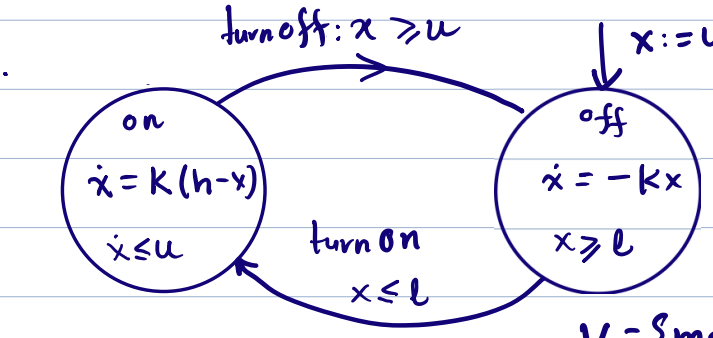
Recall the thermostat automaton

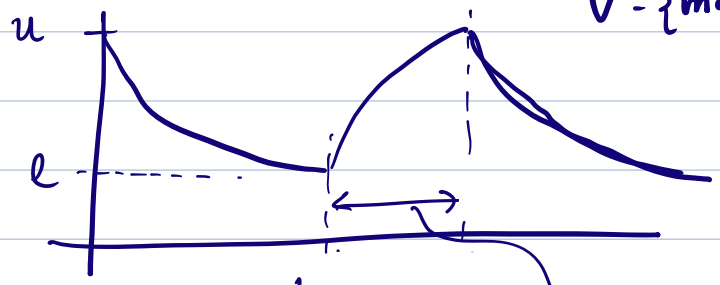
A.




Abstraction

$x(t) = x(0)e^{-Kt}$

$V = \{mode, x\}$

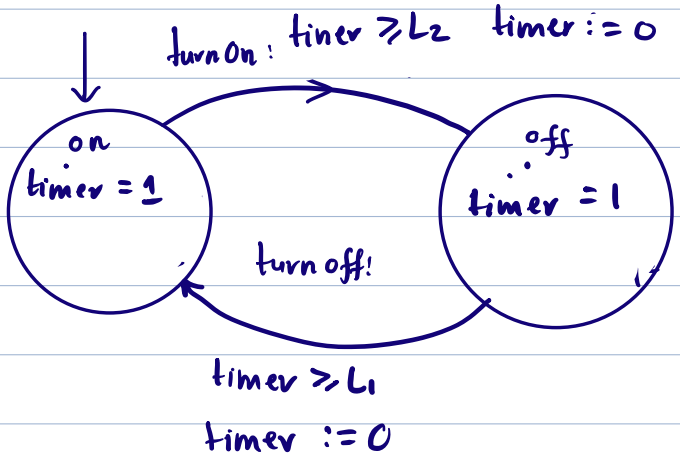



$L_1 = \frac{1}{K} \ln \frac{u}{\ell}$

$L_2 = \frac{1}{K} \ln \frac{h-\ell}{h-u}$

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

B.




$L_1, L_2 \in \mathbb{Z}$

ITA

① How can we show that $\mathcal{B}$ indeed has the "same" timing behaviour as A?

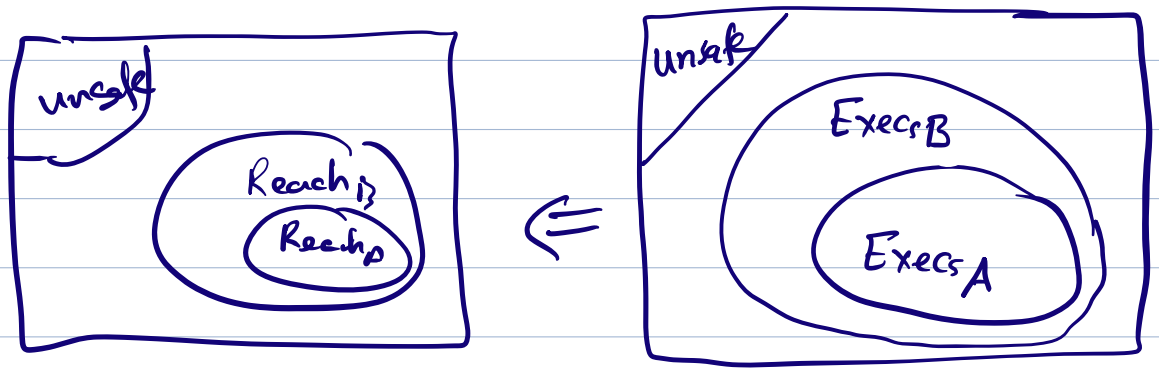
② More generally, we may only care about certain aspects of A's executions such as

- timing
- Properties / Predicates on Val(V) — Predicate Abstraction
- Subset variable
- Subset of trans

How can we show that $\mathcal{B}$ 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" $\mathcal{B}$ that is simpler to analyze?

④ Instead of "Equivalence" it may be sufficient to have a $\mathcal{B}$ that is simpler and "contains" all the relevant behaviors of A.



We would like to show that

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

$Execs_A \subseteq Execs_B$

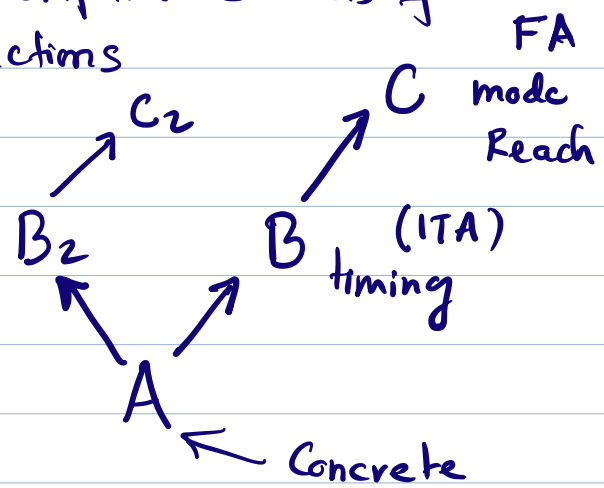
$trace(\alpha) = trace(\beta)$

$timing(\alpha) = timing(\beta)$

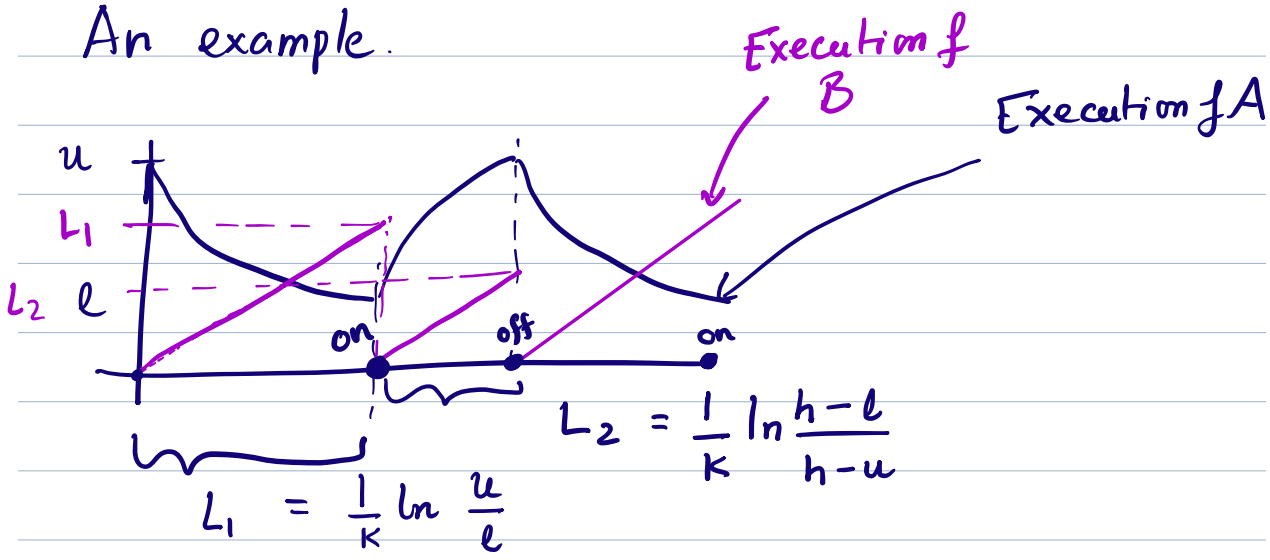
if the variable and action names of A and B do not exactly match up then $\forall \alpha \; \exists \beta$ such that $trace(\alpha) = trace(\beta)$

**Def** B is said to be an <u>Abstraction</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. $A = \langle V_A, \Theta_A, D_A, \mathcal{T}_A \rangle$

$B = \langle V_B, \Theta_B, D_B, \mathcal{T}_B \rangle$

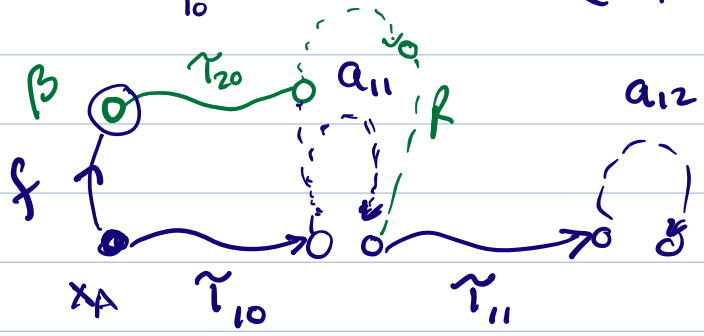
$Execs_A \subseteq Execs_B$

$\forall \alpha \in Execs_A \quad \exists \beta \in Exec_B \quad timing(\alpha) = timing(\beta)$

$f : Val(V_A) \longrightarrow Val(V_B)$

$\alpha = \tau_{10}\, a_{11}\, \tau_{11}\, a_{12}\, \tau_{12} \ldots$ $\quad R \subseteq Val(V_A) \times Val(V_B)$

$f(\alpha)$ ?? $\quad f(\tau_{10}(t))$ $\quad x_A R x_B$ / $(x_A, x_B) \in R$




Prop. 8.1 Given $A, B$ suppose we have
$R \subseteq Val(V_A) \times Val(V_B)$

(1) Start $\quad \forall x_A \in \Theta_A \; \exists x_B \in \Theta_B \quad x_A R x_B$.

(2) trans. $\quad \forall x_A, x_A' \in Val(V_A) \; a \in A_A \quad x_A \xrightarrow{a} x_A'$
$\forall x_B \in Val(V_B) \quad x_A R x_B$
$\exists x_B' \in Val(V_B) \quad x_B \xrightarrow{a} x_B' \wedge x_A' R x_B'$

(3) traj $\quad \forall x_A, x_A' \in Val(V_A) \; \tau_1 \in \mathcal{T}_A \quad \tau_1.fstate = x_A \ldots x_A'$
$\forall x_B \in Val(V_B) \quad \exists \tau_2 \in \mathcal{T}_B \quad \tau_2.ltime = \tau_1.ltime$
$x_A R x_B \qquad x_A' R \tau_2.lstate$.
Then $\forall \alpha \; \exists \beta \quad timing(\alpha) = timing(\beta)$.

**Proof**

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

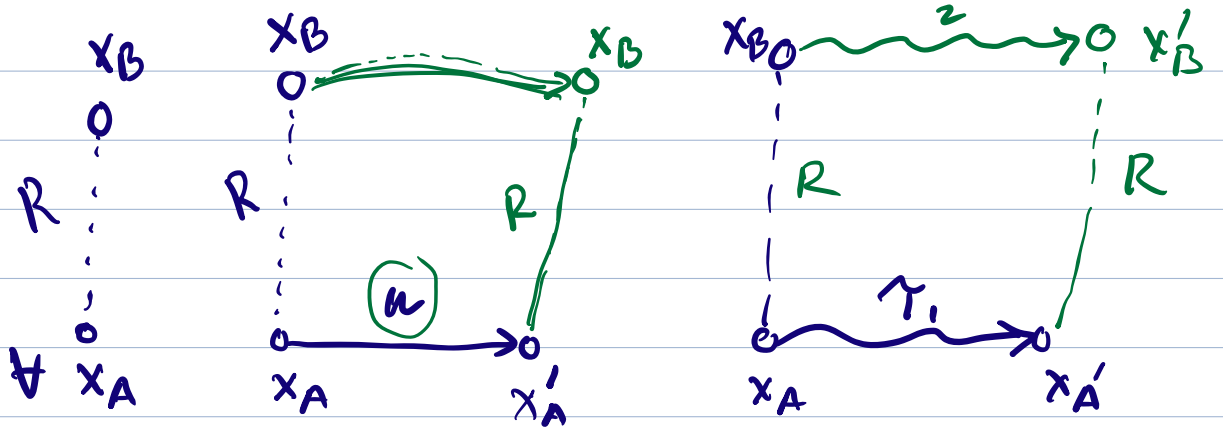
(1) Using Start Cond $\exists\, x_{B0}$ s.t $\tau_{10}(0)\ R\ x_{B0}$

(2) Using traj condition $\tau_{10}(0)$ and $x_{B0}$ satisfy the hypothesis. Follows $\exists\, \tau_{20} \in \tau_B$ s.t.

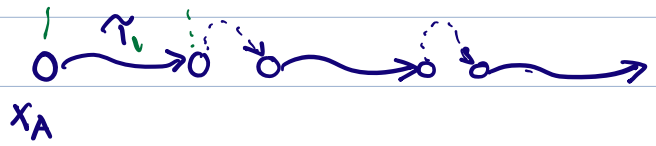
$\tau_{20}.\text{ltime} = \tau_{10}.\text{ltime}$

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

(3) Using the trans




$T_1.\text{Time} = T_2.\text{Time}$



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 $\tau_{10}$, $x_{20}$ 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 $\tau_{10}.lstate\ R\ \tau_{20}.lstate$ and $\tau_{10}.lstate \xrightarrow{a_{11}} \tau_{11}.fstate$ } 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 $\beta$.

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 $x_B \xrightarrow{\text{turnon}} x_B'$

$x_B'\lceil timer = 0$

$$\chi_B' \lceil loc = on = \chi_A' \lceil loc$$

$$\chi_B' \lceil timer = 0$$

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

$$\chi_B' \; R \; \chi_A'$$

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

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

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

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

Check that $\frac{1}{K} \ln \frac{u}{\tau_1(t)\Gamma x} = \frac{1}{K} \ln \frac{u}{\tau_1(0)\Gamma x e^{-Kt}}$

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