Exercises on modal logic

Radu Mateescu
Inria and LIG / Convecs
http://convecs.inria.fr

HML logic

(syntax)

$\varphi ::= \text{true}$	constant "true"
$\mid\ \text{false}$	constant "false"
$\mid\ \varphi_1 \vee \varphi_2$	disjunction
$\mid\ \varphi_1 \wedge \varphi_2$	conjunction
$\mid\ \neg\varphi_1$	negation
$\mid\ \langle\, \alpha \,\rangle\, \varphi_1$	possibility
$\mid\ [\, \alpha \,]\, \varphi_1$	necessity

- Duality: $[\, \alpha \,]\, \varphi \;=\; \neg \langle\, \alpha \,\rangle \neg \varphi$

HML logic

(semantics)

Let $M = (S, A, T, s_0)$. Interpretation $[[\ \varphi\ ]] \subseteq S$:

- $[[\ \text{true}\ ]] = S$
- $[[\ \text{false}\ ]] = \emptyset$
- $[[\ \varphi_1 \vee \varphi_2\ ]] = [[\ \varphi_1\ ]] \cup [[\ \varphi_2\ ]]$
- $[[\ \varphi_1 \wedge \varphi_2\ ]] = [[\ \varphi_1\ ]] \cap [[\ \varphi_2\ ]]$
- $[[\ \neg\varphi_1\ ]] = S \setminus [[\ \varphi_1\ ]]$
- $[[\ \langle\ \alpha\ \rangle\ \varphi_1\ ]] = \{\ s \in S \mid \exists\ (s, a, s') \in T\ .$
  $a \in [[\ \alpha\ ]] \wedge s' \in [[\ \varphi_1\ ]]\ \}$
- $[[\ [\ \alpha\ ]\ \varphi_1\ ]] = \{\ s \in S \mid \forall\ (s, a, s') \in T\ .$
  $a \in [[\ \alpha\ ]] \Rightarrow s' \in [[\ \varphi_1\ ]]\ \}$

Exercise: contradictions

- Show the contradictions below
  - $\langle \alpha \rangle$ false = false

Let $s \in [[\, \langle \alpha \rangle \text{ false }]]$, i.e.,
$\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha\,]] \wedge s' \in [[\text{ false }]]) \Leftrightarrow$
$\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha\,]] \wedge s' \in \varnothing) \Leftrightarrow$
$\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha\,]] \wedge \text{false}) \Leftrightarrow \exists\, (s, a, s') \in T. \text{ false} \Leftrightarrow \text{false}$
i.e., $s \in [[\, \langle \alpha \rangle \text{ false }]] \Leftrightarrow$ false, so $[[\, \langle \alpha \rangle \text{ false }]] = \varnothing = [[\text{ false }]]$

  - $\langle \text{false} \rangle\, \varphi$ = false

Let $s \in [[\, \langle \text{false} \rangle\, \varphi\,]]$, i.e.,
$\exists\, (s, a, s') \in T.\ (a \in [[\text{ false }]] \wedge s' \in [[\, \varphi\,]]) \Leftrightarrow$
$\exists\, (s, a, s') \in T.\ (a \in \varnothing \wedge s' \in [[\, \varphi\,]]) \Leftrightarrow$
$\exists\, (s, a, s') \in T.\ (\text{false} \wedge s' \in [[\, \varphi\,]]) \Leftrightarrow \exists\, (s, a, s') \in T. \text{ false} \Leftrightarrow \text{false}$
i.e., $s \in [[\, \langle \text{false} \rangle\, \varphi\,]] \Leftrightarrow$ false, so $[[\, \langle \text{false} \rangle\, \varphi\,]] = \varnothing = [[\text{ false }]]$

Exercise: tautologies

- Show the tautologies below
  - $[\ \alpha\ ]$ true = true

Start with the contradiction already established

$\langle\ \alpha\ \rangle$ false = false $\Leftrightarrow$ // apply $\neg$ on both sides

$\neg \langle\ \alpha\ \rangle$ false = $\neg$ false $\Leftrightarrow$ // propagate $\neg$ using duality

$[\ \alpha\ ]$ true = true

  - $[$ false $]\ \varphi$ = true

Start with the contradiction already established (for any φ)

$\langle$ false $\rangle\ (\neg\varphi)$ = false $\Leftrightarrow$ // apply $\neg$ on both sides

$\neg \langle$ false $\rangle\ (\neg\varphi)$ = $\neg$ false $\Leftrightarrow$ // propagate $\neg$ using duality

$[$ false$]\ \varphi$ = true

Exercise: distributivity of $\langle\ \rangle$ over $\vee$

- Show the distributivity of $\langle\ \rangle$ over $\vee$
  - $\langle \alpha \rangle \varphi_1 \vee \langle \alpha \rangle \varphi_2 = \langle \alpha \rangle (\varphi_1 \vee \varphi_2)$

Let $s \in [[\, \langle \alpha \rangle \varphi_1 \vee \langle \alpha \rangle \varphi_2 \,]]$, i.e.,

$\exists\, (s, a, s') \in T.\ (\ (a \in [[\, \alpha \,]] \wedge s' \in [[\, \varphi_1 \,]]) \vee$

$(a \in [[\, \alpha \,]] \wedge s' \in [[\, \varphi_2 \,]])\ )$ $\Leftrightarrow$ // factor

$\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha \,]] \wedge (s' \in [[\, \varphi_1 \,]] \vee s' \in [[\, \varphi_2 \,]]))$ $\Leftrightarrow$ // by [[.]]

$\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha \,]] \wedge (s' \in [[\, \varphi_1 \vee \varphi_2 \,]]))$ $\Leftrightarrow$ // by [[.]]

$s \in [[\, \langle \alpha \rangle (\varphi_1 \vee \varphi_2) \,]]$

- $\langle \alpha_1 \rangle \varphi \vee \langle \alpha_2 \rangle \varphi = \langle \alpha_1 \vee \alpha_2 \rangle \varphi$

(Hint: similar reasoning as above.)

Exercise: distributivity of [ ] over $\wedge$

- Show the distributivity of [ ] over $\wedge$
  - $[\,\alpha\,]\,\varphi_1 \wedge [\,\alpha\,]\,\varphi_2 = [\,\alpha\,]\,(\varphi_1 \wedge \varphi_2)$
  - $[\,\alpha_1\,]\,\varphi \wedge [\,\alpha_2\,]\,\varphi = [\,\alpha_1 \vee \alpha_2\,]\,\varphi$

(Hint: use the identities for distributivity of $\langle\ \rangle$ over $\vee$ and apply the duality between $\langle\ \rangle$ and [ ].)

Exercise: monotonicity of $\langle\ \rangle$

- Show the monotonicity of $\langle \alpha \rangle \varphi$ over φ and α
  - $(\varphi_1 \Rightarrow \varphi_2) \Rightarrow (\langle \alpha \rangle \varphi_1 \Rightarrow \langle \alpha \rangle \varphi_2)$

  Let $s \in [[\, \langle \alpha \rangle \varphi_1 \,]]$, i.e., $\exists\, (s, a, s') \in T.\ (a \in [[\, \alpha \,]] \wedge s' \in [[\, \varphi_1 \,]])$. Since $\varphi_1 \Rightarrow \varphi_2$, and $s' \in [[\, \varphi_1 \,]]$, it follows that $s' \in [[\, \varphi_2 \,]]$, and so $s \in [[\, \langle \alpha \rangle \varphi_2 \,]]$.

  - $(\alpha_1 \Rightarrow \alpha_2) \Rightarrow (\langle \alpha_1 \rangle \varphi \Rightarrow \langle \alpha_2 \rangle \varphi)$

  (Hint: similar reasoning as above.)

Exercise: monotonicity of [ ]

- Show the monotonicity of $[\,\alpha\,]\,\varphi$ over φ and α
  - $(\varphi_1 \Rightarrow \varphi_2) \Rightarrow ([\,\alpha\,]\,\varphi_1 \Rightarrow [\,\alpha\,]\,\varphi_2)$

Start with the (established) monotonicity of $\langle\,\alpha\,\rangle\,\varphi$ over φ

$((\neg\varphi_2) \Rightarrow (\neg\varphi_1)) \Rightarrow (\langle\,\alpha\,\rangle\,(\neg\varphi_2) \Rightarrow \langle\,\alpha\,\rangle\,(\neg\varphi_1))$ $\Leftrightarrow$ // counterpose

$(\varphi_1 \Rightarrow \varphi_2) \Rightarrow (\neg\langle\,\alpha\,\rangle\,(\neg\varphi_1) \Rightarrow \neg\langle\,\alpha\,\rangle\,(\neg\varphi_2))$ $\Leftrightarrow$ // by duality

$(\varphi_1 \Rightarrow \varphi_2) \Rightarrow ([\,\alpha\,]\,\varphi_1 \Rightarrow [\,\alpha\,]\,\varphi_2)$

$\boxed{(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)}$

  - $(\alpha_1 \Rightarrow \alpha_2) \Rightarrow ([\,\alpha_2\,]\,\varphi \Rightarrow [\,\alpha_1\,]\,\varphi)$

(Hint: similar reasoning as above, starting with

$(\alpha_1 \Rightarrow \alpha_2) \Rightarrow (\langle\,\alpha_1\,\rangle\,(\neg\varphi) \Rightarrow \langle\,\alpha_2\,\rangle\,(\neg\varphi))$

)

Exercise: HML identity

- Show the identity below

$$\langle \alpha \rangle \text{true} \wedge [\, \alpha \,]\, \varphi \;=\; \langle \alpha \rangle\, \varphi \wedge [\, \alpha \,]\, \varphi$$

"$\Leftarrow$": Holds by monotonicity of modalities over φ
($\langle \alpha \rangle$ true $\Leftarrow \langle \alpha \rangle\, \varphi$)

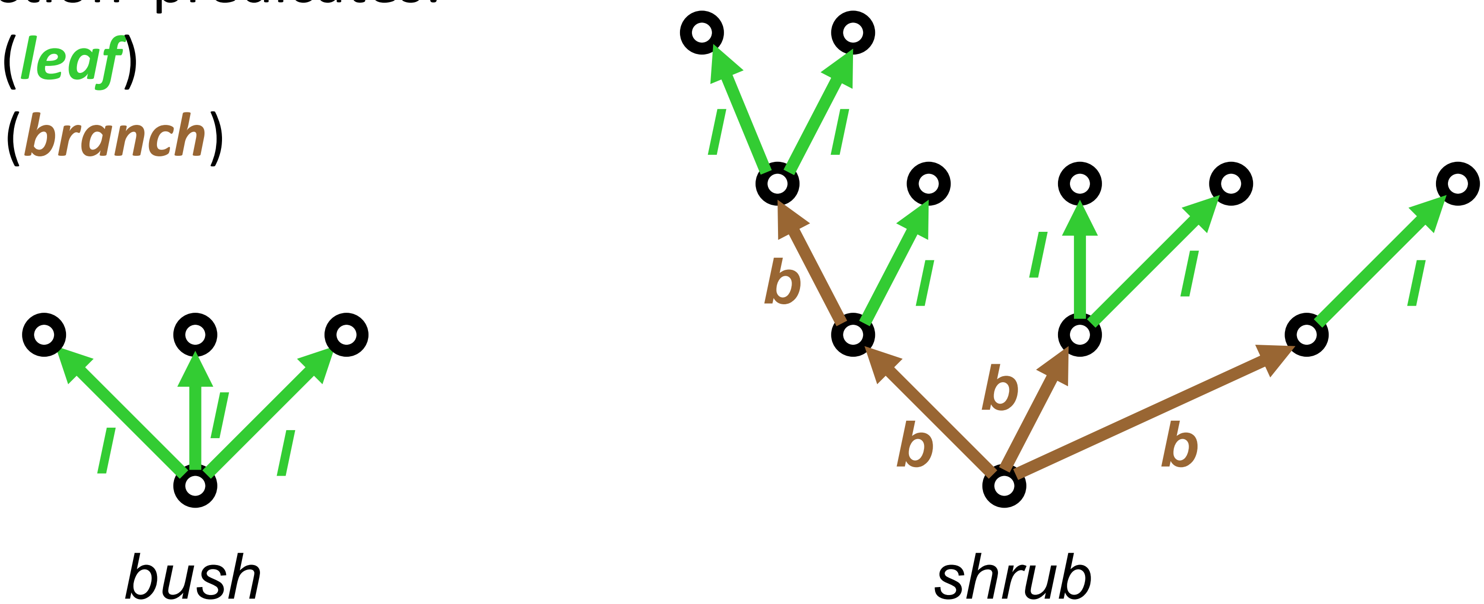
"$\Rightarrow$": Let $s \in [[\, \langle \alpha \rangle \text{true} \wedge [\, \alpha \,]\, \varphi \,]]$, i. e.,

$$\left.\begin{array}{l} \exists\, (s, a', s') \in T.\ a' \in [[\, \alpha \,]] \\ \wedge \\ \forall\, (s, a'', s'') \in T.\ (a'' \in [[\, \alpha \,]] \Rightarrow s'' \in [[\, \varphi \,]]) \end{array}\right\} \Rightarrow s' \in [[\, \varphi \,]]$$

$$\Rightarrow \quad \left.\begin{array}{l} s \in [[\, \langle \alpha \rangle\, \varphi \,]] \\ s \in [[\, [\, \alpha \,]\, \varphi \,]] \end{array}\right\} \Leftrightarrow s \in [[\, \langle \alpha \rangle\, \varphi \wedge [\, \alpha \,]\, \varphi \,]]$$

Exercise

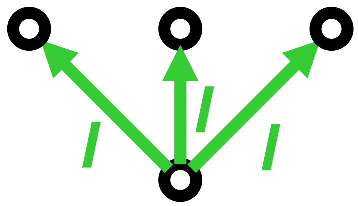
- Characterize in HML the tree-like LTSs below
  - Action predicates:
    l (***leaf***)
    b (***branch***)



Solution (bush)

- State formula characterizing deadlocks (sink states):

  deadlock = [true] false



bush = ⟨ *l* ⟩ true // there is at least one leaf transition

∧

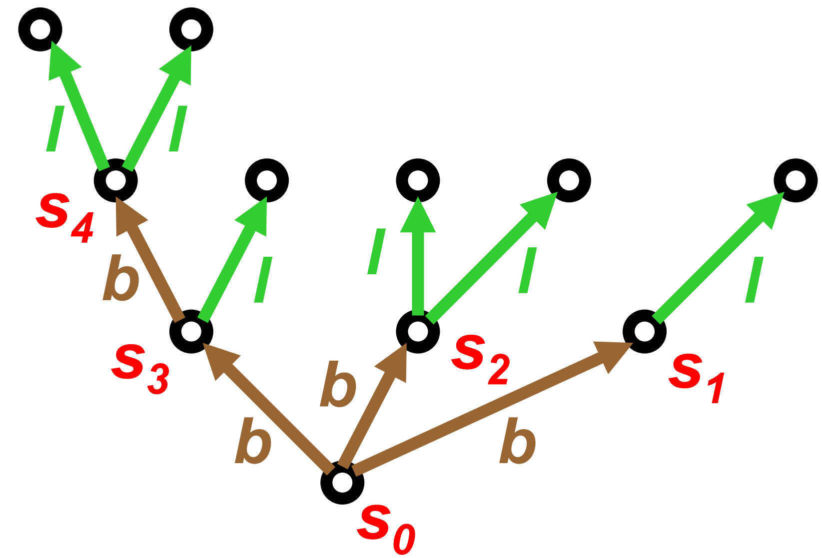
[*l*] *deadlock* // all leaves lead to deadlocks

∧

[¬*l*] false // no transition other than a leaf

- **Remark:** the *bush* formula cannot distinguish bushes with different number of leaves (they are *strongly bisimilar*).

Solution (shrub)



- Define HML subformulas characterizing each subtree rooted at s_1 … s_4:

s1 = s2 = s4 = *bush*

$$s3 = \underbrace{\langle\, l \,\rangle\ \mathit{deadlock}}_{\substack{\text{there is an } l \text{ from}\\ s_3 \text{ to a deadlock}}} \ \wedge\ \underbrace{\langle\, b \,\rangle\ s4}_{\substack{\text{there is a } b\\ \text{from } s_3 \text{ to } s_4}} \ \wedge\ \underbrace{[\, b \,]\ s4}_{\substack{\text{all } b \text{ from}\\ s_3 \text{ lead to } s_4}} \ \wedge\ \underbrace{[\, \neg(b \vee l) \,]\ \mathrm{false}}_{\substack{\text{no action but}\\ b \text{ or } l \text{ from } s_3}}$$

$$\mathit{shrub} = \langle\, b \,\rangle\ s1 \wedge \langle\, b \,\rangle\ s2 \wedge \langle\, b \,\rangle\ s3 \wedge [\, b \,]\ (s1 \vee s2 \vee s3) \wedge \underbrace{[\, \neg b \,]\ \mathrm{false}}_{\substack{\text{no action but}\\ b \text{ from } s_0}}$$

characterizes s_0

replace s1, s2 by their bodies and simplify

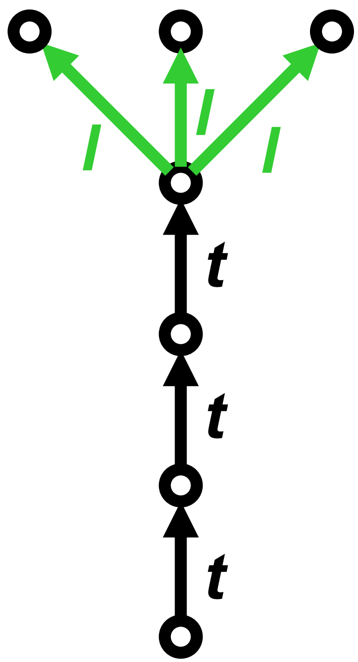
$$= \langle\, b \,\rangle\ \mathit{bush} \wedge \langle\, b \,\rangle\ s3 \wedge [\, b \,]\ (\mathit{bush} \vee s3) \wedge [\, \neg b \,]\ \mathrm{false}$$

Exercise

- Characterize in HML the tree-like LTS below
  - Action predicates:

    l (***leaf***)

    t (***trunk***)

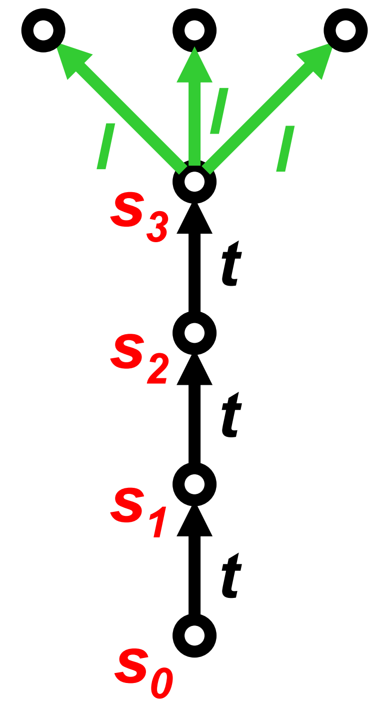


palm tree

Solution (palm tree)

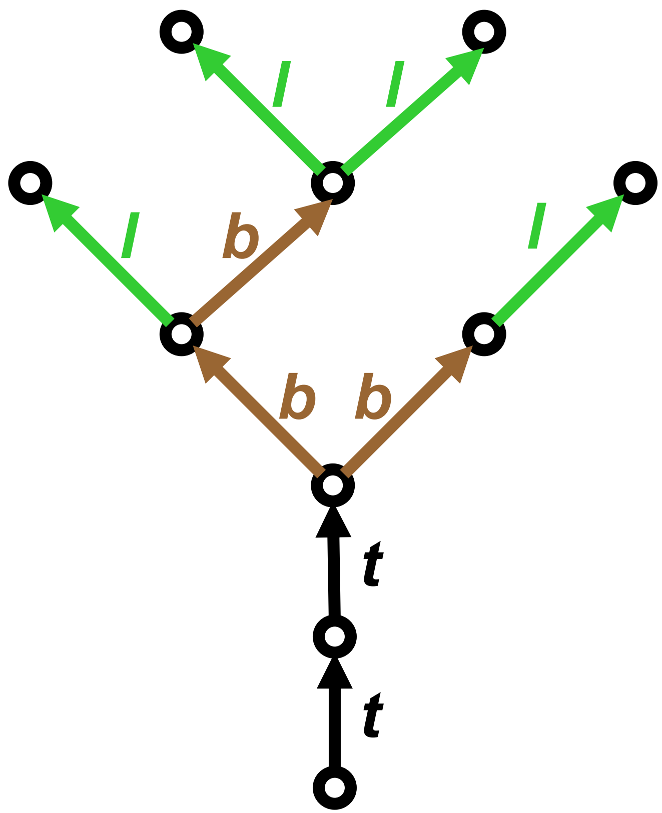
- Characterize each subtree rooted at s_0 … s_3 by a HML subformula:

$$
palm = \left.\begin{array}{l}
\langle \mathbf{t} \rangle (\\
\quad \left.\begin{array}{l}
\langle \mathbf{t} \rangle (\\
\quad \left.\begin{array}{l}
\langle \mathbf{t} \rangle \, \overbrace{bush}^{s_3} \\
\wedge \\
[\, \neg \mathbf{t} \,] \text{ false}
\end{array}\right\} s_2 \\
) \wedge \\
[\, \neg \mathbf{t} \,] \text{ false}
\end{array}\right\} s_1 \\
) \wedge \\
[\, \neg \mathbf{t} \,] \text{ false}
\end{array}\right\} s_0
$$



Exercise

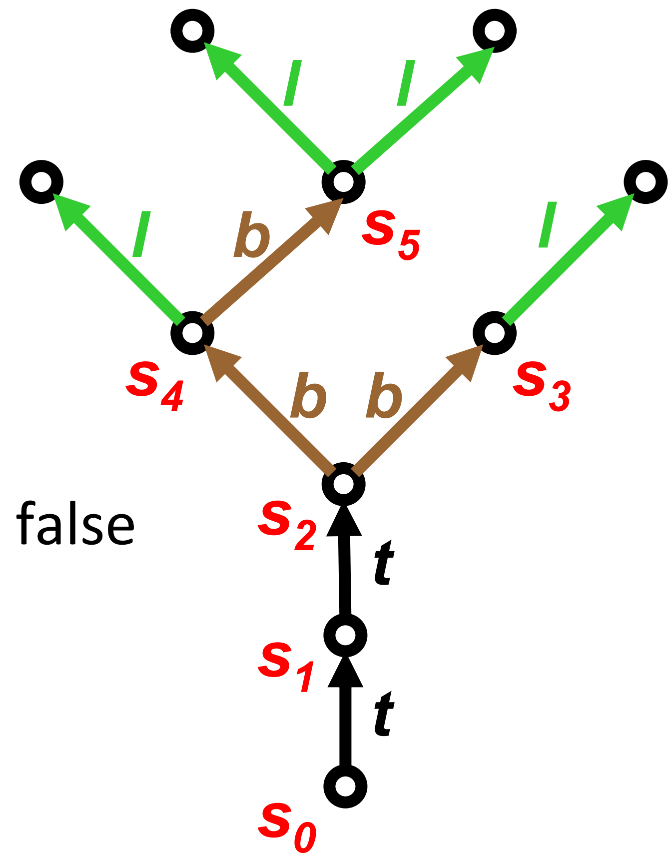
- Characterize in HML the tree-like LTS below



tree

Solution

- Characterize each subtree rooted at s_0 … s_5 using an HML formula:



s3 = s5 = *bush*

s4 = $\langle\, l \,\rangle$ deadlock $\wedge \langle\, b \,\rangle$ s5 $\wedge$
$[\, b \,]$ s5 $\wedge\, [\, \neg(b \vee l) \,]$ false

s2 = $\langle\, b \,\rangle$ s3 $\wedge \langle\, b \,\rangle$ s4 $\wedge\, [\, b \,]$ (s3 $\vee$ s4) $\wedge\, [\, \neg b \,]$ false

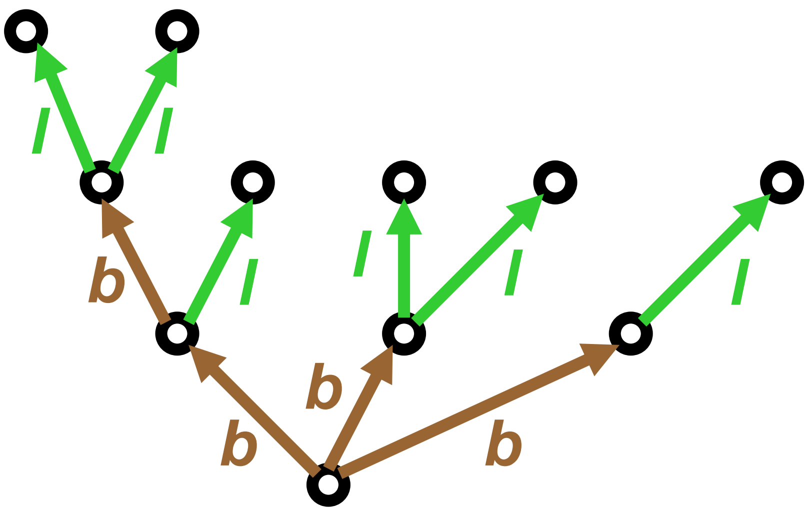
s1 = $\langle\, t \,\rangle$ s2 $\wedge\, [\, t \,]$ s2 $\wedge\, [\, \neg t \,]$ false

tree = $\langle\, t \,\rangle$ s1 $\wedge\, [\, t \,]$ s1 $\wedge\, [\, \neg t \,]$ false

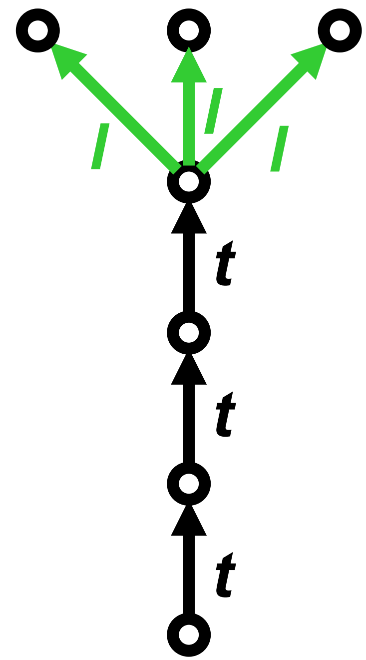
characterizes s_0

Exercise: ACTL

- Characterize in ACTL the tree-like LTSs below

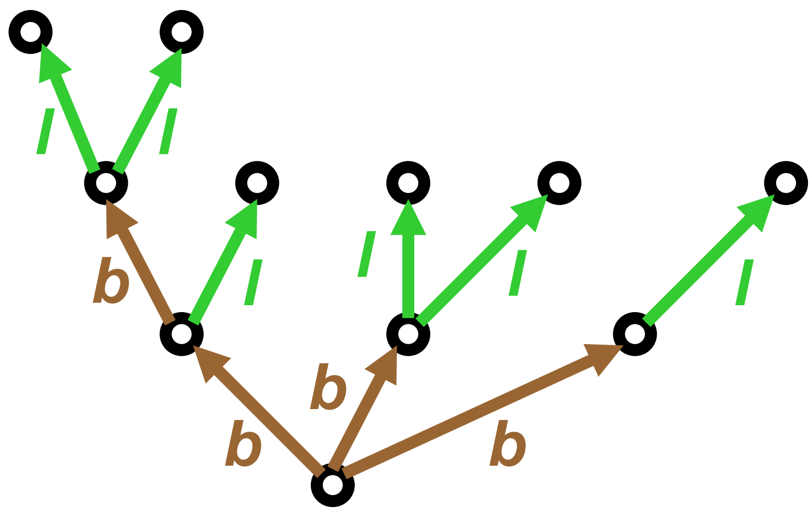


shrub

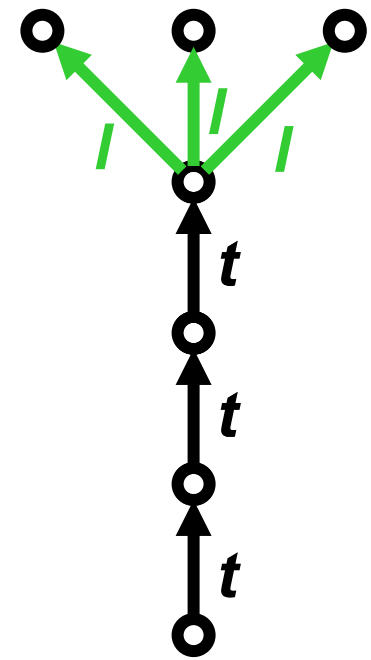


palm tree

Solution



shrub



palm tree

$shrub = \text{A} [\text{ true}_b \text{ U}_l \textit{ deadlock }]$ $\qquad$ $palm = \text{A} [\text{ true}_t \text{ U } \textit{bush }]$

- **Remark:** all trunk/branch/leaf actions are assumed to be visible ($\neq \tau$).

Exercise: ACTL

- Characterize in ACTL the tree-like LTS below

(Hint: use nested ACTL operators.)