Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **November 26, 2018**

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: $(\mathsf{Loc}, \mathsf{Act}, \mathsf{Effect}, \rightarrow, \mathsf{Loc}_0)$ where:

- $\mathsf{Loc} = \{$ left, right, conflict $\}$ is a set of locations with initial locations $\mathsf{Loc}_0 = \{$ left $\}$.

  Intuitively, left and right represent the location of the ferryman; conflict represents the conflict situation when the cabbage or the goat is eaten.

- $\mathsf{Act} = \{$ carry-lr-goat, carry-rl-goat, carry-lr-cabbage, carry-rl-cabbage, carry-lr-wolf, carry-rl-wolf, cross-rl, cross-lr, eat-cabbage, 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 $\mathsf{Var} = \{\mathsf{goat}, \mathsf{cabbage}, \mathsf{wolf}\}$ and the corresponding domains are $\{l, r\}$.

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

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

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

(1) Define a suitable effect function $\mathsf{Effect} : \mathsf{Act} \times \mathsf{Eval}(\mathsf{Var}) \to \mathsf{Eval}(\mathsf{Var})$.

(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 $\to \ \subseteq \ \mathsf{Loc} \times (Cond(\mathsf{Var}) \times \mathsf{Act}) \times \mathsf{Loc}$

such that there is no $\phi \in Cond(\mathsf{Var}), \alpha \in Act, l \in \mathsf{Loc}$ such that $(\text{conflict}, \phi, \alpha, l) \in \to$.

(It is not necessary to exhaustively present the definition of the transition relation $\to$; you can explain how it is defined in general and give some examples)

(3) Describe the transition system $TS(PG) = (S, \mathsf{Act}, \to, I, AP, L)$ of the program graph $(\mathsf{Loc}, \mathsf{Act}, \mathsf{Effect}, \to, \mathsf{Loc}_0, g_0)$ constructed before.

(It is not necessary to exhaustively present the definition of the transition relation $\to$ or the labelling function; you can explain how they are defined in general and give some examples)

(4) Describe:

- $\mathsf{Post}(<\text{left}, \beta >, \text{carry-lr-goat})$, where $\beta(\mathsf{goat}) = l, \beta(\mathsf{cabbage}) = \beta(\mathsf{wolf}) = r$.
- $\mathsf{Post}(<\text{left}, \beta >, \text{carry-rl-goat})$, where $\beta(\mathsf{goat}) = l, \beta(\mathsf{cabbage}) = \beta(\mathsf{wolf}) = r$.
- $\mathsf{Post}(<\text{left}, \beta >)$, where $\beta(\mathsf{goat}) = l, \beta(\mathsf{cabbage}) = \beta(\mathsf{wolf}) = r$.
- $\mathsf{Post}(<\text{right}, \beta >)$, where $\beta(\mathsf{goat}) = \beta(\mathsf{cabbage}) = l, \beta(\mathsf{wolf}) = r$.
- $\mathsf{Post}(\{<\text{right}, \beta >, <\text{right}, \beta' >\})$, where $\beta(\mathsf{goat}) = \beta(\mathsf{cabbage}) = l, \beta(\mathsf{wolf}) = r$ and $\beta'(\mathsf{goat}) = \beta(\mathsf{wolf}) = l, \beta(\mathsf{cabbage}) = r$
- $\mathsf{Pre}(<\text{conflict}, \beta >)$, where $\beta(\mathsf{goat}) = \beta(\mathsf{cabbage}) = l,\ \beta(\mathsf{wolf}) = r$.
- $\mathsf{Pre}(<\text{conflict}, \beta >)$, where $\beta(\mathsf{goat}) = \beta(\mathsf{wolf}) = \beta(\mathsf{cabbage}) = r$.

(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 $<\text{right}, \beta >$ with $\beta(\mathsf{goat}) = \beta(\mathsf{cabbage}) = \beta(\mathsf{wolf}) = r$ reachable?

Please submit your solution until Sunday, December 2, 2018 at 17:00. 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.
- Hand it in to me (Room B225) or drop it in the box in front of Room B224.