

Exercises for “Formal Specification and Verification” Exercise sheet 6

Exercise 6.1:

You may recall the puzzle of a ferryman, goat, cabbage, and wolf all on one side of a river. The ferryman can cross the river with at most one passenger in his boat. There is a behavioural conflict between:

1. the goat and the cabbage; and
2. the goat and the wolf;

if they are on the same river bank but the ferryman is not on that river bank (the goat eats the cabbage, resp. the wolf eats the goat).

Define a “program graph” describing this system: $(\text{Loc}, \text{Act}, \text{Effect}, \rightarrow, \text{Loc}_0)$ where:

- $\text{Loc} = \{ \text{left}, \text{right}, \text{conflict} \}$ is a set of locations with initial locations $\text{Loc}_0 = \{ \text{left} \}$.
Intuitively, left and right represent the location of the ferryman; conflict represents the conflict situation when the cabbage or the goat is eaten.
- $\text{Act} = \{ \text{carry-lr-goat}, \text{carry-rl-goat}, \text{carry-lr-cabbage}, \text{carry-rl-cabbage}, \text{carry-lr-wolf}, \text{carry-rl-wolf}, \text{cross-rl}, \text{cross-lr}, \text{eat-cabbage}, \text{eat-goat} \}$ is a set of actions.

(For instance:

- carry-lr-goat means: the ferryman carries the goat from the left to the right river bank
- carry-rl-goat means: the ferryman carries the goat from the right to the left river bank
- cross-rl (resp. cross-lr) means: the ferryman crosses the river from right to left (left to right) without carrying anything.
- eat-cabbage means: the goat eats the cabbage
- eat-goat means: the wolf eats the goat.)

Assume that $\text{Var} = \{ \text{goat}, \text{cabbage}, \text{wolf} \}$ and the corresponding domains are $\{l, r\}$.

Let $\text{Eval}(\text{Var}) = \{ \beta \mid \beta : \text{Var} \rightarrow \{l, r\} \}$.

(Intuitively, $\beta(x) = l$ means that x is on the left side of the river, and $\beta(x) = r$ means that x is on the right side of the river.)

Assume that $\text{Cond}(\text{Var}) = \{ \text{goat} \approx l, \text{goat} \approx r, \text{cabbage} \approx l, \text{cabbage} \approx r, \text{wolf} \approx l, \text{wolf} \approx r \}$ and that the initial condition is

$$g_0 := (\text{goat} \approx l) \wedge (\text{cabbage} \approx l) \wedge (\text{wolf} \approx l)$$

- (1) Define a suitable effect function $\text{Effect} : \text{Act} \times \text{Eval}(\text{Var}) \rightarrow \text{Eval}(\text{Var})$.
(It is not necessary to exhaustively present the definition of this function, you can present some examples and explain how it is defined in general)
- (2) Define a suitable transition relation $\rightarrow \subseteq \text{Loc} \times (\text{Cond}(\text{Var}) \times \text{Act}) \times \text{Loc}$
such that there is no $\phi \in \text{Cond}(\text{Var}), \alpha \in \text{Act}, l \in \text{Loc}$ such that $(\text{conflict}, \phi, \alpha, l) \in \rightarrow$.
(It is not necessary to exhaustively present the definition of the transition relation \rightarrow ; you can explain how it is defined in general and give some examples)
- (3) Describe the transition system $TS(PG) = (S, \text{Act}, \rightarrow, I, AP, L)$ of the program graph $(\text{Loc}, \text{Act}, \text{Effect}, \rightarrow, \text{Loc}_0, g_0)$ constructed before.
(It is not necessary to exhaustively present the definition of the transition relation \rightarrow or the labelling function; you can explain how they are defined in general and give some examples)
- (4) Describe:
- $\text{Post}(\langle \text{left}, \beta \rangle, \text{carry-lr-goat})$, where $\beta(\text{goat}) = l, \beta(\text{cabbage}) = \beta(\text{wolf}) = r$.
 - $\text{Post}(\langle \text{left}, \beta \rangle, \text{carry-rl-goat})$, where $\beta(\text{goat}) = l, \beta(\text{cabbage}) = \beta(\text{wolf}) = r$.
 - $\text{Post}(\langle \text{left}, \beta \rangle)$, where $\beta(\text{goat}) = l, \beta(\text{cabbage}) = \beta(\text{wolf}) = r$.
 - $\text{Post}(\langle \text{right}, \beta \rangle)$, where $\beta(\text{goat}) = \beta(\text{cabbage}) = l, \beta(\text{wolf}) = r$.
 - $\text{Post}(\{\langle \text{right}, \beta \rangle, \langle \text{right}, \beta' \rangle\})$, where $\beta(\text{goat}) = \beta(\text{cabbage}) = l, \beta(\text{wolf}) = r$ and $\beta'(\text{goat}) = \beta(\text{wolf}) = l, \beta(\text{cabbage}) = r$
 - $\text{Pre}(\langle \text{conflict}, \beta \rangle)$, where $\beta(\text{goat}) = \beta(\text{cabbage}) = l, \beta(\text{wolf}) = r$.
 - $\text{Pre}(\langle \text{conflict}, \beta \rangle)$, where $\beta(\text{goat}) = \beta(\text{wolf}) = \beta(\text{cabbage}) = r$.
- (5) Is the transition system you constructed action-deterministic? Is it AP -deterministic?
- (7) Are there terminal states in the system?
- (8) Is the state $\langle \text{right}, \beta \rangle$ with $\beta(\text{goat}) = \beta(\text{cabbage}) = \beta(\text{wolf}) = r$ reachable?

Please submit your solution until Wednesday, June 12, 2013 at 10:00. Please do not forget to write your name on your solution.

Submission possibilities:

- By e-mail to sofronie@uni-koblenz.de with the keyword "Homework FSV" in the subject.