Modeling and Analysis of Hybrid Systems - SS 2015

First Exam

Monday, July 27, 2015

Forename and surname:	**Matriculation number:**
Sign here:	

- Do not open the exam until we give the start signal.
- Please place your student identity card on your desk for identification purposes.
- The duration of the exam is 120 minutes.
- Use a blue or black (permanent) pen only.
- Please write your name and matriculation number on each page of this exam.
- Please write clear and legible answers.
- If you need more sheets, indicate this by a hand signal. Please use a separate sheet for each task.
- Please clearly cross out parts you do *not* wish to be evaluated.
- If you have problems understanding a task, indicate this by a hand signal.
- You are not allowed to use auxiliary material except for a pen. In particular, switch off your electronic devices! Cheating disqualifies from the exam.

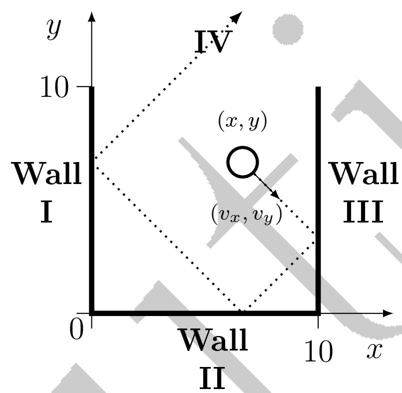
Task:	1.)	2.)	3.)	4.)	5.)	6.)	**Total**
Maximum score:	18	14	16	15	10	7	80
Reached score:							

Good luck!

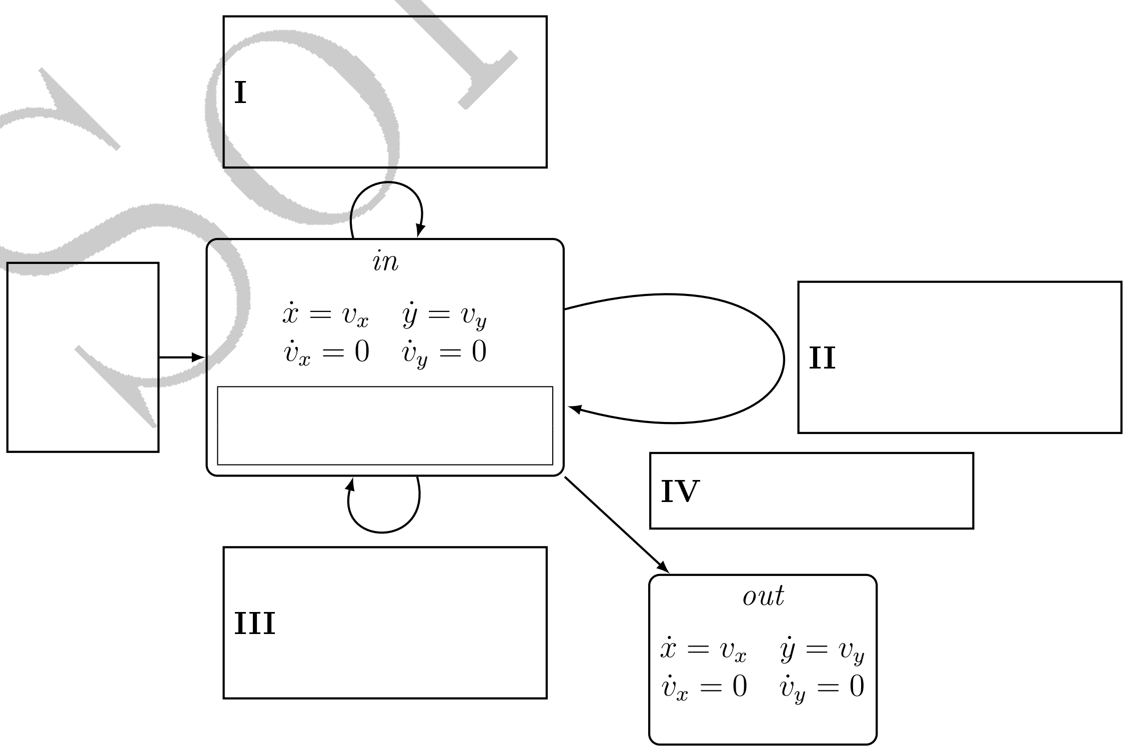
Task 1. Hybrid systems modeling (10 + 5 + 3 points)

a) Consider a *bouncing ball in a box in the 2-dimensional space.*

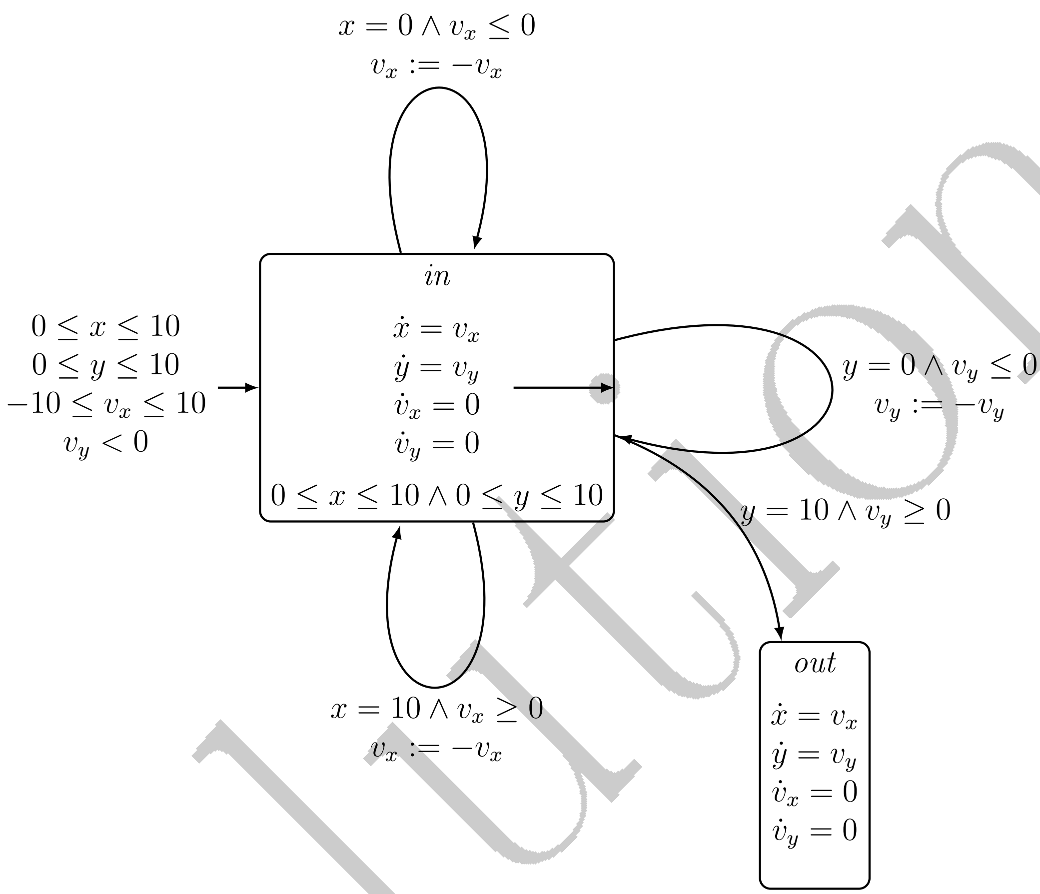
- The box has 3 walls (**I**,**II**,**III**) and is open at the top. The width and the height of the box are both 10 units, the left bottom corner being at $(0, 0)$.
- The position of the ball, which is abstracted as a point, is denoted by (x, y), its velocity by (v_x, v_y).
- The ball is initially located *inside* the box with an initial velocity in the x-dimension between -10 and 10 and a *negative* velocity in the y-dimension.
- Whenever the ball reaches a wall it bounces (the sign of its velocity in the dimension orthogonal to the wall is inverted). As we have an ideal ball, there is *no dampening.*
- If the ball leaves the box (**IV**), the system switches to a sink mode (the ball is *out*).



Please *fill in the missing parts* in the following incomplete hybrid automaton according to the above specification.



Solution:



b) Please explain the terms *Zeno behavior* and *time lock*. Does the above automaton exhibit such phenomena? Argue why! *Solution:*

- *Zeno behavior:* We refer to Zeno behavior of a hybrid automaton, if it is possible to execute an infinite number of discrete steps in a finite or even zero time.

  The automaton exhibits Zeno behavior: Whenever the x-position is 0 or 10 (the ball is at wall I or wall III) and the x-velocity v_x is 0, it is possible to take the transitions I or III respectively infinitely often.

- *Time lock:* A timed automaton exhibits a time lock if there is a reachable state from which there exists no time-diverging path.

  The automaton has no time lock - even in the scenario described above it is always possible to give a time-divergent path for location *in*, as $v_y \neq 0$ allows time-divergent paths.

c) Please give the formal *operational semantics of a discrete step* (jump) for hybrid automata.

Solution:

$$\frac{(l, a, \mu, l') \in Edge \quad (\nu, \nu') \in \mu \quad \nu' \in Inv(l')}{(l, \nu) \xrightarrow{a} (l', \nu')} \ \texttt{Rule}_{\texttt{discrete}}$$

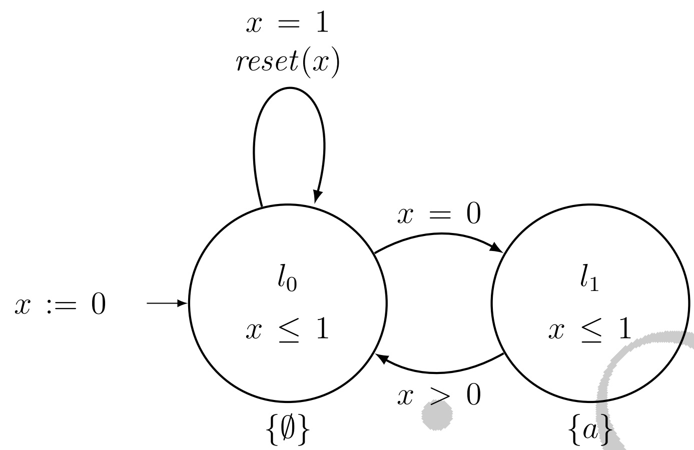
$\mu \in V \times V$

Alternatively: An edge $e = (l, a, \mu, l') \in Edge$ consists of the components

- *Source location:* The location l the system currently resides in.
- *Guard:* $\varphi_{e,guard}[\nu(x)/x]$ has to be fulfilled by the current variable valuations $\nu(x)$ in order to enable the transition.
- *Reset function:* In case the transition is taken, the reset function (realized by the formula $\varphi_{e,reset}[\nu(x), \nu'(x)/x, x']$) can modify the valuations of the variables. The result of the reset function ν' has to fulfill the invariant of the target location.
- *Target location:* The location l' the system will reside in after taking the transition.
- *Label (optional):* A label a, which can be used for synchronization purposes.

Task 2. Timed automata **($2 + 6 + 3 + 3$ points)**

Consider the following timed automaton $\mathcal{T}$ and the TCTL formula $\varphi = AF^{\leq 2}a$:

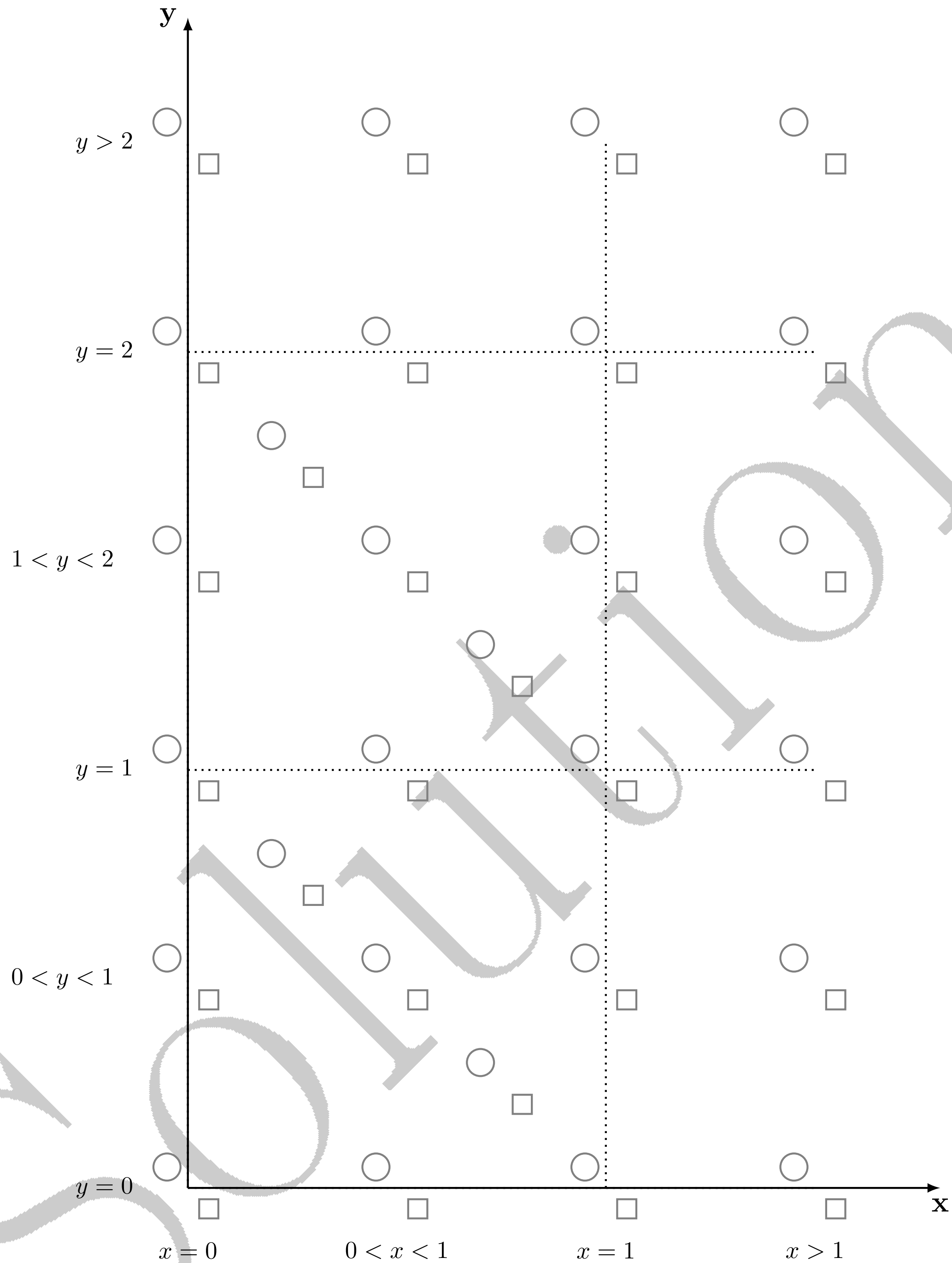


a) Please eliminate in φ the syntactic sugar for the finally operator (F) and *construct* $\hat{\varphi}$ by eliminating timing parameters. Use the name y for the auxiliary clock.
Solution:

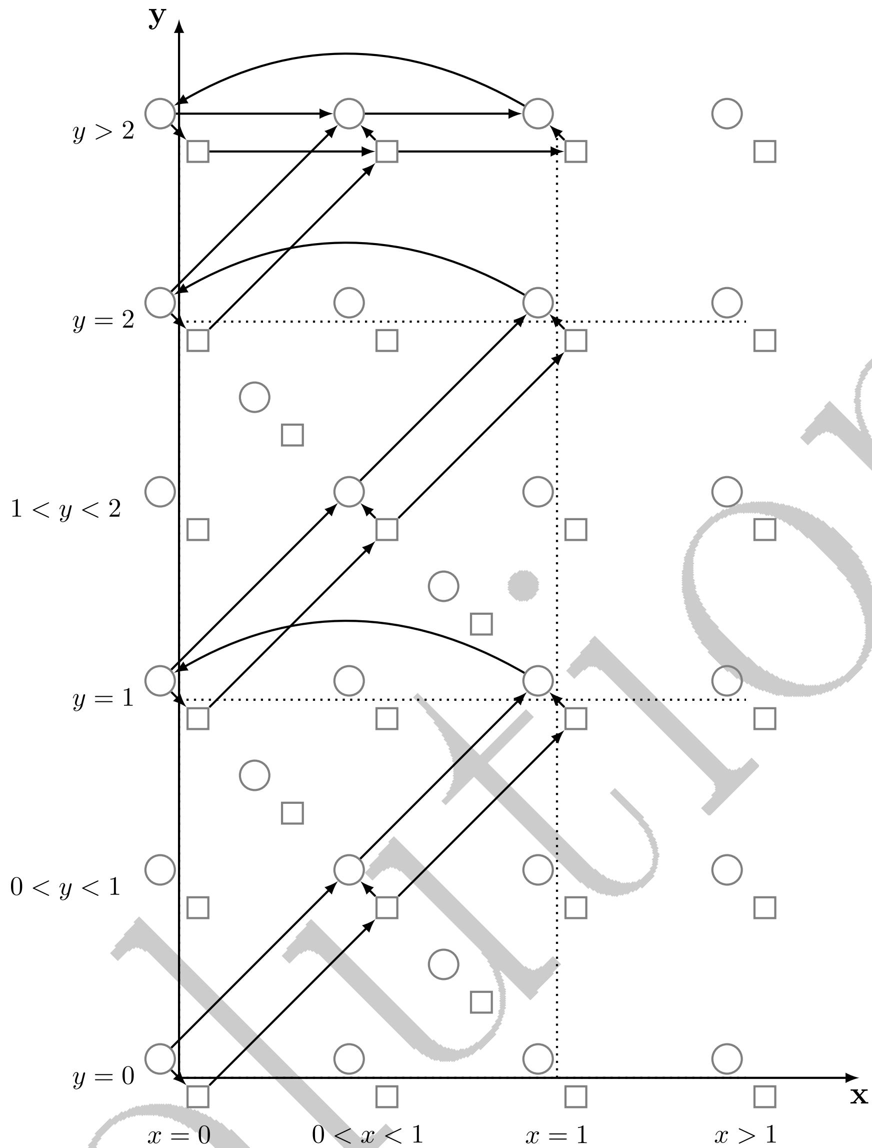
$$\hat{\varphi} = AF(y \leq 2 \wedge a)$$
$$\Leftrightarrow A(true\, \mathcal{U}(y \leq 2 \wedge a))$$

b) Construct the *region transition system* (*RTS*) $\mathcal{R}$, such that $\mathcal{T} \models_{TCTL} \varphi$ iff $\mathcal{R} \models_{CTL} \hat{\varphi}$. As $\mathcal{R}$ will become big, use the prepared grid below to sketch the RTS (by adding the RTS transitions) as follows:

- ◯ represents a state, where the location is l_0.
- □ represents a state, where the location is l_1.
- The position of a state in the grid determines, which clock region the state represents.
- Please draw only the reachable fragment of $\mathcal{R}$.



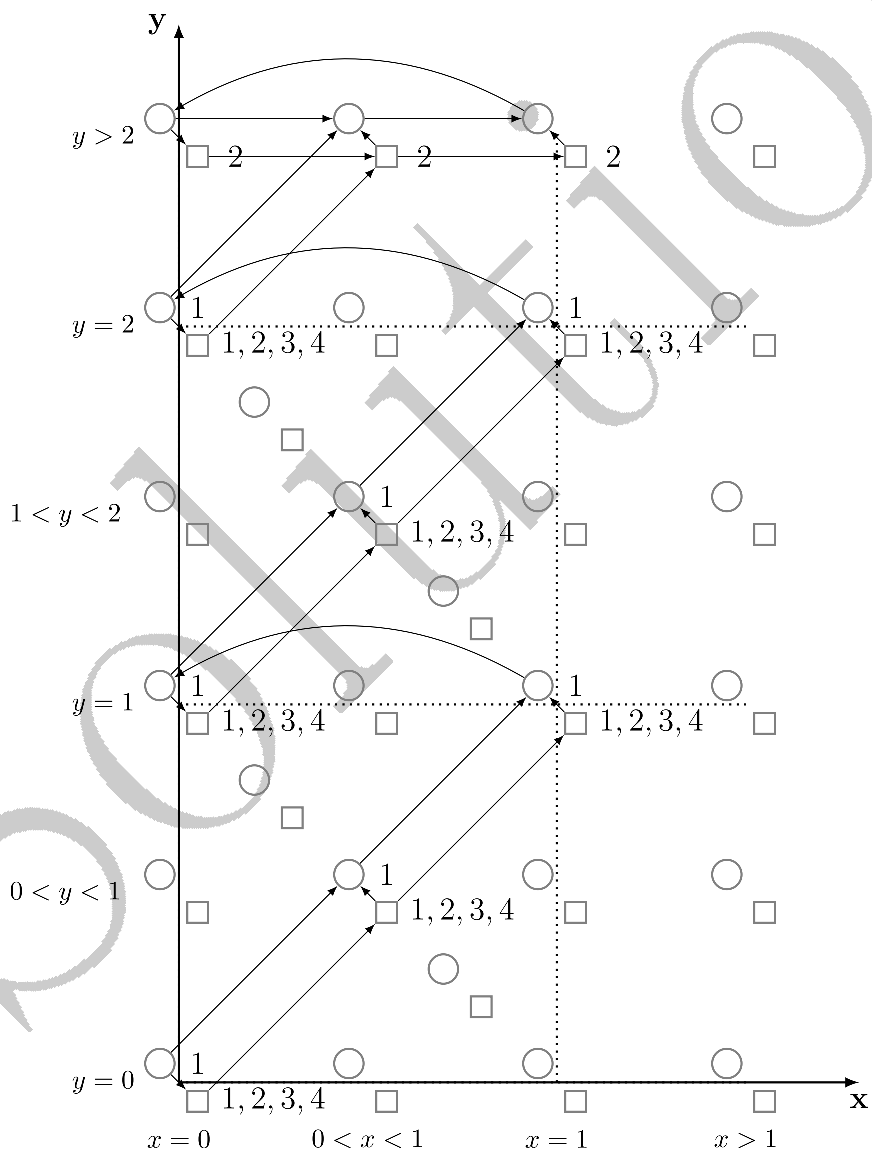
Solution:


y
y > 2
y = 2
1 < y < 2
y = 1
0 < y < 1
y = 0
x
x = 0
0 < x < 1
x = 1
x > 1

c) Apply *CTL model checking* to determine whether or not $\mathcal{R} \models_{CTL} \hat{\varphi}$. Please give names for the subformulas of $\hat{\varphi}$ and label the RTS states with them on the previous page. Does $\hat{\varphi}$ hold in $\mathcal{R}$, i.e., does $\mathcal{R} \models_{CTL} \hat{\varphi}$ hold?

Solution:

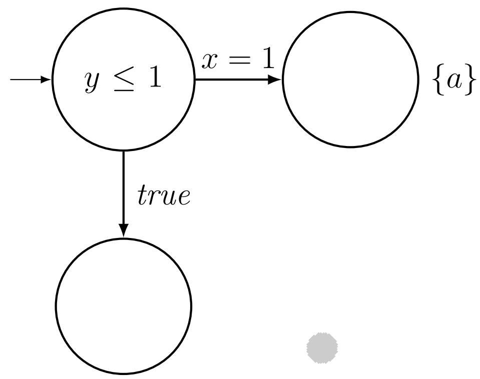
$$\underbrace{A(true\ \mathcal{U}\ \underbrace{\underbrace{(y \le 2)}_{\psi_1} \wedge \underbrace{a}_{\psi_2}}_{\psi_3})}_{\psi_4}$$



As there is no initial state where $y = 0$, $\hat{\varphi}$ does not hold.

d) Prove that for timed automata with l being a location and x, y being clocks, the states (l, ν) and (l, ν') with $\nu(x) = 0.2, \nu(y) = 0.8$ and $\nu'(x) = 0.8, \nu'(y) = 0.2$ are in general *not* *bisimilar* (you can give a counterexample timed automaton along with a TCTL formula, which distinguishes ν from ν').

Solution: We can give a timed automaton $\mathcal{T}$ as a counterexample:



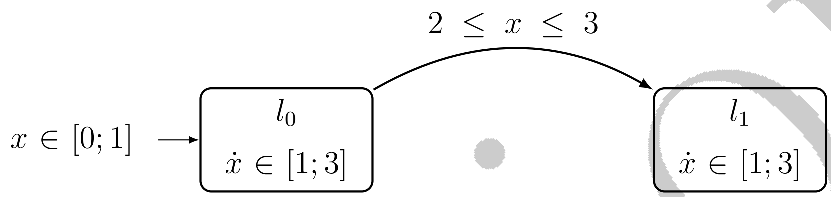
In the given automaton, the states ν, ν' are not bisimilar, as EFa does not hold in the state ν but in ν'.

Task 3. Rectangular automata (1 + 5 + 10 points)

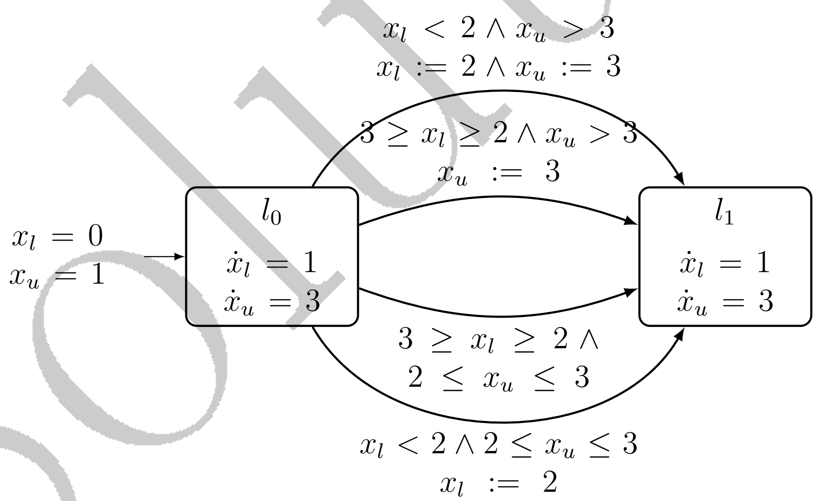
a) What does it mean that a hybrid automaton is *initialized*?

Solution: A hybrid automaton $\mathcal{H}$ is initialized if for each variable x of $\mathcal{H}$ and each transition from a location l to a location l' the following holds: If the slope for x is different in l and l' then x is reset to a constant value or interval on the transition.

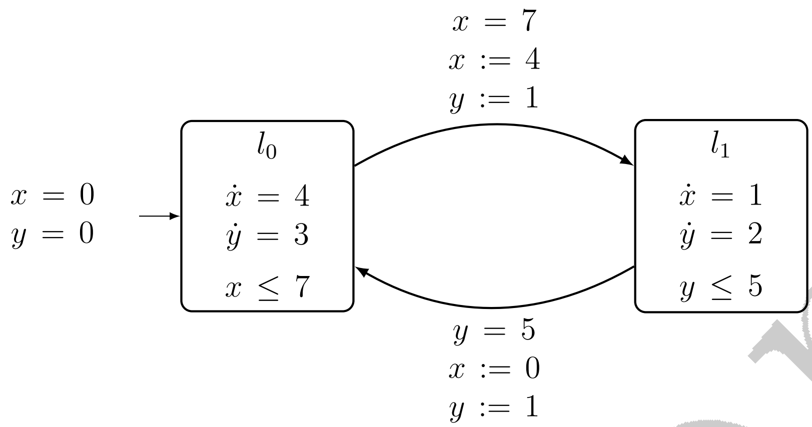
b) Consider the following initialized rectangular automaton $\mathcal{R}$:



Please reduce $\mathcal{R}$ to an *initialized singular* automaton $\mathcal{R}'$.
Solution:

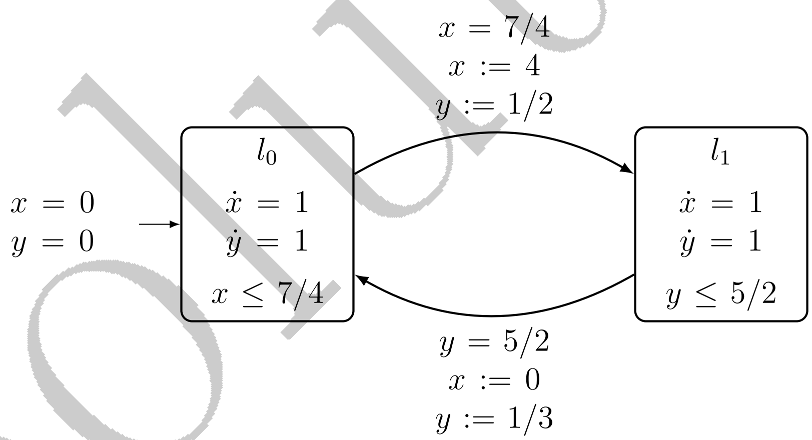


c) Consider the following initialized singular automaton $\mathcal{S}$:



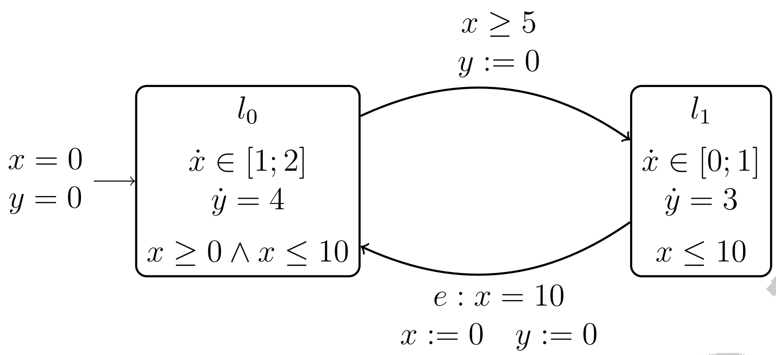
Please transform $\mathcal{S}$ to an *initialized stopwatch* automaton $\mathcal{S}'$, where clocks may be reset to arbitrary constants, not only to 0.

Solution: We transform $\mathcal{S}$ to an initialized stopwatch automaton by adjusting clocks and constraints accordingly:



Task 4. Linear hybrid automata **($6+4+2+3$ points)**

Consider the following linear hybrid automaton:



a) Please compute the set $T^+_{l_0}(x = 0 \land y = 0)$ reachable from $x = 0 \land y = 0$ in location l_0 by letting *time elapse*, using forward analysis as presented in the lecture. Reduce your result whenever possible and eliminate all quantifiers!

Solution:

$$\begin{aligned} T^+_{l_0}(x = 0 \land y = 0) = & \exists x^{pre}.\exists y^{pre}.\exists t.\ t \geq 0 \land x^{pre} = 0 \land y^{pre} = 0 \land \\ & x \geq x^{pre} + t \land x \leq x^{pre} + 2t \land \\ & y = y^{pre} + 4t \land \\ & x \geq 0 \land x \leq 10 \\ = & \exists t.\ t \geq 0 \land t \leq x \leq 2t \land y = 4t \land 0 \leq x \leq 10 \\ = & y \geq 0 \land \frac{y}{4} \leq x \leq \frac{y}{2} \land 0 \leq x \leq 10 \end{aligned}$$

b) Please compute the set $D^+_e(x = y \land x \leq 10)$ reachable from $x = y \land x \leq 10$ in location l_1 by *taking the transition* e from l_1 to l_0, using forward analysis as presented in the lecture. Reduce your result whenever possible and eliminate all quantifiers! *Solution:*

$$\begin{aligned} D^+_e(x = y \land x \leq 10) = & \exists x^{pre}.\exists y^{pre}. \\ & x^{pre} \leq 10 \land x^{pre} = y^{pre} \land x^{pre} = 10 \\ & x = 0 \land y = 0 \land 0 \leq x \leq 10 \\ = & x = 0 \land y = 0 \end{aligned}$$

c) What are the *differences* between LHA I (linear hybrid automata of type I) and general hybrid automata?

Solution: In LHA I automata the flow is limited to an interval or constants, which results in a linear flow. All predicates used as guards, invariants or reset conditions are linear.

d) Please explain the *difference* between forward analysis and backward analysis.

Solution: In forward analysis we start from the initial set and compute the reachable set up to a certain boundary, fixpoint or until the set of bad states is declared reachable. Backward analysis computes the predecessors of the bad states iteratively until a certain boundary, a fixpoint or if the initial states are reachable.

Task 5. Polyhedra **($1 + 7 + 2$ points)**

a) What is the *difference* between polytopes and polyhedra?

Solution: Polyhedra are the more general definition of a set probably specified by intersection of halfspaces. This definition allows unbounded sets, whereas polytopes are a subclass which only contains bounded sets.

b) Please name and shortly explain both ways mentioned in the lecture for *representing convex polytopes*. Fill the table below with the names of the representations and with

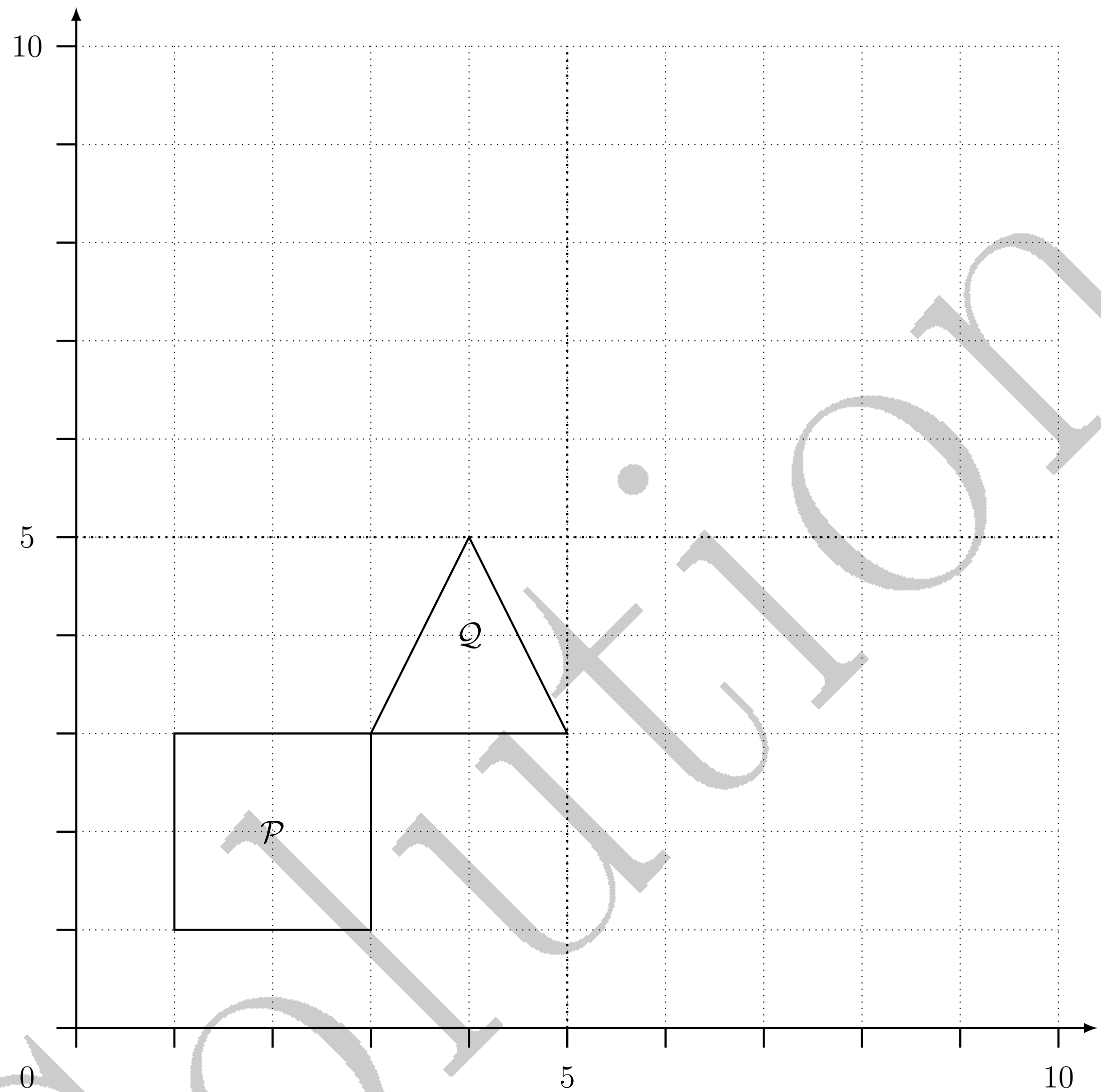
- $+$, where there exists a polynomial approach for the operation
- $-$, if there is no efficient method known.

Solution:

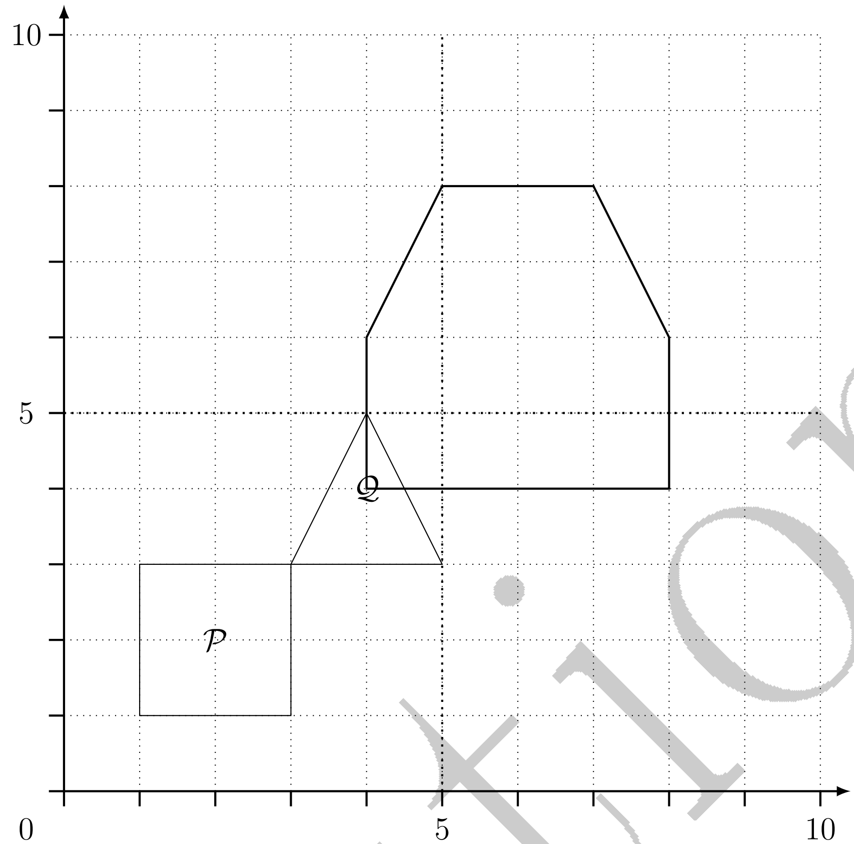
- $\mathcal{V}$-representation: The polytope is represented as the convex hull of a finite set of points.
- $\mathcal{H}$-representation: The polytope is represented as the intersection of a finite set of halfspaces.

Representation	$conv(\cdot \bigcup \cdot)$	$\cdot \bigcap \cdot$	$\in$
$\mathcal{V}$-representation	$+$	-	$+$
$\mathcal{H}$-representation	-	$+$	$+$

c) Given two convex polyhedra $\mathcal{P}, \mathcal{Q}$, please sketch below the result of the *Minkowski sum* of both.



Solution:


10
5
0
5
10
$\mathcal{Q}$
$\mathcal{P}$

Task 6. General hybrid automaton reachability analysis

($2 + 2 + 2 + 1$ points)

a) Please specify, why the *choice of state set representation* is crucial in the reachability analysis for hybrid systems.

Solution: The choice of an appropriate state set representation is always a trade-off between precision and computational effort. A more precise representation reduces the over-approximation error but usually introduces more complex computations. A less precise representation reduces the computational effort but introduces a larger over-approximation error.

b) Why is *bloating* needed during hybrid automaton reachability analysis?

Solution: Bloating is used to over-approximate the initial set to cover the dynamics. Additionally bloating is used to over-approximate the effects of external input.

c) For which computation steps in the reachability analysis for hybrid automata is the operation *intersection* needed and why?

Solution: Intersection is used whenever we want to test, if a guard is satisfied. When the intersection is nonempty, the corresponding transition is enabled and we can take a jump to the respective target location. Another step where intersection is needed is when verifying against the invariant or to check if the bad states are reachable.

d) What do we have to modify in the presented reachability analysis algorithms in order to be able to *prove* reachability of a given set of states in a hybrid automaton?

Solution: By using under-approximation in reachability analysis (instead of over-approximation).