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

Radu Mateescu

Inria and LIG / Convecs

http://convecs.inria.fr

Action-based temporal logics

- Regular logics
- Fixed point logics

Regular logics

- They allow to reason about the regular execution sequences of an LTS
- Basic operators:
  - ***Regular formulas***

    two states are linked by a sequence whose concatenated actions form a word of a regular language
  - ***Modalities on sequences***

    from a state, some (all) outgoing regular transition sequences lead to certain states
- **Propositional Dynamic Logic** (PDL) [Fischer-Ladner-79]

Regular formulas

(syntax)

$\beta ::=$	α	one-step sequence
$\mid$	nil	empty sequence
$\mid$	$\beta_1 . \beta_2$	concatenation
$\mid$	$\beta_1 \mid \beta_2$	choice
$\mid$	$\beta_1{}^*$	iteration ($\geq$ 0 times)
$\mid$	$\beta_1{}^+$	iteration ($\geq$ 1 times)

- Some identities:

nil = false* $\beta^+ = \beta . \beta^*$

Regular formulas

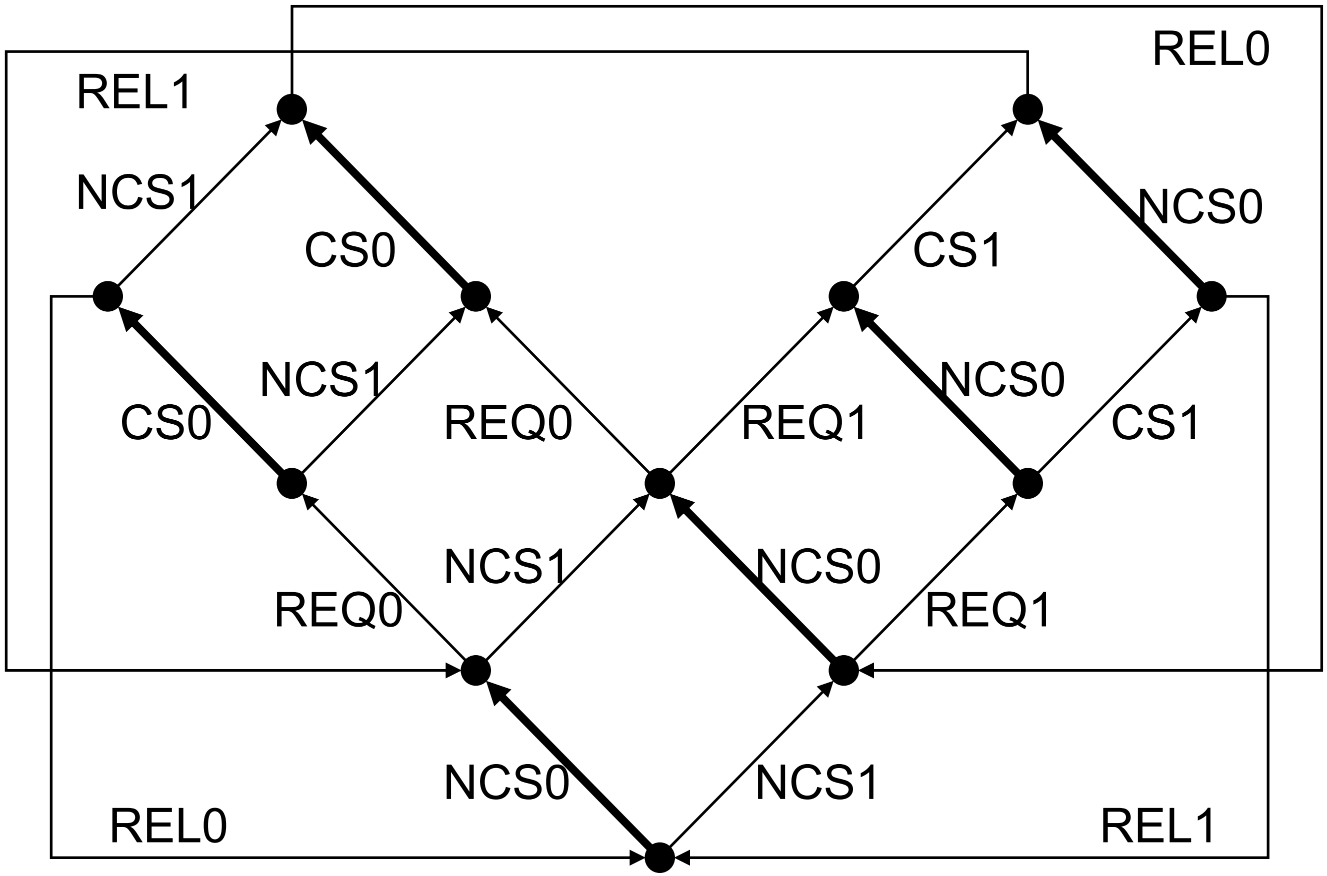
(semantics)

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

- $[[\, \alpha \,]] = \{ (s, s') \mid \exists a \in [[\, \alpha \,]] \,.\, (s, a, s') \in T \}$
- $[[\, \text{nil} \,]] = \{ (s, s) \mid s \in S \}$ (identity)
- $[[\, \beta_1 \,.\, \beta_2 \,]] = [[\, \beta_1 \,]] \circ [[\, \beta_2 \,]]$ (composition)
- $[[\, \beta_1 \mid \beta_2 \,]] = [[\, \beta_1 \,]] \cup [[\, \beta_2 \,]]$ (union)
- $[[\, \beta_1{}^* \,]] = [[\, \beta_1 \,]]^*$ (transitive reflexive closure)
- $[[\, \beta_1{}^+ \,]] = [[\, \beta_1 \,]]^+$ (transitive closure)

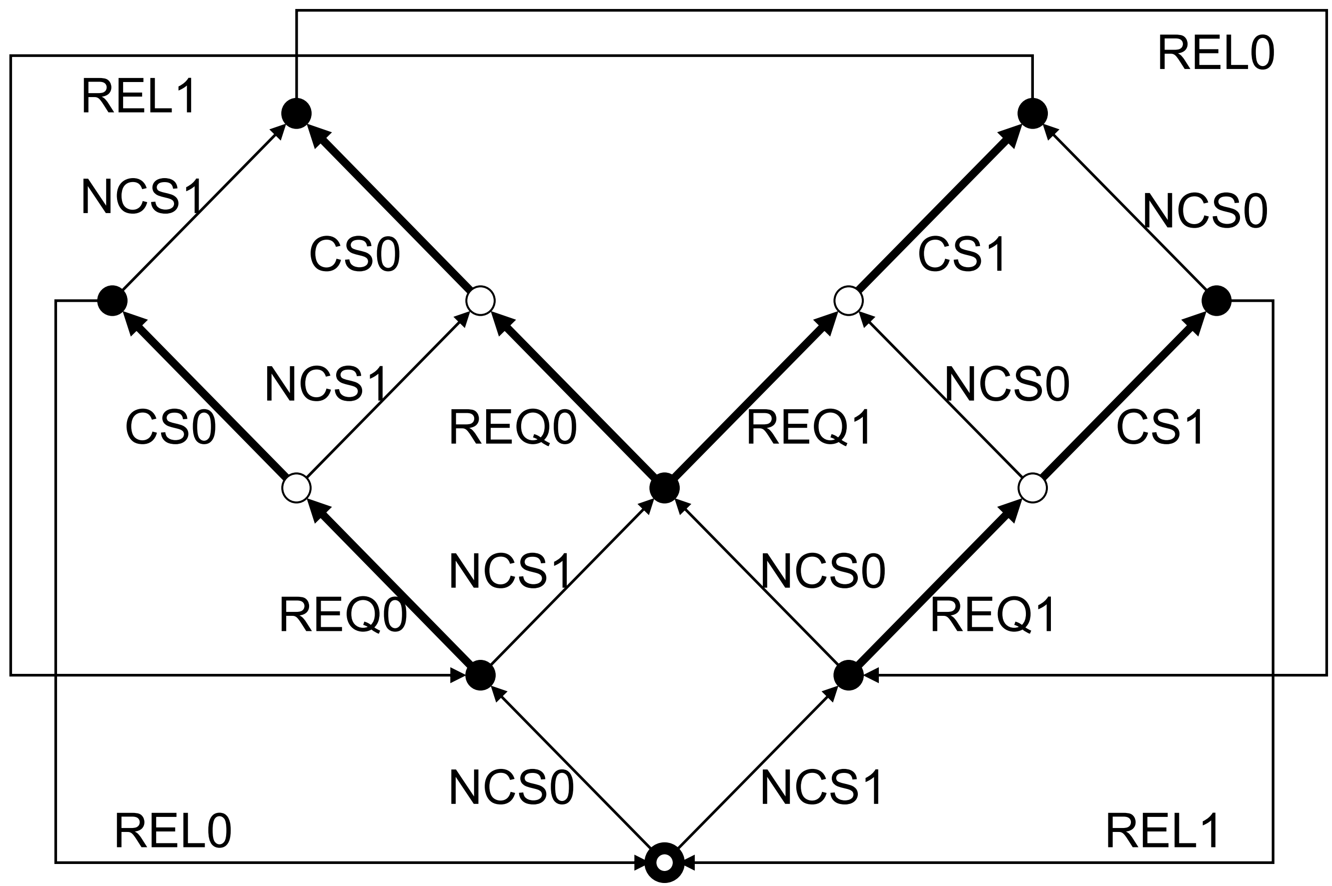
Example (1/3)

One-step sequences: $\mathbf{NCS_0 \vee CS_0}$



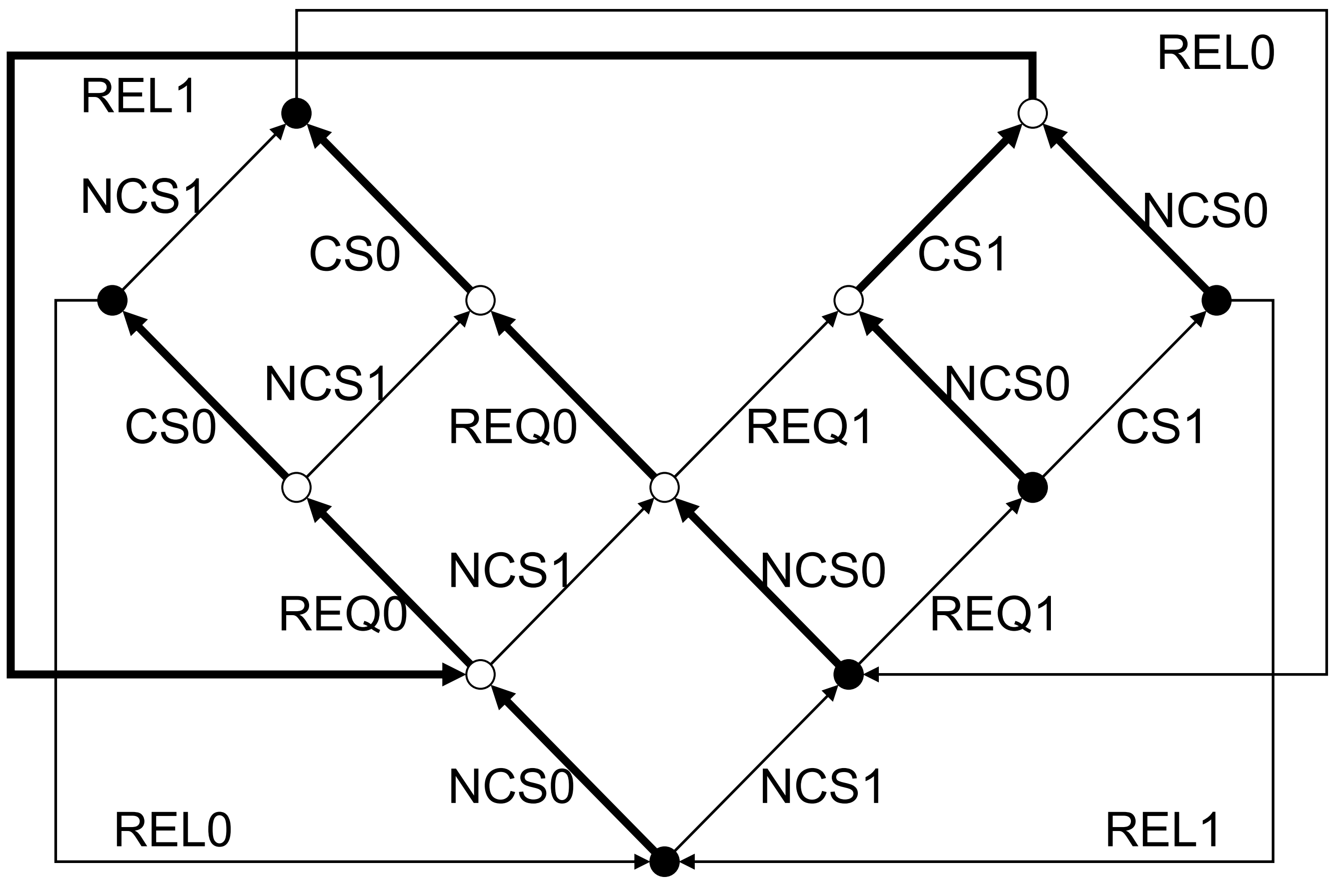
Example (2/3)

Alternative sequences: **$(REQ_0 \,.\, CS_0) \mid (REQ_1 \,.\, CS_1)$**



Example (3/3)

Sequences with repetition: **$NCS_0 \,.\, (\neg NCS_1)^* \,.\, CS_0$**



PDL logic

(syntax)

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

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

PDL logic

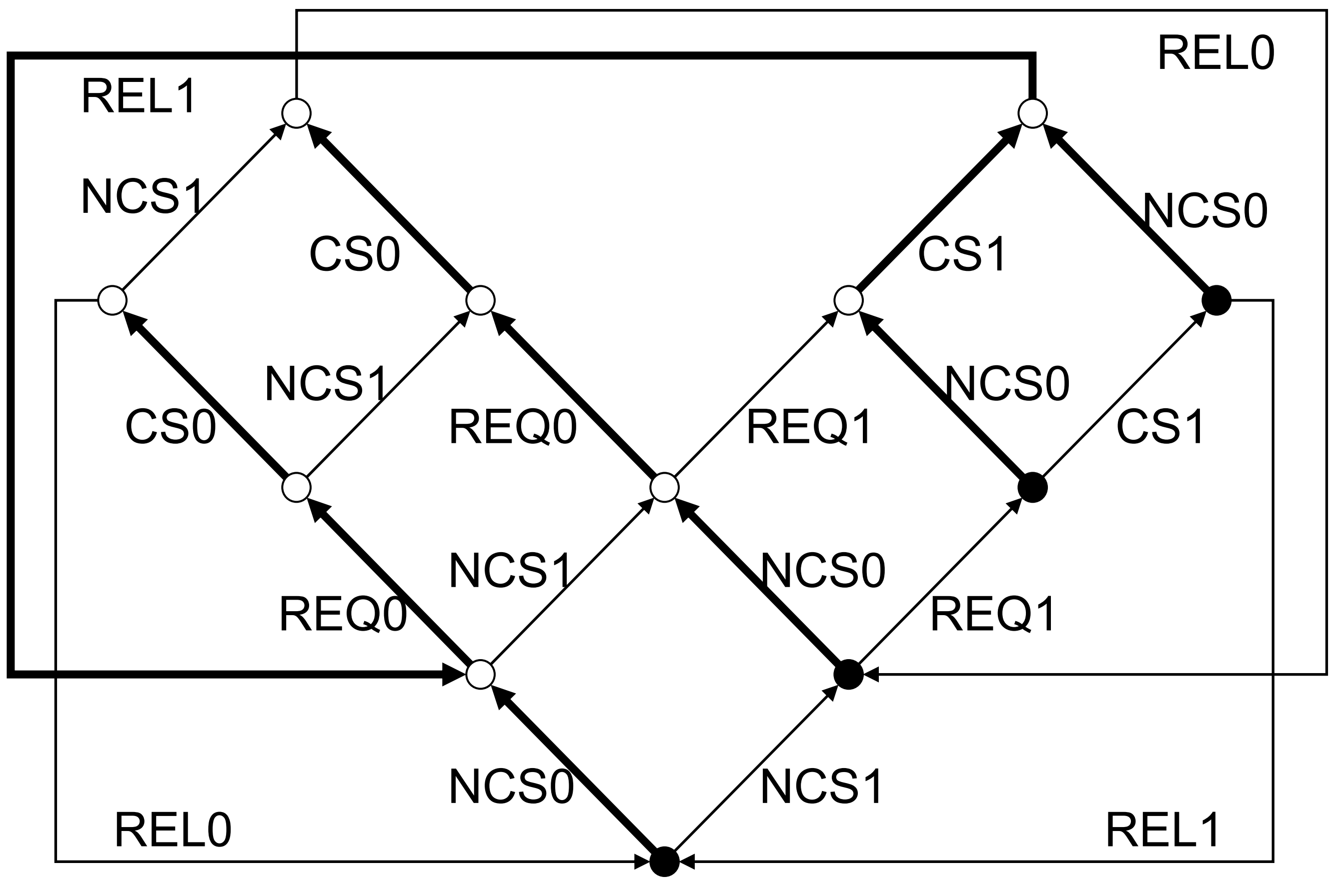
(semantics)

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

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

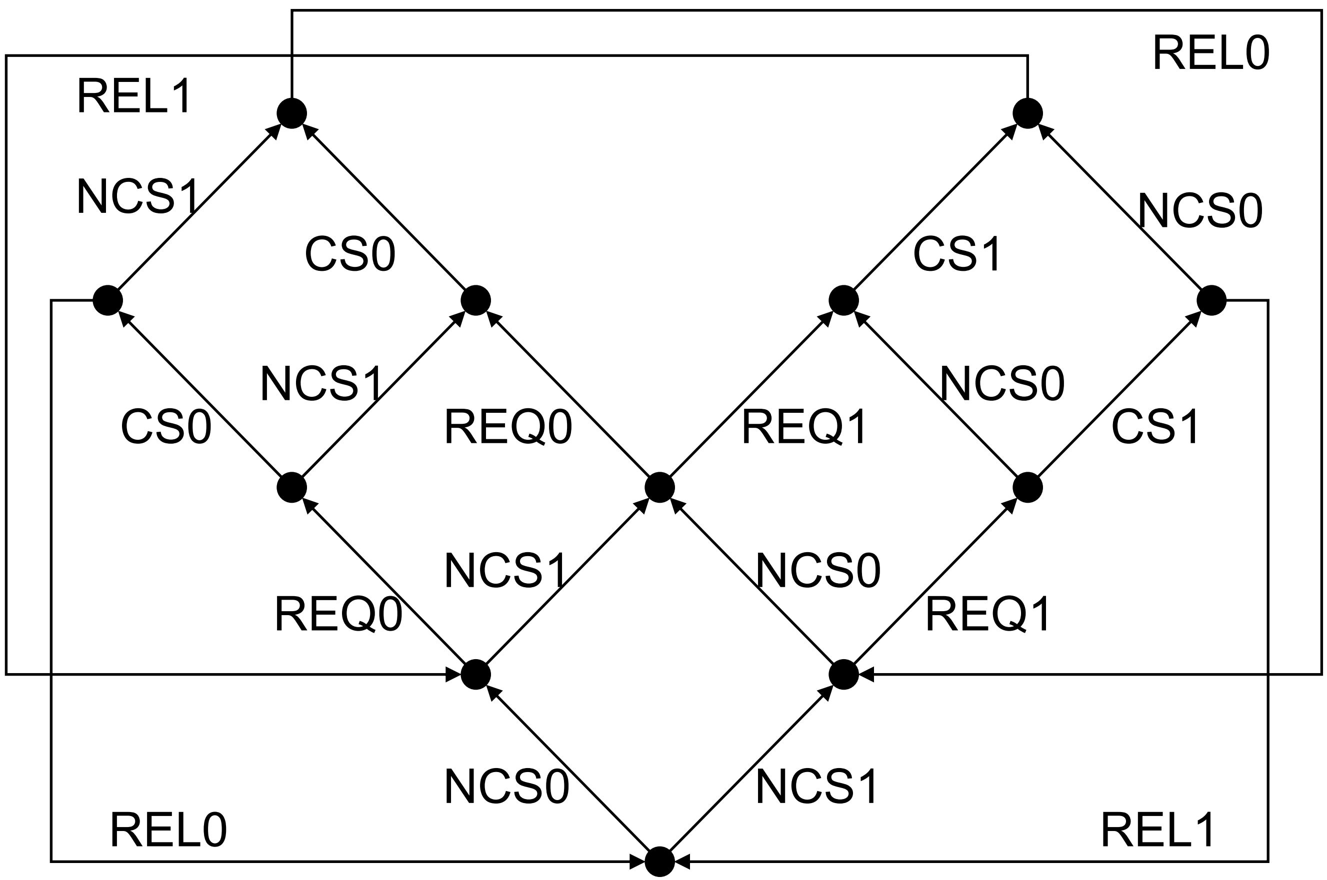
Example (1/2)

Potential reachability of critical section: $\langle\, \mathbf{NCS_0\ .\ true^*\ .\ CS_0} \,\rangle\, \mathbf{true}$



Example (2/2)

Mutual exclusion: **[CS_0 . ($\neg REL_0$)* . CS_1] false**

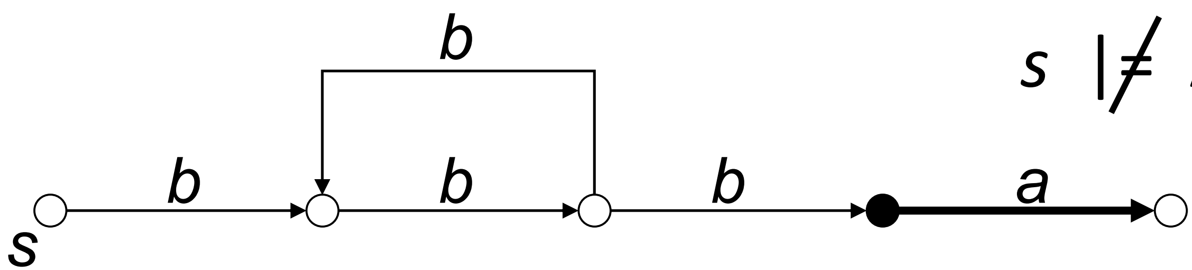


Some identities

- Distributivity of regular operators over $\langle\ \rangle$ and $[\ ]$:
  - $\langle \beta_1 . \beta_2 \rangle \varphi = \langle \beta_1 \rangle \langle \beta_2 \rangle \varphi$
  - $\langle \beta_1 \mid \beta_2 \rangle \varphi = \langle \beta_1 \rangle \varphi \vee \langle \beta_2 \rangle \varphi$
  - $\langle \beta^* \rangle \varphi = \varphi \vee \langle \beta \rangle \langle \beta^* \rangle \varphi$
  - $[\beta_1 . \beta_2] \varphi = [\beta_1] [\beta_2] \varphi$
  - $[\beta_1 \mid \beta_2] \varphi = [\beta_1] \varphi \wedge [\beta_2] \varphi$
  - $[\beta^*] \varphi = \varphi \wedge [\beta] [\beta^*] \varphi$
- Potentiality and invariance operators of ACTL:
  - $EF_\alpha\, \varphi = \langle \alpha^* \rangle \varphi$
  - $AG_\alpha\, \varphi = [\alpha^*] \varphi$

Fairness properties

- Problem: from the initial state of the LTS, there is no inevitable execution of action CS_0, so process P_1 can enter its critical section indefinitely often



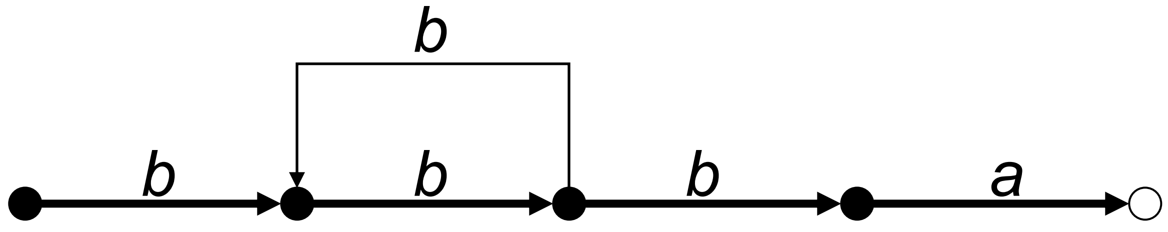
$s \not\models \mathrm{A}\ [\ \mathrm{true}_{\mathrm{true}}\ \mathrm{U}_{a}\ \mathrm{true}\ ]$

- ***Fair execution*** of an action *a*: from a state, all transition sequences that do not cycle indefinitely contain action *a*
- Action-based counterpart of the ***fair reachability of predicates*** [Queille-Sifakis-82]

Fair execution

- Fair execution of an action *a* expressed in PDL:

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

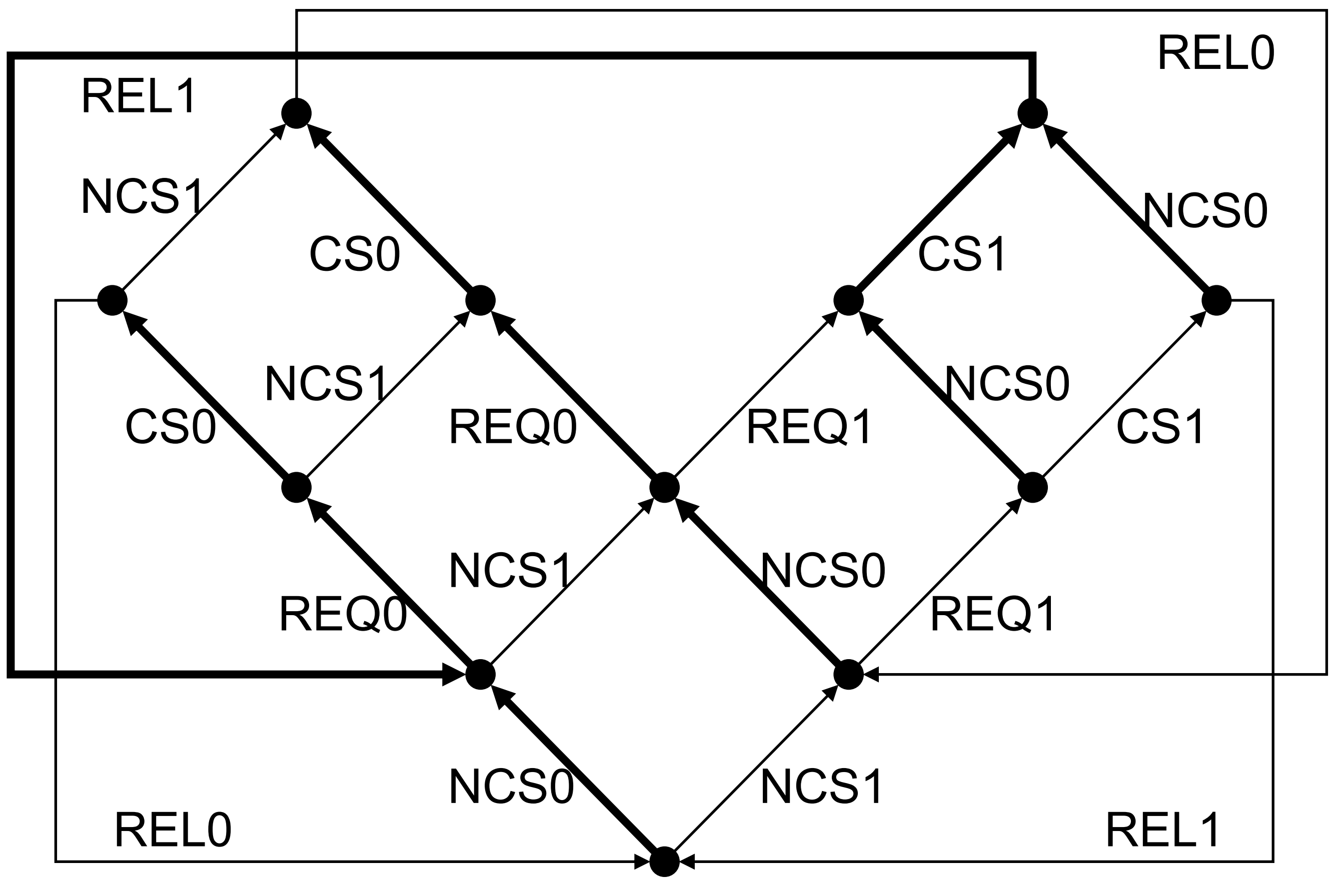


- Equivalent formulation in ACTL:

$$\text{fair}\,(a) \;=\; \text{AG}_{\neg a}\, \text{EF}_{\text{tt}}\, \langle\, a \,\rangle\, \text{true}$$

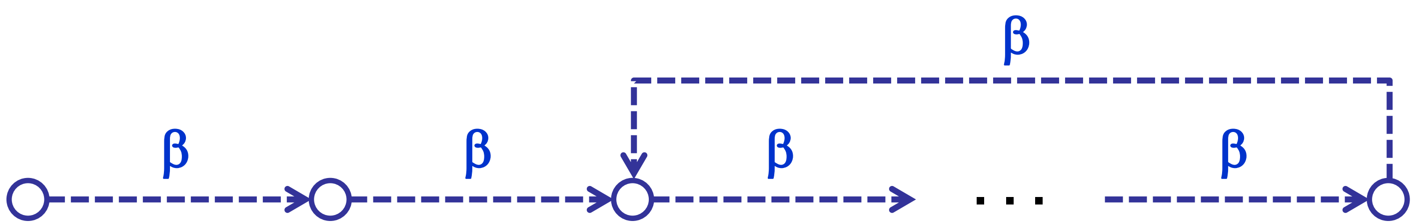
Example

Fair execution of critical section: $[\ (\neg CS_0)^*\ ]\ \langle\ true^*.\ CS_0\ \rangle\ true$



Branching-time vs regular logics

- ACTL and PDL have uncomparable expressiveness:
  - A [$\text{true}_{\text{true}}$ U_a true] $\notin$ PDL (inevitable execution of *a*)
  - $\langle$ (*a** . *b*)* . *c* $\rangle$ true $\notin$ ACTL (nested iterations)
- The extension PDL-Δ (PDL with looping) subsumes ACTL:
  - < β > @ infinite looping operator (infinite repetition of β)



  - A [$\text{true}_{\text{true}}$ U_a true] = $\neg$ (< ($\neg a$)* > *deadlock* $\vee$ < $\neg a$ > @)

Regular logics

(summary)

- They allow a direct and natural description of regular execution sequences in LTSs

- More intuitive description of safety properties:
  - Mutual exclusion:

    $[\ CS_0\ ]\ AG_{\neg REL0}\ [\ CS_1\ ]$ false $=$ (in ACTL)

    $[\ CS_0\ .\ (\neg REL_0)^*\ .\ CS_1\ ]$ false (in PDL)

- But:
  - Not sufficiently powerful to express inevitability operators (expressiveness uncomparable with branching-time logics)

Fixed point logics

- Very expressive logics ("temporal logic assembly languages") allowing to characterize finite or infinite tree-like patterns in LTSs
- Basic temporal operators:
  - ***Minimal fixed point*** (μ)

    "recursive function" defined over the LTS:
    finite execution trees going out of a state
  - ***Maximal fixed point*** (ν)

    dual of the minimal fixed point operator:
    infinite execution trees going out of a state
- **Modal mu-calculus** [Kozen-83,Stirling-01]

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:
  - $\neg\, \text{false} = \text{true}$
  - $\neg\, (\varphi_1 \vee \varphi_2) = \neg\, \varphi_1 \wedge \neg\, \varphi_2$
  - $\neg \langle\, \alpha \,\rangle\ \varphi = [\, \alpha \,] \neg\, \varphi$
  - $\neg\, \mu X \,.\, \varphi\, (X) = \nu X \,.\, \neg\, \varphi\, (\neg\, X)$

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

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

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

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

Minimal fixed point

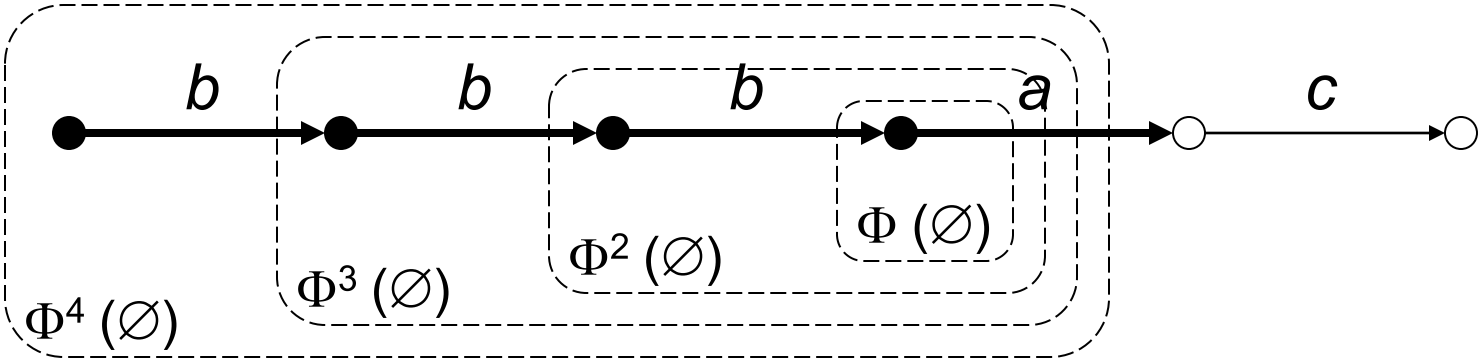
- Potential reachability of an action *a* (existence of a sequence leading to a transition labeled by *a*):

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

- Associated functional:

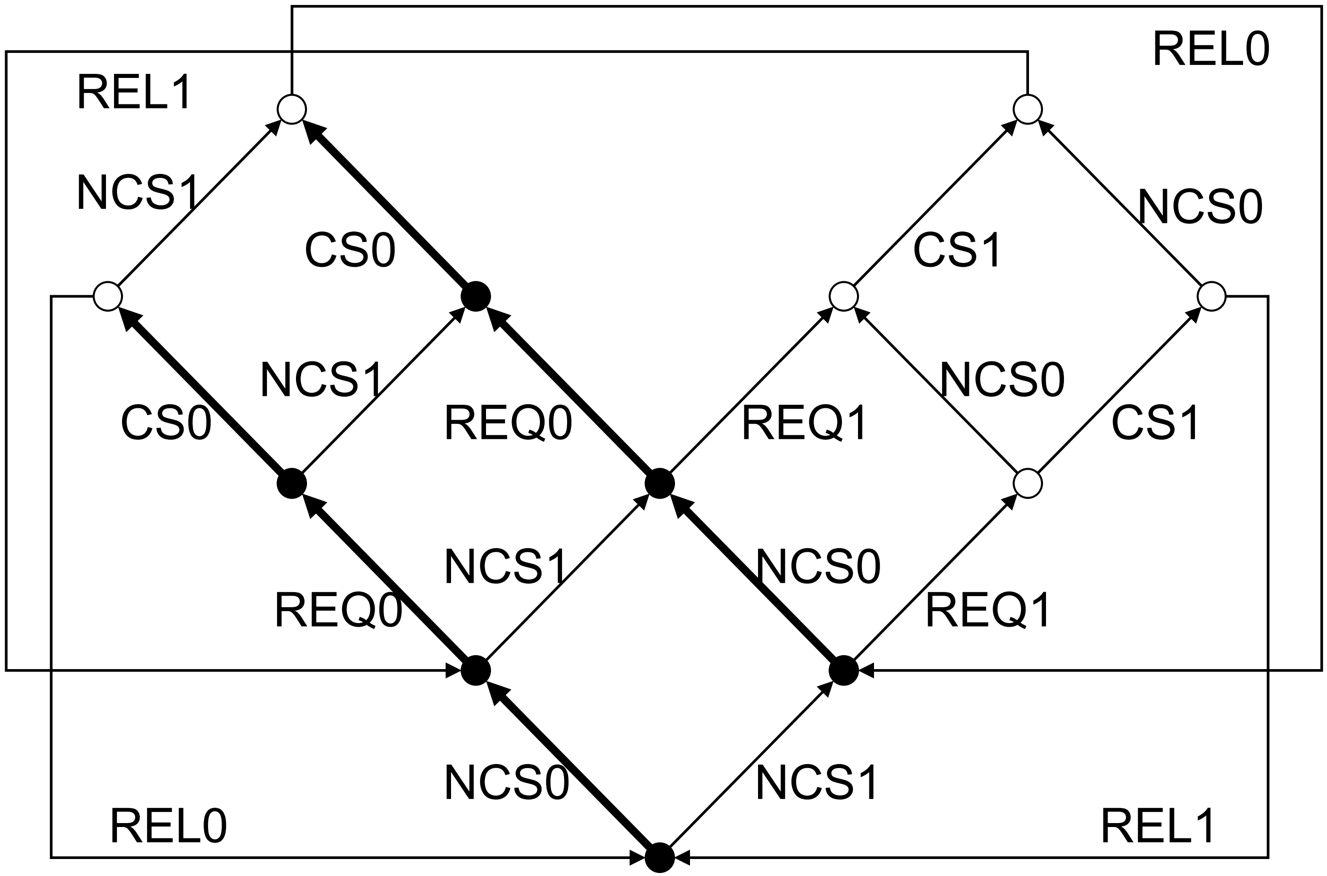
$$\Phi\ (U) = [[\, \langle\, a \,\rangle\, \text{true} \vee \langle\, \text{true} \,\rangle\, X \,]]\ \ [\, U \,/\, X \,]$$

- Evaluation on an LTS:



Example

Potential reachability: $\mu X \,.\, \langle\, CS_0 \,\rangle\, \mathbf{true} \vee \langle\, \neg(REL_1 \vee REL_0)\,\rangle\, X$



Maximal fixed point

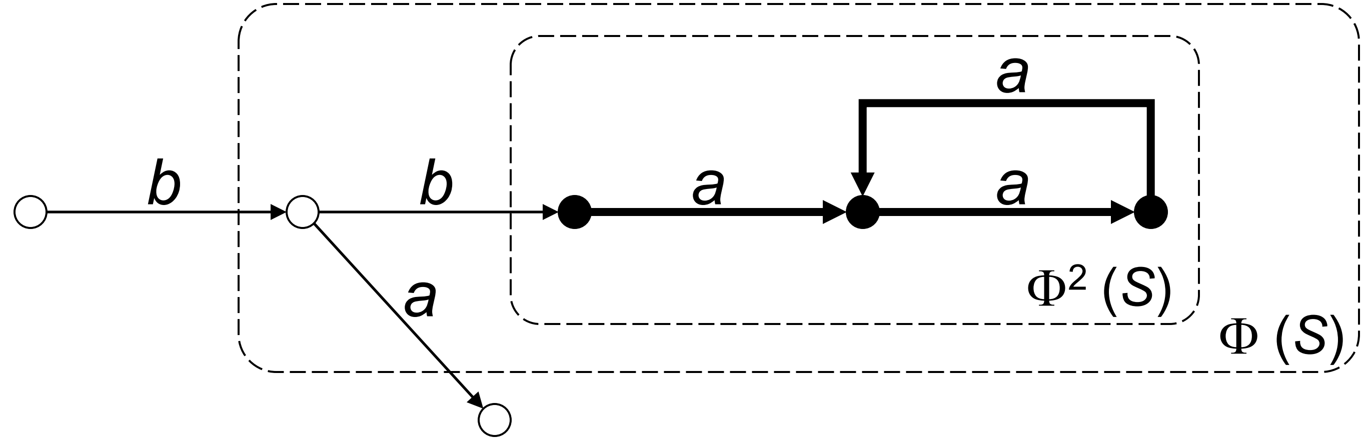
- Infinite repetition of an action *a* (existence of a cycle containing only transitions labeled by *a*):

  $\nu X \,.\, \langle\, a \,\rangle\, X$

- Associated functional:

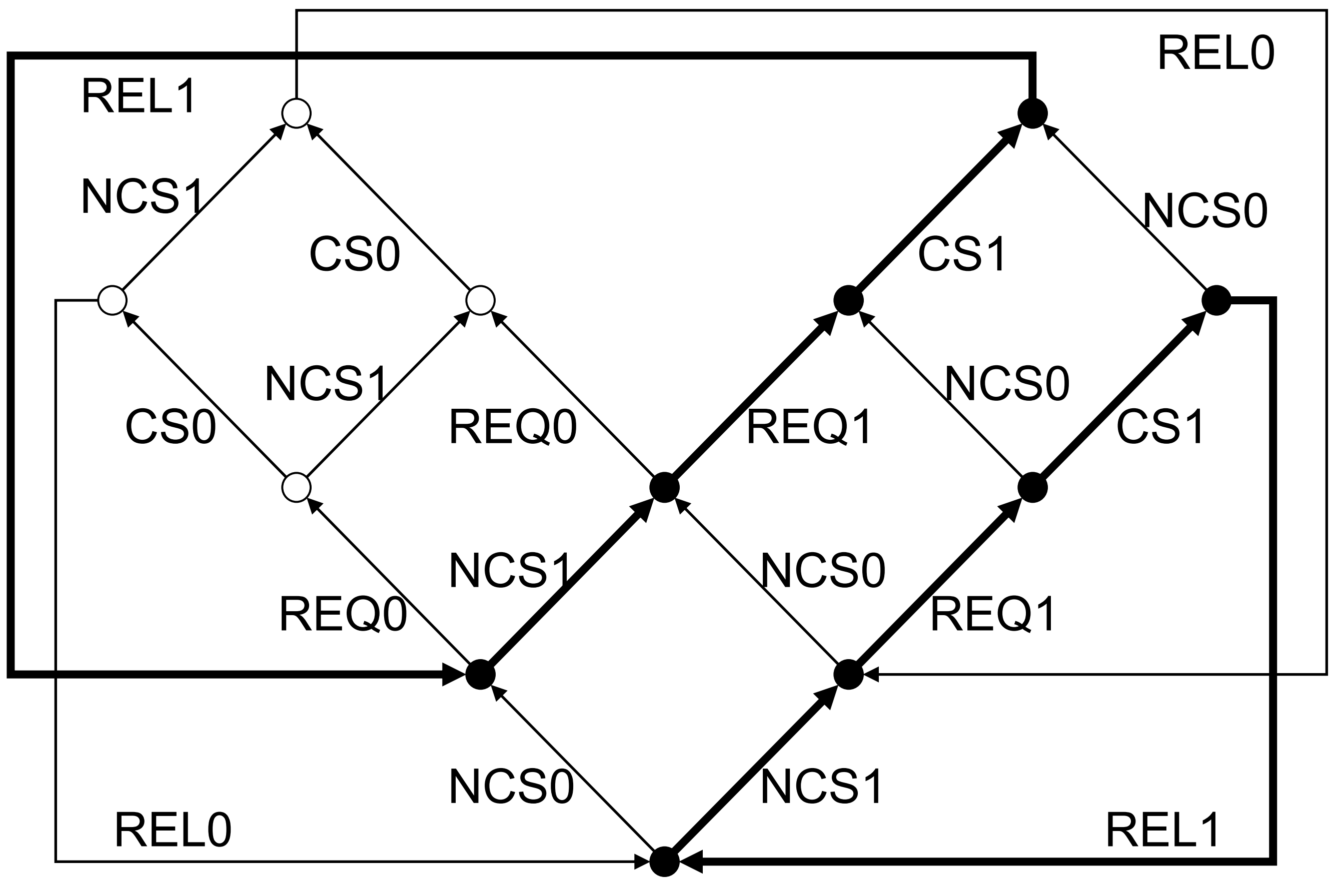
  $\Phi\ (U) = [[\,\langle\, a \,\rangle\, X\,]]\ \ [\, U \,/\, X\,]$

- Evaluation on an LTS:



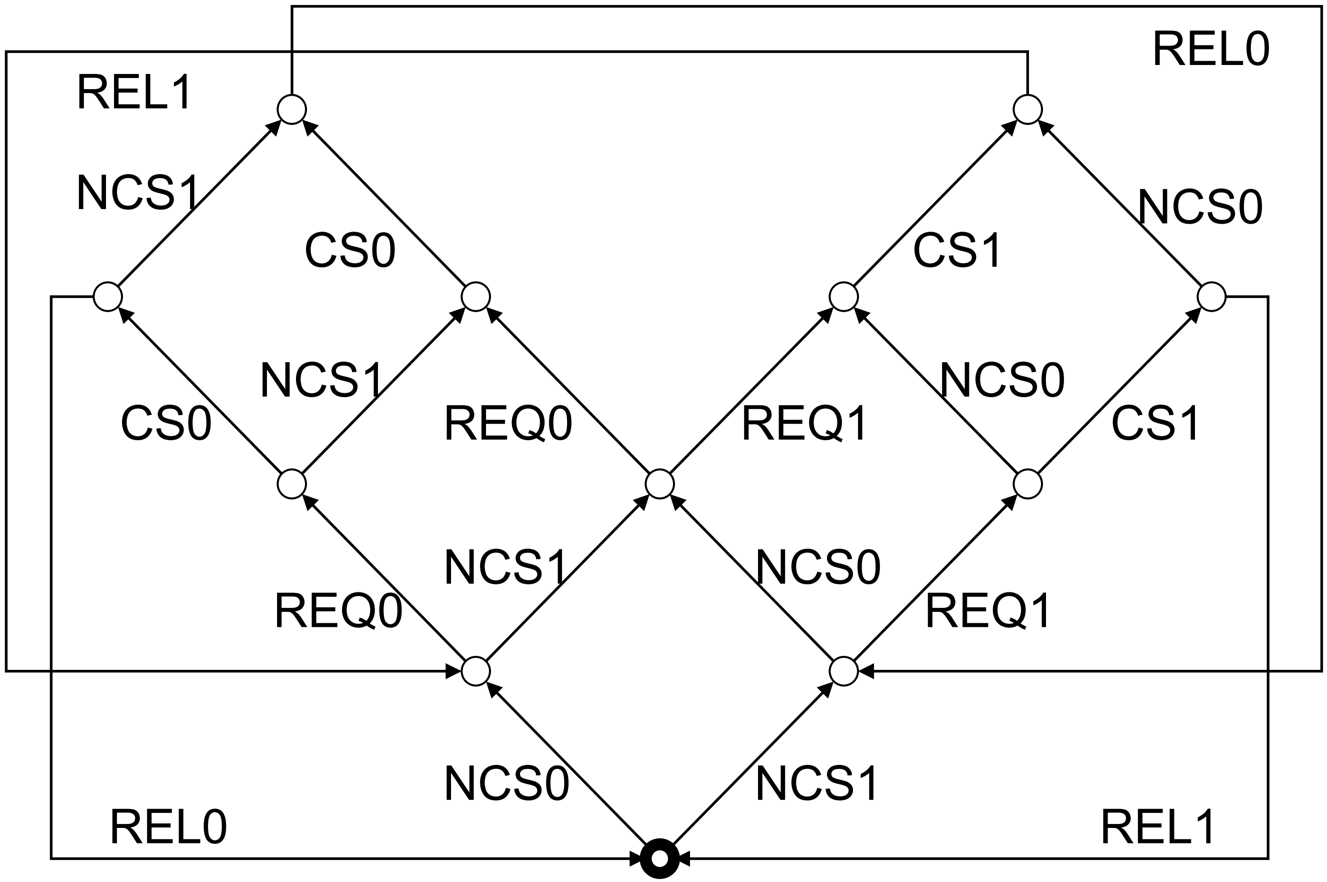
Example

Infinite repetition: $\nu X \,.\, \langle\, NCS_1 \vee REQ_1 \vee CS_1 \vee REL_1 \,\rangle\, X$



Exercise: semantics

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



Encodings of temporal operators

- Some ACTL operators:
  - $E\,[\,\varphi_{1\alpha 1}\,U_{\alpha 2}\,\varphi_2\,] = \mu X\,.\,\varphi_1 \wedge (\langle\,\alpha_2\,\rangle\,\varphi_2 \vee \langle\,\alpha_1\,\rangle\,X)$
  - $A\,[\,\varphi_{1\alpha 1}\,U_{\alpha 2}\,\varphi_2\,] = \mu X\,.\,\varphi_1 \wedge \langle\,\text{true}\,\rangle\,\text{true} \wedge [\neg(\alpha_1 \vee \alpha_2)\,]\,\text{false}$
    $\wedge\,[\,\neg\alpha_1 \wedge \alpha_2\,]\,\varphi_2 \wedge [\,\neg\alpha_2\,]\,X \wedge [\,\alpha_1 \wedge \alpha_2\,]\,(\varphi_2 \vee X)$
  - $EF_\alpha\,\varphi = \mu X\,.\,\varphi \vee \langle\,\alpha\,\rangle\,X$
  - $AF_\alpha\,\varphi = \mu X\,.\,\varphi \vee (\langle\,\text{true}\,\rangle\,\text{true} \wedge [\,\neg\alpha\,]\,\text{false} \wedge [\,\alpha\,]\,X)$

- PDL iteration modalities:
  - $\langle\,\beta^*\,\rangle\,\varphi = \mu X\,.\,\varphi \vee \langle\,\beta\,\rangle\,X$
  - $[\,\beta^*\,]\,\varphi = \nu X\,.\,\varphi \wedge [\,\beta\,]\,X$

Regular modalities vs fixed points (conciseness)

- PDL:

$$\langle \text{send} . (\text{true}^*. \text{err})^* . \text{recv} \rangle \text{true}$$

- Mu-calculus:

$$\langle \text{send} \rangle \langle (\text{true}^*. \text{err})^* \rangle \langle \text{recv} \rangle \text{true}$$

$$= \langle \text{send} \rangle \mu X . (\langle \text{recv} \rangle \text{true} \vee \langle \text{true}^*. \text{err} \rangle X)$$

$$= \langle \text{send} \rangle \mu X . (\langle \text{recv} \rangle \text{true} \vee \langle \text{true}^*. \text{err} \rangle X)$$

$$= \langle \text{send} \rangle \mu X . (\langle \text{recv} \rangle \text{true} \vee \mu Y . (\langle \text{err} \rangle X \vee \langle \text{true} \rangle Y))$$

Inevitable reachability

- Inevitable reachability of an action *a*:

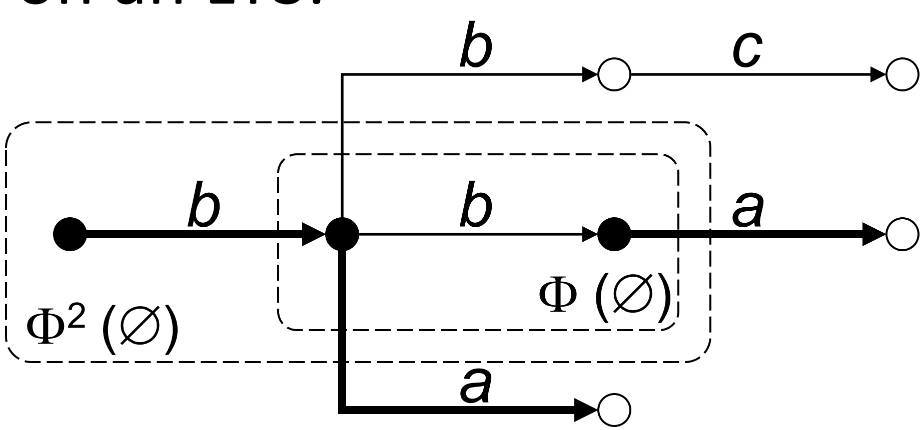
$$\text{access}\,(a) = AF_{tt}\,\langle\, a \,\rangle\,\text{true} =$$

$$\mu X\,.\,\langle\, a \,\rangle\,\text{true} \vee (\langle\,\text{true}\,\rangle\,\text{true} \wedge [\,\text{true}\,]\,X\,)$$

- Associated functional:

$$\Phi\,(U) = [[\,\langle\, a \,\rangle\,\text{true} \vee (\langle\,\text{true}\,\rangle\,\text{true} \wedge [\,\text{true}\,]\,X\,)\,]]\;[\,U\,/\,X\,]$$

- Evaluation on an LTS:



Inevitable execution

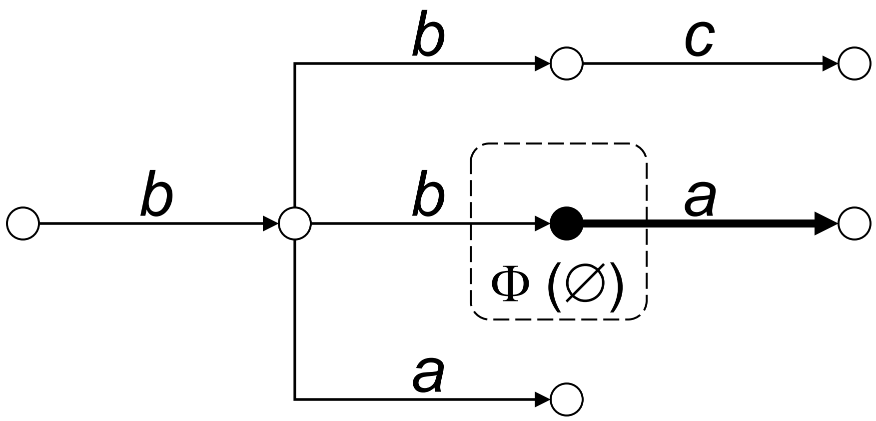
- Inevitable execution of an action *a*:

$$\text{inev}(a) = \mu X \,.\, \langle \text{true} \rangle \text{true} \wedge [\neg a]\, X$$

- Associated functional:

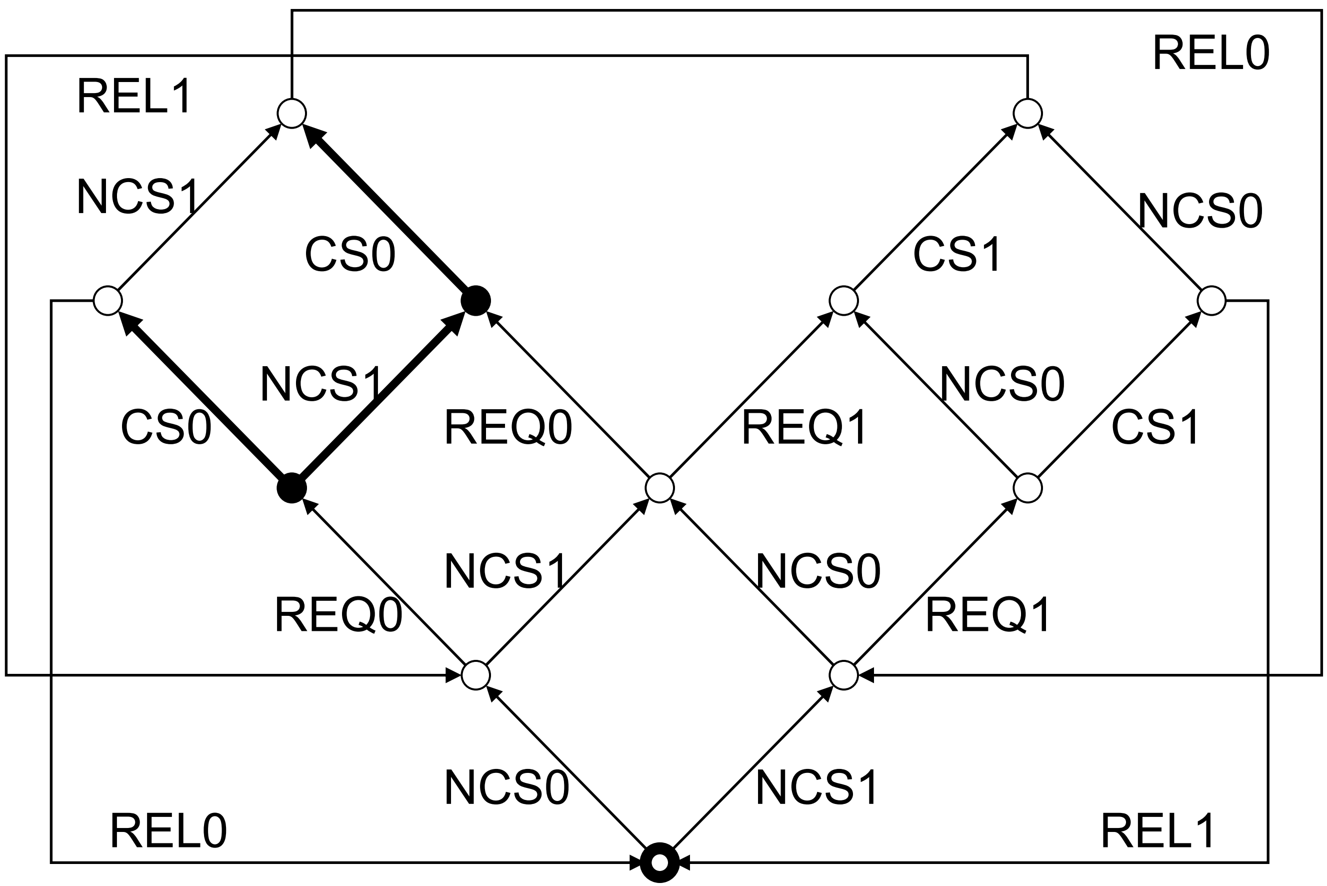
$$\Phi(U) = [[\, \langle \text{true} \rangle \text{true} \wedge [\neg a]\, X \,]] \;\; [U / X]$$

- Evaluation on an LTS:



Example

Inevitable execution: $\mu X . \langle \text{true} \rangle \text{true} \wedge [\neg CS_0] X$



Fair execution

- Fair execution of an action a:

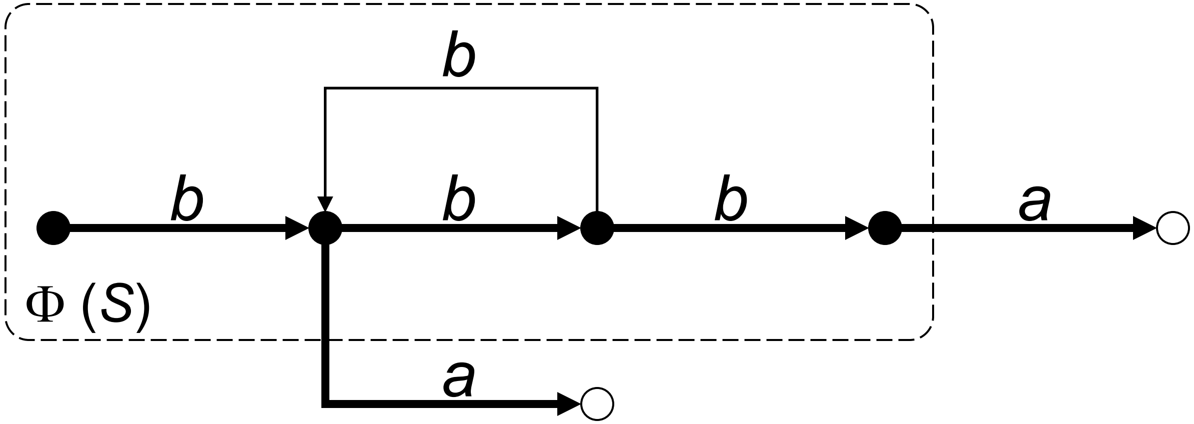
$$\text{fair}\,(a) = [\,(\neg a)^*\,]\,\langle\, \text{true}^*.\, a\,\rangle\,\text{true}$$

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

- Associated functional:

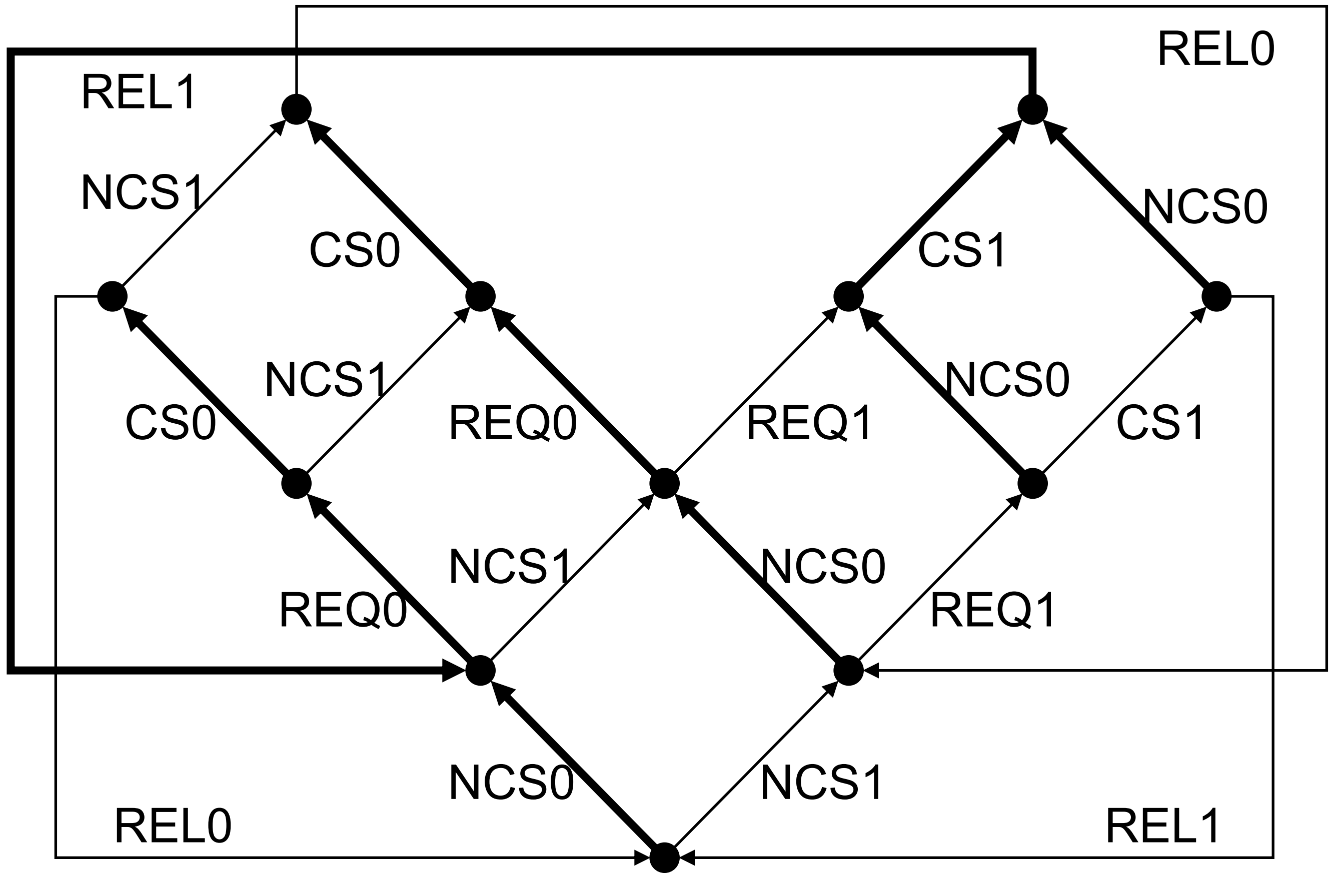
$$\Phi\,(U) = [[\,\langle\, \text{true}^*.\, a\,\rangle\,\text{true} \wedge [\,\neg a\,]\,X\,]]\;\;[\,U\,/\,X\,]$$

- Evaluation on an LTS:



Example

Fair execution: $[\ (\neg CS_0)^*\ ]\ \langle\ true^*.\ CS_0\ \rangle\ true$



Fixed point logics

(summary)

- They allow to encode virtually all TL proposed in the literature
- Expressive power obtained by *nesting* the fixed point operators:

$$\langle\, (a \,.\, b^*)^* \,.\, c \,\rangle \text{ true} =$$

$$\mu X \,.\, \langle\, c \,\rangle \text{ true} \vee \langle\, a \,\rangle\, \mu Y \,.\, (X \vee \langle\, b \,\rangle\, Y\,)$$

- Alternation depth of a formula: degree of mutual recursion between μ and ν fixed points

  Example of alternation depth 2 formula:

$$\nu X \,.\, \langle\, a^* . \, b \,\rangle\, X \;=\; \nu X \,.\, \mu Y \,.\, \langle\, b \,\rangle\, X \vee \langle\, a \,\rangle\, Y$$

Some verification tools

(for action-based logics)

- CWB (Edinburgh)

  and

- Concurrency Factory (State University of New York)
  - Modal μ-calculus (fixed point operators)

- UMC (University of Pisa, Italy)
  - μ-ACTL (modal μ-calculus combined with ACTL)

- CADP (Inria Grenoble - Rhône-Alpes / CONVECS)
  - Regular alternation-free μ-calculus (PDL modalities and fixed point operators)