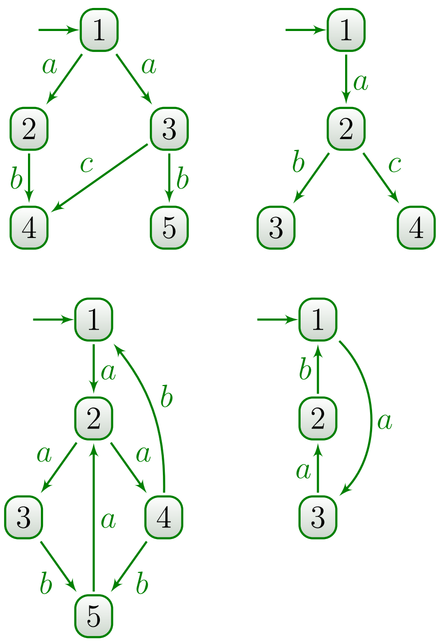
Technische Universität München **Summer Semester 2015**
I7
J. Esparza / A. Durand-Gasselin / D. Suwimonteerabuth **July 2015**

Model Checking – Solution sheet 11

Exercise 11.1: Simulation and bisimulation



1. T_2 simulates T_1, e.g. the relation $R_{2\to 1}$: $\{(1,1),(2,2),(2,3),(3,4),(3,5),(4,4)\}$
2. T_1 simulates T_2, e.g. the relation $R_{1\to 2}$: $\{(1,1),(3,2),(4,4),(5,3)\}$
3. Player 1 picks T_1, goes to 2: player 2 must go to 2 in T_2. Then player 1 picks T_2, goes to 4 with c. Player 2 can't respond, hence T_1 and T_2 aren't bisimilar.
4. Remark the bisimulation relation $R_{3\leftrightarrow 4}$: $\{(1,1),(5,1),(2,3),(3,2),(4,2)\}$. As a strategy, to answer any move of Player 1, Player 2 just needs to pick an element that is reachable with the same action as Player 1 fired, and that is in relation $R_{3\leftrightarrow 4}$ to the element reached by Player 1, which she can always do as $R_{3\leftrightarrow 4}$ is a bisimulation relation.
5. If S_1 and S_2 are bisimilar and S_2 and S_3 are bisimilar, denote $R_{1\leftrightarrow 2}$ and $R_{2\leftrightarrow 3}$ explicit bisimulation relations. We define the relation $R_{1\leftrightarrow 3}$ as follows: $R_{1\leftrightarrow 3} = \{(x_1,x_3) \mid \exists x_2 \,.\, (x_1,x_2) \in R_{1\leftrightarrow 2} \wedge (x_2,x_3) \in R_{2\leftrightarrow 3}\}$.

   Let us show that $R_{1\leftrightarrow 3}$ is a simulation relation of S_1 by S_3. We need to show that if $(x_1,x_3) \in R_{1\leftrightarrow 3}$, then for any action α, and any $x'_1 \in S_1$, if $x_1 \xrightarrow{\alpha} x'_1$ is feasible in S_1, we can find x'_3 such that $(x'_1,x'_3) \in R_{1\leftrightarrow 3}$ and $x_3 \xrightarrow{\alpha} x'_3$ is feasible in S_3.

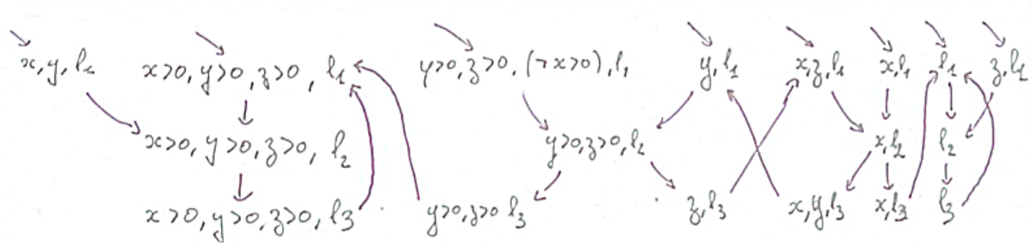
   By definition of $R_{1\leftrightarrow 3}$ there exists x_2 such that $(x_1,x_2) \in R_{1\leftrightarrow 2}$ and $(x_2,x_3) \in R_{2\leftrightarrow 3}$. Since $R_{1\leftrightarrow 2}$ is a bisimulation relation, it is also a simulation relation of S_1 by S_2, thus we can find x'_2 such that $x_2 \xrightarrow{\alpha} x'_2$ and $(x'_1,x'_2) \in R_{1\leftrightarrow 2}$. Since $R_{2\leftrightarrow 3}$ is a bisimulation relation, it is also a simulation relation of S_2 by S_3, thus we can find x'_3 such that $x_3 \xrightarrow{\alpha} x'_3$ and $(x'_2,x'_3) \in R_{2\leftrightarrow 3}$. Clearly $(x'_1,x'_3) \in R_{1\leftrightarrow 3}$, therefore. $R_{1\leftrightarrow 3}$ is a simulation relation of S_1 by S_3.

   In a similar manner we can show that $R_{1\leftrightarrow 3}$ is also simulation relation of S_3 by S_1, hence a bisimulation relation, therefore S_1 and S_3 are bisimilar.

Exercise 11.2: Abstraction of a simple program

```
while(true) {
    z  = y;
    y  = y + x;
    x  = z;
}
```

1. The size of the transition system is infinite: $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \{1, 2, 3\}$.

2. 

Exercise 11.3: Abstraction of a more complex program

1. In the abstract Kripke structure, we may reach a state where all values are negative (e.g. when branching, always chosing the transition that decreases the number of predicates holding)

2. In the concrete transition system, we may reach a state where all values are negative (e.g `x=1; y=3; z=1`; remark that these initial values do not concretizes the aforementioned abstract path).

3. We can easily find a loop where all predicates always hold (hence all predicates *eventually* always hold).

4. `x=2; y=1; z=1;`

5. The two systems cannot be bisimilar, typically the concrete transition sytem is deterministic while the abstract Kripke structure is not: the concrete transition system cannot simulate the abstract Kripke structure.