Formal techniques for software and hardware verification

Lecturers:

Vladimir Zakharov

Vladislav Podymov

e-mail:

valdus@yandex.ru

2020, fall semester

Seminar 2

Kripke structures

Safety and liveness

LTL

Fairness

Exercise 1

Formalize the following system as a Kripke structure over the following atomic propositions

The system:

```
cobegin
  x := 1; y := 2
||
  y := 1; x := 2
coend
```

+ the initial data state `[x/0, y/0]`

The propositions: `x` = i and `y` = i ,
$i \in \{0, 1, -1, 2, -2, \dots\}$

Exercise 1

Formalize the following system as a Kripke structure over the following atomic propositions

The system: `cobegin x := x + x || x := x + x coend`

\+ the initial data state `[x/1]`

The propositions: `x = i` , $i \in \mathbb{Z}$

Exercise 1

Formalize the following system as a Kripke structure over the following atomic propositions

The system: `cobegin x := x + x || x := x + x coend`

\+ the initial data state `[x/1]`

The propositions: `x` $= i$, $i \in \mathbb{Z}$

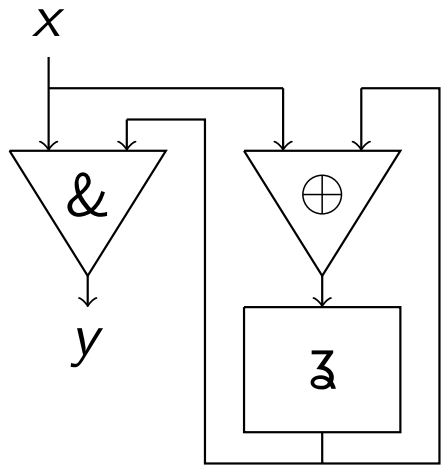
Harder variant: the sum-assignment is implemented as 3 atomic actions:

1. obtain value of the left argument of the sum
2. obtain value of the right argument of the sum
3. store sum of obtained values into the target variable

Exercise 1

Formalize the following system as a Kripke structure over the following atomic propositions

The system: boolean circuit with delay elements



The propositions: $(i \in \{0, 1\})$

- x_i: input value x equals to i
- y_i: output value y equals to i

Exercise 1

Formalize the following system as a Kripke structure over the following atomic propositions

The system: the river crossing puzzle ("Ferry" from lectures)

Atomicity variants:

1. 1 action: embark+sail+disembark
2. 3 actions: embark everyone; sail; disembark everyone
3. 9 actions: embark an actor; sail; disembark an actor

Action choice freedom variants:

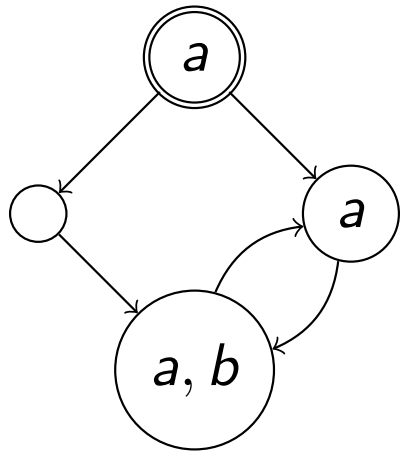
1. Actors are eaten immediately when possible (w.r.t. rules)
2. Actors are eaten in one transition when possible
3. Actors are not obliged to be eaten

The propositions:

- *wr*, *gr*, *cr*: the wolf/goat/cabbage is at the right side
- *ga*, *ca*: the goat/cabbage is "alive" (not eaten)

Exercise 2

Construct all paths and all traces of the following Kripke structure



(S) is a state labeled with the set $\{S\}$ of atomic propositions

Transitions are depicted as graph arcs

◎ is an initial state

Exercise 3

Suggest an ltl-formula corresponding to the following sentence:

1. The processes P_1, P_2 do not execute in their critical sections simultaneously

   c_i is a proposition "P_i executes in its critical section"

2. A green traffic light will eventually turn yellow, and will not turn red before that

   g, y, r are propositions "the light is green", "the light is yellow", and "the light is red" respectively,

3. The message cannot be lost inifinitely many times

   miss is a proposition "the message is lost"

Exercise 3

Suggest an ltl-formula corresponding to the following sentence:

4. The operation cannot be executed during more than three consequtive cycles

   p is a proposition "the operation is being executed"

5. The system constantly indicates an error until it becomes functional

   ok is a proposition "the system is functional"

   err is a proposition "the system indicates an error"

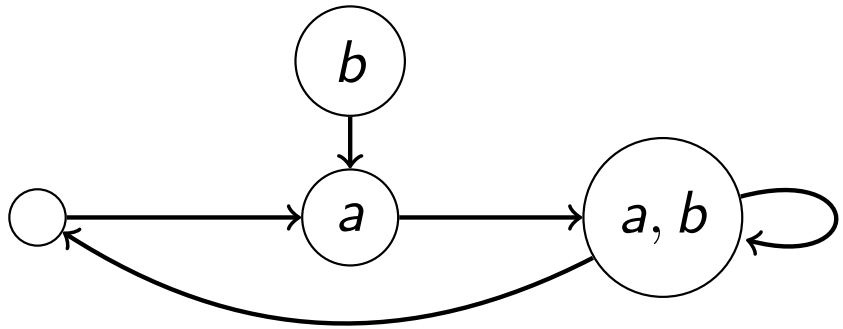
6. The one who trains a lot eventually achieves perfection

   t is a proposition "The one trains"

   p is a proposition "The one has achieved perfection"

Exercise 4

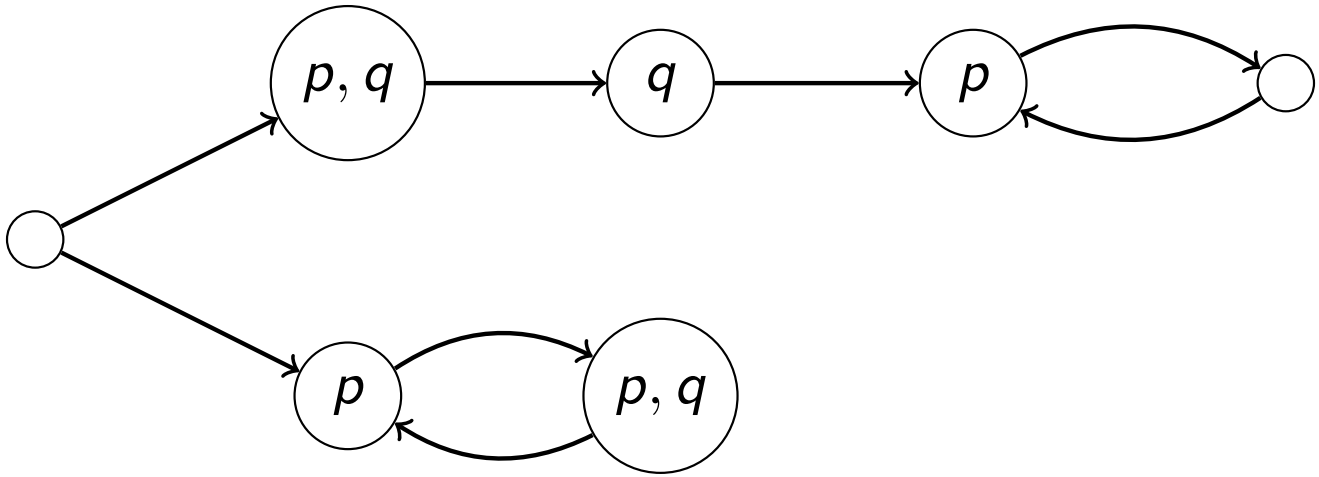
Which states of the following Kripke structure satisfy the given formula?



- $\mathbf{A}a$
- $\mathbf{AXX}a$
- $\mathbf{AG}a$
- $\mathbf{AGF}a$
- $\mathbf{AFG}a$
- $\mathbf{A}(\neg b \mathbf{U} a \,\&\, b)$
- $\mathbf{A}(a \mathbf{U} \neg a)$

Exercise 4

Which states of the following Kripke structure satisfy the given formula?



- $\mathbf{AF}(\mathbf{X}p\mathbf{UG}\neg q)$

Exercise 5

Is the following set of traces over the nonempty set AP of atomic propositions

a) a safety property?

b) a liveness property?

1. $(2^{AP})^{\omega}$
2. $\emptyset$
3. $\{a, b\}^{\omega}$ $\quad (2^{AP} = \{a, b, c, d\})$
4. $\{a, b\}^{*} \cdot \{a\}^{\omega}$ $\quad (2^{AP} = \{a, b\})$
5. $\{a\}^{*} \cdot \{b\} \cdot \{a\}^{\omega}$ $\quad (2^{AP} = \{a, b\})$
6. $\{ab\}^{\omega}$ $\quad (2^{AP} = \{a, b\})$
7. $\{a, b, c\}^{*} \cdot \{d\} \cdot \{a\}^{\omega}$ $\quad (2^{AP} = \{a, b, c, d\})$

$X^{\omega} = \{w_1 w_2 w_3 \cdots \mid w_i \in X\}$
$X^{*} = \{w_1 w_2 \ldots w_k \mid w_i \in X,\ k \in \mathbb{N}_0\}$
$X \cdot Y = \{w_x w_y \mid w_x \in X,\ w_y \in Y\}$

Exercise 6

Does the following statement hold in general?

1. If P_1 and P_2 are safety properties, then $P_1 \cap P_2$ is a safety property

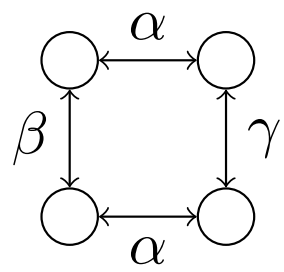
2. If P_1 and P_2 are safety properties, then $P_1 \cup P_2$ is a safety property

3. If P_1 and P_2 are liveness properties, then $P_1 \cap P_2$ is a liveness property

4. If P_1 and P_2 are liveness properties, then $P_1 \cup P_2$ is a liveness property

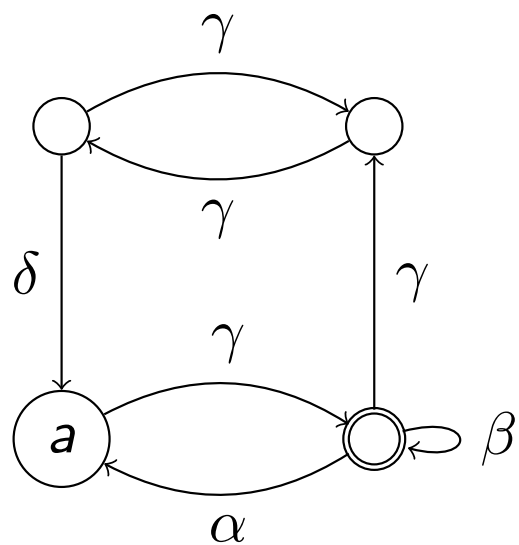
Exercise 7

Which paths of the following Kripke structure M do **not** belong to the set $Tr(M, Fair)$ for the given fairness constraints $Fair = (WeakFair, StrongFair)$?



1. $WeakFair = \emptyset$, $StrongFair = \emptyset$;
2. $WeakFair = \{\alpha\}$, $StrongFair = \emptyset$;
3. $WeakFair = \{\alpha, \beta\}$, $StrongFair = \emptyset$;
4. $WeakFair = \{\alpha\}$, $StrongFair = \{\beta\}$;
5. $WeakFair = \emptyset$, $StrongFair = \{\alpha, \beta\}$;
6. $WeakFair = \emptyset$, $StrongFair = \{\alpha, \beta, \gamma\}$;

Exercise 8

Construct all fairness constraints $Fair = (WeakFair, StrongFair)$ such that $M, Fair \models \mathbf{AGF}a$

M: