Modeling and Analysis of Hybrid Systems - SS 2016

Second Exam

Wednesday, September 21st, 2016

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.)	7.)	**Total**
Maximum score:	13	21	28	16	17	7	18	120
Reached score:								

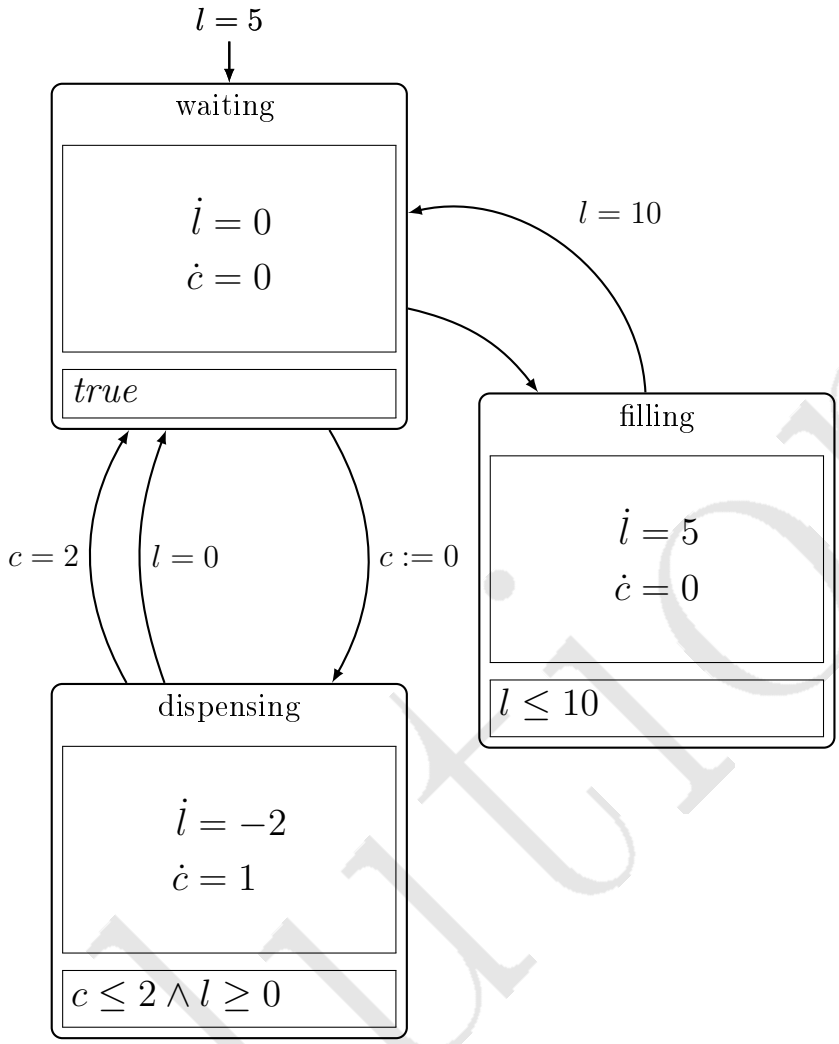
Good luck!

Task 1. Hybrid systems modeling (11 + 2 points)

a) Assume a coffee machine with the following properties:

- The coffee machine has a water tank of height 10 cm. We denote the **water level** in the tank by l $[cm]$.
- The machine is always in exactly one of the following modi: *waiting*, *filling* the tank, or *dispensing* coffee.
- Initially, the machine is waiting with $l = 5$.
- When waiting, the water level does not change.
- When waiting, the machine can change its modus to *filling* and start to increase the water height in the tank by 5 cm/s. Filling is completed if the tank is full. Upon completion, the machine starts waiting again.
- When waiting, the machine can change its modus to *dispensing*. Dispensing decreases the water level in the tank by 2 cm/s. Dispensing is completed if either the tank is empty or if the water level in the tank has been decreased by exactly 4 cm since the start of dispensing. In both cases, the machine returns to the *waiting* modus.

Please complete the hybrid automaton below to derive a formal model for the coffee machine, such that assignments only assign **constant values** to variables. Besides l you may use one more variable in the model.


$l = 5$
waiting
$\dot{l} = 0$
$\dot{c} = 0$
$true$
$l = 10$
filling
$\dot{l} = 5$
$\dot{c} = 0$
$l \leq 10$
$c = 2$
$l = 0$
$c := 0$
dispensing
$\dot{l} = -2$
$\dot{c} = 1$
$c \leq 2 \wedge l \geq 0$

b) Please explain what it means that a hybrid automaton has *Zeno behavior*, and argue whether the completed hybrid automaton model from the previous task has *Zeno behavior*.

A *Zeno path* is a time-convergent infinite path π within which infinitely many *discrete* actions (*jumps*) are executed.

A hybrid automaton has *Zeno behavior* iff it has a Zeno path that starts in an *initial* state.

The modeled automaton has Zeno behavior, as it is possible to switch infinitely often in zero time between waiting and filling, when the water tank is full or between waiting and dispensing, when the water tank is empty.

Task 2. TCTL

(6 + 12 + 3 points)

a) Consider the following two TCTL formulas φ_1 and φ_2. For each formula φ_i, please construct $\hat{\varphi}_i$ by **first** eliminating syntactic sugar (AF, AG, EF, EG) and **second** eliminating timing parameters.

$\varphi_1 = EF^{\leq 3}a$:

Add new clock c_1 which is never reset and use it as follows:

$$\begin{aligned}\varphi_1 &= EF^{\leq 3}a \\ &\equiv E(trueU^{\leq 3}a) \\ \hat{\varphi}_1 &= E(trueU(c_1 \leq 3 \wedge a))\end{aligned}$$

$\varphi_2 = AFEG^{\leq 3}a$:

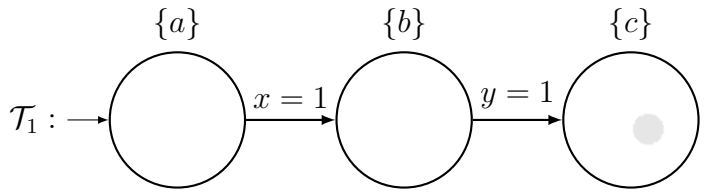
Add new clock c_2 which is never reset and use it as follows

$$\begin{aligned}\varphi_2 &= AFEG^{\leq 3}a \\ &\equiv AF\neg AF^{\leq 3}\neg a \\ &\equiv AF\neg A(trueU^{\leq 3}\neg a) \\ &\equiv A(trueU\neg A(trueU^{\leq 3}\neg a)) \\ \hat{\varphi}_2 &= A(trueU\neg A(trueUc_2 \leq 3 \wedge \neg a))\end{aligned}$$

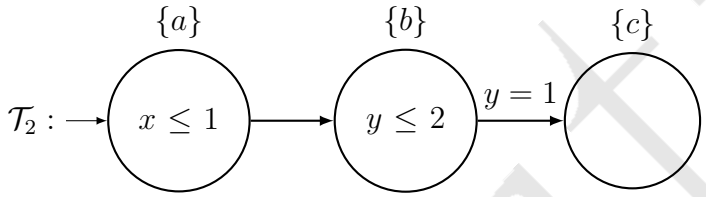
b) Consider the timed automata given below and the following TCTL formulas:

1) $\varphi_1 = EGa \wedge EFEGc$
2) $\varphi_2 = EF^{\leq 1}c$
3) $\varphi_3 = AF^{\leq 1}c$
4) $\varphi_4 = AF^{\leq 1}b$
5) $\varphi_5 = EGa \wedge EFEGb \wedge EFEGc$

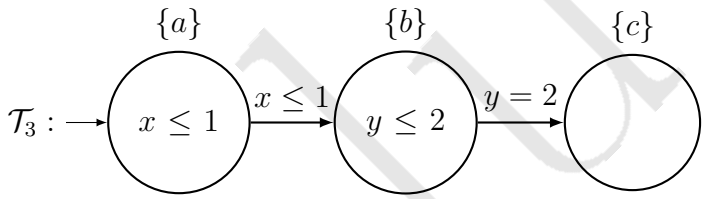
For each automaton, please fill out the table on the right side. Add a symbol +, where the respective formula holds and a symbol - where the formula does not hold.



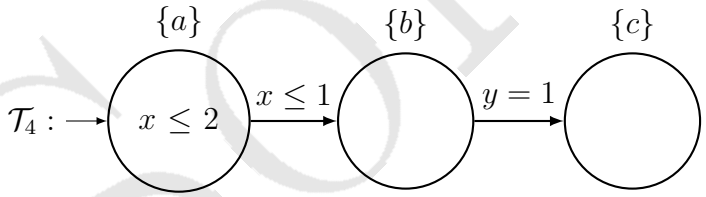
φ_1	φ_2	φ_3	φ_4	φ_5
+	+	-	-	+



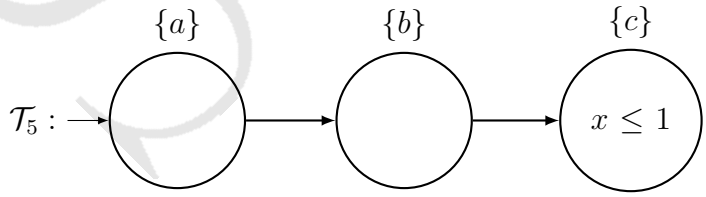
φ_1	φ_2	φ_3	φ_4	φ_5
-	+	+	+	-



φ_1	φ_2	φ_3	φ_4	φ_5
-	-	-	+	-



φ_1	φ_2	φ_3	φ_4	φ_5
-	+	-	+	-



φ_1	φ_2	φ_3	φ_4	φ_5
-	+	-	-	-

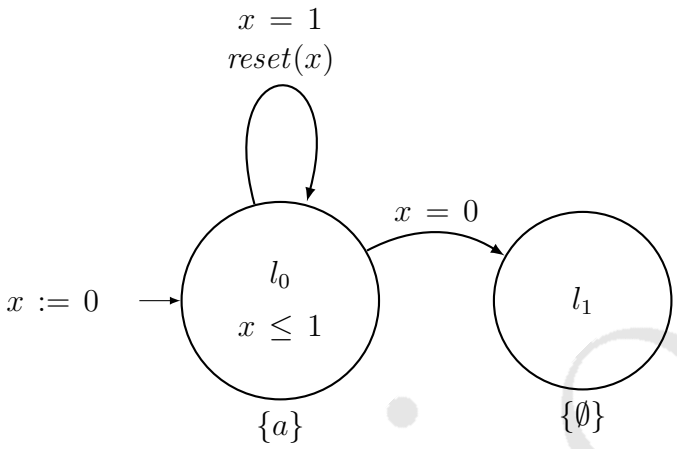
c) Please name one of the previously (c.f. Task 2b) presented timed automata that is *not timelock-free*. Justify your answer!

A timed automaton is timelock-free if none of its reachable states has a timelock, i.e., for each of its reachable states there exists a time-divergent infinite path starting in it.
The second, the fourth and the fifth automata contain a timelock:

- Second automaton: When the control stays one time unit in the left and more than zero time unit in the middle location then from the states reached there is no infinite time-divergent execution possible.
- Fourth automaton: When the control stays longer than one time unit in the left location then it reaches states from which no infinite time-divergent executions are possible.
- Fifth automaton: The control can reach over the location in the middle the location on the right. In the right location the control cannot stay forever but it can neither leave the location. Therefore there are no time-divergent paths starting in the right location.

Task 3. Timed automata model checking (7 + 12 + 9 points)

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

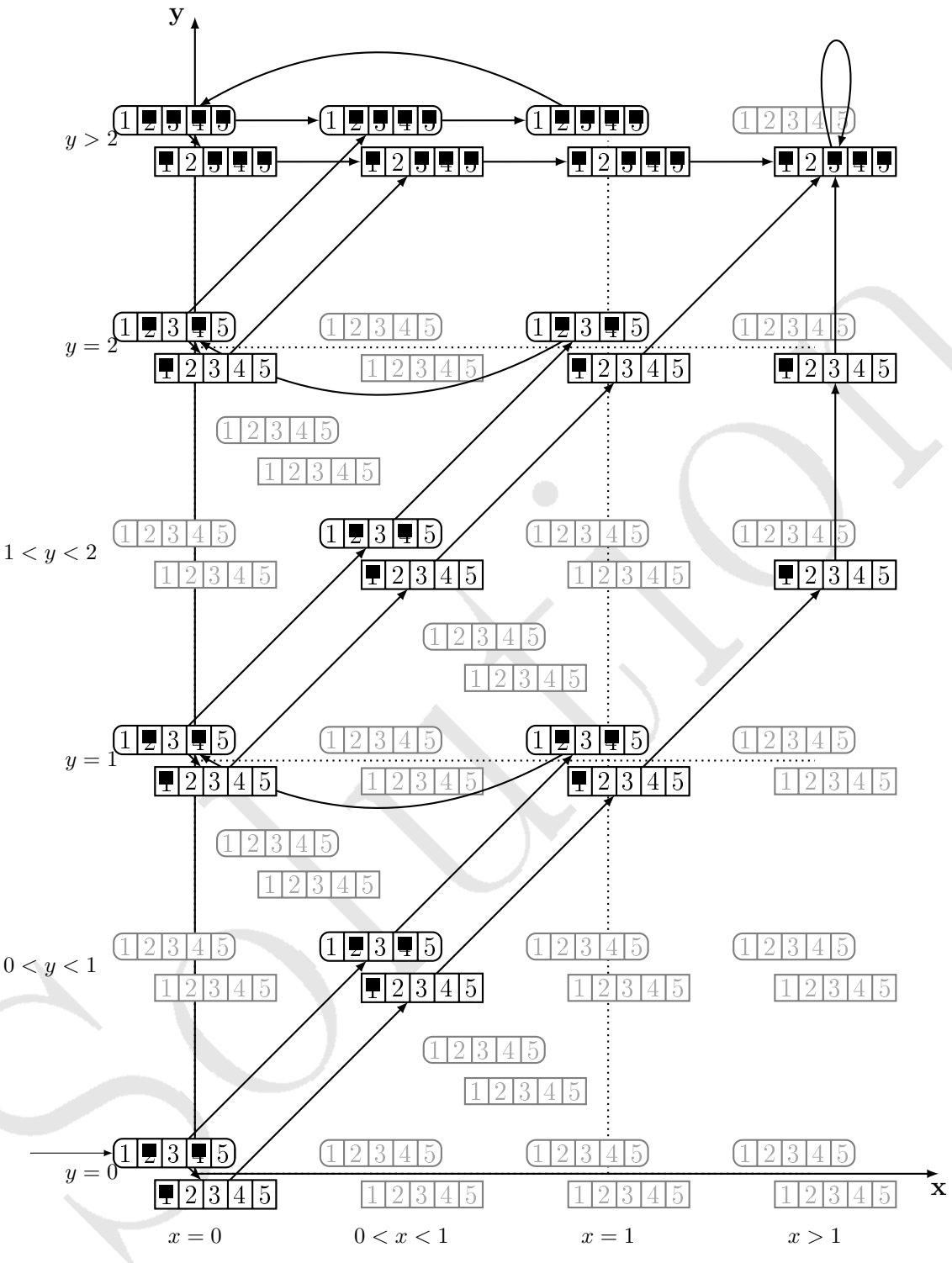


After eliminating syntactic sugar and timing parameters from φ, we obtain:

$$\hat{\varphi} = E(true\ \mathcal{U}(y \leq 2 \wedge \neg a))$$

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:

- (1|2|3|4|5) represents a state, where the location is l_0.
- [1|2|3|4|5] represents a state, where the location is l_1.
- The position of a state in the grid determines, which clock region the state represents. (The numbers are not relevant for this but for the next task.)
- Please draw only the reachable fragment of $\mathcal{R}$.



b) Apply *CTL model checking* to determine whether or not $\mathcal{R} \models_{CTL} \hat{\varphi}$. Please use the following subformula naming:

$$\hat{\varphi} = E(\mathit{true}\ \mathcal{U}\ \underbrace{\underbrace{(y \leq 2)}_{\psi_3} \wedge \neg \underbrace{a}_{\psi_1}}_{\psi_2})$$

ψ_4 spans $\psi_3 \wedge \neg \psi_1$; ψ_5 spans $E(\mathit{true}\ \mathcal{U}\ \psi_4)$.

For all **reachable** nodes of the automaton that you constructed in the previous task, mark each of the five fields $i = 1, \ldots, 5$ clearly by

- either **filling/coloring it completely** to denote that φ_i **does not hold**,
- or **under- or over-line** them with a thick line to denote that φ_i **does hold**.

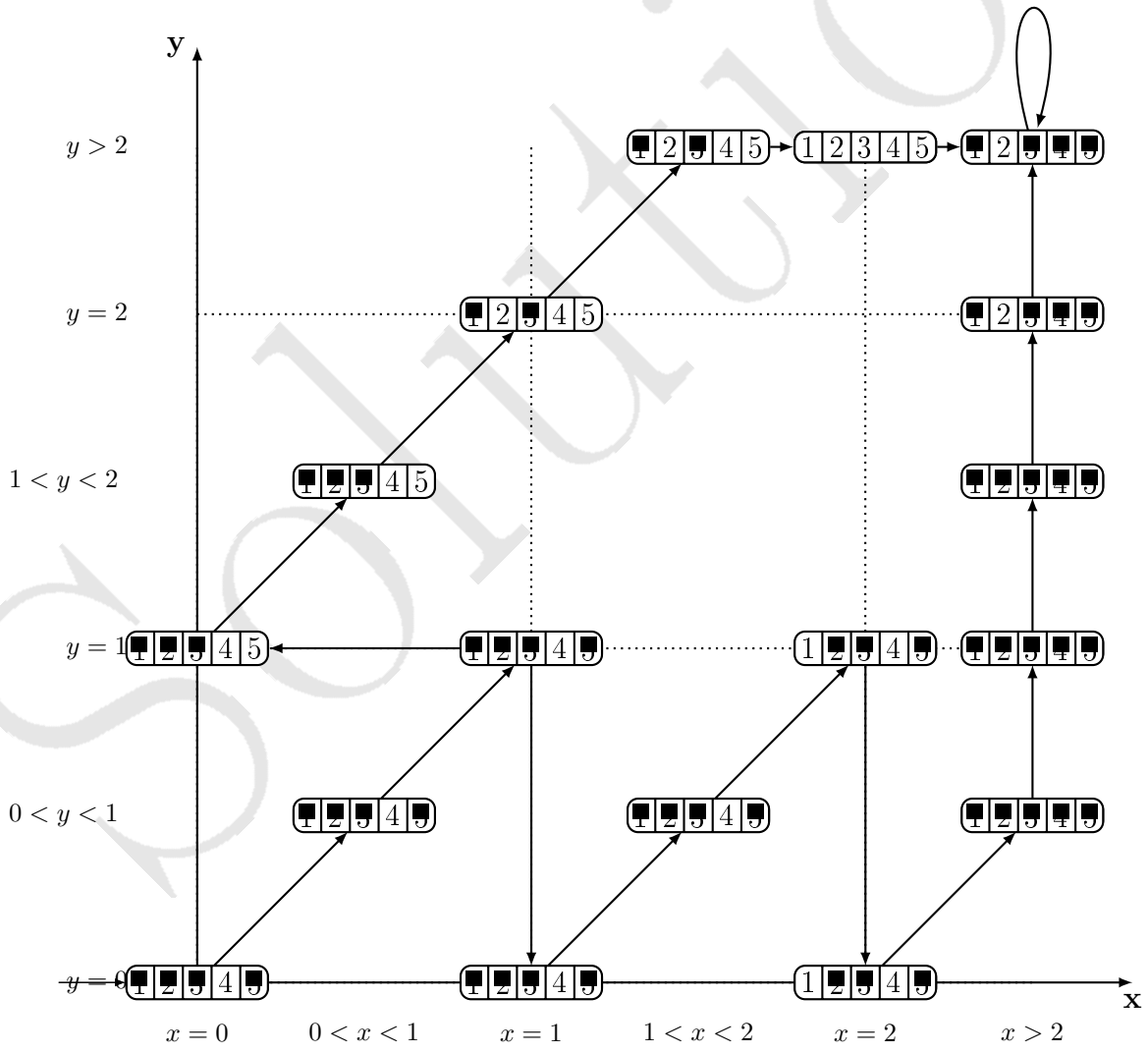
For example,  indicates that for the corresponding location φ_2, φ_4 and φ_5 hold but φ_1 and φ_3 not.

c) Please perform *CTL model checking* on the RTS $\mathcal{R}$ given below and determine whether or not $\mathcal{R} \models_{CTL} \hat{\varphi}$ holds, where

$$\hat{\varphi} = A(\underbrace{x \leq 2}_{\psi_4} \; U \; (\underbrace{\underbrace{y \geq 2}_{\psi_2} \wedge \underbrace{x = 2}_{\psi_1}}_{\psi_3})) \, .}_{\psi_5}$$

As in the previous task, for all **reachable** nodes, mark each of the five fields $i = 1, \ldots, 5$ clearly by

- either **filling/coloring it completely** to denote that φ_i **does not hold**,
- or **under- or over-line** them with a thick line to denote that φ_i **does hold**.

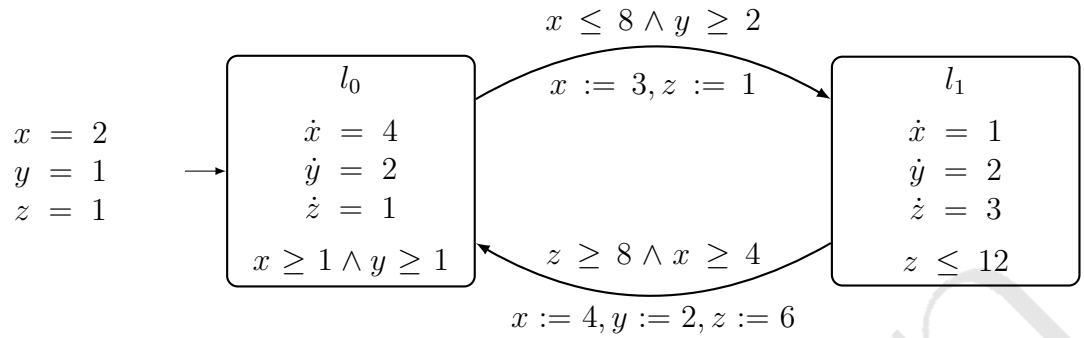


Task 4. Rectangular automata (2 + 7 + 7 points)

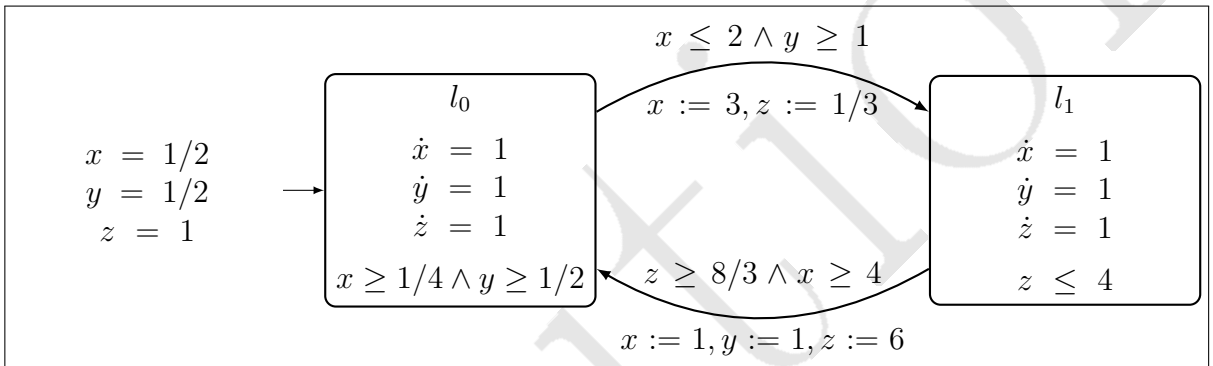
a) In the transformation of initialized rectangular automata to timed automata, name a transformation step that is not applicable if the rectangular automaton is *not initialized*. Please justify your answer!

- In the transformation from singular to stopwatch automata: If a discrete transition causes the change of a variable's slope, the transformation rescales the current variable value. This is possible, if the value is reset on the transition. However, if there is no reset, linear expressions are required for rescaling, which is not in the syntax of stopwatch automata.
- In the transformation from stopwatch to timed automata: If a discrete transition does not initialize a new value for a stopwatch whose slope changes from 1 to 0, the transformation would generate an infinite number of copies to store the current value of the stopped stopwatch.

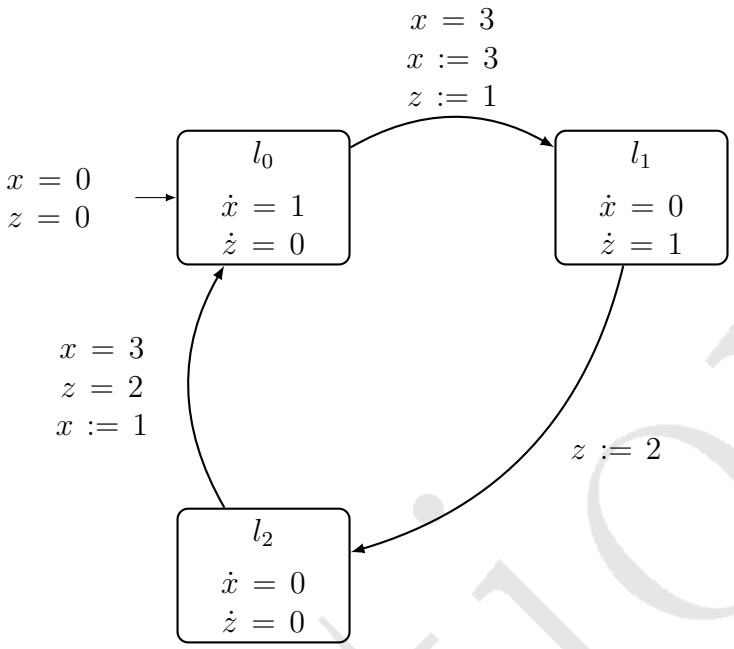
b) Consider the following initialized singular automaton $\mathcal{R}$:



Please reduce $\mathcal{R}$ to an *initialized stopwatch* automaton $\mathcal{R}'$ using the transformation presented in the lecture.

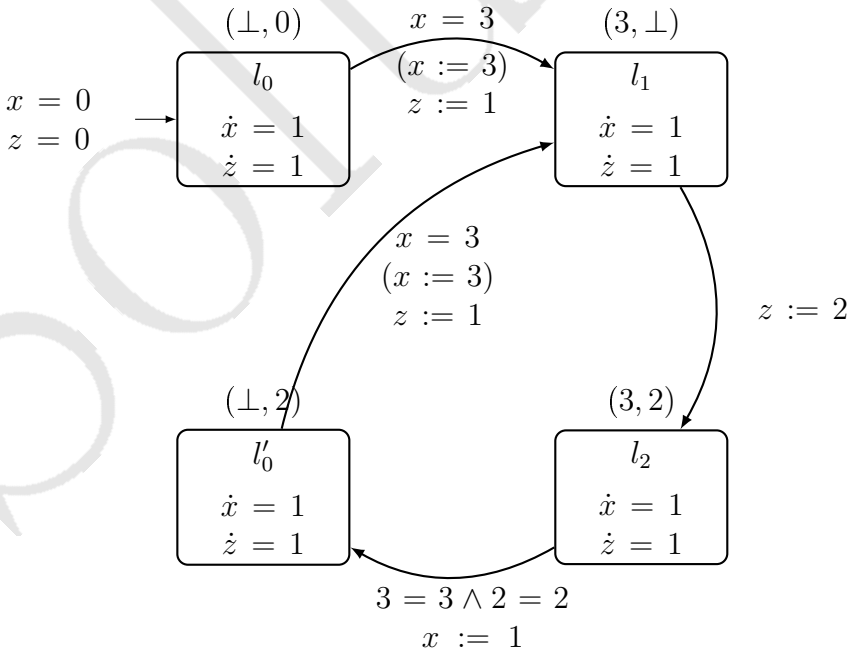


c) Consider the following initialized stopwatch automaton $\mathcal{S}$:



Please transform $\mathcal{S}$ to a *timed automaton* $\mathcal{T}$ which allows clock resets to arbitrary constants $c \geq 0$ as presented in the lecture.

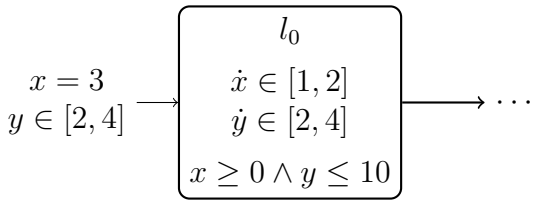
We transform $\mathcal{S}$ to a timed automaton by adjusting clocks and annotating nodes, which requires to create a new node l_0':



Task 5. Linear hybrid automata

(11 + 6 points)

Consider the following excerpt of a linear hybrid automaton:



a) Please compute the set $T^+_{l_0}(x = 3 \wedge 2 \leq y \wedge y \leq 4)$ reachable from $x = 3 \wedge y \in [2, 4]$ 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 in the order x^{pre}, y^{pre}, t. Please use *Gaussian elimination* when possible and *Fourier-Motzkin variable elimination* otherwise, and eliminate all fractions from your final result!

$$
\begin{aligned}
& T^+_{l_0}(x = 3 \wedge 2 \leq y \wedge y \leq 4) \\
&= \exists x^{pre}.\exists y^{pre}.\exists t.\ t \geq 0 \wedge x^{pre} = 3 \wedge 2 \leq y^{pre} \wedge y^{pre} \leq 4 \wedge \\
&\quad x \geq x^{pre} + t \wedge x \leq x^{pre} + 2t \wedge \\
&\quad y \geq y^{pre} + 2t \wedge y \leq y^{pre} + 4t \wedge \\
&\quad x \geq 0 \wedge y \leq 10 \\
&\overset{El.\ x^{pre}}{=} \exists y^{pre}.\exists t.\ t \geq 0 \wedge 2 \leq y^{pre} \wedge y^{pre} \leq 4 \wedge \\
&\quad x \geq 3 + t \wedge x \leq 3 + 2t \wedge \\
&\quad y \geq y^{pre} + 2t \wedge y \leq y^{pre} + 4t \wedge \\
&\quad x \geq 0 \wedge y \leq 10 \\
&\overset{El.\ y^{pre}}{=} \exists t.\ t \geq 0 \wedge \\
&\quad x \geq 3 + t \wedge x \leq 3 + 2t \wedge \\
&\quad x \geq 0 \wedge y \leq 10 \wedge \\
&\quad 2 \leq y - 2t \wedge y - 4t \leq 4 \\
&\overset{El.\ t}{=} x \geq 0 \wedge y \leq 10 \\
&\quad 0 \leq x - 3 \wedge 0 \leq \frac{y}{2} - 1 \wedge \\
&\quad \frac{x}{2} - \frac{3}{2} \leq x - 3 \wedge \frac{x}{2} - \frac{3}{2} \leq \frac{y}{2} - 1 \wedge \\
&\quad \frac{y}{4} - 1 \leq x - 3 \wedge \frac{y}{4} - 1 \leq \frac{y}{2} - 1 \\
&\overset{simpl.}{=} \cancel{x \geq 0} \wedge y \leq 10 \wedge 3 \leq x \wedge 2 \leq y \wedge \cancel{\frac{3}{2} \leq \frac{x}{2}} \wedge x - y \leq 1 \wedge 4x - y \geq 8 \wedge \cancel{0 \leq y} \\
&\overset{red.}{=} 3 \leq x \wedge 2 \leq y \wedge y \leq 10 \wedge x - y \leq 1 \wedge 4x - y \geq 8
\end{aligned}
$$

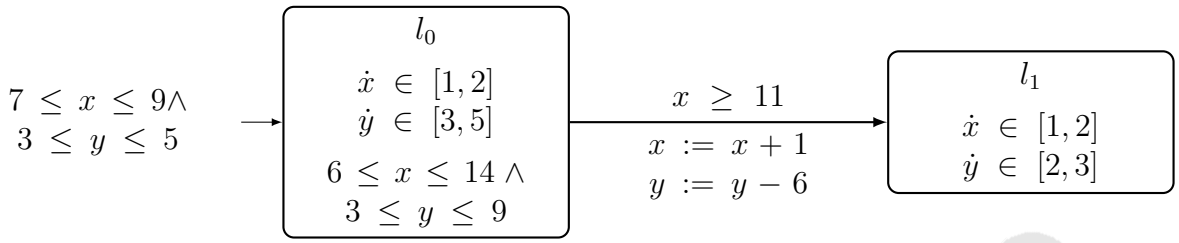
Eliminate y^{pre}:

$\leq$	
2	4
$y - 4t$	$y - 2t$

Eliminate t:

$\leq$	
0	$x - 3$
$\frac{x}{2} - \frac{3}{2}$	$\frac{y}{2} - 1$
$\frac{y}{4} - 1$	

b) Consider the following linear hybrid automaton:



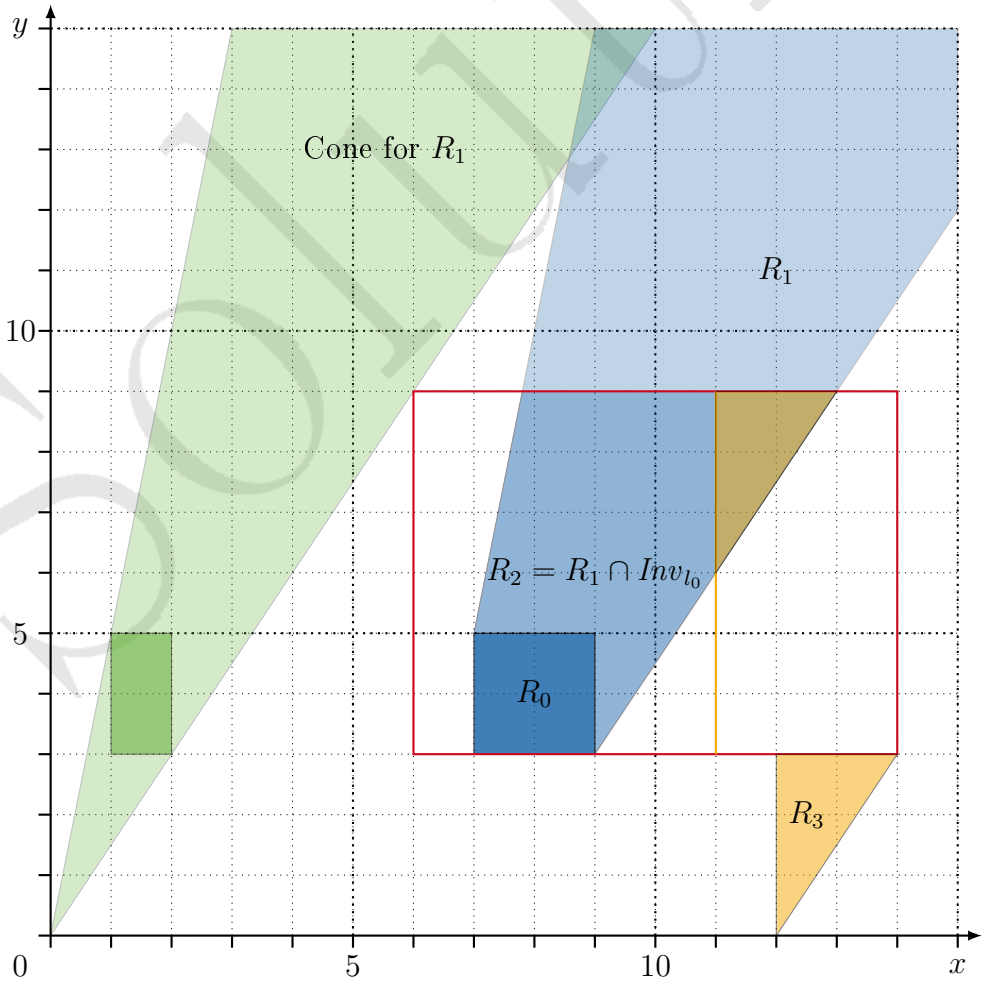
Please use the prepared canvas to sketch the following:

i) Please sketch the initial set R_0 in location l_0.

ii) Extend your sketch by adding the set of reachable states by depicting the states R_1 reachable from R_0 via time elapse in l_0, without considering invariants. Construct the **cone first**, then add it to the initial set.

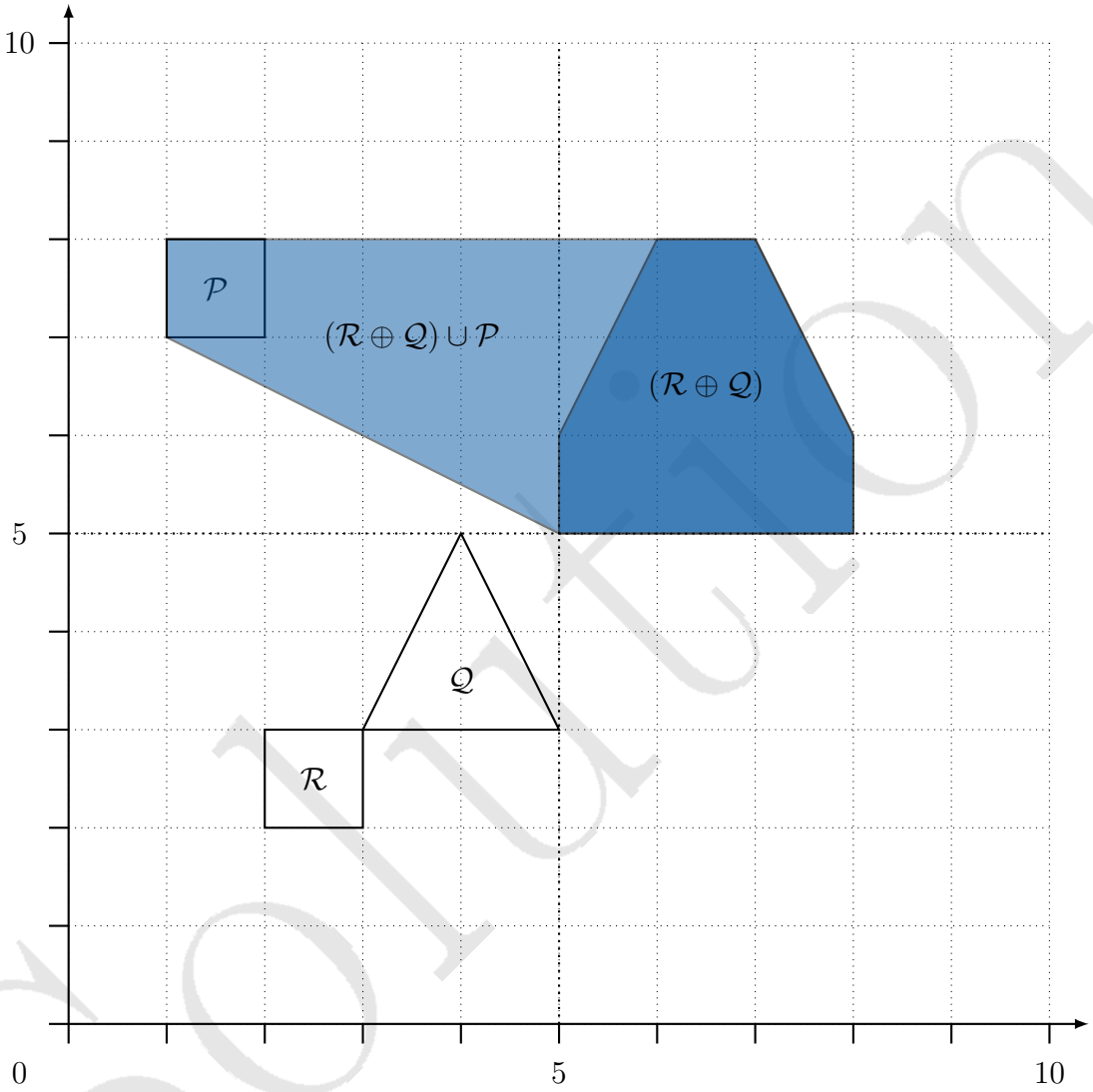
iii) Sketch the time successors R_2 of R_0 in l_0 when considering invariants.

iv) State whether the guard of the outgoing transition is satisfied and, if it is, sketch the state set R_3 reachable from it in l_1 via the jump from (l_0, R_2).



Task 6. Polyhedra and Boxes (4 + 3 points)

a) Given three convex polyhedra $\mathcal{P}, \mathcal{Q}, \mathcal{R}$, please sketch below the result of the nested operation $\mathit{convHull}((\mathcal{R} \oplus \mathcal{Q}) \cup \mathcal{P})$.



b) Assume two boxes $A, B \in \mathbb{R}^d$ represented by the d-dimensional interval vectors

$$I_A = [\underline{a_0}, \overline{a_0}] \times \ldots \times [\underline{a_d}, \overline{a_d}], \quad I_B = [\underline{b_0}, \overline{b_0}] \times \ldots \times [\underline{b_d}, \overline{b_d}].$$

Please give a formal definition for the intersection $C = A \cap B$ of A and B.

$I_C = [\max(\underline{a_0}, \underline{b_0}), \min(\overline{a_0}, \overline{b_0})] \times \ldots \times [\max(\underline{a_d}, \underline{b_d}), \min(\overline{a_d}, \overline{b_d})]$

Note that it can happen that for some dimension i the lower bound is larger than the upper bound, i.e. $\max(\underline{a_i}, \underline{b_i}) > \min(\overline{a_i}, \overline{b_i})$. In this case, the intersection is empty.

Task 7. General hybrid automaton reachability analysis

(14 + 2 + 2 points)

a) Assume a location l of a hybrid automaton with flow $\dot{x} = Ax$, and $\mathcal{I}$ being an initial valuation set in $\mathcal{V}$-representation with

$$A = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \quad \mathcal{I} = \mathit{convHull}\left\{ \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix} \right\}$$

Please compute the matrix exponential exactly for time step length $\delta = 1$. Note that you do not need to extend the matrix to cope with constants. Assume that the box $\mathcal{B}_1 = [-1, 1]^2$ can be used for bloating to account for non-linear behavior. Please compute the over-approximation Ω_0 of the first flowpipe segment using $\mathcal{V}$-polytopes as a state set representation starting from the initial set $\mathcal{I}$. Please sketch your result in the prepared canvas and give a *reduced* list of vertices representing the computed first segment.

Matrix exponential computation:

$\delta A = A$, $(\delta A)^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $(\delta A)^1 = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$, $(\delta A)^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$e^{\delta A} = \sum_{k=0}^{\infty} \frac{(\delta A)^k}{k!} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$

The valuation set reachable from $\mathcal{I}$ in location l at time δ is:

$$e^{\delta A}\mathcal{I} \;=\; convHull\left\{ \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix} \right\} .$$

We use $\mathcal{B}_1 = [-1, 1]^2$ for bloating:

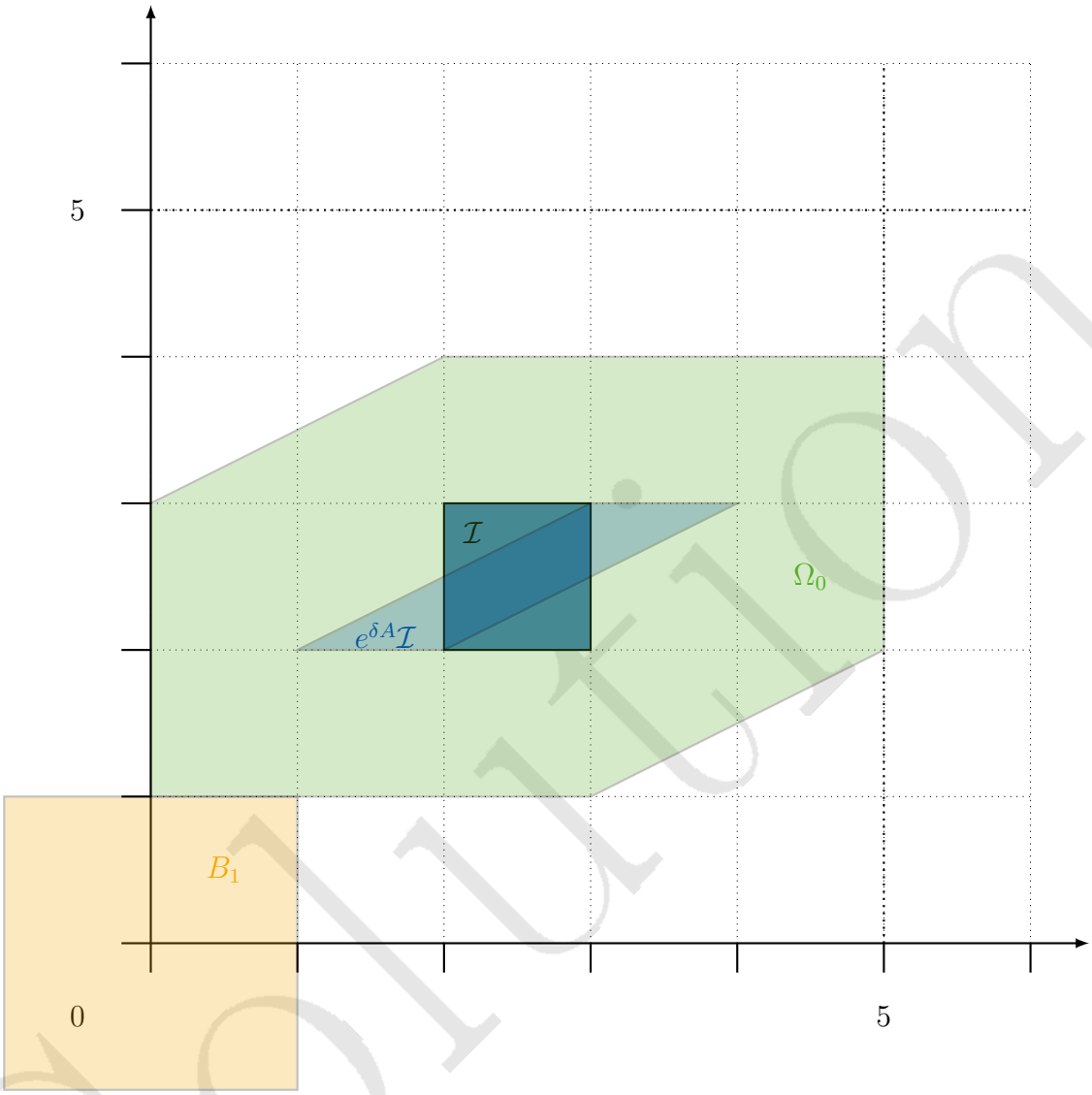
$$\begin{aligned} e^{\delta A}\mathcal{I} \oplus \mathcal{B}_1 \;=\; convHull\Bigg\{ & \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \\ & \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 4 \end{pmatrix} \Bigg\} . \end{aligned}$$

The first segment $\Omega_0 = convHull\left\{\mathcal{I} \cup (e^{\delta A}\mathcal{I} \oplus \mathcal{B}_1)\right\}$ is the convex hull of the initial set $\mathcal{I}$ and the previously computed bloated set:

$$\begin{aligned} \Omega_0 \;=\; & convHull\Bigg\{ \underline{\begin{pmatrix} 2 \\ 2 \end{pmatrix}}, \underline{\begin{pmatrix} 2 \\ 3 \end{pmatrix}}, \underline{\begin{pmatrix} 3 \\ 2 \end{pmatrix}}, \underline{\begin{pmatrix} 3 \\ 3 \end{pmatrix}}, \\ & \underline{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}, \underline{\begin{pmatrix} 1 \\ 3 \end{pmatrix}}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \underline{\begin{pmatrix} 3 \\ 3 \end{pmatrix}}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \underline{\begin{pmatrix} 2 \\ 1 \end{pmatrix}}, \underline{\begin{pmatrix} 2 \\ 3 \end{pmatrix}}, \\ & \underline{\begin{pmatrix} 3 \\ 2 \end{pmatrix}}, \underline{\begin{pmatrix} 3 \\ 4 \end{pmatrix}}, \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \underline{\begin{pmatrix} 2 \\ 2 \end{pmatrix}}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \underline{\begin{pmatrix} 4 \\ 2 \end{pmatrix}}, \underline{\begin{pmatrix} 4 \\ 4 \end{pmatrix}} \Bigg\} \\ = \; & convHull\left\{ \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right\} . \end{aligned}$$

The resulting set and all intermediate sets can be visualized as shown in the canvas below.

Visualization:



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

The choice of an appropriate state set representation is usually 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 usually introduces a larger over-approximation error.

c) What influences has the *time step size* in hybrid automata reachability analysis as presented in the lecture on the resulting flowpipe and its segments?

The time step decides about the number and in general also the size of the flowpipe segments. A larger time step results in lesser but usually larger segments, whereas a smaller time step often increases the precision but also the computational effort, as more flowpipe segments need to be computed.