
Hybrid Systems

Problem Set Solutions

Question 1:

1.1. The hybrid automaton for the bouncing ball is

- $Q = \{Fly\}$ (one discrete state);
- $X = \mathbb{R}^2$, $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, x_1 ball height, x_2 ball vertical velocity;
- $f(Fly, x) = \begin{bmatrix} x_2 \\ -g \end{bmatrix}$;
- $Init = \{(Fly, x) \in Q \times \mathbb{R}^2 \mid x_1 \geq 0\}$;
- $D(Fly) = \{x \in \mathbb{R}^2 \mid x_1 \geq 0\}$;
- $E = \{(Fly, Fly)\}$;
- $G(Fly, Fly) = \{x \in \mathbb{R}^2 \mid (x_1 \leq 0) \wedge (x_2 \leq 0)\}$.
- $R(Fly, Fly, x) = \left\{ \begin{bmatrix} x_1 \\ -cx_2 \end{bmatrix} \right\}$

1.2. According to the definition, for continuous evolution to be possible from a state x_0 , there must exist $\epsilon > 0$ such that for all $t \in [0, \epsilon)$

$$x(t) \in D(Fly)$$

where $x(\cdot) : [0, \epsilon) \rightarrow \mathbb{R}^2$ is the solution of the differential equation

$$\dot{x} = f(Fly, x), \text{ starting at } x(0) = x_0$$

This is clearly impossible if initially $x_1 < 0$: since $x(0) \notin D(Fly)$ there cannot exist $\epsilon > 0$ such that for all $t \in [0, \epsilon)$, $x(t) \in D(Fly)$. If on the other hand $x_1 > 0$, this is possible. Because the solution $x : [0, \epsilon) \rightarrow \mathbb{R}^n$ of the differential equation is a continuous (in fact, differentiable) function of time, if $x_1(0) > 0$ there exists some sufficiently small ϵ such that $x(t) > 0$ for all $t \in [0, \epsilon)$ (strictly speaking you need to invoke the fact that f is Lipschitz continuous to be able to make this assertion).

What if initially $x_1 = 0$? We need to distinguish three cases. If $x_2 > 0$ then continuous evolution is possible: x_1 will soon be greater than zero since its derivative is positive. If $x_2 < 0$ then continuous evolution is impossible: x_1 would have to become negative since its derivative is negative. If $x_2 = 0$ then continuous evolution is also impossible. If continuous evolution were to take place, x_2 would have to become negative (since $\dot{x}_2 = -g < 0$), and therefore x_1 would have to become negative.

This argument can be made more formal because we can explicitly solve the differential equation. The solution for x_1 is

$$x_1(t) = x_1(0) + x_2(0)t - gt^2/2$$

The sign of the first not-zero term in this quadratic dominates the sign of $x_1(t)$ for small enough t . In summary

$$Trans = \{(Fly, x) \in Q \times X \mid [x_1 < 0] \vee [(x_1 = 0) \wedge (x_2 \leq 0)]\}$$

1.3. Before we check whether BB is non-blocking and deterministic let us compute the set of reachable states. Clearly

$$Init = \{(Fly, x) \in Q \times \mathbb{R}^2 \mid x_1 \geq 0\} \subseteq Reach$$

We will show that $Init$ is invariant. Then, according to Proposition 2, Handout 6, $Reach \subseteq Init$, and therefore $Reach = Init$.

To show $Init$ is invariant we can use the induction procedure in Handout 6. Clearly, throughout continuous evolution we must have $x_1 \geq 0$ (since throughout continuous evolution we must have $x(t) \in D(Fly)$). Moreover, if a discrete transition takes place from a state where $x_1 \geq 0$, then after the discrete transition we will still have $x_1 \geq 0$, since R leaves x_1 unchanged. Therefore, by induction, $x_1 \geq 0$ throughout all the executions of BB . Hence $Init$ is invariant and

$$Reach = \{(Fly, x) \in Q \times \mathbb{R}^2 \mid x_1 \geq 0\}$$

To see if BB is non-blocking apply Lemma 1, Handout 6. Consider an arbitrary $(Fly, x) \in Reach \cap Trans$. This implies that $x_1 = 0$ and $x_2 \leq 0$. Therefore, $x \in G(Fly, Fly)$ (i.e. a discrete transition is possible from (Fly, x)). By Lemma 1, BB is deterministic.

1.4. To see if BB is deterministic apply Lemma 2, Handout 6. The first condition of the Lemma is satisfied: if $x \in G(Fly, Fly)$, then $x_1 \leq 0$ and $x_2 \leq 0$, therefore, $(Fly, x) \in Trans$. The second condition is trivial since there is only one discrete state and the third condition is obvious by the definition of R . Therefore, BB is deterministic.

1.5. To show that BB is Zeno, let us assume that initially $x_1 = 0$ and $x_2 = v > 0$. The time to the first bounce is

$$\tau'_0 = 2v/g$$

The speed at impact will be v (there is no energy lost during the flight). After the first bounce the speed will be cv . Therefore, the time between the first and second bounce will be

$$\tau'_1 - \tau_1 = 2cv/g$$

In general, the time between the i^{th} and the $i + 1^{st}$ bounce will be

$$\tau'_i - \tau_i = 2c^i v/g$$

Therefore, if $0 \leq c < 1$

$$\sum_{i=0}^{\infty} (\tau'_i - \tau_i) = \sum_{i=0}^{\infty} 2c^i v/g = 2v/g \sum_{i=0}^{\infty} c^i = \frac{2v}{(1-c)g}$$

and the execution takes an infinite number of discrete transitions in a finite amount of time. (Notice that the system is not Zeno if $c \geq 1$.)

Question 2:

2.1. The hybrid automaton for the thermostat is

- $Q = \{OFF, ON\}$;
- $X = \mathbb{R}$, where x is the room temperature;
- $f(OFF, x) = -ax$, $f(ON, x) = -a(x - 30)$;
- $Init = \{(q, x) \in Q \times \mathbb{R} \mid x = 20\}$;
- $D(OFF) = \{x \in \mathbb{R} \mid x \geq 18\}$, $D(ON) = \{x \in \mathbb{R} \mid x \leq 22\}$;
- $E = \{(OFF, ON), (ON, OFF)\}$;

- $G(OFF, ON) = \{x \in \mathbb{R} \mid x \leq 19\}$, $G(ON, OFF) = \{x \in \mathbb{R} \mid x \geq 21\}$.
- $R(OFF, ON, x) = R(ON, OFF, x) = \{x\}$.

2.2. Continuous evolution is impossible outside the domains, hence

$$Trans \supseteq \{(OFF, x) \mid x < 18\} \cup \{(ON, x) \mid x > 22\}$$

Continuous evolution is possible in the interior of the domain, hence

$$Trans \subseteq \{(OFF, x) \mid x \leq 18\} \cup \{(ON, x) \mid x \geq 22\}$$

It remains to determine what happens on the boundary of the domain, i.e. on the set

$$\{(OFF, x) \mid x = 18\} \cup \{(ON, x) \mid x = 22\}$$

Notice that if $q = OFF$ and $x = 18$, then $\dot{x} = -ax < 0$. If continuous evolution were to take place from this state we would immediately have $x(t) < 18$, which is not allowed. Therefore $(OFF, 18) \in Trans$. Likewise, if $q = ON$ and $x = 22$, then $\dot{x} = -a(x - 30) > 0$, therefore $(ON, 22) \in Trans$. In summary

$$Trans = \{(OFF, x) \mid x \leq 18\} \cup \{(ON, x) \mid x \geq 22\}$$

2.3. To determine whether Th is nonblocking we use Lemma 1, Handout 6. If $(q, x) \in Trans$, then either $q = OFF$ and $x \leq 18$ or $q = ON$ and $x \geq 22$. In the former case, $x \in G(OFF, ON)$. In the latter, $x \in G(ON, OFF)$. Therefore, Th is nonblocking. Notice that in this case we do not need to compute the set $Reach$. The condition holds for all $(q, x) \in Q \times X$, therefore it must also hold for all $(q, x) \in Reach \subseteq Q \times X$.

2.4. Th is not deterministic. Conditions 2 and 3 of Lemma 2, Handout 6 are satisfied, but the automaton fails condition 1. For example, the state $(OFF, 19)$ is in $G(OFF, ON)$ but not in $Trans$. At that state there is a choice between continuous evolution and discrete transition. (Strictly speaking you also need to show that $(OFF, 19)$ is reachable. This is true, for example the execution starting at $(OFF, 20)$ reaches $(OFF, 19)$ after $-\ln(19/20)/a$ time instants of continuous evolution.)

2.5. We will show that the set $M = \{(q, x) \mid x \in [18, 22]\}$ is invariant.

Let us check that the state cannot leave M along continuous evolution. Take an arbitrary $(\hat{q}, \hat{x}) \in M$ and assume that $\hat{q} = OFF$ (the argument is similar if $\hat{q} = ON$). Then along continuous evolution $\dot{x} = -ax$ and $x(t) \in D(ON)$. These two facts combined imply that $x \geq 18$ and $x(t)$ decreases as a function of t , in particular $x(t) \leq x(0) = \hat{x} \leq 22$. Therefore, $x(t) \in [18, 22]$ throughout continuous evolution. Next, we check that the state cannot leave M through a discrete transition. Notice that discrete transitions leave x unchanged. Therefore, after a discrete transition from a state in M the state will still be in M . Therefore, M is invariant.

Clearly the room temperature starts in the range $[18, 22]$, since initially $x = 20$. Since $Init \subseteq M$ and M is invariant by Proposition 2 Handout 6 we can immediately infer that all reachable states are in M , i.e.

$$Reach \subseteq M$$

In fact it turns out that $Reach = M$, any state in M is reachable by a suitable execution.

2.6. The set $M' = \{(q, x) \mid x \in [19, 21]\}$ is not invariant. The state can leave this set along continuous evolution. For example, consider the execution starting at $(OFF, 19)$ and moving according to the differential equation $\dot{x} = -ax$. The solution to the differential equation is

$$x(t) = 19e^{-at}$$

The system can follow this solution for $-\ln(18/19)/a$ time units to the state $(OFF, 18)$ which is outside M' .

2.7. Th is not Zeno. Any infinite sequence of transitions will be a repetition of

$$ON \rightarrow OFF \rightarrow ON \rightarrow OFF$$

etc. When an $ON \rightarrow OFF$ transition takes place we know that $x \geq 21$. For the subsequent $OFF \rightarrow ON$ to take place we need $x \leq 19$. In between these two transitions, $q = OFF$, therefore $\dot{x} = -ax$. Since initially $x \geq 21$

$$x(t) \geq 21e^{-at}$$

For $OFF \rightarrow ON$ we need $x(t) \leq 19$, which implies that

$$t \geq -\frac{\ln 19/21}{a} > 0$$

Since the time between the transitions is bigger than a positive constant (*bounded away from zero*) there cannot be an infinite number of discrete transitions in a finite amount of time.

Question 3: Assume David's model is $H = (Q, X, f, Init, D, E, G, R)$. Define a hybrid automaton, \widehat{H} , by

- same discrete states, $\widehat{Q} = Q$,
- same continuous states, $\widehat{X} = X$,
- same initial conditions, $\widehat{Init} = Init$,
- same continuous dynamics, $\widehat{f}(q, x) = f(q, x)$ for all $q \in Q, x \in X$,
- same domain, $\widehat{D}(q) = D(q)$ for all $q \in Q$,
- throw away discrete transitions whose guards are empty or whose reset is empty for all x in the guard

$$\widehat{E} = \{e \in E \mid \exists x \in G(e) \text{ with } R(e, x) \neq \emptyset\}$$

- Throw away from each guard points whose reset is empty

$$\widehat{G}(e) = \{x \in G(e) \mid R(e, x) \neq \emptyset\}$$

- trim down $R(e, x)$ to be non-empty only when $x \in G(e)$ (optional)

$$\widehat{R}(e, x) = \{x' \in X \mid x \in G(e) \wedge x' \in R(e, x)\}.$$

The components \widehat{E} , \widehat{G} , and \widehat{R} satisfy our requirements: for all $e \in E$, $G(e) \neq \emptyset$ and for all $e \in E$ and all $x \in G(e)$, $R(e, x) \neq \emptyset$.

It remains to show that \widehat{H} accepts the same executions as H . This is somewhat tedious, but conceptually straightforward.

First of all, notice that since $\widehat{E} \subseteq E$, $\widehat{G}(e) \subseteq G(e)$ and $\widehat{R}(e, x) \subseteq R(e, x)$, all executions of \widehat{H} must also be executions of H (\widehat{H} imposes more constraints than H).

To show the converse (that all executions of H are also executions of \widehat{H}) consider an arbitrary execution (τ, q, x) of H and show inductively that it is also an execution of \widehat{H} . Since $\widehat{Init} = Init$, $(q_0(\tau_0), x_0(\tau_0)) \in \widehat{Init}$. Assume that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^{N-1}[\tau_N, \tau_N]$ (i.e. everything up to end including the first point of the N^{th} interval of τ) is an execution of \widehat{H} . First show that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N$ (i.e. everything up to end including the last point of the N^{th} interval of τ) is an execution of \widehat{H} . This involves an argument about continuous evolution. Because (τ, q, x) is an execution of H , $x_N(\cdot)$ is the solution of the differential equation

$$\dot{x} = f(q_N(\tau_N), x) \text{ starting at } x(0) = x_N(\tau_N)$$

and $x_N(t) \in D(q_N(t))$ for all $t \in [\tau_N, \tau'_N]$. Because $\widehat{f} = f$, this is also a solution of

$$\dot{x} = \widehat{f}(q_N(\tau_N), x) \text{ starting at } x(0) = x_N(\tau_N)$$

Moreover, because $D(q_N(t)) = \widehat{D}(q_N(t))$, $x_N(t) \in \widehat{D}(q_N(t))$ for all $t \in [\tau_N, \tau'_N]$. Therefore, the prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N$ is also an execution of \widehat{H} .

If this is the last interval in τ we are done! Otherwise, show that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N[\tau_{N+1}, \tau_{N+1}]$ (i.e. everything up to end including the first point of the $N + 1^{\text{st}}$ interval of τ) is an execution of \widehat{H} . This involves an argument about discrete evolution. Since (τ, q, x) is an execution of H ,

$$\begin{aligned} (q_N(\tau'_N), q_{N+1}(\tau_{N+1})) &\in E, \\ x_N(\tau'_N) &\in G(q_N(\tau'_N), q_{N+1}(\tau_{N+1})) \\ x_{N+1}(\tau_{N+1}) &\in R(q_N(\tau'_N), q_{N+1}(\tau_{N+1}), x_N(\tau'_N)) \end{aligned}$$

This implies that $G(q_N(\tau'_N), q_{N+1}(\tau_{N+1})) \neq \emptyset$ (it contains at least the element $x_N(\tau'_N)$) and $R((q_N(\tau'_N), q_{N+1}(\tau_{N+1}), x) \neq \emptyset$ for some $x \in X$ (namely for $x = x_N(\tau'_N)$). Therefore, $(q_N(\tau'_N), q_{N+1}(\tau_{N+1})) \in \widehat{E}$. In addition, $x_N(\tau'_N) \in \widehat{G}(q_N(\tau'_N), q_{N+1}(\tau_{N+1}))$ and $x_{N+1}(\tau_{N+1}) \in \widehat{R}(q_N(\tau'_N), q_{N+1}(\tau_{N+1}), x_N(\tau'_N))$. Therefore, the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N[\tau_{N+1}, \tau_{N+1}]$ is also an execution of \widehat{H} .

By induction, (τ, q, x) is an execution of \widehat{H} . Therefore all executions of H are executions of \widehat{H} and vice versa.

Question 4: We repeat in detail the argument sketched out in class. Consider an execution (τ, q, x) of the water tank hybrid automaton. We use induction to show that the set $M = \{(q, x) \in Q \times X \mid (x_1 \geq r_1) \wedge (x_2 \geq r_2)\}$ is invariant.

Notice that $(q_0(\tau_0), x_0(\tau_0)) \in \text{Init} = M$. Assume that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^{N-1}[\tau_N, \tau_N]$ (i.e. everything up to end including the first point of the N^{th} interval of τ) remains in M , i.e.

$$\forall i = 0, \dots, N-1, \forall t \in [\tau_i, \tau'_i], (q_i(t), x_i(t)) \in M, \text{ and } (q_N(\tau_N), x_N(\tau_N)) \in M$$

First show that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N$ (i.e. everything up to end including the last point of the N^{th} interval of τ) stays in M . This involves an argument about continuous evolution. Because (τ, q, x) is an execution, $x_N(\cdot)$ is the solution of the differential equation

$$\dot{x} = f(q_N(\tau_N), x) \text{ starting at } x(0) = x_N(\tau_N)$$

and $x_N(t) \in D(q_N(t))$ for all $t \in [\tau_N, \tau'_N]$. We distinguish two cases:

1. If $q_N(\tau_N) = q_1$, then $\dot{x}_1 > 0$ (since $w > \max\{v_1, v_2\} \geq v_1$). Because initially $x_1 \geq r_1$ and x_1 increases, we will have $x_1 \geq r_1$ throughout $[\tau_N, \tau'_N]$. Moreover, because $x_N(t) \in D(q_N(t)) = \{x \in \mathbb{R}^2 \mid x_2 \geq r_2\}$ we will have $x_2 \geq r_2$ throughout $[\tau_N, \tau'_N]$.
2. If $q_N(\tau_N) = q_2$, then $\dot{x}_2 > 0$ (since $w > \max\{v_1, v_2\} \geq v_2$). Because initially $x_2 \geq r_2$ and x_2 increases, we will have $x_2 \geq r_2$ throughout $[\tau_N, \tau'_N]$. Moreover, because $x_N(t) \in D(q_N(t)) = \{x \in \mathbb{R}^2 \mid x_1 \geq r_1\}$ we will have $x_1 \geq r_1$ throughout $[\tau_N, \tau'_N]$.

Overall, the prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N$ remains in M .

If τ contains only N intervals we are done. Otherwise, show that the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N[\tau_{N+1}, \tau_{N+1}]$ (i.e. everything up to end including the first point of the $N + 1^{\text{st}}$ interval of τ) stays in M . This involves an argument about discrete evolution. This is quite easy in this case, because M does not depend on q and R leaves x unaffected. If $(q_N(\tau'_N), x_N(\tau'_N)) \in M$, then $x_{N+1}(\tau_{N+1}) = x_N(\tau'_N)$ and $(q_{N+1}(\tau_{N+1}), x_{N+1}(\tau_{N+1})) \in M$. Therefore, the finite prefix of (τ, q, x) defined over $\{[\tau_i, \tau'_i]\}_{i=0}^N[\tau_{N+1}, \tau_{N+1}]$ is also an execution of \widehat{H} .

By induction, (τ, q, x) remains in M throughout.

Like all proofs about hybrid systems, the above analysis involves an argument that holds along all executions of the system. The problem is that there are no executions defined after the point where the tanks drain, because the system becomes Zeno at that time. This highlights a possible problem of systems with Zeno executions: the analysis will fail to predict any properties of the system after the Zeno time (accumulation point of discrete transitions). The problem is not with the methods used for analysis, it is with the abstraction we used to model the physical system: some important aspects of the physical process were lost when the system was modelled as a hybrid automaton.

Question 5:

5.1. We need to define $\delta(q, u, d)$ for all $q \in \{q_1, \dots, q_{10}\}$, $u \in \{1, 2\}$ and $d \in \{1, 2\}$. This makes 40 points at which we need to specify δ !

$$\begin{aligned}
\delta(q_1, 1, 1) &= \delta(q_1, 1, 2) = q_4, \delta(q_1, 2, 1) = q_1, \delta(q_1, 2, 2) = q_2 \\
\delta(q_2, 1, 1) &= \delta(q_2, 1, 2) = \delta(q_2, 2, 1) = \delta(q_2, 2, 2) = q_1 \\
\delta(q_3, 1, 1) &= q_2, \delta(q_3, 1, 2) = q_6, \delta(q_3, 2, 1) = \delta(q_3, 2, 2) = q_7 \\
\delta(q_4, 1, 1) &= q_5, \delta(q_4, 1, 2) = \delta(q_4, 2, 2) = q_3, \delta(q_4, 2, 1) = q_9 \\
\delta(q_5, 1, 1) &= \delta(q_5, 1, 2) = q_9, \delta(q_5, 2, 1) = \delta(q_5, 2, 2) = q_{10} \\
\delta(q_6, 1, 1) &= q_7, \delta(q_6, 1, 2) = q_8, \delta(q_6, 2, 1) = q_5, \delta(q_6, 2, 2) = q_3 \\
\delta(q_7, 1, 1) &= \delta(q_7, 1, 2) = q_7, \delta(q_7, 2, 1) = q_6, \delta(q_7, 2, 2) = q_3 \\
\delta(q_8, 1, 1) &= \delta(q_8, 1, 2) = \delta(q_8, 2, 1) = \delta(q_8, 2, 2) = q_{10} \\
\delta(q_9, 1, 1) &= \delta(q_9, 1, 2) = \delta(q_9, 2, 1) = \delta(q_9, 2, 2) = q_{10} \\
\delta(q_{10}, 1, 1) &= \delta(q_{10}, 1, 2) = q_7, \delta(q_{10}, 2, 1) = \delta(q_{10}, 2, 2) = q_9
\end{aligned}$$

5.2. The procedure is very similar to the backward reachability algorithm.

Algorithm 1 (Controlled Invariance)

initialisation: $W_0 = F$, $i = 0$
repeat
 $W_{i+1} = \text{Pre}_{(u,d)}(W_i) \cap W_i$
 $i = i + 1$
until $W_i = W_{i-1}$
return W_i

Let us apply this algorithm to the system in Figure 4. We start with $W_0 = \{q_1, \dots, q_8\} = F$. At the first step, the set q_5 needs to be dropped: if $u = 1$, then $\delta(q_5, 1, *) = q_9 \notin W_0$ and if $u = 2$, then $\delta(q_5, 2, *) = q_{10} \notin W_0$. Therefore, $q_5 \notin \text{Pre}_{(u,d)}(W_0)$ since for all u there exists a d such that the next state is outside W_0 . q_8 also needs to be dropped: whatever Ursula or David do, the next state will be q_{10} , i.e. outside W_0 . For the rest of the states Ursula has an action to keep the state in W_0 : from q_4 she can choose $u = 1$ and go to either q_3 or q_5 , both of which are in W_0 , etc. Therefore

$$\begin{aligned}
W_1 &= \{q_1, q_2, q_3, q_4, q_6, q_7\} \\
W_2 &= \{q_1, q_2, q_3, q_7\} \\
W_3 &= W_2
\end{aligned}$$

Therefore, the set of states from which Ursula can win the game (if she plays her cards right) is $\{q_1, q_2, q_3, q_7\}$.

Notice that at each step of the algorithm we need to intersect $\text{Pre}_{(u,d)}(W_i)$ with W_i . This is to ensure that winning states for David are not be relabelled as winning states for Ursula at later steps of the algorithm. For example, without the intersection operation q_{10} would be added to W_1 .

5.3. In state q_1 Ursula should choose $u = 2$. This ensures that the next state is either q_1 or q_2 both of which are winning states for her. If she chooses $u = 1$ she will find herself in q_4 next time, from where David can win. Repeating this process for the remaining winning states for Ursula we get the feedback controller

$$g_u(q) = \begin{cases} \{2\} & q = q_1 \\ \{1, 2\} & q = q_2 \\ \{2\} & q = q_3 \\ \{1\} & q = q_7 \end{cases}$$

Notice that if in q_3 Ursula plays $u = 1$ she may get lucky and end up in q_2 , if David chooses the wrong move ($d = 1$). However, because she cannot count on David being cooperative, she has to play safe and go to q_7 .

David wants to ensure that the state progresses towards $\{q_9, q_{10}\}$. In q_5 and q_8 he can do whatever he wants, the state will be either q_9 or q_{10} next time around. In q_4 he wants to choose $d = 1$ (otherwise the state will go to q_3 from where Ursula wins).

Notice that at q_6 neither player can win for sure using a feedback strategy. If David chooses $d = 1$ Ursula can choose $u = 1$ and bring the state to q_7 from where she wins. If David chooses $d = 2$, Ursula can choose $u = 2$ and bring the state to q_3 , from where she wins. A similar argument holds the other way around. If either player knows what the other is planning to do they can win from q_6 . If neither knows what the other is planning to do (which is what a feedback map implicitly assumes) then they cannot win for sure.

Question 5: The figure contains two copies of \mathbb{R}^2 : one corresponding to $q = q_1$ and one corresponding to $q = q_2$. Each copy is split into the triangles, lines, etc. forming the region graph. Both copies together form the state space of the system, $\{q_1, q_2\} \times \mathbb{R}^2$.

Let us compute the Pre 's of the sets P_1, \dots, P_4 . No states can find themselves in P_1 or P_2 after a transition $e_1 = (q_1, q_2)$, because in P_1 and P_2 the discrete state is q_1 . Likewise, no states can find themselves in P_3 and P_4 after e_2 . Therefore,

$$Pre_{e_1}(P_1) = Pre_{e_1}(P_2) = Pre_{e_2}(P_3) = Pre_{e_2}(P_4) = \emptyset$$

e_2 leaves x unchanged. Therefore, one would expect all states in the set labelled Q_1 to find themselves in P_1 after the transition e_2 . However, for e_2 to take place we need $x_1 \leq 1$. None of the states in Q_1 satisfy that conditions. Therefore

$$Pre_{e_2}(P_1) = Q_1 \cap (\{q_2\} \times \{x_1 \leq 1\}) = \emptyset$$

Likewise, all states in the set labelled Q_2 in Figure 6 can find themselves in P_2 after the transition e_2 . Moreover, all of these states satisfy $x_1 \leq 1$, therefore e_2 is possible from them.

$$Pre_{e_2}(P_2) = Q_2 \cap (\{q_2\} \times \{x_1 \leq 1\}) = Q_2$$

Notice that e_1 resets x_1 to 0. Therefore, after transition e_1 one would expect to see $x_1 = 0$. In the set P_3 , however, all the states have $x_1 > 1$. Therefore none of them are possible states after the transition e_1 , i.e.

$$Pre_{e_1}(P_3) = \emptyset$$

All states in P_4 on the other hand are such that $x_1 = 0$. States that end up in P_4 after x_1 is set of zero are all states such that $x_1 \in [0, \infty)$ and $x_2 \in (1, 2)$. Transition e_1 is possible only from some of these states, namely those where $x_1 \leq 3$ and $x_2 \leq 2$. Therefore

$$Pre_{e_1}(P_4) = \{q_1\} \times \{(0 \leq x_1 \leq 3) \wedge (1 < x_2 < 2)\}$$

As discussed in class we are only interested in the region $x_1 \geq 0$ and $x_2 \geq 0$. Moreover, the domains impose no restriction on the continuous evolution. Therefore

$$\begin{aligned} Pre_T(P_2) &= P_2 \cup (\{q_1\} \times \{x_1 = x_2 = 0\}) \\ Pre_T(P_3) &= P_3 \cup (\{q_2\} \times \{(1 < x_1 < 2) \wedge x_2 = 0\}) \\ Pre_T(P_4) &= P_4 \end{aligned}$$

Finally $Pre_T(P_1)$ consists of P_1 , the horizontal straight line segment $\{q_1\} \times \{(1 < x_1 < 2) \wedge (x_2 = 1)\}$, the open triangle $\{q_1\} \times \{(1 < x_1 < 2) \wedge (0 < x_2 < 1) \wedge (x_1 - 1 < x_2)\}$, the vertical line segment $\{q_1\} \times \{(x_1 = 1) \wedge (0 < x_2 < 1)\}$, the open triangle $\{q_1\} \times \{(0 < x_1 < 1) \wedge (0 < x_2 < 1) \wedge (x_1 > x_2)\}$, and the horizontal straight line segment $\{q_1\} \times \{(0 < x_1 < 1) \wedge (x_2 = 0)\}$.

All of the Pre sets are unions of elements of the region graph. Even though it is not a complete proof, this supports the argument that the region graph is a bisimulation.

Question 7: Consider the set

$$\mathcal{D} = \bigcup_{q \in Q} \{q\} \times D(q) \subseteq Q \times X$$

If all reachable states are such that $\hat{x} \in D(\hat{q})$, then

$$\text{Reach} \subseteq \mathcal{D}$$

The state stays in *Reach* for ever, therefore it stays in \mathcal{D} therefore the automaton is domain preserving. To show 2, consider an arbitrary execution (τ, q, x) . We show that $x_i(t) \in D(q_i(t))$ for all $I_i \in \tau$, and all $t \in I_i$ by induction. Since for all $(\hat{q}, \hat{x}) \in \text{Init}$, $\hat{x} \in D(\hat{q})$ clearly we have that $x_0(\tau_0) \in D(q_0(\tau_0))$. Assume $x_i(\tau_i) \in D(q_i(\tau_i))$ for some $I_i \in \tau$. If $\tau'_i > \tau_i$, $x_i(t) \in D(q_i(\tau_i)) = D(q_i(t))$ for all $t \in [\tau_i, \tau'_i)$, by the definition of an execution. If I_i is the last interval in τ the proof is complete (this is true if $I_i = [\tau_i, \tau'_i]$, or if $I_i = [\tau_i, \tau'_i)$, or if $I_i = [\tau_i, \infty)$, or even if $\tau_i = \tau'_i$). Otherwise, $x_i(\tau'_i) \in D(q_i(\tau'_i))$, since $D(q_i(\tau'_i))$ is a closed set. Otherwise, $x_{i+1}(\tau_{i+1}) \in R(q_i(\tau'_i), q_{i+1}(\tau_{i+1}), x_i(\tau'_i)) \subseteq D(q_{i+1}(\tau_{i+1}))$ and therefore $x_{i+1}(\tau_{i+1}) \in D(q_{i+1}(\tau_{i+1}))$ (this is true even if $\tau_i = \tau'_i$). The claim follows by induction. The argument establishes that the set \mathcal{D} is invariant. As discussed in the notes, similar induction arguments can be used to establish that more general sets of states are invariant. The argument does not require the system to have any executions (e.g. be non-blocking). It states that “along all executions $x \in D(q)$ ”, which is trivially true if there are no executions.

Question 8: To show that infinite runs exist for all initial conditions recall that J_T is closed and

$$\begin{aligned} R^{-1}(X) &= \{x \in X_T \mid x_1 \geq 21 \text{ and } x_2 \geq 20\} \\ &\quad \cup \{x \in X_T \mid x_1 \leq 19 \text{ and } x_2 \leq 20\} \\ &\supseteq \{x \in X_T \mid x_1 \geq 22 \text{ and } x_2 \geq 20\} \\ &\quad \cup \{x \in X_T \mid x_1 \leq 18 \text{ and } x_2 \leq 20\} \\ &= J_T. \end{aligned}$$

To show that K is invariant notice that R_T leaves x_1 unchanged and maps $x_2 = 30$ to $x_2 = 0$ and vice versa. Moreover,

$$\begin{aligned} K \setminus J_T &= \{x \in X_T \mid x_1 > 21 \text{ and } x_2 = 0\} \\ &\quad \cup \{x \in X_T \mid x_1 < 19 \text{ and } x_2 = 30\} \end{aligned}$$

Therefore, for all $x \in K \setminus J_T$, $T_K(x) = \{v \in X_T \mid v_2 = 0\} \supseteq F_T(x)$.

$L \cap J_T = \emptyset$, therefore the first condition of the viability theorem is vacuously satisfied for L . Moreover

$$\begin{aligned} L \setminus R^{-1}(L) &= \{x \in X_T \mid x_1 > 19 \text{ or } x_1 = 18 \text{ and } x_2 > 20\} \\ &\quad \cup \{x \in X_T \mid x_1 < 21 \text{ or } x_1 = 21 \text{ and } x_2 < 20\} \end{aligned}$$

For x such that $19 < x_1 < 21$, $T_L(x) = X_T$ and therefore $F_T(x) \cap T_L(x) = F_T(x) \neq \emptyset$. For x such that $x_1 = 19$ and $x_2 > 20$

$$\begin{aligned} F_T(x) &= \{v \in X_T \mid v_1 \in [a(x_1 - x_2), b(x_1 - x_2)]\} \\ &\subseteq \{v \in X_T \mid v_1 > 0\} = T_K(x) \end{aligned}$$

(recall that $a \leq b < 0$). A similar conclusion holds if $x_1 = 21$ and $x_2 < 20$. Therefore, L is viable. L is not invariant. This makes sense intuitively (it is possible for the temperature to go outside the range $[19, 21]$). It is also easy to see that the system violates the second condition of the invariance theorem for the set L . Since the conditions of the theorem are both necessary and sufficient, L cannot be invariant. To see that M is invariant, recall that R_T leaves x_1 unchanged, therefore $R(M) \subseteq M$. Moreover

$$\begin{aligned} M \setminus J_T &= \{x \in X_T \mid x_1 > 18 \text{ or } x_1 = 18 \text{ and } x_2 > 20\} \\ &\quad \cup \{x \in X_T \mid x_1 < 22 \text{ or } x_1 = 22 \text{ and } x_2 < 20\} \end{aligned}$$

The above argument shows that for all $x \in M \setminus J_T$, $F_T(x) \subseteq T_M(x)$.