2G1516 Formal Methods   2G1521 Formal Methods for SEDS

SOLUTIONS
22 August 2005, 2pm–7pm

Mads Dam
KTH/IMIT

1.

1. skolem 1 y; flatten; split; inst 1 y
2. Let R be the relation $\{(0,0)\}$ on binary numbers $\{0,1\}$, and let $Q(x)$ be the proposition $0 = 1$, i.e. false. Then $(\forall x.R(x,x)) \rightarrow Q(0)$ and $R(0,0)$ are both valid, but $Q(0)$ is not.

2.

1. $[]((\mathit{begin\_read} \rightarrow O\,\mathit{end\_read}) \wedge (\mathit{begin\_write} \rightarrow O\,\mathit{end\_write}))$
2. $[]((\mathit{begin\_read} \rightarrow <>\ \mathit{end\_read}) \wedge (\mathit{begin\_write} \rightarrow <>\ \mathit{end\_write}))$
3. $[](\mathit{begin\_read} \vee \mathit{begin\_write} \vee \mathit{end\_read} \vee \mathit{end\_write})$
4. $<>\ []\neg \mathit{begin\_write}$
5. $([](\neg \mathit{end\_write} \wedge \neg \mathit{begin\_read}) \vee ((\neg \mathit{begin\_read}) U\, \mathit{end\_write}))$

---

3. The Buchi automaton has two states, s_1 and s_2. Both are accepting, and s_1 is initial. There are three transitions, from s_1 to s_1 labelled $(\neg \mathit{begin\_read}) \wedge (\neg \mathit{end\_write})$, from s_1 to s_2 labelled *end_write*, and from s_2 to s_2 labelled *true*.

4.

```
{true}
{forall j. 1 <= j && j < 1 implies 0 >= a[j]}
x := 0 ;
{forall j. 1 <= j && j < 1 implies x >= a[j]}
i := 1 ;
{forall j. 1 <= j && j < i implies x >= a[j]}
while i <= m do
  {i <= m && forall j. 1 <= j && j < i implies x >= a[j]}
  if a[i] > x
```

```
  then
    {i <= m && a[i] > x &&
     forall j. 1 <= j && j < i implies x >= a[j]}
    {i <= m && a[i] >= a[i] &&
      forall j. 1 <= j && j < i implies a[i] >= a[j]}
    x := a[i]
    {i <= m && x >= a[i] && forall j. 1 <= j && j < i implies x >= a[j]}
  else
    {i <= m && a[i] <= x &&
     forall j. 1 <= j && j < i implies x >= a[j]}
    skip
    {i <= m && a[i] <= x &&
     forall j. 1 <= j && j < i implies x >= a[j]}
  endif ;
  {i <= m && x >= a[i] && forall j. 1 <= j && j < i implies x >= a[j]}
  {i <= m && forall j. 1 <= j && j < i+1 implies x >= a[j]}
  i := i + 1
  {forall j. 1 <= j && j < i implies x >= a[j]}
od
{i > m && forall j. 1 <= j && j < i implies x >= a[j]}
{forall j. 1 <= j && j <= m implies x >= a[i]}
```

---

5. Both equivalences hold. Let $P = \tau.a.0 + b.0$, $Q = \tau.a.0 + \tau.b.0 + b.0$, $R = a.0 + \tau.a.0 + b.0$, and let I be the identity relation on CCS terms. The relations $I \cup \{(P, Q)\}$ and $I \cup \{(P, R)\}$ are weak bisimulation relations. I leave out the check of this assertion (which should be done).

---

6. The following relation is a weak bisimulation relation:

$$\{(S^2, I), (S^2_1, (S^1_1[c/v]|S^1[\overline{c}/p])\backslash\{c\}), (s^2_1, (S^1[c/v]|S^1_1[\overline{c}/p])\backslash\{c\}), (s^2_2, (S^1_1[c/v]|S^1_1[\overline{c}/p])\backslash\{c\})\}$$

   Again I leave out the check of the weak bisimulation conditions.