
**C2** – a coin of 2 Euros is given back as change

Assume that the user first choose the product and then insert the coins. **[10 points]**

- b) Write a CTL formula specifying that “the vending machine cannot output product X without first (earlier) a user has pressed button B1” **[10 points]**
- c) Let P be the atomic proposition “the user has pressed button B1” and Q be the atomic proposition “the machine has output product X”. Label with P each state with an incoming transition labelled by **B1**, and label with Q each state with an incoming transition labelled by **OX**. Does the state where the user chooses the product satisfies your CTL specification above. **[10 points]**

2. Let p and q be two atomic propositions.

- a) Show from the CTL definition of AU that  $A[T \ U \ q]$  holds if q holds somewhere along every path. **[10 points]**
- b) Using the fixed-point method described in the course, give the set of all states of the following transition system satisfying the CTL formula  $E[p \ U \ EG \ q]$ . **[10 points]**



3. Prove the partial correctness of following Hoare triple: [10 points]

$$(\{ a[i] = x \wedge a[j] = y \}) z := a[i] ; a[i] := a[j] ; a[j] := z (\{ a[i] = y \wedge a[j] = x \})$$

4. Explain why one needs to introduce logical variables when reasoning about partial and total correctness of a command. [10 points]

5. Let  $a[0..n]$  be an array of integer and consider the following program MIN:

```
t := 1;
min := a[0]
while t ≤ n {
  if a[t] < min then {
    min := a[t]
  } else {
    skip
  }
  t := t + 1
}
```

- Write a postcondition  $\phi$  expressing the fact that the above program calculates the minimum number in the array  $a[0..n]$ . [10 points]
- Give an invariant for the while command establishing the postcondition  $\phi$ . [10 points]
- Give the variant function for proving the termination of the while command. [10 points]
- Give a proof outline for the total correctness of  $(\{ \text{true} \}) \text{MIN} (\{ \phi \})$ . [10 points]

The final score is given by the sum of the points obtained divided by 10 (with a maximum of 10).

---

### Proof system for partial correctness:

- |  |   |
|--|---|
| <p>1. <math>(\{ \phi \}) \text{skip} (\{ \phi \})</math></p> <p>3. <math display="block">\frac{(\{ \phi \}) c1 (\{ \phi \}) (\{ \phi \}) c2 (\{ \psi \})}{(\{ \phi \}) c1 ; c2 (\{ \psi \})}</math></p> <p>5. <math display="block">\frac{(\{ \phi \wedge b \}) c (\{ \phi \})}{(\{ \phi \}) \text{while } b \text{ do } \{ c \} (\{ \phi \wedge \neg b \})}</math> </p> | <p>2. <math>(\{ \phi[e/x] \}) x := e (\{ \phi \})</math></p> <p>4. <math display="block">\frac{(\{ \phi \wedge b \}) c1 (\{ \psi \}) (\{ \phi \wedge \neg b \}) c2 (\{ \psi \})}{(\{ \phi \}) \text{if } b \text{ then } \{ c1 \} \text{ else } \{ c2 \} (\{ \psi \})}</math></p> <p>6. <math display="block">\frac{\phi \Rightarrow \phi1 (\{ \phi1 \}) c (\{ \psi1 \}) \psi1 \Rightarrow \psi}{(\{ \phi \}) c (\{ \psi \})}</math> </p> |
|--|---|