Action-Based Temporal Logics and Model Checking (part II)

Radu Mateescu

Inria and LIG / Convecs

http://convecs.inria.fr

PDL logic

(syntax)

$\varphi ::=$	true | false	boolean constants
|	$\varphi_1 \vee \varphi_2$	disjunction
|	$\varphi_1 \wedge \varphi_2$	conjunction
|	$\neg\varphi_1$	negation
|	$\langle \beta \rangle \varphi_1$	possibility
|	$[\beta]\varphi_1$	necessity

- Duality: $[\beta]\varphi = \neg\langle \beta \rangle \neg\varphi$

PDL logic

(semantics)

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

- $[[\ \text{true}\ ]] = S$
- $[[\ \text{false}\ ]] = \varnothing$
- $[[\ \varphi_1 \vee \varphi_2\ ]] = [[\ \varphi_1\ ]] \cup [[\ \varphi_2\ ]]$
- $[[\ \varphi_1 \wedge \varphi_2\ ]] = [[\ \varphi_1\ ]] \cap [[\ \varphi_2\ ]]$
- $[[\ \neg\varphi_1\ ]] = S \setminus [[\ \varphi_1\ ]]$
- $[[\ \langle\ \beta\ \rangle\ \varphi_1\ ]] = \{\ s \in S \mid \exists\ s' \in S\ .$
  $(s, s') \in [[\ \beta\ ]] \wedge s' \in [[\ \varphi_1\ ]]\ \}$
- $[[\ [\ \beta\ ]\ \varphi_1\ ]] = \{\ s \in S \mid \forall\ s' \in S\ .$
  $(s, s') \in [[\ \beta\ ]] \Rightarrow s' \in [[\ \varphi_1\ ]]\ \}$

Exercise: distributivity of concatenation

- Show the identity below
  - $\langle \beta_1 . \beta_2 \rangle \varphi = \langle \beta_1 \rangle \langle \beta_2 \rangle \varphi$

$(x, y) \in R_1 \circ R_2 \quad \Leftrightarrow$
$\exists z . (x, z) \in R_1 \wedge (z, y) \in R_2$

Let $s \in [[\langle \beta_1 . \beta_2 \rangle \varphi]]$, i.e.,

$\exists s' \in S . (s, s') \in [[\beta_1 . \beta_2]] \wedge s' \in [[\varphi]] =$ // by def. $[[\beta]]$

$\exists s' \in S . (s, s') \in [[\beta_1]] \circ [[\beta_2]] \wedge s' \in [[\varphi]] =$ // by def. of 'o'

$\exists s' \in S . \exists s'' \in S . (s, s'') \in [[\beta_1]] \wedge (s'', s') \in [[\beta_2]] \wedge s' \in [[\varphi]] =$

$\exists s'' \in S . ((s, s'') \in [[\beta_1]] \wedge \exists s' \in S . (s'', s') \in [[\beta_2]] \wedge s' \in [[\varphi]]) =$

$\exists s'' \in S . ((s, s'') \in [[\beta_1]] \wedge s'' \in [[\langle \beta_2 \rangle \varphi]]) =$

$s \in [[\langle \beta_1 \rangle \langle \beta_2 \rangle \varphi]]$

Quantifier propagation:
$\exists x . (P \vee Q (x)) = P \vee \exists x . Q (x)$
$\exists x . (P \wedge Q (x)) = P \wedge \exists x . Q (x)$

Exercise: distributivity of choice

- Show the identity below
  - $\langle \beta_1 \mid \beta_2 \rangle \varphi = \langle \beta_1 \rangle \varphi \vee \langle \beta_2 \rangle \varphi$

(Hint: use a similar reasoning as for concatenation.)

Exercise: distributivity of iteration (1/2)

- Show the identity below
  - $\langle \beta^* \rangle \varphi = \varphi \vee \langle \beta \rangle \langle \beta^* \rangle \varphi$

$R^* = \cup_{k \geq 0} R^k$, where
$R^k = R \circ \ldots \circ R$, $R^0 = \mathrm{Id}$

Let $s \in [[\langle \beta^* \rangle \varphi]]$, i.e.,

$\exists\, s' \in S\,.\,((s, s') \in [[\beta^*]] \wedge s' \in [[\varphi]]) =$

$\exists\, s' \in S\,.\,\exists\, k \geq 0\,.\,((s, s') \in [[\beta]]^k \wedge s' \in [[\varphi]]) =$

$\exists\, s' \in S\,.\,(((s, s') \in [[\beta]]^0 \vee \exists\, k \geq 0\,.\,(s, s') \in [[\beta]]^{k+1}) \wedge s' \in [[\varphi]]) =$

$\exists\, s' \in S\,.\,((s = s' \vee \exists\, k \geq 0\,.\,(s, s') \in [[\beta]] \circ [[\beta]]^k) \wedge s' \in [[\varphi]]) =$

$\exists\, s' \in S\,.\,(s = s' \wedge s' \in [[\varphi]]) \vee$

$\quad \exists\, s' \in S\,.\,\exists\, k \geq 0\,.\,((s, s') \in [[\beta]] \circ [[\beta]]^k) \wedge s' \in [[\varphi]]) =$

$s \in [[\varphi]] \vee$

$\quad \exists\, s' \in S\,.\,\exists\, k \geq 0\,.\,(\exists\, s'' \in S\,.\,(s, s'') \in [[\beta]] \wedge (s'', s') \in [[\beta]]^k) \wedge s'$
$\in [[\varphi]]) = \ldots / \ldots$

Exercise: distributivity of iteration (2/2)

$s \in [[\ \varphi\ ]] \vee$
$\exists\, s' \in S\ .\ \exists\, k \geq 0\ .\ (\exists\, s'' \in S\ .\ (s, s'') \in [[\ \beta\ ]] \wedge (s'', s') \in [[\ \beta\ ]]^k) \wedge s' \in [[\ \varphi\ ]]) =$

$s \in [[\ \varphi\ ]] \vee$
$\exists\, s' \in S\ .\ (\exists\, s'' \in S\ .\ (s, s'') \in [[\ \beta\ ]] \wedge \exists\, k \geq 0\ .\ (s'', s') \in [[\ \beta\ ]]^k) \wedge s' \in [[\ \varphi\ ]]) =$

$s \in [[\ \varphi\ ]] \vee$
$\exists\, s'' \in S\ .\ (s, s'') \in [[\ \beta\ ]] \wedge \exists\, s' \in S\ .\ ((s'', s') \in [[\ \beta\ ]]^*) \wedge s' \in [[\ \varphi\ ]]) =$

$s \in [[\ \varphi\ ]] \vee \exists\, s'' \in S\ .\ (s, s'') \in [[\ \beta\ ]] \wedge s'' \in [[\ \langle\ \beta^*\ \rangle\ \varphi\ ]] =$

$s \in [[\ \varphi\ ]] \vee s \in [[\ \langle\ \beta\ \rangle \langle\ \beta^*\ \rangle\ \varphi\ ]] =$

$s \in [[\ \varphi\ \vee \langle\ \beta\ \rangle \langle\ \beta^*\ \rangle\ \varphi\ ]]$

Exercise: nil regular formula

- Show the identities below
  - $\langle \text{nil} \rangle \varphi = \varphi$

$\langle \text{nil} \rangle \varphi =$ // by definition of nil
$\langle \text{false}^* \rangle \varphi =$ // by distrib. of iteration
$\varphi \vee \langle \text{false} \rangle \langle \text{false}^* \rangle \varphi =$ // by $\langle \text{false} \rangle \psi = \text{false}$
φ // (contradiction)

  - $[\text{nil}]\, \varphi = \varphi$

(Hint: use the duality between $\langle\ \rangle$ and $[\ ]$.)

Modal mu-calculus

(syntax)

$\varphi ::= \text{true} \mid \text{false}$	boolean constants
$\mid \varphi_1 \vee \varphi_2 \mid \neg\varphi_1$	boolean connectors
$\mid \langle \alpha \rangle \varphi_1$	possibility
$\mid [\, \alpha \,] \varphi_1$	necessity
$\mid X$	propositional variable
$\mid \mu X \,.\, \varphi_1$	minimal fixed point
$\mid \nu X \,.\, \varphi_1$	maximal fixed point

- Duality: $\nu X \,.\, \varphi = \neg\, \mu X \,.\, \neg\, \varphi\, [\neg X / X]$

Syntactic restrictions

- Syntactic monotonicity [Kozen-83]
  - Necessary to ensure the existence of fixed points
  - In every formula $\sigma X \,.\, \varphi\,(X)$, where $\sigma \in \{\, \mu, \nu \,\}$, every free occurrence of X in φ falls in the scope of an even number of negations

$$\mu X \,.\, \langle\, a \,\rangle\, X \vee \neg \langle\, b \,\rangle\, X$$

- Alternation depth 1 [Emerson-Lei-86]
  - Necessary for efficient (linear-time) verification
  - In every formula $\mu X \,.\, \varphi\,(X)$, every maximal subformula $\nu Y \,.\, \varphi'\,(Y)$ of φ is closed

$$\mu X \,.\, \langle\, a \,\rangle\, \nu Y \,.\, ([\, b \,]\, Y \wedge [\, c \,]\, X)$$

Positive Normal Form

(elimination of negations)

- Propagate negations downwards using dualities:
  - $\neg$ false = true
  - $\neg (\varphi_1 \vee \varphi_2) = \neg \varphi_1 \wedge \neg \varphi_2$
  - $\neg \langle \alpha \rangle \varphi = [\alpha] \neg \varphi$
  - $\neg \mu X . \varphi(X) = \nu X . \neg \varphi(\neg X)$

PNF transformation works because of syntactic monotonicity

- Example:

$$\neg \mu X . (\langle s \rangle \nu Y . ([r] \text{false} \wedge [\text{true}] Y) \vee \langle \text{true} \rangle X)$$

$$= \nu X . (\neg \langle s \rangle \nu Y . ([r] \text{false} \wedge [\text{true}] Y) \wedge \neg \langle \text{true} \rangle \neg X)$$

$$= \nu X . ([s] \neg \nu Y . ([r] \text{false} \wedge [\text{true}] Y) \wedge [\text{true}] X)$$

$$= \nu X . ([s] \mu Y . (\langle r \rangle \text{true} \vee \langle \text{true} \rangle Y) \wedge [\text{true}] X)$$

Modal mu-calculus

(semantics)

Let $M = (S, A, T, s_0)$ and $\rho : \boldsymbol{X} \rightarrow 2^S$ a context mapping propositional variables to state sets.

Interpretation $[[\ \varphi\ ]] \subseteq S$:

- $[[\ X\ ]]\ \rho = \rho\ (X\ )$
- $[[\ \mu X\ .\ \varphi\ ]]\ \rho = \bigcup_{k \geq 0} \Phi_\rho^{\ k}\ (\emptyset)$
- $[[\ \nu X\ .\ \varphi\ ]]\ \rho = \bigcap_{k \geq 0} \Phi_\rho^{\ k}\ (S)$

where $\quad \Phi_\rho : 2^S \rightarrow 2^S$,

$$\Phi_\rho\ (U) \ = \ [[\ \varphi\ ]]\ \rho\ [\ U\ /\ X\ ]$$

Exercise: contradictions

- Show the identities below
  - $\mu X \,.\, X = \text{false}$

$\Phi\,(U) = [[\,X\,]]\;\;[\,U\,/\,X\,] = U \quad \Rightarrow \quad \Phi^k\,(U) = U$

$[[\,\mu X \,.\, X\,]] = \mathrm{U}_{k\,\geq\,0}\,\Phi^k\,(\varnothing) = \mathrm{U}_{k\,\geq\,0}\,\varnothing = \varnothing$

  - $\mu X \,.\, \langle\,\alpha\,\rangle\, X = \text{false}$

$\Phi\,(U) = [[\,\langle\,\alpha\,\rangle\, X\,]]\;\;[\,U\,/\,X\,] =$

$\{\, s \in S \,.\, \exists\,(s, a, s') \in T \,.\, a \in [[\,\alpha\,]] \wedge s' \in U\,\}$

$\Phi\,(\varnothing) = \{\, s \in S \,.\, \exists\,(s, a, s') \in T \,.\, a \in [[\,\alpha\,]] \wedge s' \in \varnothing\,\} = \varnothing$

$\Rightarrow \;\; \Phi^k\,(\varnothing) = \varnothing$

$[[\,\mu X \,.\, \langle\,\alpha\,\rangle\, X\,]] = \mathrm{U}_{k\,\geq\,0}\,\Phi^k\,(\varnothing) = \mathrm{U}_{k\,\geq\,0}\,\varnothing = \varnothing$

Exercise: tautologies

- Show the identities below
  - $\nu X \,.\, X$ = true

$\nu X \,.\, X =$ // by duality

$\neg\, \mu X \,.\, \neg\, (X\, [\neg\, X \,/\, X]) =$ // by syntactic substitution

$\neg\, \mu X \,.\, \neg\, (\neg\, X) =$

$\neg\, \mu X \,.\, X =$ // by using the contradiction

$\neg$ false = true

  - $\nu X \,.\, [\ \alpha\ ]\ X$ = true

(Hint: use duality as above.)

Exercise: monotonicity of modal formulas in PNF (1/3)

- Let φ be a modal formula in PNF (i.e., without negations) with X the only free variable. Show that
  - $U_1 \subseteq U_2 \;\Rightarrow\; [[\, \varphi \,]]\,[\, U_1/X \,] \subseteq [[\, \varphi \,]]\,[\, U_2/X \,]$

  By structural induction on φ.

  - $\varphi ::= X$:
    $[[\, X \,]]\,[\, U_1/X \,] = U_1 \subseteq$ // by hypothesis
    $U_2 = [[\, X \,]]\,[\, U_2/X \,]$.

  - $\varphi ::=$ false (similar for true):
    $[[\, \text{false} \,]]\,[\, U_1/X \,] = \emptyset = [[\, \text{false} \,]]\,[\, U_2/X \,]$.

Exercise: monotonicity of modal formulas in PNF (2/3)

- $\varphi ::= \varphi_1 \vee \varphi_2$ (similar for $\wedge$):
  $[[\ \varphi_1 \vee \varphi_2\ ]]\ [\ U_1/X\ ] = [[\ \varphi_1\ ]]\ [\ U_1/X\ ] \cup [[\ \varphi_2\ ]]\ [\ U_1/X\ ] \subseteq$
  // by induction hypothesis
  $[[\ \varphi_1\ ]]\ [\ U_2/X\ ] \cup [[\ \varphi_2\ ]]\ [\ U_2/X\ ] = [[\ \varphi_1 \vee \varphi_2\ ]]\ [\ U_2/X\ ]$.

- $\varphi ::= \langle\ \alpha\ \rangle\ \varphi_1$ (similar for $[\ \alpha\ ]\ \varphi_1$):
  $[[\ \langle\ \alpha\ \rangle\ \varphi_1\ ]]\ [\ U_1/X\ ] =$
  $\{\ s \in S \mid \exists (s, a, s') \in T.\ (a \in [[\ \alpha\ ]] \wedge s' \in [[\ \varphi_1\ ]]\ [\ U_1/X\ ])\ \} \subseteq$
  // by induction hypothesis and monotonicity of $\langle\ \rangle$
  $\{\ s \in S \mid \exists (s, a, s') \in T.\ (a \in [[\ \alpha\ ]] \wedge s' \in [[\ \varphi_1\ ]]\ [\ U_2/X\ ])\ \} =$
  $[[\ \langle\ \alpha\ \rangle\ \varphi_1\ ]]\ [\ U_2/X\ ]$.

Exercise: monotonicity of modal formulas in PNF (3/3)

- Let φ be a modal formula in PNF with *X* the only free variable. Show that
  - $\forall k \geq 0 \,.\, \Phi^k(\emptyset) \subseteq \Phi^{k+1}(\emptyset)$

By induction on *k*:

- $k = 0$: $\Phi^0(\emptyset) = \emptyset \subseteq \Phi(\emptyset) = \Phi^1(\emptyset)$.
- $k := k+1$:

  $\Phi^{k+1}(\emptyset) = \Phi(\Phi^k(\emptyset)) \supseteq$ // by induction hypothesis // and monotonicity of φ

  $\Phi(\Phi^{k-1}(\emptyset)) = \Phi^k(\emptyset)$.

Exercise: monotonicity of fixed points

- Let φ_1, φ_2 be modal formulas in PNF with X the only free variable. Show that
  - $(\varphi_1 \Rightarrow \varphi_2) \Rightarrow (\mu X . \varphi_1 \Rightarrow \mu X . \varphi_2)$

$\Phi_1 (U) = [[\ \varphi_1\ ]]\ [\ U / X\ ]$ and $\Phi_2 (U) = [[\ \varphi_2\ ]]\ [\ U / X\ ]$

By induction on k, we show $\Phi_1^k (\emptyset) \subseteq \Phi_1^k (\emptyset)$.

- $k = 0$: $\Phi_1^0 (\emptyset) = \emptyset \subseteq \emptyset = \Phi_2^0 (\emptyset)$.
- $k := k+1$:

  $\Phi_1^{k+1} (\emptyset) = \Phi_1 (\Phi_1^k (\emptyset)) \subseteq$ // by induction hypothesis

  // and monotonicity of φ_1

  $\Phi_1 (\Phi_2^k (\emptyset)) \subseteq$ // by hypothesis

  $\Phi_2 (\Phi_2^k (\emptyset)) = \Phi_2^{k+1} (\emptyset)$.

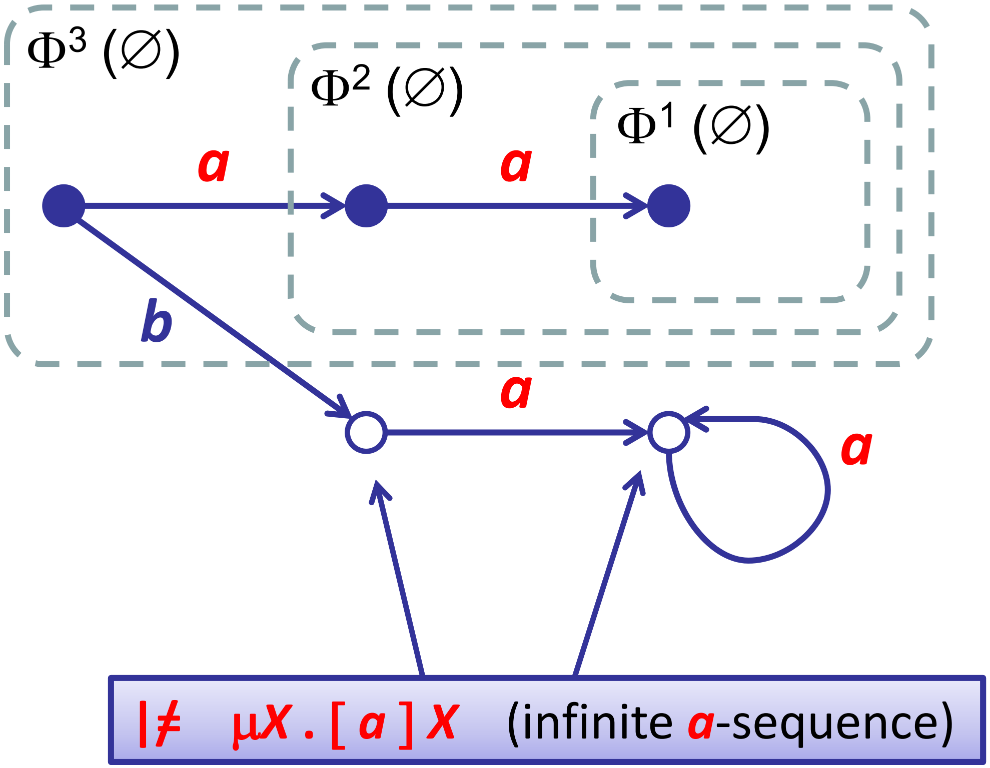
Exercise: absorption

- Show the statement below (where φ is a modal formula in PNF)
  - $\mu X \,.\, X \vee \varphi\,(X) \;=\; \mu X \,.\, \varphi\,(X)$

(Hint: by induction on *k*, as for the monotonicity exercise.)

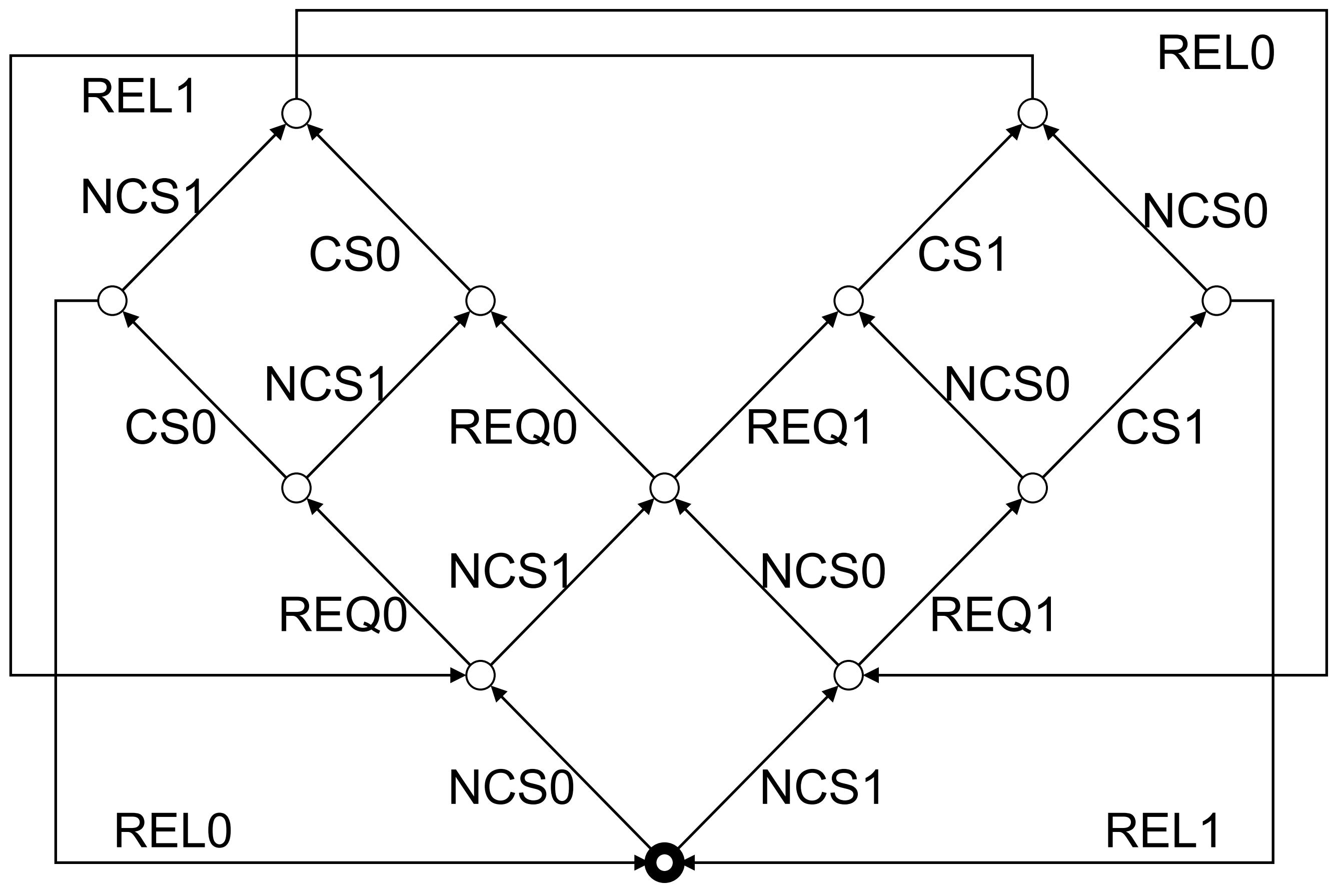
Exercise: fixed point semantics

- Evaluate the formula: $\mu X \,.\, [\, a \,]\, X$
  - $\Phi\,(U) = [[\,[\,a\,]\,X\,]]\,[\,U / X\,] = \{\, s \in S \mid \forall (s, a, s') \in T \,.\, s' \in U \,\}$



Exercise: fixed point semantics

Evaluate the formula: $\mu X \,.\, \langle\, CS_0 \,\rangle\, \mathbf{true} \vee ([\, NCS_0 \,]\, \mathbf{false} \wedge \langle\, \mathbf{true} \,\rangle\, X\,)$



Fair execution

- Fair execution of an action a:

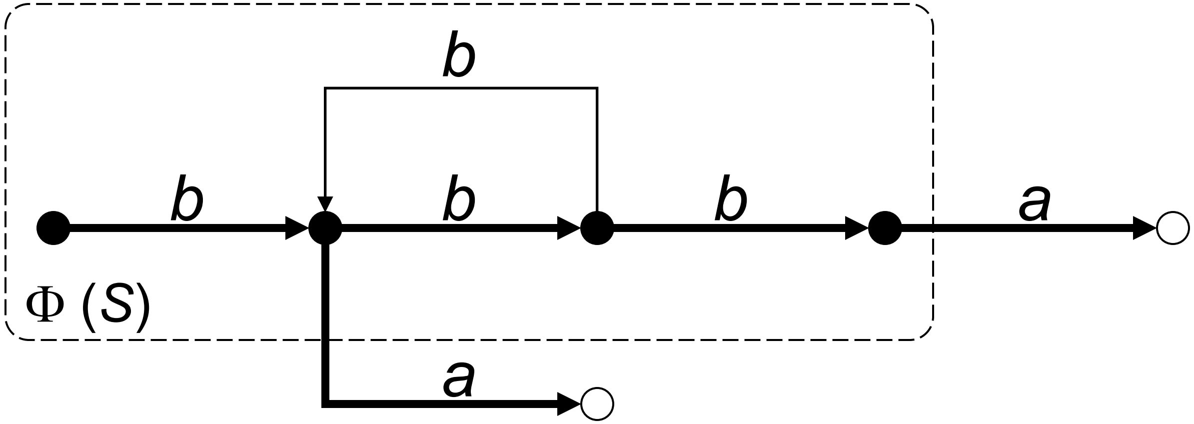
$$\text{fair}\ (a) = [\ (\neg a)^*\ ]\ \langle\ \text{true}^*.\ a\ \rangle\ \text{true}$$

$$= \nu X\ .\ \langle\ \text{true}^*.\ a\ \rangle\ \text{true} \wedge [\ \neg a\ ]\ X$$

- Associated functional:

$$\Phi\ (U) = [[\ \langle\ \text{true}^*.\ a\ \rangle\ \text{true} \wedge [\ \neg a\ ]\ X\ ]]\ \ [\ U\ /\ X\ ]$$

- Evaluation on an LTS:



Exercise: fair execution

- Show the identity below
  - $[\ (\neg a)^*\ ]\ \langle\ \text{true}^*.\ a\ \rangle\ \text{true} = [\ (\neg a)^*\ ]\ \langle\ (\neg a)^*.\ a\ \rangle\ \text{true}$

Let φ_1 and φ_2 be the μ-calculus encodings of the diamond modalities:

$\varphi_1 = \langle\ \text{true}^*.\ a\ \rangle\ \text{true} = \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ \text{true}\ \rangle\ X$

$\varphi_2 = \langle\ (\neg a)^*.\ a\ \rangle\ \text{true} = \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ \neg a\ \rangle\ X$

$\varphi_1 = \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ \text{true}\ \rangle\ X$ // by $a \vee \neg a = \text{true}$

$= \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ a \vee \neg a\ \rangle\ X$ // by distrib. of $\langle\ \rangle$ over $\vee$

$= \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ a\ \rangle\ X \vee \langle\ \neg a\ \rangle\ X$ // by monotonicity of $\langle\ \rangle$

$= \mu X\ .\ \langle\ a\ \rangle\ \text{true} \vee \langle\ \neg a\ \rangle\ X$

$= \varphi_2$