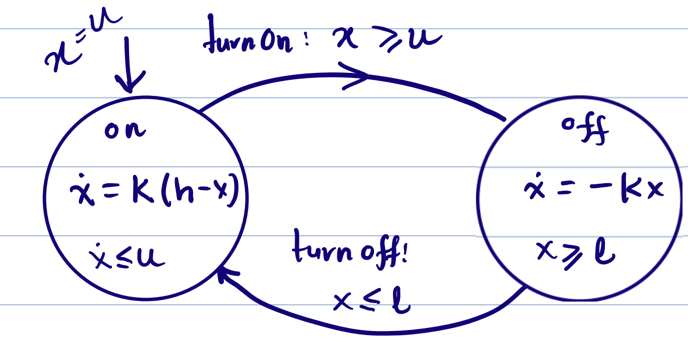
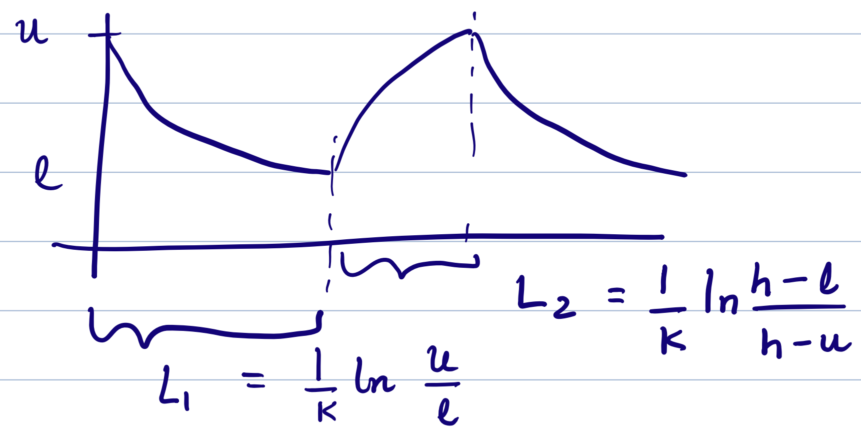
Recall the thermostat automaton

A.



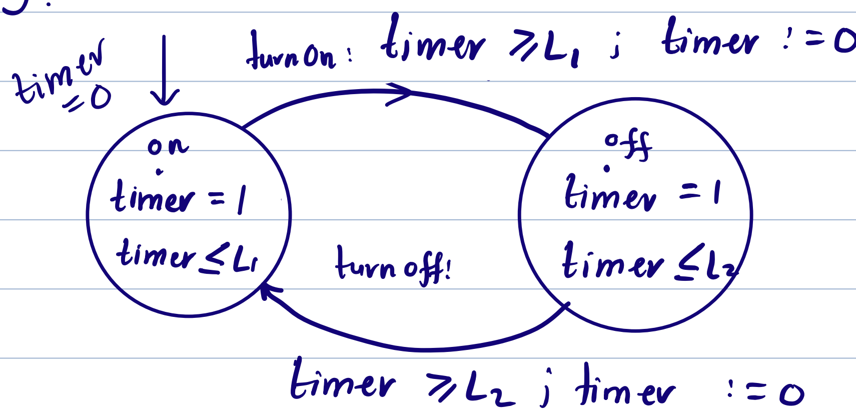
Linear DE

$x(t) = x(0)\, e^{-kt}$



If we only cared about the timing behavior of the thermostat, we could have worked with a Timed Automaton model:

B.



(1) How can we show that B indeed has the "same" timing behaviour as A?

(2) More generally, we may only care about certain aspects of A's executions such as

- timing
- subset of continuous variables $Y \subseteq X$
- control state reachability, etc.

How can we show that B is <u>equivalent</u> to A w.r.t the aspects of behavior we care about?

(3) How can we come up with an "equivalent" B that is simpler to analyze?

Recall ITA to equivalent FA for mode reachability

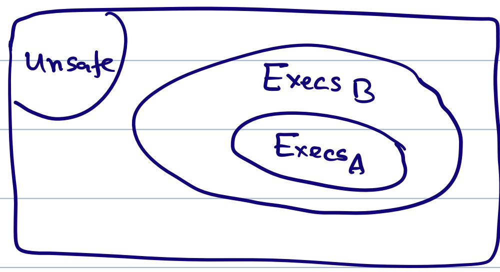
(4) Instead of "Equivalence" it may be sufficient to have a B that is simpler and "contains" all the relevant behaviors of A.

Then proving safety of B
$\Rightarrow$ safety of A.

E.g. we dropped the mode invariants of B

We would like to show that

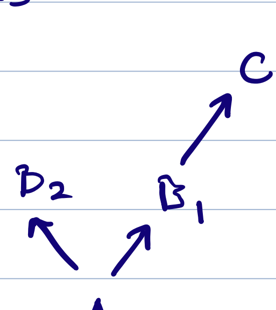
$\forall \alpha \in Execs_A \ \exists \beta \in Execs_B$ such that $\alpha = \beta$



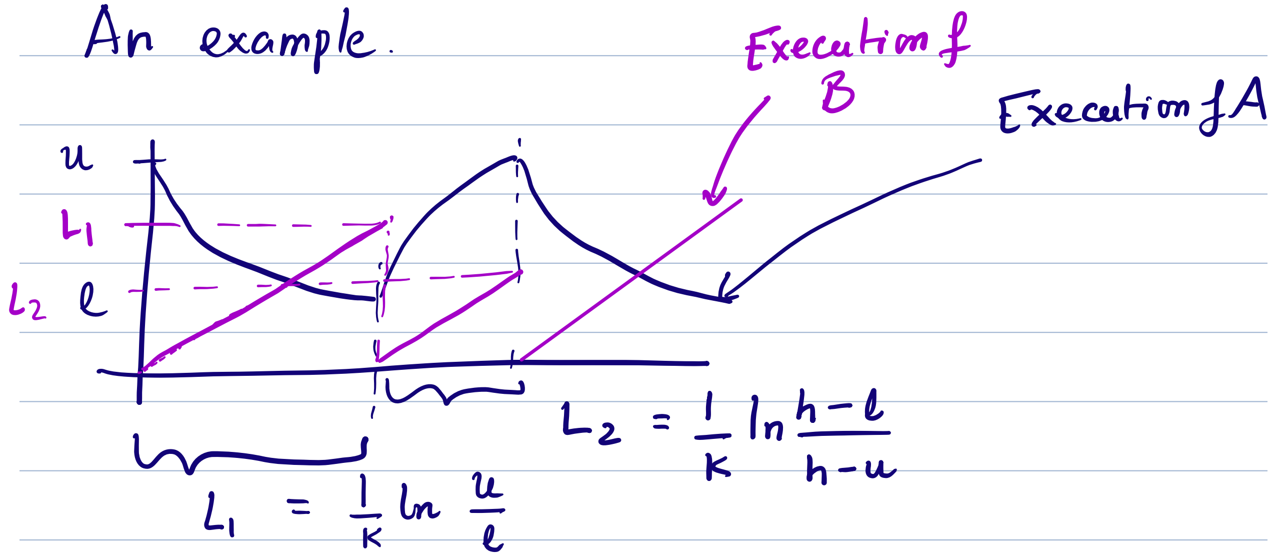
if the variable and action names of A and B do not exactly match up then $\forall \alpha \ \exists \beta$ such that $trace(\alpha) = trace(\beta)$

B is said to be an <u>Absraction</u> of A.

Abstraction defines a preorder on Automata with comparable sets of variable and actions



An example.



We have to reason about both A & B

To prove properties of A we worked with an invariant $I \subseteq Val(V_A)$ now we have to work with a relation
$R \subseteq Val(V_A) \times Val(V_B)$

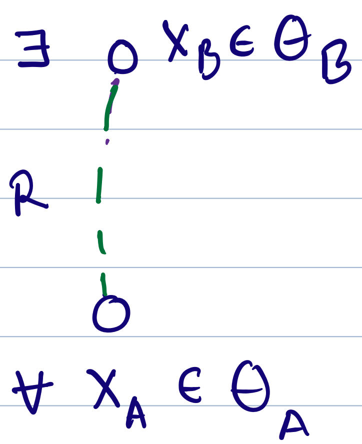
Setup. $A = \langle V_A, \Theta_A, D_A, \tau_A \rangle$

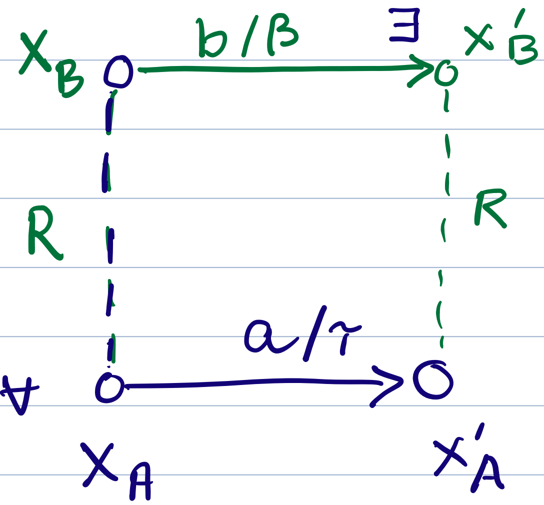
$V_A = \{x, loc\}$

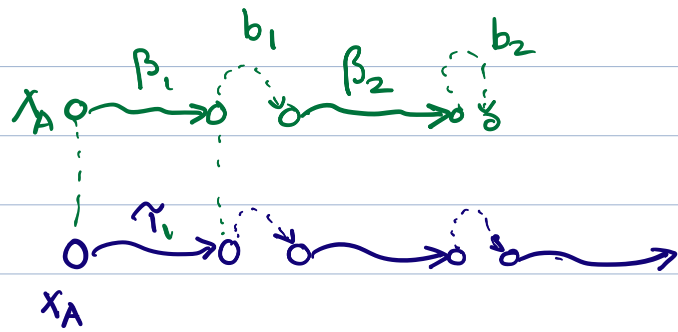
$B = \langle V_B, \Theta_B, D_B, \tau_B \rangle$

$V_B = \{timer, loc\}$

Can we relate the states of A B so that this relationship always holds?
Then, from an execution of A we can construct the corresponding execution B using this relation.







$a = b$
$\tau = \beta$ or generally

$\text{trace}(a) = \text{trace}(b)$

$\text{trace}(\tau) = \text{trace}(\beta)$

$\text{timing}(\tau) = \text{timing}(\beta)$

How can we show that R always holds?

Proposition 8.1. if

(a) Start condition. $\forall x_A \in \Theta_A \; \exists x_B \in \Theta_B \; x_A R x_B$

(b) Transition condition. $\forall x_A, x_A' \in Val(V_A) \quad a \in A_A$

$\forall x_B \in Val(V_B)$ s.t. $x_A \xrightarrow{a} x_A' \quad x_A R x_B$

$\exists x_B' \in Val(V_B)$ s.t. $x_B' \xrightarrow{a} x_B' \quad x_A' R x_B'$

(c) Trajectory condition. $\forall x_A, x_A' \in Val(V_A) \quad \tau \in \mathcal{T}_A$

$\forall x_B \in Val(V_B)$ s.t. $\tau.fstate = x_A \; \tau.lstate = x_A' \; x_A R x_B$

$\exists x_B' \in Val(V_B) \; \tau_2 \in \mathcal{T}_B$ s.t. $\tau_2.fstate = x_B \quad x_A' R x_B'$

$\tau_2.lstate = x_B'$

Such that $\tau_1.ltime = \tau_2.ltime$.

Then $\forall \alpha \in Exec_A \; \exists \beta \in Exec_B$ s.t. $timing(\alpha) = timing(\beta)$

Proof. Fix $\alpha \in Exec_A$

$$\alpha = \tau_{10}\, a_{11}\, \tau_{11}\, a_{12} \cdots \tau_{1n}$$

① Using start condition we know

$$\exists\, x_{20} \in \Theta_B \qquad \tau_{10}(0)\ R\ x_{20}$$

② Notice τ_{10}, x_{20} satisfy hypothesis of trajectory condition. Therefore using trajectory condition it follows

$\exists\, \tau_{20} \in \mathcal{T}_B$ such that

$\tau_{10}.ltime = \tau_{20}.ltime$ and

$\tau_{10}.lstate\ R.\ \tau_{20}.lstate$

③ $\left.\begin{array}{l} \tau_{10}.lstate\ R\ \tau_{20}.lstate \text{ and} \\ \tau_{10}.lstate \xrightarrow{a_{11}} \tau_{11}.fstate \end{array}\right\}$ Satisfies Hypothesis of transition Condition

it follows that is

$\exists\, a_{21} = a_{11}$ such that $\tau_{20}.lstate \xrightarrow{a_{21}} x_2$ and

$\tau_{11}.fstate\ R\ x_2$

We can continue this way to construct β.

Particular relation for thermostat

$R \subseteq Val(V_A) \times Val(V_B)$

$(x_A, x_B) \in R$ iff

$(x_A, x_B) \in R$ is also written as $x_A \, R \, x_B$

$x_A \lceil loc = x_B \lceil loc$ and

if $x_B \lceil loc = on$ then $x_B \lceil timer \geq \frac{1}{K} \ln \frac{h - \ell}{h - x_A \lceil x}$

else $x_B \lceil timer \geq \frac{1}{K} \ln \frac{u}{x_A \lceil x}$

(1) Start condition

$x_A \lceil loc = on \qquad x_A \lceil x = u$

$\Rightarrow x_B \lceil loc = On \qquad x_B \lceil timer = 0 \geq 0$

(2) Consider any $x_A \xrightarrow{\text{turn on}} x_A'$

we know $x_A \lceil loc = off$ and $x_A \lceil x \leq \ell$

and $x_B \, R \, x_A \Rightarrow x_B \lceil loc = off$

$$x_B \lceil timer \geq \frac{1}{K} \ln \frac{u}{x_A \lceil x} \geq \frac{1}{K} \ln \frac{u}{\ell} = L_1$$

action is enabled

and in the post state $x_B \xrightarrow{\text{turnon}} x_B'$

$x_B' \lceil timer = 0$

$$x_B' \lceil loc = on = x_A' \lceil loc$$

$$x_B' \lceil timer = 0$$

$$RHS = \frac{1}{K} \ln \frac{h-\ell}{h - x_A' \lceil x} = \frac{1}{K} \ln \frac{h-\ell}{h-\ell} = 0$$

$$x_B' \; R \; x_A'$$

Similarly we can check the condition for $x_A \xrightarrow{turnoff} x_A'$

(3) trajectory condition

Consider any $\tau_1 \in \mathcal{T}_A$ $\quad \tau_1(0) \lceil loc = off$

$$\tau_1(t) \lceil x = \tau_1(0) \lceil x \, e^{-Kt} \quad \wedge \; \tau(t) \lceil x \geq \ell$$

Let τ_2 be a trajectory from $\tau_2(0) \lceil loc = off$

$$\tau_2(0) \lceil timer = \frac{1}{K} \ln \frac{u}{\tau_1(0) \lceil x}$$

$$\tau_2(t) \lceil timer = \frac{1}{K} \ln \frac{u}{\tau_1(0) \lceil x} + t$$