universität innsbruck

26S lecture 10

Logic

Luca Campa Philipp Dablander Aaron Groß Aart Middeldorp
Alexander Montag Johannes Niederhauser Vera Schmitt

Outline

1. **Summary of Previous Lecture**
2. **Symbolic Model Checking**
3. **Intermezzo**
4. **Linear–Time Temporal Logic (LTL)**
5. **Further Reading**

Definitions

boolean function f is

- **monotone** if $f(x_1, \ldots, x_n) \leqslant f(y_1, \ldots, y_n)$ for all $x_1 \leqslant y_1, \ldots, x_n \leqslant y_n$
- **self–dual** if $f(x_1, \ldots, x_n) = \overline{f(\overline{x}_1, \ldots, \overline{x}_n)}$
- **affine** if $f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n$ for some $c_0, \ldots, c_n \in \{0, 1\}$

Theorem (Post's Adequacy Theorem)

set X of boolean functions is adequate if and only if following conditions hold:

1. $\exists\, f_1 \in X$ such that $f_1(0, \ldots, 0) \neq 0$
2. $\exists\, f_2 \in X$ such that $f_2(1, \ldots, 1) \neq 1$
3. $\exists\, f_3 \in X$ which is not monotone
4. $\exists\, f_4 \in X$ which is not self–dual
5. $\exists\, f_5 \in X$ which is not affine

Definitions

- CTL (computation tree logic) formulas are built from atoms, logical connectives, and temporal connectives AX, EX, AF, EF, AG, EG, AU, EU according to BNF grammar

$$\varphi \ ::= \bot \mid \top \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid (\mathsf{AX}\,\varphi) \mid (\mathsf{EX}\,\varphi) \mid$$
$$(\mathsf{AF}\,\varphi) \mid (\mathsf{EF}\,\varphi) \mid (\mathsf{AG}\,\varphi) \mid (\mathsf{EG}\,\varphi) \mid \mathsf{A}[\varphi\,\mathsf{U}\,\varphi] \mid \mathsf{E}[\varphi\,\mathsf{U}\,\varphi]$$

- transition system (model) is triple $\mathcal{M} = (S, \to, L)$ with
  - set of states S
  - transition relation $\to \subseteq S \times S$ such that $\forall\, s \in S \ \ \exists\, t \in S$ with $s \to t$ ("no deadlock")
  - labelling function $L \colon S \to \mathcal{P}(\text{atoms})$
- satisfaction $\mathcal{M}, s \vDash \varphi$ of CTL formula φ in state $s \in S$ of model $\mathcal{M} = (S, \to, L)$ is defined by induction on φ

Definition

CTL formulas φ and ψ are semantically equivalent $(\varphi \equiv \psi)$ if

$$\mathcal{M}, s \vDash \varphi \iff \mathcal{M}, s \vDash \psi$$

for all models $\mathcal{M} = (S, \rightarrow, L)$ and states $s \in S$

Theorem

$$\neg\,\mathsf{AF}\,\varphi \equiv \mathsf{EG}\,\neg\varphi \qquad \mathsf{AF}\,\varphi \equiv \mathsf{A}[\top\,\mathsf{U}\,\varphi]$$

$$\neg\,\mathsf{EF}\,\varphi \equiv \mathsf{AG}\,\neg\varphi \qquad \mathsf{EF}\,\varphi \equiv \mathsf{E}[\top\,\mathsf{U}\,\varphi]$$

$$\neg\,\mathsf{AX}\,\varphi \equiv \mathsf{EX}\,\neg\varphi \qquad \mathsf{A}[\varphi\,\mathsf{U}\,\psi] \equiv \neg(\mathsf{E}[\neg\psi\,\mathsf{U}\,(\neg\varphi \wedge \neg\psi)] \vee \mathsf{EG}\,\neg\psi)$$

Theorem

satisfaction of CTL formulas in finite models is decidable

CTL Model Checking Algorithm

input: • model $\mathcal{M} = (S, \rightarrow, L)$ and CTL formula φ

output: • $\{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

label each state $s \in S$ by those subformulas of φ that are satisfied in s

p label s $\iff$ $p \in L(s)$

$\neg\varphi$ label s $\iff$ s is not labelled with φ

$\varphi \wedge \psi$ label s $\iff$ s is labelled with both φ and ψ

$\mathsf{EX}\,\varphi$ label s $\iff$ t is labelled with φ for some t with $s \rightarrow t$

$\mathsf{EG}\,\varphi$
① label every s that is labelled with φ
② remove label from s $\iff$ t is not labelled with $\mathsf{EG}\,\varphi$ for all t with $s \rightarrow t$
③ repeat ② until no change

$\mathsf{E}[\varphi\,\mathsf{U}\,\psi]$ label s $\iff$
① s is labelled with ψ
② s is labelled with φ and t with $\mathsf{E}[\varphi\,\mathsf{U}\,\psi]$ for some t with $s \rightarrow t$
③ repeat ② until no change

Part I: Propositional Logic

algebraic normal forms, binary decision diagrams, conjunctive normal forms, DPLL, Horn formulas, natural deduction, Post's adequacy theorem, resolution, SAT, semantics, sorting networks, soundness and completeness, syntax, Tseitin's transformation

Part II: Predicate Logic

natural deduction, quantifier equivalences, resolution, semantics, Skolemization, syntax, undecidability, unification

Part III: Model Checking

adequacy, branching–time temporal logic, CTL^*, fairness, linear–time temporal logic, model checking algorithms, symbolic model checking

Part I: Propositional Logic

algebraic normal forms, binary decision diagrams, conjunctive normal forms, DPLL, Horn formulas, natural deduction, Post's adequacy theorem, resolution, SAT, semantics, sorting networks, soundness and completeness, syntax, Tseitin's transformation

Part II: Predicate Logic

natural deduction, quantifier equivalences, resolution, semantics, Skolemization, syntax, undecidability, unification

Part III: Model Checking

adequacy, branching–time temporal logic, CTL*, fairness, linear–time temporal logic, model checking algorithms, symbolic model checking

Outline

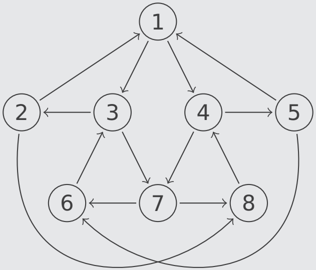
symbolic model checking = (CTL) model checking with BDDs

symbolic model checking = (CTL) model checking with BDDs

Questions

- how to represent sets of states?
- how to represent transition relation?
- how to implement model checking algorithm?

Example



model $\mathcal{M} = (S, \rightarrow, L)$

$$S = \{1,2,3,4,5,6,7,8\}$$

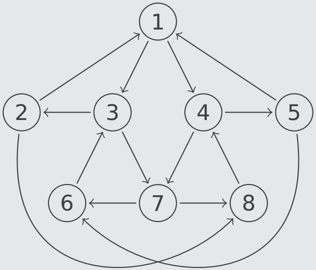
$L(1) = \{I_A, I_B\}$ $L(5) = \{I_A, P_B\}$

$L(2) = \{P_A, I_B\}$ $L(6) = \{R_A, P_B\}$

$L(3) = \{R_A, I_B\}$ $L(7) = \{R_A, R_B\}$

$L(4) = \{I_A, R_B\}$ $L(8) = \{P_A, R_B\}$

Example



model $\mathcal{M} = (S, \rightarrow, L)$

$$S = \{1,2,3,4,5,6,7,8\}$$

$L(1) = \{I_A, I_B\}$ $\quad$ $L(5) = \{I_A, P_B\}$

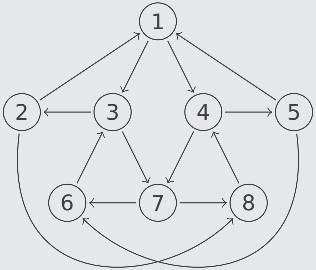
$L(2) = \{P_A, I_B\}$ $\quad$ $L(6) = \{R_A, P_B\}$

$L(3) = \{R_A, I_B\}$ $\quad$ $L(7) = \{R_A, R_B\}$

$L(4) = \{I_A, R_B\}$ $\quad$ $L(8) = \{P_A, R_B\}$

- 8 states require 3 boolean variables

Example



model $\mathcal{M} = (S, \rightarrow, L)$

$$S = \{1,2,3,4,5,6,7,8\}$$

$L(1) = \{I_A, I_B\}$ $\quad$ $L(5) = \{I_A, P_B\}$

$L(2) = \{P_A, I_B\}$ $\quad$ $L(6) = \{R_A, P_B\}$

$L(3) = \{R_A, I_B\}$ $\quad$ $L(7) = \{R_A, R_B\}$

$L(4) = \{I_A, R_B\}$ $\quad$ $L(8) = \{P_A, R_B\}$

- 8 states require 3 boolean variables

state	x	y	z		state	x	y	z	
1	0	0	0	$\overline{x}\,\overline{y}\,\overline{z}$	5	1	0	0	$x\overline{y}\,\overline{z}$
2	0	0	1	$\overline{x}\,\overline{y}z$	6	1	0	1	$x\overline{y}z$
3	0	1	0	$\overline{x}y\overline{z}$	7	1	1	0	$xy\overline{z}$
4	0	1	1	$\overline{x}yz$	8	1	1	1	xyz

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

variable ordering

$[x, y, z]$

set of states $\{1\}$

boolean function $\overline{x}\,\overline{y}\,\overline{z}$

reduced OBDD

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

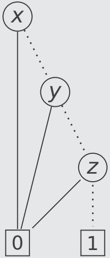
variable ordering

$[x, y, z]$

set of states $\{1\}$

boolean function $\overline{x}\,\overline{y}\,\overline{z}$

reduced OBDD



Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

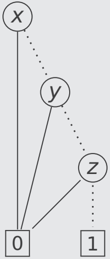
variable ordering

$[x, y, z]$

set of states $\{1\}$ $\{1, 2\}$

boolean function $\overline{x}\,\overline{y}\,\overline{z}$

reduced OBDD

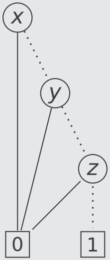


Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

variable ordering

$[x, y, z]$

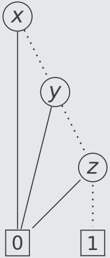
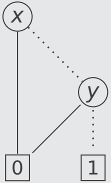
set of states	$\{1\}$	$\{1, 2\}$
boolean function	$\overline{x}\,\overline{y}\,\overline{z}$	$\overline{x}\,\overline{y}$
reduced OBDD		

Example (cont'd)

state		state		state		state	
1	$\bar{x}\bar{y}\bar{z}$	3	$\bar{x}y\bar{z}$	5	$x\bar{y}\bar{z}$	7	$xy\bar{z}$
2	$\bar{x}\bar{y}z$	4	$\bar{x}yz$	6	$x\bar{y}z$	8	xyz

variable ordering

$[x, y, z]$

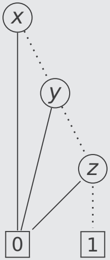
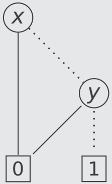
set of states	$\{1\}$	$\{1, 2\}$
boolean function	$\bar{x}\bar{y}\bar{z}$	$\bar{x}\bar{y}$
reduced OBDD		

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

variable ordering

$[x, y, z]$

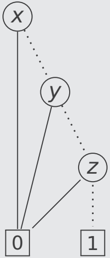
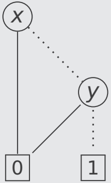
set of states	$\{1\}$	$\{1,2\}$	$\varnothing$
boolean function	$\overline{x}\,\overline{y}\,\overline{z}$	$\overline{x}\,\overline{y}$	
reduced OBDD			

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

variable ordering

$[x, y, z]$

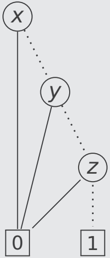
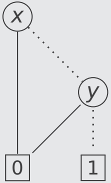
set of states	$\{1\}$	$\{1, 2\}$	$\varnothing$
boolean function	$\overline{x}\,\overline{y}\,\overline{z}$	$\overline{x}\,\overline{y}$	0
reduced OBDD			

Example (cont'd)

state		state		state		state	
1	$\overline{x}\overline{y}\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

variable ordering

$[x, y, z]$

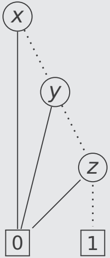
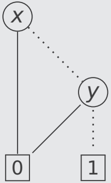
set of states	$\{1\}$	$\{1, 2\}$	$\varnothing$	$\{2, 3, 6\}$
boolean function	$\overline{x}\overline{y}\overline{z}$	$\overline{x}\overline{y}$	0	
reduced OBDD				

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

variable ordering

$[x, y, z]$

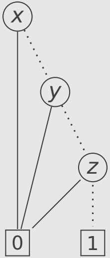
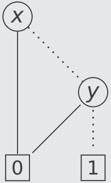
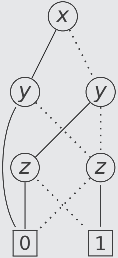
set of states	$\{1\}$	$\{1, 2\}$	$\varnothing$	$\{2, 3, 6\}$
boolean function	$\overline{x}\,\overline{y}\,\overline{z}$	$\overline{x}\,\overline{y}$	0	$\overline{y}z + \overline{x}y\overline{z}$
reduced OBDD				

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

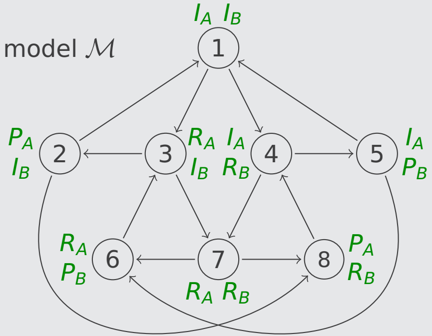
variable ordering

$[x, y, z]$

set of states	$\{1\}$	$\{1,2\}$	$\varnothing$	$\{2,3,6\}$
boolean function	$\overline{x}\,\overline{y}\,\overline{z}$	$\overline{x}\,\overline{y}$	0	$\overline{y}z + \overline{x}y\overline{z}$
reduced OBDD				

Example (cont'd)

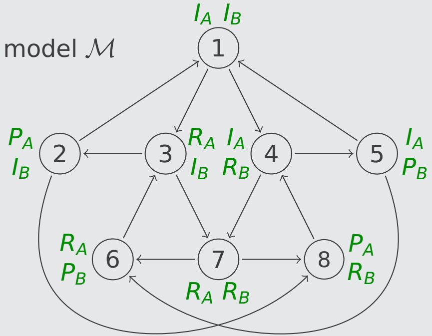
state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$



Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

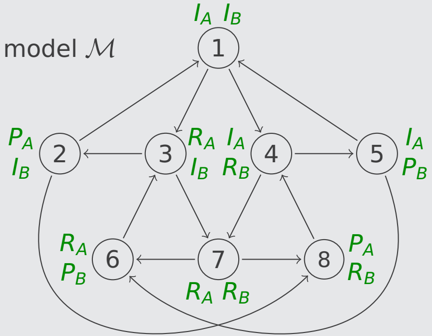
transition	
$1 \to 3$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{x}'\,y'\,\overline{z}'$



Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

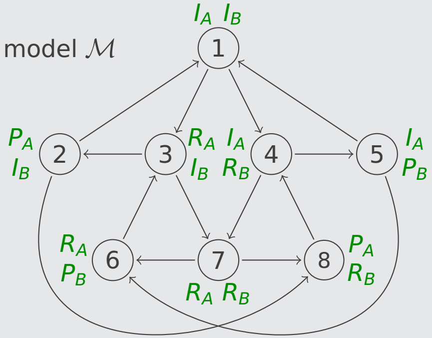
transition	
$1 \to 3$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{x}'\,y'\,\overline{z}'$
$1 \to 4$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{x}'\,y'\,z'$



Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

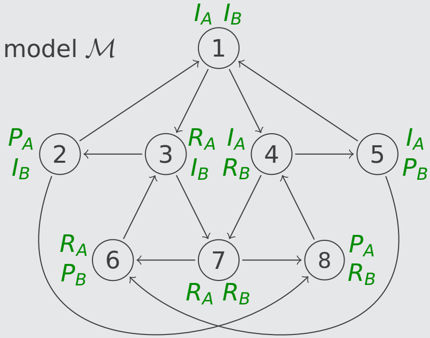
transition	
$1 \to 3$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{x}'\,y'\,\overline{z}'$
$1 \to 4$	$\overline{x}\,\overline{y}\,\overline{z}\,\overline{x}'\,y'\,z'$
$2 \to 1$	$\overline{x}\,\overline{y}\,z\,\overline{x}'\,\overline{y}'\,\overline{z}'$



Example (cont'd)

state		state		state		state	
1	$\overline{x}\overline{y}\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

transition		transition	
$1 \to 3$	$\overline{x}\overline{y}\overline{z}\overline{x}'y'\overline{z}'$	$4 \to 7$	$\overline{x}yzx'y'\overline{z}'$
$1 \to 4$	$\overline{x}\overline{y}\overline{z}\overline{x}'y'z'$	$5 \to 1$	$x\overline{y}\overline{z}\overline{x}'\overline{y}'\overline{z}'$
$2 \to 1$	$\overline{x}\overline{y}z\overline{x}'\overline{y}'\overline{z}'$	$5 \to 6$	$x\overline{y}\overline{z}x'\overline{y}'z'$
$2 \to 8$	$\overline{x}\overline{y}zx'y'z'$	$6 \to 3$	$x\overline{y}z\overline{x}'y'\overline{z}'$
$3 \to 2$	$\overline{x}y\overline{z}\overline{x}'\overline{y}'z'$	$7 \to 6$	$xy\overline{z}x'\overline{y}'z'$
$3 \to 7$	$\overline{x}y\overline{z}x'y'\overline{z}'$	$7 \to 8$	$xy\overline{z}x'y'z'$
$4 \to 5$	$\overline{x}yzx'\overline{y}'\overline{z}'$	$8 \to 4$	$xyz\overline{x}'y'z'$

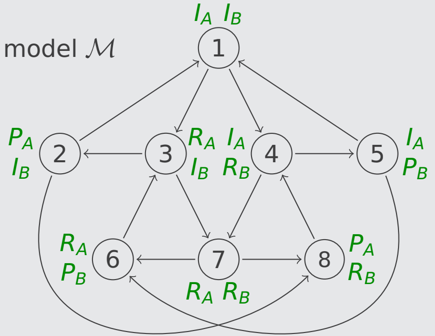


Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\,\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\,\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

transition relation

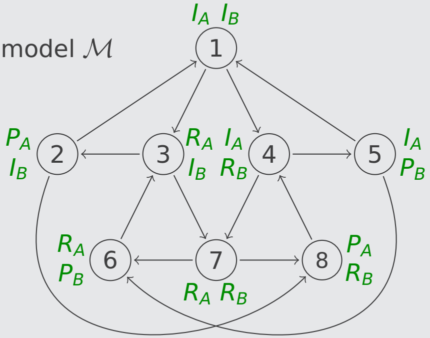
$$
\begin{aligned}
&\overline{x}\,\overline{y}\left(\overline{z}\,\overline{x'}y' + z(\overline{x'}\,\overline{y'}\,\overline{z'} + x'y'z')\right)\\
+\,&\overline{x}y\left(\overline{z}(\overline{x'}\,\overline{y'}z' + x'y'\overline{z'}) + zx'\overline{z'}\right)\\
+\,&x\overline{y}\left(\overline{z}(\overline{x'}\,\overline{y'}\,\overline{z'} + x'\overline{y'}z') + z\overline{x'}y'\overline{z'}\right)\\
+\,&xy\left(\overline{z}x'z' + z\overline{x'}y'z'\right)
\end{aligned}
$$



Example (cont'd)

state		state		state		state	
1	$\overline{x}\overline{y}\overline{z}$	3	$\overline{x}y\overline{z}$	5	$x\overline{y}\overline{z}$	7	$xy\overline{z}$
2	$\overline{x}\overline{y}z$	4	$\overline{x}yz$	6	$x\overline{y}z$	8	xyz

model $\mathcal{M}$



transition relation

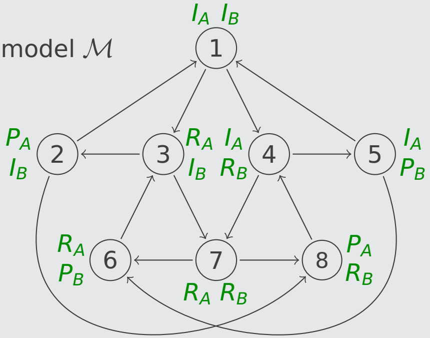
$$
\begin{aligned}
&\overline{x}\,\overline{y}\left(\overline{z}\,\overline{x}'y' + z(\overline{x}'\overline{y}'\overline{z}' + x'y'z')\right)\\
+&\,\overline{x}y\left(\overline{z}(\overline{x}'\overline{y}'z' + x'y'\overline{z}') + zx'\overline{z}'\right)\\
+&\,x\overline{y}\left(\overline{z}(\overline{x}'\overline{y}'\overline{z}' + x'\overline{y}'z') + z\overline{x}'y'\overline{z}'\right)\\
+&\,xy\left(\overline{z}x'z' + z\overline{x}'y'z'\right)
\end{aligned}
$$

reduced OBDD with variable ordering $[x, y, z, x', y', z']$ has 24 nodes

Example (cont'd)

state		state		state		state	
1	$\overline{x}\,\overline{y}\,\overline{z}$	3	$\overline{x}\,y\,\overline{z}$	5	$x\,\overline{y}\,\overline{z}$	7	$x\,y\,\overline{z}$
2	$\overline{x}\,\overline{y}\,z$	4	$\overline{x}\,y\,z$	6	$x\,\overline{y}\,z$	8	$x\,y\,z$

model $\mathcal{M}$



transition relation

$$\begin{aligned} & \overline{x}\,\overline{y}\left(\overline{z}\,\overline{x}'y' + z(\overline{x}'\,\overline{y}'\,\overline{z}' + x'y'z')\right) \\ + & \overline{x}y\left(\overline{z}(\overline{x}'\,\overline{y}'z' + x'y'\overline{z}') + zx'\overline{z}'\right) \\ + & x\overline{y}\left(\overline{z}(\overline{x}'\,\overline{y}'\,\overline{z}' + x'\overline{y}'z') + z\overline{x}'y'\overline{z}'\right) \\ + & xy\left(\overline{z}x'z' + z\overline{x}'y'z'\right) \end{aligned}$$

reduced OBDD with variable ordering $[x, y, z, x', y', z']$ has 24 nodes ($B_{\rightarrow}$)

Definition

model $\mathcal{M} = (S, \rightarrow, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Definition

model $\mathcal{M} = (S, \to, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$[\![\top]\!] = S$$

Definition

model $\mathcal{M} = (S, \rightarrow, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$[\![\top]\!] = S$$

$$[\![\bot]\!] = \varnothing$$

Definition

model $\mathcal{M} = (S, \rightarrow, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$[\![\top]\!] = S \qquad [\![p]\!] = \{s \in S \mid p \in L(s)\}$$

$$[\![\bot]\!] = \varnothing$$

Definition

model $\mathcal{M} = (S, \rightarrow, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$[\![\top]\!] = S$$

$$[\![\bot]\!] = \varnothing$$

$$[\![\neg\varphi]\!] = S - [\![\varphi]\!]$$

$$[\![p]\!] = \{s \in S \mid p \in L(s)\}$$

Definition

model $\mathcal{M} = (S, \to, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$[\![\top]\!] = S$$

$$[\![\bot]\!] = \varnothing$$

$$[\![\neg\varphi]\!] = S - [\![\varphi]\!]$$

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$

$$[\![p]\!] = \{s \in S \mid p \in L(s)\}$$

Definition

model $\mathcal{M} = (S, \to, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$
\begin{aligned}
[\![\top]\!] &= S \\
[\![\bot]\!] &= \varnothing \\
[\![\neg\varphi]\!] &= S - [\![\varphi]\!] \\
[\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \cap [\![\psi]\!] \\
[\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \cup [\![\psi]\!]
\end{aligned}
$$

$$[\![p]\!] = \{s \in S \mid p \in L(s)\}$$

Definition

model $\mathcal{M} = (S, \to, L)$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$

Lemma

$$
\begin{aligned}
[\![\top]\!] &= S \\
[\![\bot]\!] &= \varnothing \\
[\![\neg\varphi]\!] &= S - [\![\varphi]\!] \\
[\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \cap [\![\psi]\!] \\
[\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \cup [\![\psi]\!] \\
[\![\varphi \to \psi]\!] &= (S - [\![\varphi]\!]) \cup [\![\psi]\!]
\end{aligned}
$$

$$[\![p]\!] = \{s \in S \mid p \in L(s)\}$$

Definition

model $\mathcal{M} = (S, \to, L)$ $\quad X \subseteq S$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$
- $\mathrm{pre}_\forall(X) = \{s \in S \mid t \in X \text{ for all } t \text{ with } s \to t\}$

Lemma

$$
\begin{aligned}
[\![\top]\!] &= S \\
[\![\bot]\!] &= \varnothing \\
[\![\neg\varphi]\!] &= S - [\![\varphi]\!] \\
[\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \cap [\![\psi]\!] \\
[\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \cup [\![\psi]\!] \\
[\![\varphi \to \psi]\!] &= (S - [\![\varphi]\!]) \cup [\![\psi]\!]
\end{aligned}
$$

$$
\begin{aligned}
[\![p]\!] &= \{s \in S \mid p \in L(s)\} \\
[\![\mathrm{AX}\,\varphi]\!] &= \mathrm{pre}_\forall([\![\varphi]\!])
\end{aligned}
$$

Definition

model $\mathcal{M} = (S, \rightarrow, L) \quad X \subseteq S$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$
- $\text{pre}_\forall(X) = \{s \in S \mid t \in X \text{ for all } t \text{ with } s \rightarrow t\}$
- $\text{pre}_\exists(X) = \{s \in S \mid s \rightarrow t \text{ for some } t \in X\}$

Lemma

$$[\![\top]\!] = S \qquad [\![p]\!] = \{s \in S \mid p \in L(s)\}$$

$$[\![\bot]\!] = \varnothing \qquad [\![\text{AX}\,\varphi]\!] = \text{pre}_\forall([\![\varphi]\!])$$

$$[\![\neg\varphi]\!] = S - [\![\varphi]\!] \qquad [\![\text{EX}\,\varphi]\!] = \text{pre}_\exists([\![\varphi]\!])$$

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$

$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$

$$[\![\varphi \rightarrow \psi]\!] = (S - [\![\varphi]\!]) \cup [\![\psi]\!]$$

Definition

model $\mathcal{M} = (S, \to, L) \quad X \subseteq S$

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$
- $\text{pre}_\forall(X) = \{s \in S \mid t \in X \text{ for all } t \text{ with } s \to t\}$
- $\text{pre}_\exists(X) = \{s \in S \mid s \to t \text{ for some } t \in X\}$

Lemma

$$[\![\top]\!] = S \qquad [\![p]\!] = \{s \in S \mid p \in L(s)\}$$

$$[\![\bot]\!] = \varnothing \qquad [\![\text{AX}\,\varphi]\!] = \text{pre}_\forall([\![\varphi]\!])$$

$$[\![\neg\varphi]\!] = S - [\![\varphi]\!] \qquad [\![\text{EX}\,\varphi]\!] = \text{pre}_\exists([\![\varphi]\!])$$

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$

$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$

$$[\![\varphi \to \psi]\!] = (S - [\![\varphi]\!]) \cup [\![\psi]\!] \qquad \text{pre}_\forall(X) = S - \text{pre}_\exists(S - X)$$

Symbolic Model Checking Operations

	required operations
complement	$S - X$
union	$X \cup Y$
intersection	$X \cap Y$
	$\text{pre}_\exists(X)$

Symbolic Model Checking Operations

required operations		BDD representation
complement	$S - X$	$\textcolor{red}{\mathsf{apply}}(\oplus, B_S, B_X)$
union	$X \cup Y$	
intersection	$X \cap Y$	
	$\mathsf{pre}_\exists(X)$	

Symbolic Model Checking Operations

required operations		BDD representation
complement	$S - X$	$\text{apply}(\oplus, B_S, B_X)$
union	$X \cup Y$	$\text{apply}(+, B_X, B_Y)$
intersection	$X \cap Y$	
	$\text{pre}_{\exists}(X)$	

Symbolic Model Checking Operations

	required operations	BDD representation
complement	$S - X$	$\text{apply}(\oplus, B_S, B_X)$
union	$X \cup Y$	$\text{apply}(+, B_X, B_Y)$
intersection	$X \cap Y$	$\text{apply}(\,\cdot\,, B_X, B_Y)$
	$\text{pre}_\exists(X)$	

Symbolic Model Checking Operations

required operations		BDD representation
complement	$S - X$	$\text{apply}(\oplus, B_S, B_X)$
union	$X \cup Y$	$\text{apply}(+, B_X, B_Y)$
intersection	$X \cap Y$	$\text{apply}(\,\cdot\,, B_X, B_Y)$
	$\text{pre}_\exists(X)$	$\text{apply}(\,\cdot\,, B_\to, \underbrace{B_{X'}}_{\text{replace } x_1,\dots,x_n \text{ by } x'_1,\dots,x'_n \text{ in } B_X})$

Symbolic Model Checking Operations

required operations		BDD representation
complement	$S - X$	$\mathsf{apply}(\oplus, B_S, B_X)$
union	$X \cup Y$	$\mathsf{apply}(+, B_X, B_Y)$
intersection	$X \cap Y$	$\mathsf{apply}(\,\cdot\,, B_X, B_Y)$
	$\mathsf{pre}_\exists(X)$	$\mathsf{exists}(x'_1, \cdots (\mathsf{exists}(x'_n, \mathsf{apply}(\,\cdot\,, B_\to, \underbrace{B_{X'}}_{\text{replace } x_1,\dots,x_n \text{ by } x'_1,\dots,x'_n \text{ in } B_X}))) \cdots)$

Symbolic Model Checking Operations

required operations		BDD representation
complement	$S - X$	$\mathsf{apply}(\oplus, B_S, B_X)$
union	$X \cup Y$	$\mathsf{apply}(+, B_X, B_Y)$
intersection	$X \cap Y$	$\mathsf{apply}(\,\cdot\,, B_X, B_Y)$
	$\mathrm{pre}_\exists(X)$	$\mathsf{exists}(x_1', \cdots (\mathsf{exists}(x_n', \mathsf{apply}(\,\cdot\,, B_\to, \underbrace{B_{X'}}_{\text{replace } x_1, \dots, x_n \text{ by } x_1', \dots, x_n' \text{ in } B_X}))) \cdots)$

$$\mathsf{exists}(x', B) = \mathsf{apply}(+, \mathsf{restrict}(0, x', B), \mathsf{restrict}(1, x', B))$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_{\forall}([\![\mathsf{AF}\,\varphi]\!])$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!])$$

$$[\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!])$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

$$[\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \qquad [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))$$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

$$[\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \qquad [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))$$

Remark

- $[\![\mathsf{AF}\,\varphi]\!]$ is least fixed point of function $F_{\mathsf{AF}}(X) = [\![\varphi]\!] \cup \mathsf{pre}_\forall(X)$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

$$[\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \qquad [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))$$

Remark

- $[\![\mathsf{AF}\,\varphi]\!]$ is least fixed point of function $F_{\mathsf{AF}}(X) = [\![\varphi]\!] \cup \mathsf{pre}_\forall(X)$
- $[\![\mathsf{EG}\,\varphi]\!]$ is greatest fixed point of function $F_{\mathsf{EG}}(X) = [\![\varphi]\!] \cap \mathsf{pre}_\exists(X)$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

$$[\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \qquad [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))$$

Remark

- $[\![\mathsf{AF}\,\varphi]\!]$ is least fixed point of function $F_{\mathsf{AF}}(X) = [\![\varphi]\!] \cup \mathsf{pre}_\forall(X)$
- $[\![\mathsf{EG}\,\varphi]\!]$ is greatest fixed point of function $F_{\mathsf{EG}}(X) = [\![\varphi]\!] \cap \mathsf{pre}_\exists(X)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$

Lemma

$$[\![\mathsf{AF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \qquad [\![\mathsf{EF}\,\varphi]\!] = [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!])$$

$$[\![\mathsf{AG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \qquad [\![\mathsf{EG}\,\varphi]\!] = [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!])$$

$$[\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \qquad [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))$$

Remark

- $[\![\mathsf{AF}\,\varphi]\!]$ is least fixed point of function $F_{\mathsf{AF}}(X) = [\![\varphi]\!] \cup \mathsf{pre}_\forall(X)$
- $[\![\mathsf{EG}\,\varphi]\!]$ is greatest fixed point of function $F_{\mathsf{EG}}(X) = [\![\varphi]\!] \cap \mathsf{pre}_\exists(X)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing))$ monotonicity

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ induction

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing)$ $|S| = n$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ $|S| = n$
- $F^i(\varnothing)$ is fixed point of F

Theorem (Knaster–Tarski)

every monotone function $F \colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F \colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ — $|S| = n$
- $F^n(\varnothing)$ is fixed point of F — $F^i(\varnothing) = F^n(\varnothing)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ — $|S| = n$
- $F^n(\varnothing)$ is fixed point of F — $F^i(\varnothing) = F^n(\varnothing)$
- assume X is fixed point of F

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ $|S| = n$
- $F^n(\varnothing)$ is fixed point of F $F^i(\varnothing) = F^n(\varnothing)$
- assume X is fixed point of F
- $\varnothing \subseteq X$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ — $|S| = n$
- $F^n(\varnothing)$ is fixed point of F — $F^i(\varnothing) = F^n(\varnothing)$
- assume X is fixed point of F
- $F(\varnothing) \subseteq F(X) = X$ — monotonicity

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\quad \mu F = F^n(\varnothing)$
- greatest fixed point $\quad \nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ — $|S| = n$
- $F^n(\varnothing)$ is fixed point of F — $F^i(\varnothing) = F^n(\varnothing)$
- assume X is fixed point of F
- $F^n(\varnothing) \subseteq X$ — induction

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $\varnothing \subseteq F(\varnothing) \subseteq F(F(\varnothing)) \subseteq \cdots \subseteq F^n(\varnothing) \subseteq F^{n+1}(\varnothing)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(\varnothing) = F^{i+1}(\varnothing) = F(F^i(\varnothing))$ — $|S| = n$
- $F^n(\varnothing)$ is fixed point of F — $F^i(\varnothing) = F^n(\varnothing)$
- assume X is fixed point of F
- $F^n(\varnothing) \subseteq X$ — induction
- $F^n(\varnothing)$ is least fixed point of F

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S))$ monotonicity

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ induction

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ $|S| = n$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ $|S| = n$
- $F^i(S)$ is fixed point of F

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$
- assume X is fixed point of F

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$
- assume X is fixed point of F
- $S \supseteq X$

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$
- assume X is fixed point of F
- $F(S) \supseteq F(X) = X$ — monotonicity

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$
- assume X is fixed point of F
- $F^n(S) \supseteq X$ — induction

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- greatest fixed point $\nu F = F^n(S)$

function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y \subseteq S$

Proof

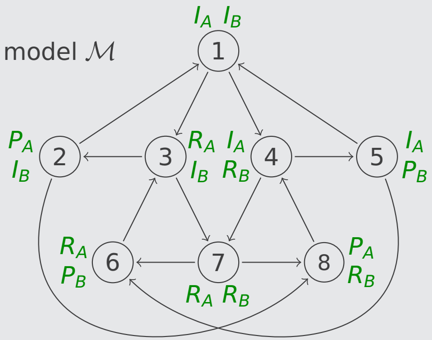
- $S \supseteq F(S) \supseteq F(F(S)) \supseteq F^n(S) \supseteq F^{n+1}(S)$ — induction
- $\exists\, 0 \leqslant i \leqslant n$ such that $F^i(S) = F^{i+1}(S)$ — $|S| = n$
- $F^n(S)$ is fixed point of F — $F^i(S) = F^n(S)$
- assume X is fixed point of F
- $F^n(S) \supseteq X$ — induction
- $F^n(S)$ is greatest fixed point of F

Definition

function $F_{\mathrm{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{AF}}(X) = [\![\varphi]\!] \cup \mathrm{pre}_{\forall}(X)$

Example

$\varphi = I_B$



$[\![\mathrm{AF}\, I_B]\!] =$

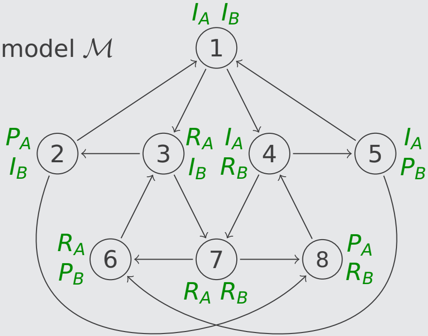
Definition

function $F_{\mathrm{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{AF}}(X) = [\![\varphi]\!] \cup \mathrm{pre}_{\forall}(X)$

Example

$\varphi = I_B \qquad X = \varnothing$

model $\mathcal{M}$



$[\![\mathrm{AF}\, I_B]\!] =$

Definition

function $F_{\mathrm{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{AF}}(X) = [\![\varphi]\!] \cup \mathrm{pre}_{\forall}(X)$

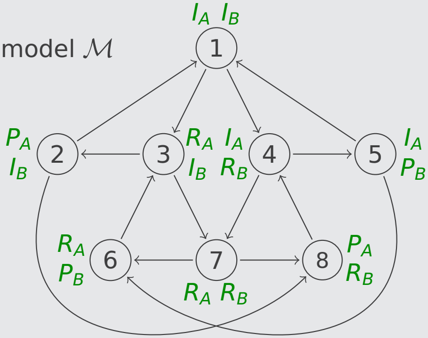
Example

$$\varphi = I_B \qquad X = \varnothing$$

$$F_{\mathrm{AF}}(X) = [\![\varphi]\!] = \{1, 2, 3\}$$

$$[\![\mathrm{AF}\, I_B]\!] =$$

model $\mathcal{M}$



Definition

function $F_{\text{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\text{AF}}(X) = [\![\varphi]\!] \cup \text{pre}_{\forall}(X)$

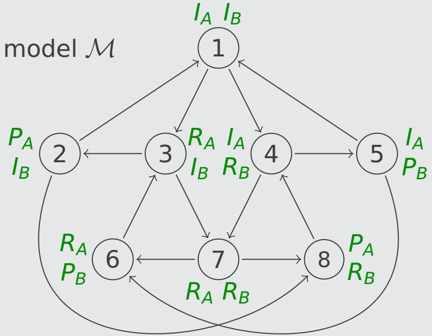
Example

$$\varphi = I_B \qquad X = \varnothing$$

$$F_{\text{AF}}(X) = \{1, 2, 3\}$$

$$F^2_{\text{AF}}(X) = F_{\text{AF}}(F_{\text{AF}}(X)) = \{1, 2, 3\} \cup \{6\}$$

$$[\![\text{AF}\, I_B]\!] =$$



Definition

function $F_{\mathrm{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{AF}}(X) = [\![\varphi]\!] \cup \mathrm{pre}_{\forall}(X)$

Example

$\varphi = I_B \qquad X = \varnothing$

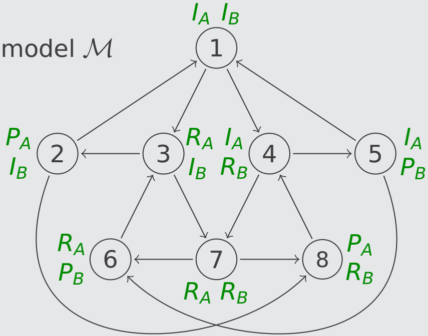
$F_{\mathrm{AF}}(X) = \{1,2,3\}$

$F^2_{\mathrm{AF}}(X) = \{1,2,3,6\}$

$F^3_{\mathrm{AF}}(X) = \{1,2,3\} \cup \{5,6\}$

$[\![\mathrm{AF}\, I_B]\!] =$

model $\mathcal{M}$



Definition

function $F_{\mathrm{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{AF}}(X) = [\![\varphi]\!] \cup \mathrm{pre}_{\forall}(X)$

Example

$$\varphi = I_B \qquad X = \varnothing$$

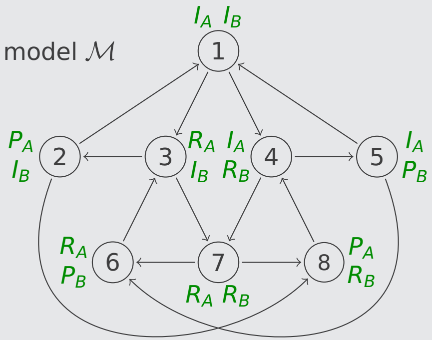
$$F_{\mathrm{AF}}(X) = \{1,2,3\}$$

$$F^2_{\mathrm{AF}}(X) = \{1,2,3,6\}$$

$$F^3_{\mathrm{AF}}(X) = \{1,2,3,5,6\}$$

$$F^4_{\mathrm{AF}}(X) = \{1,2,3\} \cup \{5,6\}$$

$$[\![\mathrm{AF}\, I_B]\!] =$$



Definition

function $F_{\text{AF}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\text{AF}}(X) = [\![\varphi]\!] \cup \text{pre}_\forall(X)$

Example

$\varphi = I_B \qquad X = \varnothing$

$F_{\text{AF}}(X) = \{1, 2, 3\}$

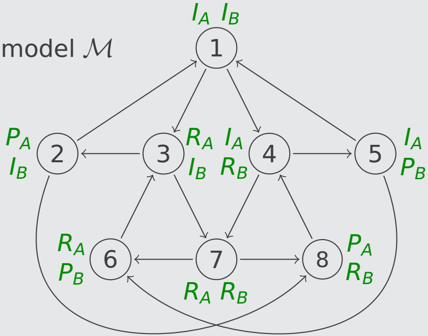
$F^2_{\text{AF}}(X) = \{1, 2, 3, 6\}$

$F^3_{\text{AF}}(X) = \{1, 2, 3, 5, 6\}$

$F^4_{\text{AF}}(X) = \{1, 2, 3, 5, 6\}$

$[\![\text{AF}\, I_B]\!] = \{1, 2, 3, 5, 6\}$

model $\mathcal{M}$



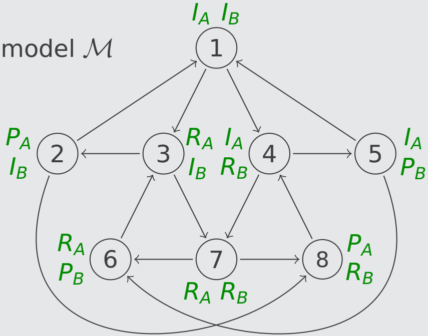
Definition

function $F_{\mathrm{EG}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{EG}}(X) = [\![\varphi]\!] \cap \mathrm{pre}_{\exists}(X)$

Example

$\varphi = P_A \vee I_B$

model $\mathcal{M}$



$[\![\mathrm{EG}(P_A \vee I_B)]\!] =$

Definition

function $F_{\mathrm{EG}} \colon \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{EG}}(X) = [\![\varphi]\!] \cap \mathrm{pre}_{\exists}(X)$

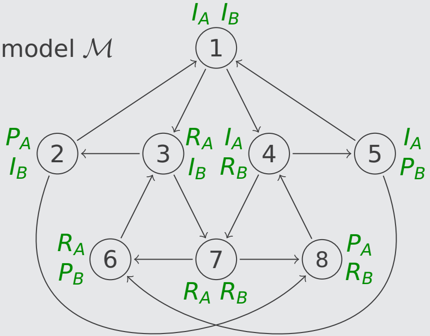
Example

$$\varphi = P_A \vee I_B$$

$$X = \{1,2,3,4,5,6,7,8\} = \mathrm{pre}_{\exists}(X)$$

$$[\![\mathrm{EG}(P_A \vee I_B)]\!] =$$

model $\mathcal{M}$



Definition

function $F_{\text{EG}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\text{EG}}(X) = [\![\varphi]\!] \cap \text{pre}_{\exists}(X)$

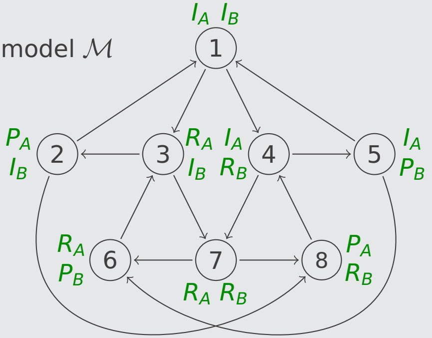
Example

$$\varphi = P_A \vee I_B$$

$$X = \{1,2,3,4,5,6,7,8\} = \text{pre}_{\exists}(X)$$

$$F_{\text{EG}}(X) = [\![\varphi]\!] = \{1,2,3,8\}$$

model $\mathcal{M}$



$$[\![\text{EG}(P_A \vee I_B)]\!] =$$

Definition

function $F_{\mathrm{EG}} \colon \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{EG}}(X) = [\![\varphi]\!] \cap \mathrm{pre}_{\exists}(X)$

Example

$$\varphi = P_A \vee I_B$$

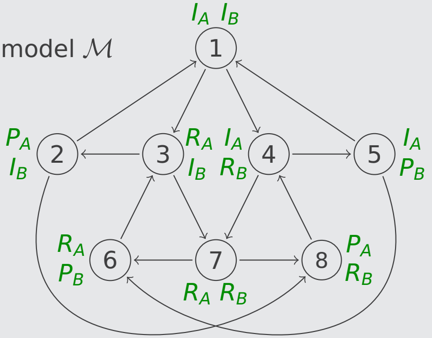
$$X = \{1,2,3,4,5,6,7,8\} = \mathrm{pre}_{\exists}(X)$$

$$F_{\mathrm{EG}}(X) = \{1,2,3,8\}$$

$$F^2_{\mathrm{EG}}(X) = \{1,2,3,8\} \cap \{1,2,3,5,6,7\}$$

$$[\![\mathrm{EG}(P_A \vee I_B)]\!] =$$

model $\mathcal{M}$



Definition

function $F_{\text{EG}}: \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\text{EG}}(X) = [\![\varphi]\!] \cap \text{pre}_{\exists}(X)$

Example

$$\varphi = P_A \vee I_B$$

$$X = \{1,2,3,4,5,6,7,8\} = \text{pre}_{\exists}(X)$$

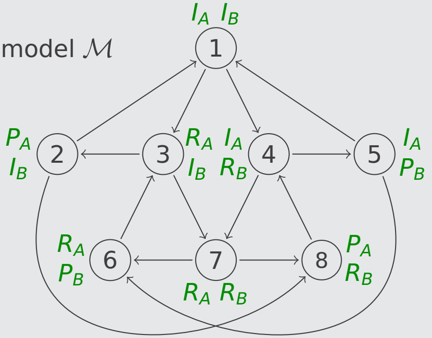
$$F_{\text{EG}}(X) = \{1,2,3,8\}$$

$$F^2_{\text{EG}}(X) = \{1,2,3\}$$

$$F^3_{\text{EG}}(X) = \{1,2,3,8\} \cap \{1,2,3,5,6\}$$

$$[\![\text{EG}\,(P_A \vee I_B)]\!] =$$

model $\mathcal{M}$



Definition

function $F_{\mathrm{EG}} \colon \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{EG}}(X) = [\![\varphi]\!] \cap \mathrm{pre}_{\exists}(X)$

Example

$$\varphi = P_A \vee I_B$$

$$X = \{1,2,3,4,5,6,7,8\} = \mathrm{pre}_{\exists}(X)$$

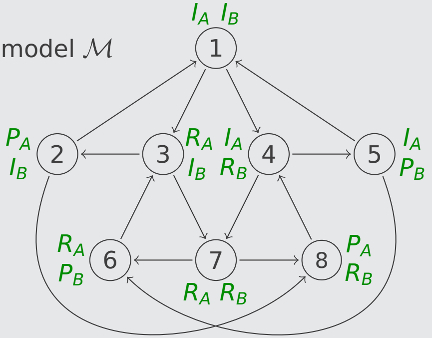
$$F_{\mathrm{EG}}(X) = \{1,2,3,8\}$$

$$F^2_{\mathrm{EG}}(X) = \{1,2,3\}$$

$$F^3_{\mathrm{EG}}(X) = \{1,2,3\}$$

$$[\![\mathrm{EG}\,(P_A \vee I_B)]\!] = \{1,2,3\}$$

model $\mathcal{M}$



Definition

function $F_{\mathsf{EU}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathsf{EU}}(X) = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_{\exists}(X))$

Definition

function $F_{\mathrm{EU}} : \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathrm{EU}}(X) = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathrm{pre}_{\exists}(X))$

Lemma

$[\![\mathrm{E}[\varphi \,\mathrm{U}\, \psi]]\!]$ is least fixed point of monotone function F_{EU}

Definition

function $F_{\mathsf{EU}} \colon \mathcal{P}(S) \to \mathcal{P}(S)$: $\quad F_{\mathsf{EU}}(X) = [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_{\exists}(X))$

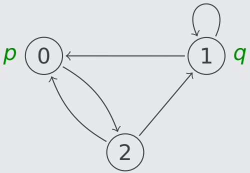
Lemma

$[\![\mathsf{E}[\varphi \, \mathsf{U} \, \psi]]\!]$ is least fixed point of monotone function F_{EU}

Algorithm

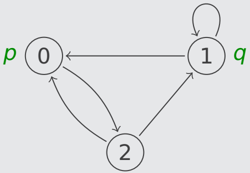
```
W := ⟦φ⟧;
X := ∅;
Y := ⟦ψ⟧;
repeat until X = Y
      X := Y;
      Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

model $\mathcal{M} = (S, \rightarrow, L)$



Example (Huth and Ryan, Exercise 6.12.2(a))

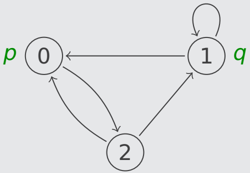
model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



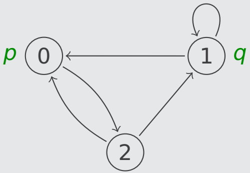
state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

x	x'	y	y'		
0	0	0	0	0	
0	0	0	1	1	$2 \rightarrow 1$
0	0	1	0	0	
0	0	1	1	1	$1 \rightarrow 1$
0	1	0	0	1	$2 \rightarrow 0$
0	1	0	1	0	
0	1	1	0	1	$1 \rightarrow 0$
0	1	1	1	0	

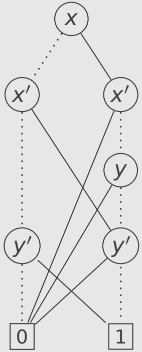
x	x'	y	y'		
1	0	0	0	1	$0 \rightarrow 2$
1	0	0	1	0	
1	0	1	0	0	
1	0	1	1	0	
1	1	0	0	0	
1	1	0	1	0	
1	1	1	0	0	
1	1	1	1	0	

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$

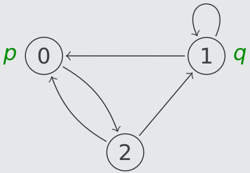


state	x	y
0	1	0
1	0	1
2	0	0
–	1	1



Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$

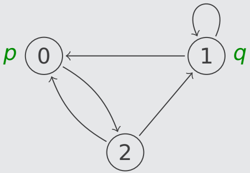


state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \overline{x}\overline{x'}y' + \overline{x}x'\overline{y'} + x\overline{x'}\overline{y}\overline{y'}$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



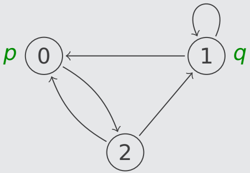
state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$\mathrm{AG}\,(p \vee \neg q)$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



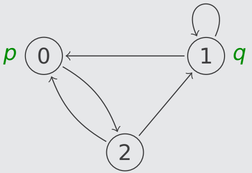
state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \; \overline{x}\,\overline{x'}\,y' + \overline{x}\,x'\,\overline{y'} + x\,\overline{x'}\,\overline{y}\,\overline{y'}$

$\mathsf{AG}\,(p \vee \neg q) \equiv \neg\,\mathsf{E}\,[\top\;\mathsf{U}\;\neg p \wedge q]$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

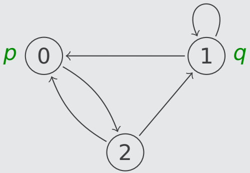
p: $x\overline{y}$

q: $\overline{x}y$

$$\mathsf{AG}\,(p \vee \neg q) \equiv \neg\mathsf{E}[\top\,\mathsf{U}\,\neg p \wedge q]$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

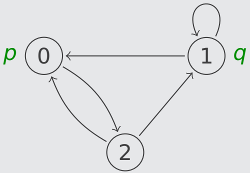
$p: \ x\overline{y}$ $\qquad \top: \ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y}$

$q: \ \overline{x}y$

$$\mathsf{AG}\,(p \vee \neg q) \equiv \neg \mathsf{E}[\top \,\mathsf{U}\, \neg p \wedge q]$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

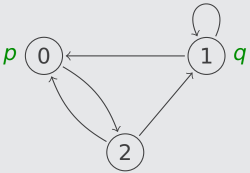
$p: \ x\overline{y}$ $\qquad \top: \ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q: \ \overline{x}y$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}\,[\top \,\mathrm{U}\, \neg p \wedge q]$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

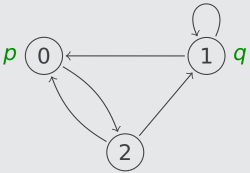
$p\colon\ x\overline{y}$ $\qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

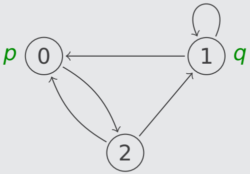
$p\colon\ x\overline{y} \qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y \qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

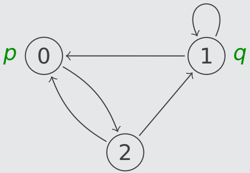
p: $x\bar{y}$ $\quad$ $S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\quad$ $\neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

$$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to: \ \overline{x}\overline{x'}y' + \overline{x}x'\overline{y'} + x\overline{x'}\overline{y}\overline{y'}$

$p: \ x\overline{y}$ $\quad S, \top: \ x\overline{y} + \overline{x}y + \overline{x}\overline{y} = \overline{x} + \overline{y}$

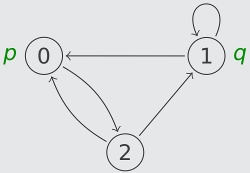
$q: \ \overline{x}y$ $\quad \neg p \wedge q: \ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$\mathsf{AG}\,(p \vee \neg q) \equiv \neg\mathsf{E}\,[\top\,\mathsf{U}\,\neg p \wedge q]$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

$p: \ x\bar{y} \qquad S, \top: \ x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

$q: \ \bar{x}y \qquad \neg p \wedge q: \ ((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

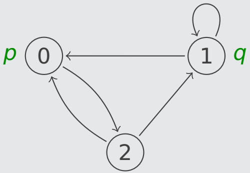
$\mathrm{W}: \ \bar{x} + \bar{y}$

$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \, \mathrm{U} \, \neg p \wedge q]$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre_∃(Y))
return Y
```

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

$p: \ x\bar{y}$ $\qquad S, \top: \ x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

$q: \ \bar{x}y$ $\qquad \neg p \wedge q: \ ((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

$W: \ \bar{x} + \bar{y}$

$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \, \mathrm{U} \, \neg p \wedge q]$

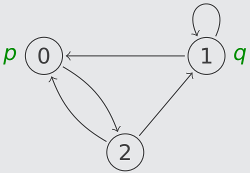
```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

$X_0 \quad 0$

$Y_0 \quad \bar{x}y$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p\colon\ x\overline{y}$ $\qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y$ $\qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W\colon\ \overline{x} + \overline{y}$

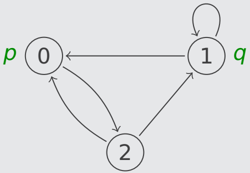
$\mathsf{AG}(p \vee \neg q) \equiv \neg\mathsf{E}[\top\,\mathsf{U}\,\neg p \wedge q]$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
     X := Y;
     Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\overline{x}y$
Y_0	$\overline{x}y$	Y_1	$Y_0 \cup (W \cap \mathrm{pre}_\exists(Y_0))$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p\colon\ x\overline{y}$ $\qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y$ $\qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$\mathsf{W}\colon\ \overline{x} + \overline{y}$

$$\mathsf{AG}\,(p \vee \neg q) \equiv \neg\mathsf{E}[\top\,\mathsf{U}\,\neg p \wedge q]$$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

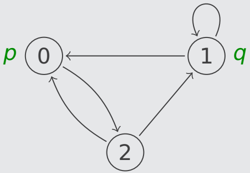
$\mathsf{X}_0 \quad 0 \qquad \mathsf{X}_1 \quad \overline{x}y$

$\mathsf{Y}_0 \quad \overline{x}y \qquad \mathsf{Y}_1 \quad \mathsf{Y}_0 \cup (\mathsf{W} \cap \mathsf{pre}_\exists(\mathsf{Y}_0))$

$$\mathsf{pre}_\exists(\mathsf{Y}_0) = \exists\,x'\,\exists\,y'\;(\rightarrow \cdot\, \mathsf{Y}_0')$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to$: $\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

p: $x\overline{y}$ $\qquad S, \top$: $x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

q: $\overline{x}y$ $\qquad \neg p \wedge q$: $((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

W: $\overline{x} + \overline{y}$

$$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X := Y;
     Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

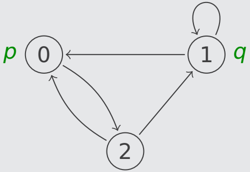
X_0 $\quad 0$ $\qquad X_1$ $\quad \overline{x}y$

Y_0 $\quad \overline{x}y$ $\qquad Y_1$ $\quad Y_0 \cup (W \cap \mathrm{pre}_\exists(Y_0))$

$$\mathrm{pre}_\exists(Y_0) = \exists x' \exists y' \, (\to \cdot Y_0')$$
$$= \exists x' \exists y' \, (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \cdot \overline{x}'y'$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow:\ \bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

$p:\ x\bar{y} \qquad S, \top:\ x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

$q:\ \bar{x}y \qquad \neg p \wedge q:\ ((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

$\mathrm{W}:\ \bar{x} + \bar{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}[\top\,\mathrm{U}\,\neg p \wedge q]$$

```
W := ⟦⊤⟧;
X := ∅;
Y := ⟦¬p ∧ q⟧;
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

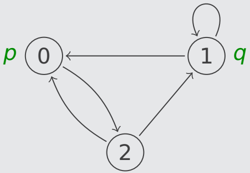
$\mathrm{X}_0 \quad 0 \qquad \mathrm{X}_1 \quad \bar{x}y$

$\mathrm{Y}_0 \quad \bar{x}y \qquad \mathrm{Y}_1 \quad \mathrm{Y}_0 \cup (\mathrm{W} \cap \mathrm{pre}_\exists(\mathrm{Y}_0))$

$$\begin{aligned}
\mathrm{pre}_\exists(\mathrm{Y}_0) &= \exists x' \exists y'\ (\rightarrow \cdot\, \mathrm{Y}_0') \\
&= \exists x' \exists y'\ (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot \bar{x}'y' \\
&= \exists x' \exists y'\ \bar{x}\bar{x}'y'
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\overline{x}\,\overline{x'}y' + \overline{x}x'\overline{y'} + x\overline{x'}\,\overline{y}\,\overline{y'}$

p: $x\overline{y}$ $\qquad S, \top$: $x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

q: $\overline{x}y$ $\qquad \neg p \wedge q$: $((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

W: $\overline{x} + \overline{y}$

$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$

```
W := ⟦⊤⟧;
X := ∅;
Y := ⟦¬p ∧ q⟧;
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

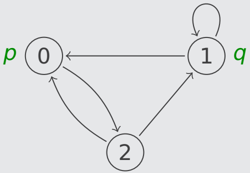
$X_0 \quad 0 \qquad X_1 \quad \overline{x}y$

$Y_0 \quad \overline{x}y \qquad Y_1 \quad Y_0 \cup (W \cap \mathrm{pre}_\exists(Y_0))$

$$\begin{aligned}
\mathrm{pre}_\exists(Y_0) &= \exists x' \exists y' \, (\rightarrow \cdot \, Y_0') \\
&= \exists x' \exists y' \, (\overline{x}\,\overline{x'}y' + \overline{x}x'\overline{y'} + x\overline{x'}\,\overline{y}\,\overline{y'}) \cdot \overline{x'}y' \\
&= \exists x' \exists y' \, \overline{x}\,\overline{x'}y' \\
&= \exists x' \, \overline{x}\,\overline{x'} = \overline{x}
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\quad$ $S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\quad$ $\neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}[\top\,\mathrm{U}\,\neg p \wedge q]$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X := Y;
     Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

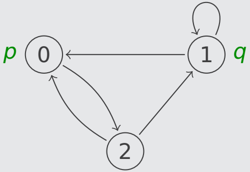
X_0 $\quad 0$ $\quad X_1$ $\quad \bar{x}y$

Y_0 $\quad \bar{x}y$ $\quad Y_1$ $\quad Y_0 \cup (W \cap \mathrm{pre}_\exists(Y_0)) = \bar{x}y + (\bar{x} + \bar{y}) \cdot \bar{x} = \bar{x}$

$$\begin{aligned}
\mathrm{pre}_\exists(Y_0) &= \exists x' \exists y' \, (\rightarrow \cdot \, Y_0') \\
&= \exists x' \exists y' \, (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot \bar{x}'y' \\
&= \exists x' \exists y' \, \bar{x}\bar{x}'y' \\
&= \exists x' \, \bar{x}\bar{x}' = \bar{x}
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow:\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p:\ x\overline{y}$ $\qquad S, \top:\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q:\ \overline{x}y$ $\qquad \neg p \wedge q:\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W:\ \overline{x} + \overline{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}[\top\, \mathrm{U}\, \neg p \wedge q]$$

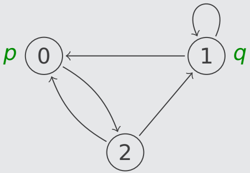
```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0 0 $\quad X_1$ $\overline{x}y$ $\quad X_2$ $\overline{x}$

Y_0 $\overline{x}y$ $\quad Y_1$ $\overline{x}$ $\quad Y_2$ $Y_1 \cup (W \cap \mathrm{pre}_\exists(Y_1))$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x'}\,y' + \overline{x}\,x'\,\overline{y'} + x\,\overline{x'}\,\overline{y}\,\overline{y'}$

$p\colon\ x\overline{y}$ $\qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y$ $\qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$\mathrm{W}\colon\ \overline{x} + \overline{y}$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

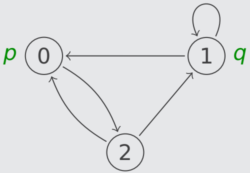
$\mathrm{X}_0 \quad 0 \qquad \mathrm{X}_1 \quad \overline{x}y \qquad \mathrm{X}_2 \quad \overline{x}$

$\mathrm{Y}_0 \quad \overline{x}y \qquad \mathrm{Y}_1 \quad \overline{x} \qquad \mathrm{Y}_2 \quad \mathrm{Y}_1 \cup (\mathrm{W} \cap \mathrm{pre}_\exists(\mathrm{Y}_1))$

$\mathrm{pre}_\exists(\mathrm{Y}_1) = \exists x'\,\exists y'\,(\rightarrow \cdot\, \mathrm{Y}_1')$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to:\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p:\ x\overline{y}$ $\qquad S, \top:\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q:\ \overline{x}y$ $\qquad \neg p \wedge q:\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$\mathrm{W}:\ \overline{x} + \overline{y}$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return  Y
```

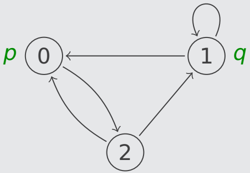
$\mathrm{X}_0 \quad 0 \qquad \mathrm{X}_1 \quad \overline{x}y \qquad \mathrm{X}_2 \quad \overline{x}$

$\mathrm{Y}_0 \quad \overline{x}y \qquad \mathrm{Y}_1 \quad \overline{x} \qquad \mathrm{Y}_2 \quad \mathrm{Y}_1 \cup (\mathrm{W} \cap \mathrm{pre}_\exists(\mathrm{Y}_1))$

$$\mathrm{pre}_\exists(\mathrm{Y}_1) = \exists x' \exists y' \, (\to \cdot\, \mathrm{Y}_1')$$
$$= \exists x' \exists y' \, (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \cdot \overline{x}'$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to\colon\ \bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

$p\colon\ x\bar{y} \qquad S, \top\colon\ x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

$q\colon\ \bar{x}y \qquad \neg p \wedge q\colon\ ((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

$\mathrm{W}\colon\ \bar{x} + \bar{y}$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return Y
```

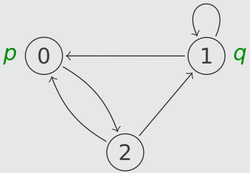
$\mathrm{X}_0 \quad 0 \qquad \mathrm{X}_1 \quad \bar{x}y \qquad \mathrm{X}_2 \quad \bar{x}$

$\mathrm{Y}_0 \quad \bar{x}y \qquad \mathrm{Y}_1 \quad \bar{x} \qquad \mathrm{Y}_2 \quad \mathrm{Y}_1 \cup (\mathrm{W} \cap \mathrm{pre}_\exists(\mathrm{Y}_1))$

$$\begin{aligned} \mathrm{pre}_\exists(\mathrm{Y}_1) &= \exists x'\,\exists y'\ (\to \cdot\, \mathrm{Y}_1') \\ &= \exists x'\,\exists y'\ (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot \bar{x}' \\ &= \exists x'\,\exists y'\ (\bar{x}\bar{x}'y' + x\bar{x}'\bar{y}\bar{y}') \end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\qquad S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\qquad \neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}[\top\, \mathrm{U}\, \neg p \wedge q]$$

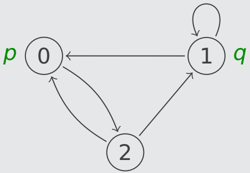
```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return  Y
```

X_0	0	X_1	$\bar{x}y$	X_2	$\bar{x}$
Y_0	$\bar{x}y$	Y_1	$\bar{x}$	Y_2	$Y_1 \cup (W \cap \mathrm{pre}_\exists(Y_1))$

$$\begin{aligned}
\mathrm{pre}_\exists(Y_1) &= \exists x' \exists y' \,(\to \cdot\, Y_1') \\
&= \exists x' \exists y' \,(\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot \bar{x}' \\
&= \exists x' \exists y' \,(\bar{x}\bar{x}'y' + x\bar{x}'\bar{y}\bar{y}') \\
&= \exists x' \,(\bar{x}\bar{x}' + x\bar{x}'\bar{y}) = \bar{x} + x\bar{y} = \bar{x} + \bar{y}
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\quad S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\quad \neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\,\mathrm{E}[\top\,\mathrm{U}\,\neg p \wedge q]$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return Y
```

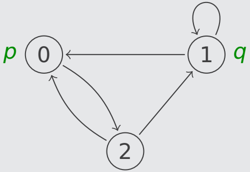
$X_0 \quad 0 \qquad X_1 \quad \bar{x}y \qquad X_2 \quad \bar{x}$

$Y_0 \quad \bar{x}y \qquad Y_1 \quad \bar{x} \qquad Y_2 \quad Y_1 \cup (W \cap \mathrm{pre}_\exists(Y_1)) = \bar{x} + \bar{y}$

$$\begin{aligned}\mathrm{pre}_\exists(Y_1) &= \exists x'\,\exists y'\,(\rightarrow \cdot\, Y_1') \\ &= \exists x'\,\exists y'\,(\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot \bar{x}' \\ &= \exists x'\,\exists y'\,(\bar{x}\bar{x}'y' + x\bar{x}'\bar{y}\bar{y}') \\ &= \exists x'\,(\bar{x}\bar{x}' + x\bar{x}'\bar{y}) = \bar{x} + x\bar{y} = \bar{x} + \bar{y}\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

p: $x\overline{y}$ $\qquad S, \top$: $x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

q: $\overline{x}y$ $\qquad \neg p \wedge q$: $((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

W: $\overline{x} + \overline{y}$

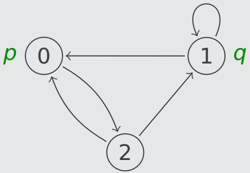
$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$Y_2 \cup (W \cap \mathrm{pre}_\exists(Y_2))$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow: \ \overline{x}\overline{x'}y' + \overline{x}x'\overline{y'} + x\overline{x'}\overline{y}\overline{y'}$

$p: \ x\overline{y}$ $\qquad S, \top: \ x\overline{y} + \overline{x}y + \overline{x}\overline{y} = \overline{x} + \overline{y}$

$q: \ \overline{x}y$ $\qquad \neg p \wedge q: \ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W: \ \overline{x} + \overline{y}$

$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$

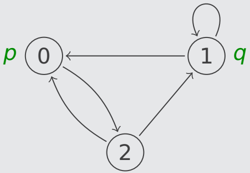
```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$Y_2 \cup (W \cap \mathrm{pre}_\exists(Y_2))$

$$\mathrm{pre}_\exists(Y_2) = \exists x' \, \exists y' \, (\rightarrow \cdot \, Y_2')$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\qquad S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\qquad \neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}\,[\top \,\mathrm{U}\, \neg p \wedge q]$$

```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return  Y
```

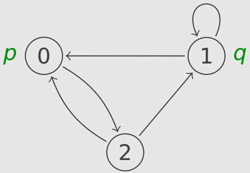
X_0	0	X_1	$\bar{x}y$	X_2	$\bar{x}$	X_3	$\bar{x} + \bar{y}$
Y_0	$\bar{x}y$	Y_1	$\bar{x}$	Y_2	$\bar{x} + \bar{y}$	Y_3	$Y_2 \cup (W \cap \mathrm{pre}_\exists(Y_2))$

$$\mathrm{pre}_\exists(Y_2) = \exists x' \exists y' \, (\rightarrow \cdot Y_2')$$

$$= \exists x' \exists y' \, (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot (\bar{x}' + \bar{y}')$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow\colon\ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p\colon\ x\overline{y} \qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y \qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W\colon\ \overline{x} + \overline{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg \mathrm{E}[\top\, \mathrm{U}\, \neg p \wedge q]$$

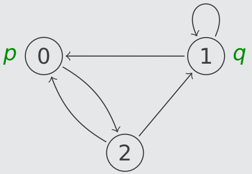
```
W  := [[⊤]];
X  := ∅;
Y  := [[¬p ∧ q]];
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$Y_2 \cup (W \cap \mathrm{pre}_\exists(Y_2))$

$$\begin{aligned} \mathrm{pre}_\exists(Y_2) &= \exists x'\, \exists y'\ (\rightarrow \cdot\, Y_2') \\ &= \exists x'\, \exists y'\ (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \cdot (\overline{x}' + \overline{y}') \\ &= \exists x'\, \exists y'\ (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\quad$ $S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\quad$ $\neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$$

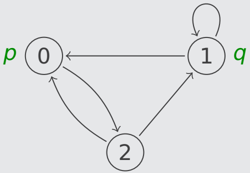
```
W  := ⟦⊤⟧;
X  := ∅;
Y  := ⟦¬p ∧ q⟧;
repeat until  X = Y
     X  := Y;
     Y  := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\bar{x}y$	X_2	$\bar{x}$	X_3	$\bar{x} + \bar{y}$
Y_0	$\bar{x}y$	Y_1	$\bar{x}$	Y_2	$\bar{x} + \bar{y}$	Y_3	$Y_2 \cup (W \cap \mathrm{pre}_\exists(Y_2))$

$$\begin{aligned}
\mathrm{pre}_\exists(Y_2) &= \exists x' \exists y' \, (\rightarrow \cdot Y_2') \\
&= \exists x' \exists y' \, (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \cdot (\bar{x}' + \bar{y}') \\
&= \exists x' \exists y' \, (\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}') \\
&= \exists x' \, (\bar{x}\bar{x}' + \bar{x}x' + x\bar{x}'\bar{y}) = \bar{x} + x\bar{y} = \bar{x} + \bar{y}
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

p: $x\overline{y}$ $\qquad S, \top$: $x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

q: $\overline{x}y$ $\qquad \neg p \wedge q$: $((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

W: $\overline{x} + \overline{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\,\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$$

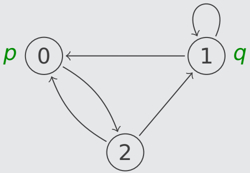
```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$\overline{x} + \overline{y}$

$$\begin{aligned}
\mathrm{pre}_\exists(Y_2) &= \exists x' \exists y' \, (\rightarrow \cdot\, Y_2') \\
&= \exists x' \exists y' \, (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \cdot (\overline{x}' + \overline{y}') \\
&= \exists x' \exists y' \, (\overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}') \\
&= \exists x' \, (\overline{x}\,\overline{x}' + \overline{x}x' + x\overline{x}'\overline{y}) = \overline{x} + x\overline{y} = \overline{x} + \overline{y}
\end{aligned}$$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to: \ \overline{x}\,\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\,\overline{y}'$

$p: \ x\overline{y} \qquad S, \top: \ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q: \ \overline{x}y \qquad \neg p \wedge q: \ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W: \ \overline{x} + \overline{y}$

$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$

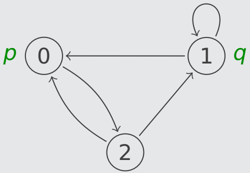
```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

$X_0 \ \ 0 \qquad X_1 \ \ \overline{x}y \qquad X_2 \ \ \overline{x} \qquad X_3 \ \ \overline{x} + \overline{y}$

$Y_0 \ \ \overline{x}y \qquad Y_1 \ \ \overline{x} \qquad Y_2 \ \ \overline{x} + \overline{y} \qquad Y_3 \ \ \overline{x} + \overline{y} \qquad X_3 = Y_3$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \rightarrow, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\rightarrow$: $\overline{x}\overline{x}'y' + \overline{x}x'\overline{y}' + x\overline{x}'\overline{y}\overline{y}'$

p: $x\overline{y}$ $\quad S, \top$: $x\overline{y} + \overline{x}y + \overline{x}\overline{y} = \overline{x} + \overline{y}$

q: $\overline{x}y$ $\quad \neg p \wedge q$: $((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

W: $\overline{x} + \overline{y}$

$\mathsf{AG}(p \vee \neg q) \equiv \neg \mathsf{E}[\top \, \mathsf{U} \, \neg p \wedge q]$

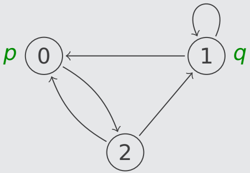
W := $[\![\top]\!]$;
X := $\varnothing$;
Y := $[\![\neg p \wedge q]\!]$;
repeat until X = Y
    X := Y;
    Y := $\mathtt{Y} \cup (\mathtt{W} \cap \mathrm{pre}_\exists(\mathtt{Y}))$
return Y

X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$		
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$\overline{x} + \overline{y}$	$X_3 = Y_3$	

$\mathsf{E}[\top \, \mathsf{U} \, \neg p \wedge q]$: $\overline{x} + \overline{y}$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to\colon\ \overline{x}\,\overline{x'}\,y' + \overline{x}\,x'\,\overline{y'} + x\,\overline{x'}\,\overline{y}\,\overline{y'}$

$p\colon\ x\overline{y}$ $\qquad S, \top\colon\ x\overline{y} + \overline{x}y + \overline{x}\,\overline{y} = \overline{x} + \overline{y}$

$q\colon\ \overline{x}y$ $\qquad \neg p \wedge q\colon\ ((\overline{x} + \overline{y}) \oplus x\overline{y}) \cdot \overline{x}y = \overline{x}y$

$W\colon\ \overline{x} + \overline{y}$

$$\mathrm{AG}\,(p \vee \neg q) \equiv \neg\,\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]$$

```
W := ⟦⊤⟧;
X := ∅;
Y := ⟦¬p ∧ q⟧;
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

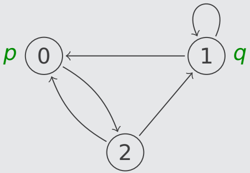
X_0	0	X_1	$\overline{x}y$	X_2	$\overline{x}$	X_3	$\overline{x} + \overline{y}$		
Y_0	$\overline{x}y$	Y_1	$\overline{x}$	Y_2	$\overline{x} + \overline{y}$	Y_3	$\overline{x} + \overline{y}$	$X_3 = Y_3$	

$\mathrm{E}\,[\top\,\mathrm{U}\,\neg p \wedge q]\colon\ \overline{x} + \overline{y}$

$\mathrm{AG}\,(p \vee \neg q)\colon\ (\overline{x} + \overline{y}) \oplus (\overline{x} + \overline{y})$

Example (Huth and Ryan, Exercise 6.12.2(a))

model $\mathcal{M} = (S, \to, L)$



state	x	y
0	1	0
1	0	1
2	0	0
–	1	1

$\to$: $\bar{x}\bar{x}'y' + \bar{x}x'\bar{y}' + x\bar{x}'\bar{y}\bar{y}'$

p: $x\bar{y}$ $\quad$ $S, \top$: $x\bar{y} + \bar{x}y + \bar{x}\bar{y} = \bar{x} + \bar{y}$

q: $\bar{x}y$ $\quad$ $\neg p \wedge q$: $((\bar{x} + \bar{y}) \oplus x\bar{y}) \cdot \bar{x}y = \bar{x}y$

W: $\bar{x} + \bar{y}$

$$\mathrm{AG}(p \vee \neg q) \equiv \neg \mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$$

```
W := [[⊤]];
X := ∅;
Y := [[¬p ∧ q]];
repeat until X = Y
    X := Y;
    Y := Y ∪ (W ∩ pre∃(Y))
return Y
```

X_0 0 $\quad$ X_1 $\bar{x}y$ $\quad$ X_2 $\bar{x}$ $\quad$ X_3 $\bar{x} + \bar{y}$

Y_0 $\bar{x}y$ $\quad$ Y_1 $\bar{x}$ $\quad$ Y_2 $\bar{x} + \bar{y}$ $\quad$ Y_3 $\bar{x} + \bar{y}$ $\quad$ $X_3 = Y_3$

$\mathrm{E}[\top \,\mathrm{U}\, \neg p \wedge q]$: $\bar{x} + \bar{y}$

$\mathrm{AG}(p \vee \neg q)$: $(\bar{x} + \bar{y}) \oplus (\bar{x} + \bar{y}) = 0$

Outline

Question

Which of the following statements about symbolic model checking are true ?

A The presented proof of the theorem of Knaster–Tarski would also work for infinite sets S.

B The set $[\![p \wedge \neg p]\!]$ corresponds to the reduced BDD $\boxed{0}$.

C Every monotone function $F \colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits a least fixed point $\mu F = F^n(S)$.

D $(S - [\![\varphi \vee \psi]\!]) = (S - [\![\varphi]\!]) \cap (S - [\![\psi]\!])$

Outline

1. **Summary of Previous Lecture**
2. **Symbolic Model Checking**
3. **Intermezzo**
4. **Linear–Time Temporal Logic (LTL)**

   Syntax Semantics Example

5. **Further Reading**

Definitions

- LTL (linear–time temporal logic) formulas are built from
  - atoms $p, q, r, p_1, p_2, \ldots$
  - logical connectives $\bot, \top, \neg, \wedge, \vee, \rightarrow$

Definitions

- LTL (linear–time temporal logic) formulas are built from
  - atoms — p, q, r, p_1, p_2, $\ldots$
  - logical connectives — $\bot$, $\top$, $\neg$, $\wedge$, $\vee$, $\rightarrow$
  - temporal connectives — X, F, G, U, W, R

Definitions

- LTL (linear–time temporal logic) formulas are built from
  - atoms $p,\ q,\ r,\ p_1,\ p_2,\ \ldots$
  - logical connectives $\bot,\ \top,\ \neg,\ \wedge,\ \vee,\ \rightarrow$
  - temporal connectives $\mathsf{X},\ \mathsf{F},\ \mathsf{G},\ \mathsf{U},\ \mathsf{W},\ \mathsf{R}$

  according to following BNF grammar:

$$
\begin{aligned}
\varphi \ ::= &\ \bot \mid \top \mid p \mid (\neg \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid \\
&\ (\mathsf{X}\,\varphi) \mid (\mathsf{F}\,\varphi) \mid (\mathsf{G}\,\varphi) \mid (\varphi\,\mathsf{U}\,\varphi) \mid (\varphi\,\mathsf{W}\,\varphi) \mid (\varphi\,\mathsf{R}\,\varphi)
\end{aligned}
$$

Definitions

- LTL (linear–time temporal logic) formulas are built from
  - atoms $p,\ q,\ r,\ p_1,\ p_2,\ \ldots$
  - logical connectives $\bot,\ \top,\ \neg,\ \wedge,\ \vee,\ \rightarrow$
  - temporal connectives $\mathsf{X},\ \mathsf{F},\ \mathsf{G},\ \mathsf{U},\ \mathsf{W},\ \mathsf{R}$

  according to following BNF grammar:

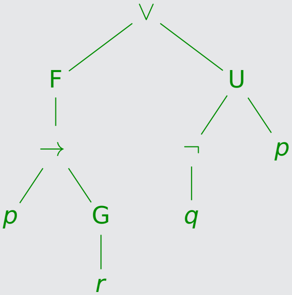
$$\varphi \ ::= \bot \mid \top \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid$$
$$(\mathsf{X}\,\varphi) \mid (\mathsf{F}\,\varphi) \mid (\mathsf{G}\,\varphi) \mid (\varphi\,\mathsf{U}\,\varphi) \mid (\varphi\,\mathsf{W}\,\varphi) \mid (\varphi\,\mathsf{R}\,\varphi)$$

- notational conventions:
  - binding precedence $\neg,\ \mathsf{X},\ \mathsf{F},\ \mathsf{G}\ >\ \mathsf{U},\ \mathsf{W},\ \mathsf{R}\ >\ \wedge,\ \vee\ >\ \rightarrow$
  - omit outer parentheses
  - $\rightarrow,\ \wedge,\ \vee$ are right–associative

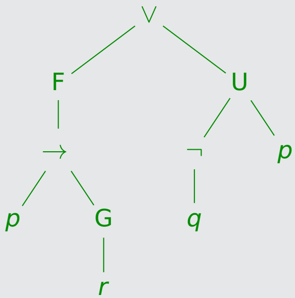
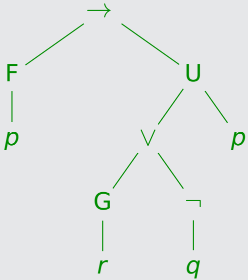
Example

formula $\mathsf{F}\,(p \rightarrow \mathsf{G}\,r) \vee \neg q\,\mathsf{U}\,p$

parse tree



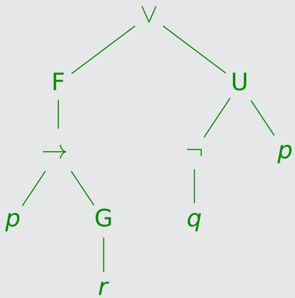
Example

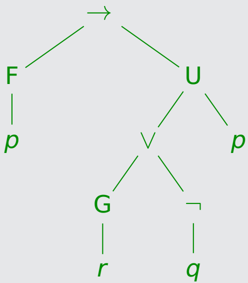
formula	$\mathsf{F}\,(p \rightarrow \mathsf{G}\,r) \vee \neg q \,\mathsf{U}\, p$	$\mathsf{F}\,p \rightarrow (\mathsf{G}\,r \vee \neg q)\,\mathsf{U}\,p$
parse tree		

Example

formula $\mathsf{F}\,(p \rightarrow \mathsf{G}\,r) \vee \neg q\,\mathsf{U}\,p$ $\quad$ $\mathsf{F}\,p \rightarrow (\mathsf{G}\,r \vee \neg q)\,\mathsf{U}\,p$

parse tree





X	next state	F	∃ future state	W	weak until
U	until	G	∀ states globally	R	release

Outline

Definition

- path in model $\mathcal{M} = (S, \to, L)$ is infinite sequence $s_1 \to s_2 \to \cdots$

Definition

- path in model $\mathcal{M} = (S, \rightarrow, L)$ is infinite sequence $s_1 \rightarrow s_2 \rightarrow \cdots$
- $\forall$ paths $\pi = s_1 \rightarrow s_2 \rightarrow \cdots$ $\forall\, i \geqslant 1$ $\pi^{i} = s_i \rightarrow s_{i+1} \rightarrow \cdots$

Definition

- path in model $\mathcal{M} = (S, \rightarrow, L)$ is infinite sequence $s_1 \rightarrow s_2 \rightarrow \cdots$
- $\forall$ paths $\pi = s_1 \rightarrow s_2 \rightarrow \cdots$ $\forall\, i \geqslant 1$ $\pi^i = s_i \rightarrow s_{i+1} \rightarrow \cdots$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \rightarrow s_2 \rightarrow \cdots$ in model $\mathcal{M} = (S, \rightarrow, L)$

$$\pi \vDash \varphi$$

Definition

- path in model $\mathcal{M} = (S, \to, L)$ is infinite sequence $s_1 \to s_2 \to \cdots$
- $\forall$ paths $\pi = s_1 \to s_2 \to \cdots \quad \forall\, i \geqslant 1 \quad \pi^i = s_i \to s_{i+1} \to \cdots$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \top \qquad\qquad \pi \nvDash \bot$$

Definition

- path in model $\mathcal{M} = (S, \rightarrow, L)$ is infinite sequence $s_1 \rightarrow s_2 \rightarrow \cdots$
- $\forall$ paths $\pi = s_1 \rightarrow s_2 \rightarrow \cdots \quad \forall\, i \geqslant 1 \quad \pi^i = s_i \rightarrow s_{i+1} \rightarrow \cdots$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \rightarrow s_2 \rightarrow \cdots$ in model $\mathcal{M} = (S, \rightarrow, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \top \qquad \pi \nvDash \bot$$

$$\pi \vDash p \iff p \in L(s_1)$$

Definition

- path in model $\mathcal{M} = (S, \to, L)$ is infinite sequence $s_1 \to s_2 \to \cdots$
- $\forall$ paths $\pi = s_1 \to s_2 \to \cdots \quad \forall\, i \geqslant 1 \quad \pi^i = s_i \to s_{i+1} \to \cdots$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \top \qquad\qquad \pi \nvDash \bot$$

$$\pi \vDash p \iff p \in L(s_1)$$

$$\pi \vDash \neg\varphi \iff \pi \nvDash \varphi$$

Definition

- path in model $\mathcal{M} = (S, \rightarrow, L)$ is infinite sequence $s_1 \rightarrow s_2 \rightarrow \cdots$
- $\forall$ paths $\pi = s_1 \rightarrow s_2 \rightarrow \cdots \quad \forall\, i \geqslant 1 \quad \pi^i = s_i \rightarrow s_{i+1} \rightarrow \cdots$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \rightarrow s_2 \rightarrow \cdots$ in model $\mathcal{M} = (S, \rightarrow, L)$

$$\pi \vDash \varphi$$

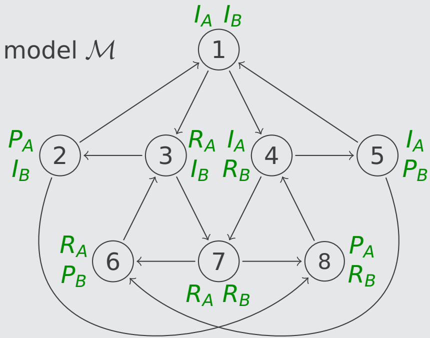
is defined by induction on φ:

$$\pi \vDash \top \qquad \pi \nvDash \bot \qquad \pi \vDash \varphi \wedge \psi \iff \pi \vDash \varphi \text{ and } \pi \vDash \psi$$

$$\pi \vDash p \iff p \in L(s_1) \qquad \pi \vDash \varphi \vee \psi \iff \pi \vDash \varphi \text{ or } \pi \vDash \psi$$

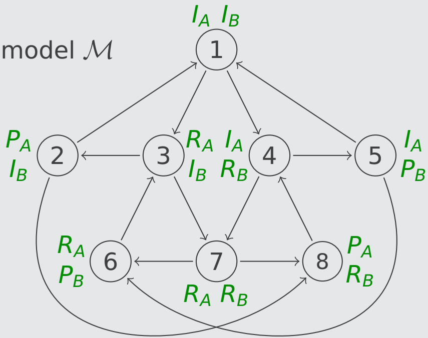
$$\pi \vDash \neg\varphi \iff \pi \nvDash \varphi \qquad \pi \vDash \varphi \rightarrow \psi \iff \pi \nvDash \varphi \text{ or } \pi \vDash \psi$$

Example


model $\mathcal{M}$
I_A I_B
1
P_A
I_B
2
3
R_A
I_B
I_A
R_B
4
5
I_A
P_B
R_A
P_B
6
7
8
P_A
R_B
R_A R_B

Example

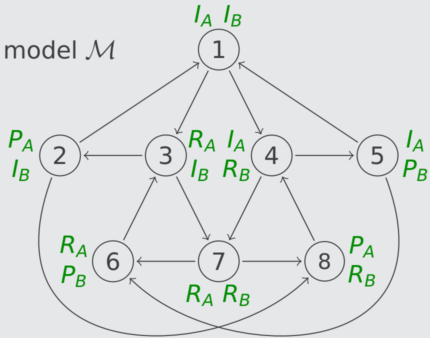
model $\mathcal{M}$



$\pi_1 = 1 \rightarrow 3 \rightarrow 2 \rightarrow 1 \rightarrow 3 \rightarrow 2 \rightarrow \cdots$

$\pi_1 \vDash I_A$

Example



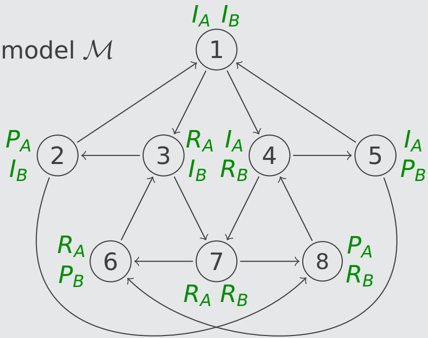
$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$\pi_1 \vDash I_A$

$\pi_1 \nvDash R_A \wedge I_B$

Example

model $\mathcal{M}$

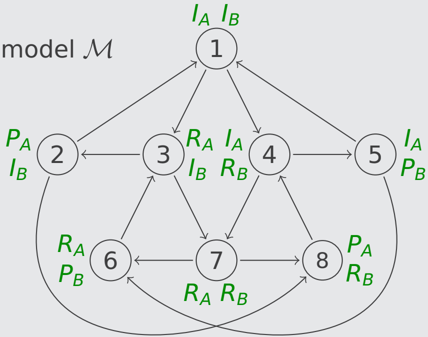


$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$\pi_1 \vDash I_A$ $\qquad$ $\pi_1 \nvDash R_A \wedge I_B$ $\qquad$ $\pi_1 \nvDash I_B \to P_A \vee R_B$

Example

model $\mathcal{M}$

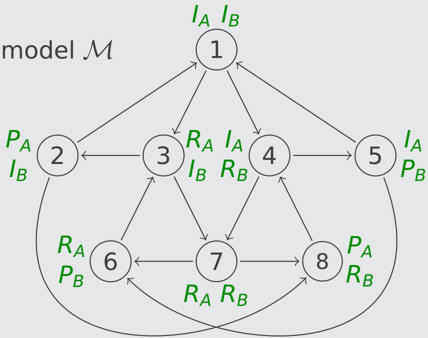


$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$$\pi_2 = 7 \to 6 \to 3 \to 7 \to 6 \to 3 \to \cdots$$

$\pi_1 \models I_A$	$\pi_1 \not\models R_A \wedge I_B$	$\pi_1 \not\models I_B \to P_A \vee R_B$
$\pi_2 \quad I_A$	$\pi_2 \quad R_A \wedge I_B$	$\pi_2 \quad I_B \to P_A \vee R_B$

Example



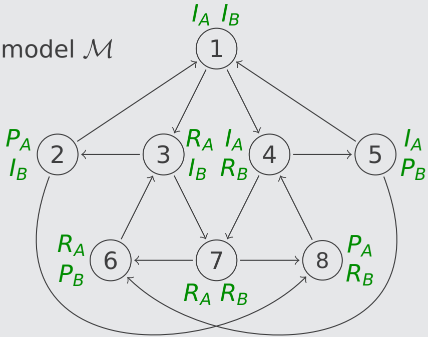
$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$$\pi_2 = 7 \to 6 \to 3 \to 7 \to 6 \to 3 \to \cdots$$

$\pi_1 \vDash I_A$	$\pi_1 \nvDash R_A \wedge I_B$	$\pi_1 \nvDash I_B \to P_A \vee R_B$
$\pi_2 \nvDash I_A$	$\pi_2 \quad R_A \wedge I_B$	$\pi_2 \quad I_B \to P_A \vee R_B$

Example

model $\mathcal{M}$

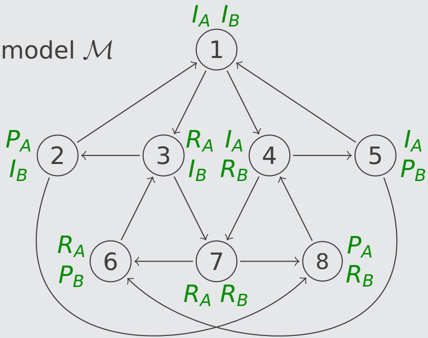


$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$$\pi_2 = 7 \to 6 \to 3 \to 7 \to 6 \to 3 \to \cdots$$

$\pi_1 \vDash I_A$	$\pi_1 \nvDash R_A \wedge I_B$	$\pi_1 \nvDash I_B \to P_A \vee R_B$
$\pi_2 \nvDash I_A$	$\pi_2^6 \vDash R_A \wedge I_B$	$\pi_2 \quad I_B \to P_A \vee R_B$

Example



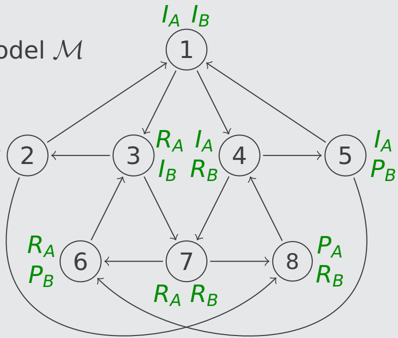
$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$

$\pi_2 = 7 \to 6 \to 3 \to 7 \to 6 \to 3 \to \cdots$

$\pi_1 \vDash I_A$ $\qquad$ $\pi_1 \nvDash R_A \wedge I_B$ $\qquad$ $\pi_1 \nvDash I_B \to P_A \vee R_B$

$\pi_2 \nvDash I_A$ $\qquad$ $\pi_2^6 \vDash R_A \wedge I_B$ $\qquad$ $\pi_2 \vDash I_B \to P_A \vee R_B$

Example



$$\pi_1 = 1 \to 3 \to 2 \to 1 \to 3 \to 2 \to \cdots$$

$$\pi_2 = 7 \to 6 \to 3 \to 7 \to 6 \to 3 \to \cdots$$

special notation for infinite paths:

$$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$$

$\pi_1 \vDash I_A$ $\qquad$ $\pi_1 \nvDash R_A \wedge I_B$ $\qquad$ $\pi_1 \nvDash I_B \to P_A \vee R_B$

$\pi_2 \nvDash I_A$ $\qquad$ $\pi_2^6 \vDash R_A \wedge I_B$ $\qquad$ $\pi_2 \vDash I_B \to P_A \vee R_B$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathsf{X}\,\varphi \quad \Longleftrightarrow \quad \pi^2 \vDash \varphi$$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathsf{X}\,\varphi \iff \pi^2 \vDash \varphi$$

$$\pi \vDash \mathsf{F}\,\varphi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathsf{X}\,\varphi \iff \pi^2 \vDash \varphi$$

$$\pi \vDash \mathsf{F}\,\varphi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \mathsf{G}\,\varphi \iff \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathsf{X}\,\varphi \iff \pi^2 \vDash \varphi$$

$$\pi \vDash \mathsf{F}\,\varphi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \mathsf{G}\,\varphi \iff \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{U}\,\psi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \psi \quad \text{and} \quad \forall\, j < i \quad \pi^j \vDash \varphi$$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathrm{X}\,\varphi \iff \pi^2 \vDash \varphi$$

$$\pi \vDash \mathrm{F}\,\varphi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \mathrm{G}\,\varphi \iff \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \varphi\,\mathrm{U}\,\psi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \psi \quad \text{and} \quad \forall\, j < i \quad \pi^j \vDash \varphi$$

$$\pi \vDash \varphi\,\mathrm{W}\,\psi \iff \big(\exists\, i \geqslant 1 \quad \pi^i \vDash \psi \quad \text{and} \quad \forall\, j < i \quad \pi^j \vDash \varphi\big) \quad \text{or} \quad \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

Definition

satisfaction of LTL formula φ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

is defined by induction on φ:

$$\pi \vDash \mathsf{X}\,\varphi \iff \pi^2 \vDash \varphi$$

$$\pi \vDash \mathsf{F}\,\varphi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \mathsf{G}\,\varphi \iff \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

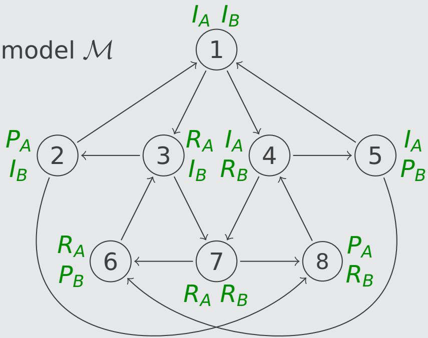
$$\pi \vDash \varphi\,\mathsf{U}\,\psi \iff \exists\, i \geqslant 1 \quad \pi^i \vDash \psi \text{ and } \forall\, j < i \quad \pi^j \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{W}\,\psi \iff (\exists\, i \geqslant 1 \quad \pi^i \vDash \psi \text{ and } \forall\, j < i \quad \pi^j \vDash \varphi) \text{ or } \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{R}\,\psi \iff (\exists\, i \geqslant 1 \quad \pi^i \vDash \varphi \text{ and } \forall\, j \leqslant i \quad \pi^j \vDash \psi) \text{ or } \forall\, i \geqslant 1 \quad \pi^i \vDash \psi$$

Example

model $\mathcal{M}$

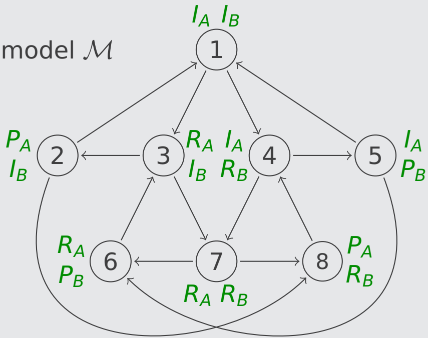


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathrm{X}\,(R_A \vee R_B)$

Example

model $\mathcal{M}$

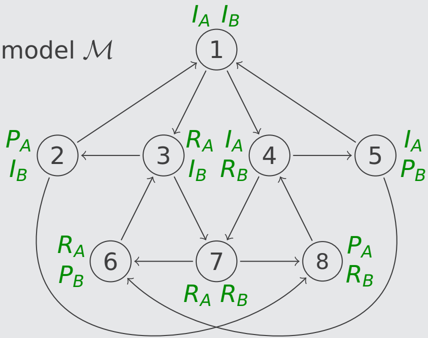


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B) \qquad \pi_1 \quad \mathsf{F}\,P_A \qquad \pi_1 \quad \mathsf{X}\,\mathsf{X}\,P_B$

Example

model $\mathcal{M}$

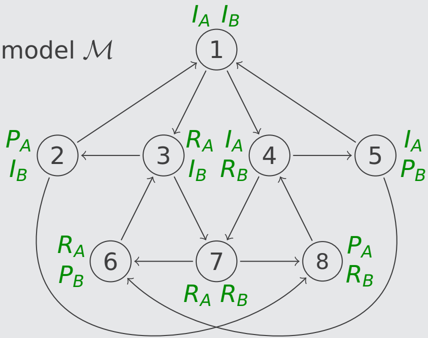


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B) \qquad \pi_1 \vDash \mathsf{F}\,P_A \qquad \pi_1 \quad \mathsf{X}\,\mathsf{X}\,P_B$

Example

model $\mathcal{M}$



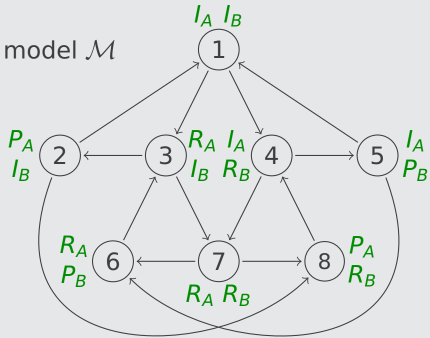
$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \models \mathsf{X}\,(R_A \vee R_B)$

$\pi_1 \models \mathsf{F}\,P_A$

$\pi_1 \not\models \mathsf{X}\,\mathsf{X}\,P_B$

Example

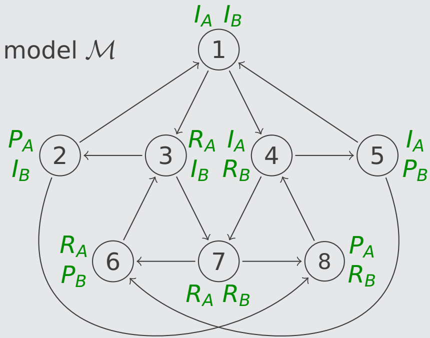


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash X\,(R_A \vee R_B)$ $\qquad$ $\pi_1 \vDash F\,P_A$ $\qquad$ $\pi_1 \nvDash X\,X\,P_B$

$\pi_2 \quad F\,P_A$ $\qquad$ $\pi_2 \quad G\,\neg I_A$ $\qquad$ $\pi_2 \quad G\,F\,P_B$

Example



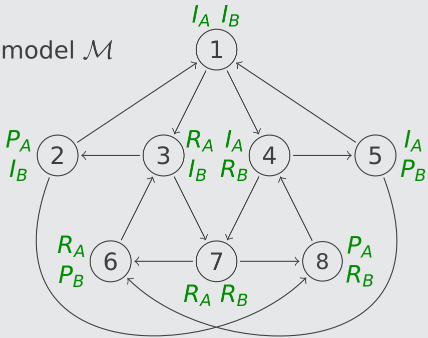
$\pi_1 = (1\,3\,2)^\omega$ $\quad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B)$ $\quad \pi_1 \vDash \mathsf{F}\,P_A$ $\quad \pi_1 \nvDash \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \nvDash \mathsf{F}\,P_A$ $\quad \pi_2 \quad \mathsf{G}\,\neg I_A$ $\quad \pi_2 \quad \mathsf{G}\,\mathsf{F}\,P_B$

Example

model $\mathcal{M}$



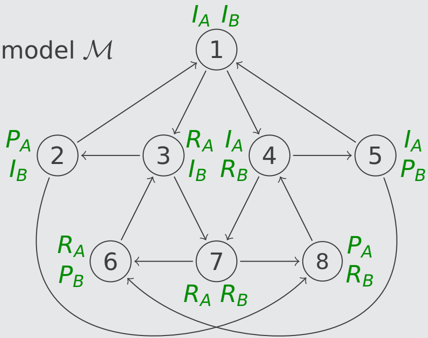
$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B)$ $\qquad$ $\pi_1 \vDash \mathsf{F}\,P_A$ $\qquad$ $\pi_1 \nvDash \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \nvDash \mathsf{F}\,P_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\neg I_A$ $\qquad$ $\pi_2 \quad \mathsf{G}\,\mathsf{F}\,P_B$

Example

model $\mathcal{M}$

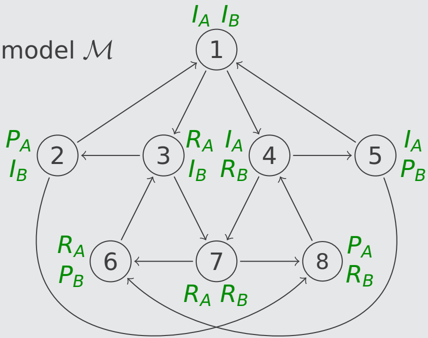


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B)$ $\qquad$ $\pi_1 \vDash \mathsf{F}\,P_A$ $\qquad$ $\pi_1 \nvDash \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \nvDash \mathsf{F}\,P_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\neg I_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\mathsf{F}\,P_B$

Example



$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

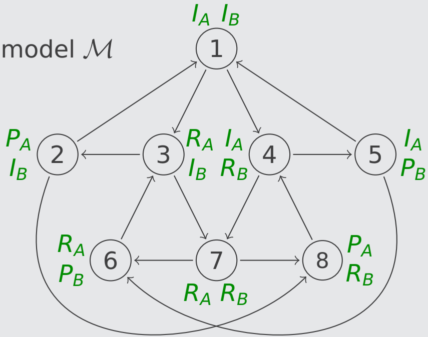
$\pi_1 \models \mathsf{X}\,(R_A \vee R_B)$ | $\pi_1 \models \mathsf{F}\,P_A$ | $\pi_1 \not\models \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \not\models \mathsf{F}\,P_A$ | $\pi_2 \models \mathsf{G}\,\neg I_A$ | $\pi_2 \models \mathsf{G}\,\mathsf{F}\,P_B$

$\pi_1 \quad I_A\,\mathsf{U}\,P_A$ | $\pi_2 \quad \neg I_A\,\mathsf{W}\,P_A$ | $\pi_2 \quad P_B\,\mathsf{R}\,R_B$

Example

model $\mathcal{M}$

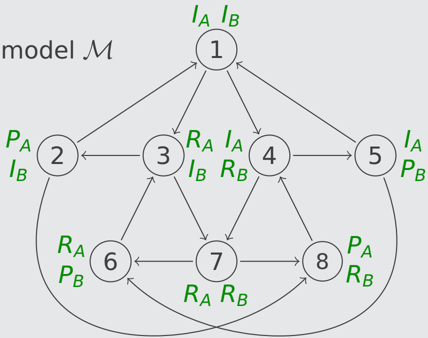


$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \models \mathrm{X}\,(R_A \vee R_B)$	$\pi_1 \models \mathrm{F}\,P_A$	$\pi_1 \not\models \mathrm{X}\,\mathrm{X}\,P_B$
$\pi_2 \not\models \mathrm{F}\,P_A$	$\pi_2 \models \mathrm{G}\,\neg I_A$	$\pi_2 \models \mathrm{G}\,\mathrm{F}\,P_B$
$\pi_1 \not\models I_A\,\mathrm{U}\,P_A$	$\pi_2 \quad \neg I_A\,\mathrm{W}\,P_A$	$\pi_2 \quad P_B\,\mathrm{R}\,R_B$

Example

model $\mathcal{M}$



$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

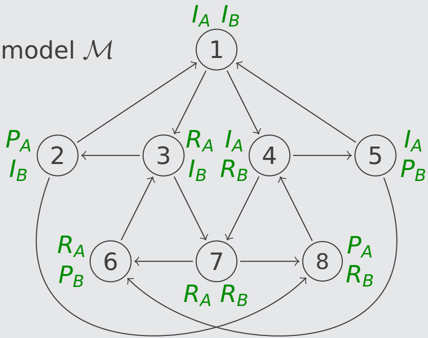
$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B)$ $\qquad$ $\pi_1 \vDash \mathsf{F}\,P_A$ $\qquad$ $\pi_1 \nvDash \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \nvDash \mathsf{F}\,P_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\neg I_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\mathsf{F}\,P_B$

$\pi_1 \nvDash I_A\,\mathsf{U}\,P_A$ $\qquad$ $\pi_2 \vDash \neg I_A\,\mathsf{W}\,P_A$ $\qquad$ $\pi_2 \quad P_B\,\mathsf{R}\,R_B$

Example

model $\mathcal{M}$



$\pi_1 = (1\,3\,2)^\omega \qquad \pi_2 = (7\,6\,3)^\omega$

$\pi_1 \vDash \mathsf{X}\,(R_A \vee R_B)$ $\qquad$ $\pi_1 \vDash \mathsf{F}\,P_A$ $\qquad$ $\pi_1 \nvDash \mathsf{X}\,\mathsf{X}\,P_B$

$\pi_2 \nvDash \mathsf{F}\,P_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\neg I_A$ $\qquad$ $\pi_2 \vDash \mathsf{G}\,\mathsf{F}\,P_B$

$\pi_1 \nvDash I_A\,\mathsf{U}\,P_A$ $\qquad$ $\pi_2 \vDash \neg I_A\,\mathsf{W}\,P_A$ $\qquad$ $\pi_2 \nvDash P_B\,\mathsf{R}\,R_B$

Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

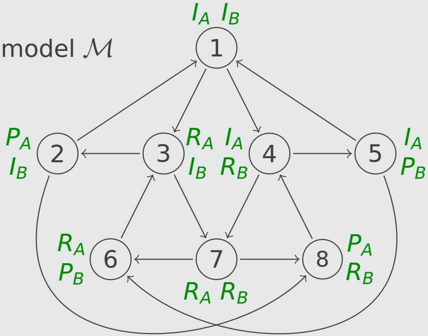
Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots$ $\pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



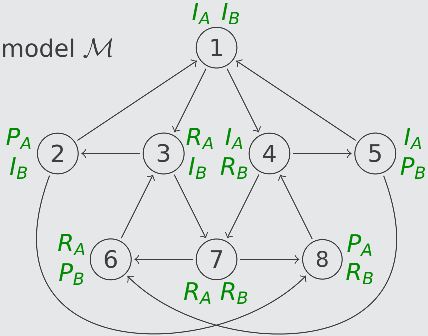
$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \rightarrow \mathsf{F}\,P_A)$

Definition

model $\mathcal{M} = (S, \to, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \to \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \to \mathsf{F}\,P_A)$

$\mathcal{M}, 4 \qquad \neg(R_B\,\mathsf{U}\,P_B)$

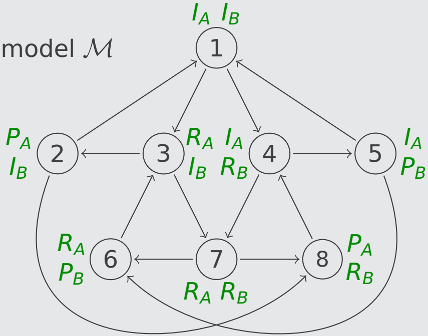
Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \rightarrow \mathsf{F}\,P_A)$

$\mathcal{M}, 4 \nvDash \neg(R_B\,\mathsf{U}\,P_B)$

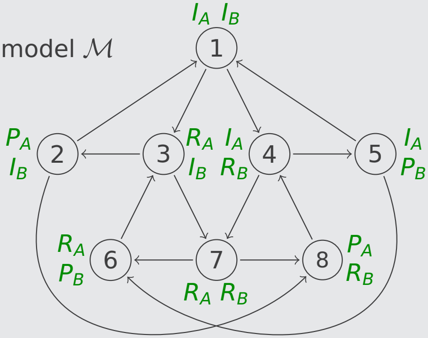
Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \rightarrow \mathsf{F}\,P_A)$

$\mathcal{M}, 4 \nvDash \neg(R_B \,\mathsf{U}\, P_B)$

$\mathcal{M}, 4 \qquad R_B \,\mathsf{U}\, P_B$

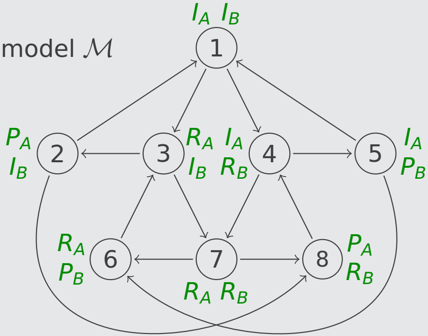
Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \rightarrow \mathsf{F}\,P_A)$

$\mathcal{M}, 4 \nvDash \neg(R_B\,\mathsf{U}\,P_B)$

$\mathcal{M}, 4 \nvDash \quad R_B\,\mathsf{U}\,P_B$

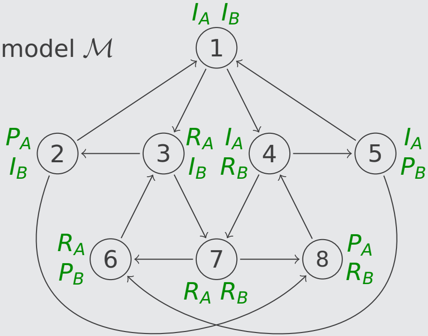
Definition

model $\mathcal{M} = (S, \to, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \quad \Longleftrightarrow \quad \forall$ paths $\pi = s \to \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \to \mathsf{F}\,P_A)$

$\mathcal{M}, 4 \nvDash \neg(R_B \,\mathsf{U}\, P_B)$

$\mathcal{M}, 4 \nvDash \quad R_B \,\mathsf{U}\, P_B$

$\mathcal{M}, 6 \quad \mathsf{X}\,(\mathsf{F}\,I_B \wedge ((\mathsf{X}\,\neg P_B)\,\mathsf{R}\,R_A))$

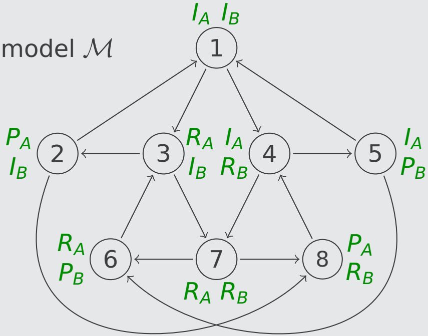
Definition

model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$\mathcal{M}, s \vDash \varphi \iff \forall$ paths $\pi = s \rightarrow \cdots \quad \pi \vDash \varphi$ "formula φ holds in state s of model $\mathcal{M}$"

Example

model $\mathcal{M}$



$\mathcal{M}, 1 \nvDash \mathsf{G}\,(R_A \rightarrow \mathsf{F}\, P_A)$

$\mathcal{M}, 4 \nvDash \neg(R_B \,\mathsf{U}\, P_B)$

$\mathcal{M}, 4 \nvDash R_B \,\mathsf{U}\, P_B$

$\mathcal{M}, 6 \vDash \mathsf{X}\,(\mathsf{F}\, I_B \wedge ((\mathsf{X}\, \neg P_B)\, \mathsf{R}\, R_A))$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \rightarrow, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \quad \Longleftrightarrow \quad \pi \vDash \psi$$

Definition

LTL formulas φ and ψ are **semantically equivalent** ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \rightarrow, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\, \varphi \equiv \mathsf{X} \neg \varphi$$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \rightarrow, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi$$

$$\neg \mathsf{F}\,\varphi \equiv \mathsf{G}\,\neg\varphi$$

$$\neg \mathsf{G}\,\varphi \equiv \mathsf{F}\,\neg\varphi$$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \rightarrow, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\, \varphi \equiv \mathsf{X} \neg \varphi$$

$$\neg \mathsf{F}\, \varphi \equiv \mathsf{G} \neg \varphi$$

$$\neg \mathsf{G}\, \varphi \equiv \mathsf{F} \neg \varphi$$

$$\neg (\varphi\, \mathsf{U}\, \psi) \equiv \neg \varphi\, \mathsf{R} \neg \psi$$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \to, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\, \varphi \equiv \mathsf{X} \neg \varphi$$

$$\neg \mathsf{F}\, \varphi \equiv \mathsf{G} \neg \varphi \qquad \mathsf{F}(\varphi \vee \psi) \equiv \mathsf{F}\, \varphi \vee \mathsf{F}\, \psi$$

$$\neg \mathsf{G}\, \varphi \equiv \mathsf{F} \neg \varphi \qquad \mathsf{G}(\varphi \wedge \psi) \equiv \mathsf{G}\, \varphi \wedge \mathsf{G}\, \psi$$

$$\neg(\varphi \,\mathsf{U}\, \psi) \equiv \neg \varphi \,\mathsf{R} \neg \psi$$

$$\neg(\varphi \,\mathsf{R}\, \psi) \equiv \neg \varphi \,\mathsf{U} \neg \psi$$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$\forall$ models $\mathcal{M} = (S, \to, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi$$

$$\neg \mathsf{F}\,\varphi \equiv \mathsf{G}\,\neg\varphi \qquad \mathsf{F}\,(\varphi \vee \psi) \equiv \mathsf{F}\,\varphi \vee \mathsf{F}\,\psi$$

$$\neg \mathsf{G}\,\varphi \equiv \mathsf{F}\,\neg\varphi \qquad \mathsf{G}\,(\varphi \wedge \psi) \equiv \mathsf{G}\,\varphi \wedge \mathsf{G}\,\psi$$

$$\neg(\varphi\,\mathsf{U}\,\psi) \equiv \neg\varphi\,\mathsf{R}\,\neg\psi \qquad \mathsf{F}\,\varphi \equiv \top\,\mathsf{U}\,\varphi$$

$$\neg(\varphi\,\mathsf{R}\,\psi) \equiv \neg\varphi\,\mathsf{U}\,\neg\psi \qquad \mathsf{G}\,\varphi \equiv \bot\,\mathsf{R}\,\varphi$$

Definition

LTL formulas φ and ψ are semantically equivalent ($\varphi \equiv \psi$) if

$$\forall \text{ models } \mathcal{M} = (S, \rightarrow, L) \quad \forall \text{ paths } \pi \text{ in } \mathcal{M} \qquad \pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\, \varphi \equiv \mathsf{X} \neg \varphi$$

$$\neg \mathsf{F}\, \varphi \equiv \mathsf{G} \neg \varphi$$

$$\neg \mathsf{G}\, \varphi \equiv \mathsf{F} \neg \varphi$$

$$\neg(\varphi\, \mathsf{U}\, \psi) \equiv \neg \varphi\, \mathsf{R} \neg \psi$$

$$\neg(\varphi\, \mathsf{R}\, \psi) \equiv \neg \varphi\, \mathsf{U} \neg \psi$$

$$\varphi\, \mathsf{U}\, \psi \equiv \varphi\, \mathsf{W}\, \psi \wedge \mathsf{F}\, \psi$$

$$\varphi\, \mathsf{W}\, \psi \equiv \varphi\, \mathsf{U}\, \psi \vee \mathsf{G}\, \varphi$$

$$\mathsf{F}(\varphi \vee \psi) \equiv \mathsf{F}\, \varphi \vee \mathsf{F}\, \psi$$

$$\mathsf{G}(\varphi \wedge \psi) \equiv \mathsf{G}\, \varphi \wedge \mathsf{G}\, \psi$$

$$\mathsf{F}\, \varphi \equiv \top\, \mathsf{U}\, \varphi$$

$$\mathsf{G}\, \varphi \equiv \bot\, \mathsf{R}\, \varphi$$

Definition

LTL formulas φ and ψ are semantically equivalent $(\varphi \equiv \psi)$ if

$\forall$ models $\mathcal{M} = (S, \rightarrow, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi$$

$$\neg \mathsf{F}\,\varphi \equiv \mathsf{G}\,\neg\varphi \qquad \mathsf{F}\,(\varphi \vee \psi) \equiv \mathsf{F}\,\varphi \vee \mathsf{F}\,\psi$$

$$\neg \mathsf{G}\,\varphi \equiv \mathsf{F}\,\neg\varphi \qquad \mathsf{G}\,(\varphi \wedge \psi) \equiv \mathsf{G}\,\varphi \wedge \mathsf{G}\,\psi$$

$$\neg(\varphi\,\mathsf{U}\,\psi) \equiv \neg\varphi\,\mathsf{R}\,\neg\psi \qquad \mathsf{F}\,\varphi \equiv \top\,\mathsf{U}\,\varphi$$

$$\neg(\varphi\,\mathsf{R}\,\psi) \equiv \neg\varphi\,\mathsf{U}\,\neg\psi \qquad \mathsf{G}\,\varphi \equiv \bot\,\mathsf{R}\,\varphi$$

$$\varphi\,\mathsf{U}\,\psi \equiv \varphi\,\mathsf{W}\,\psi \wedge \mathsf{F}\,\psi \qquad \varphi\,\mathsf{W}\,\psi \equiv \psi\,\mathsf{R}\,(\varphi \vee \psi)$$

$$\varphi\,\mathsf{W}\,\psi \equiv \varphi\,\mathsf{U}\,\psi \vee \mathsf{G}\,\varphi \qquad \varphi\,\mathsf{R}\,\psi \equiv \psi\,\mathsf{W}\,(\varphi \wedge \psi)$$

Definition

LTL formulas φ and ψ are semantically equivalent $(\varphi \equiv \psi)$ if

$\forall$ models $\mathcal{M} = (S, \to, L)$

$\forall$ paths π in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

Theorem

$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi \qquad \varphi\,\mathsf{U}\,\psi \equiv \neg(\neg\psi\,\mathsf{U}\,(\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$$

$$\neg \mathsf{F}\,\varphi \equiv \mathsf{G}\,\neg\varphi \qquad \mathsf{F}\,(\varphi \vee \psi) \equiv \mathsf{F}\,\varphi \vee \mathsf{F}\,\psi$$

$$\neg \mathsf{G}\,\varphi \equiv \mathsf{F}\,\neg\varphi \qquad \mathsf{G}\,(\varphi \wedge \psi) \equiv \mathsf{G}\,\varphi \wedge \mathsf{G}\,\psi$$

$$\neg(\varphi\,\mathsf{U}\,\psi) \equiv \neg\varphi\,\mathsf{R}\,\neg\psi \qquad \mathsf{F}\,\varphi \equiv \top\,\mathsf{U}\,\varphi$$

$$\neg(\varphi\,\mathsf{R}\,\psi) \equiv \neg\varphi\,\mathsf{U}\,\neg\psi \qquad \mathsf{G}\,\varphi \equiv \bot\,\mathsf{R}\,\varphi$$

$$\varphi\,\mathsf{U}\,\psi \equiv \varphi\,\mathsf{W}\,\psi \wedge \mathsf{F}\,\psi \qquad \varphi\,\mathsf{W}\,\psi \equiv \psi\,\mathsf{R}\,(\varphi \vee \psi)$$

$$\varphi\,\mathsf{W}\,\psi \equiv \varphi\,\mathsf{U}\,\psi \vee \mathsf{G}\,\varphi \qquad \varphi\,\mathsf{R}\,\psi \equiv \psi\,\mathsf{W}\,(\varphi \wedge \psi)$$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi))$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \iff \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)$$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\begin{aligned}
\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \quad &\Longleftrightarrow \quad \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \\
&\Longleftrightarrow \quad \text{not } \exists\, i \geqslant 1 \ \left(\pi^i \vDash \neg\varphi \wedge \neg\psi \ \text{ and } \ \forall\, j < i \ \ \pi^j \vDash \neg\psi\right)
\end{aligned}$$

Theorem

$$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$$

$$\begin{aligned}
\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \quad &\iff \quad \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \\
&\iff \quad \text{not} \ \ \exists\, i \geqslant 1 \ \ \left(\pi^i \vDash \neg\varphi \wedge \neg\psi \ \ \text{and} \ \ \forall\, j < i \ \ \pi^j \vDash \neg\psi\right) \\
&\iff \quad \forall\, i \geqslant 1 \ \ \text{not} \ \ \left(\pi^i \vDash \neg\varphi \wedge \neg\psi \ \ \text{and} \ \ \forall\, j < i \ \ \pi^j \vDash \neg\psi\right)
\end{aligned}$$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$
\begin{aligned}
\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \quad &\Longleftrightarrow \quad \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \\
&\Longleftrightarrow \quad \text{not} \;\; \exists\, i \geqslant 1 \;\; \left(\pi^i \vDash \neg\varphi \wedge \neg\psi \;\; \text{and} \;\; \forall\, j < i \;\; \pi^j \vDash \neg\psi\right) \\
&\Longleftrightarrow \quad \forall\, i \geqslant 1 \;\; \text{not} \;\; \left(\pi^i \vDash \neg\varphi \wedge \neg\psi \;\; \text{and} \;\; \forall\, j < i \;\; \pi^j \vDash \neg\psi\right) \\
&\Longleftrightarrow \quad \forall\, i \geqslant 1 \;\; \left(\pi^i \nvDash \neg\varphi \wedge \neg\psi \;\; \text{or} \;\; \text{not} \;\; \forall\, j < i \;\; \pi^j \vDash \neg\psi\right)
\end{aligned}
$$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\begin{aligned}
\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \quad &\Longleftrightarrow \quad \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \\
&\Longleftrightarrow \quad \text{not } \ \exists\, i \geqslant 1 \ \ (\pi^i \vDash \neg\varphi \wedge \neg\psi \ \text{ and } \ \forall\, j < i \ \ \pi^j \vDash \neg\psi) \\
&\Longleftrightarrow \quad \forall\, i \geqslant 1 \ \text{ not } \ (\pi^i \vDash \neg\varphi \wedge \neg\psi \ \text{ and } \ \forall\, j < i \ \ \pi^j \vDash \neg\psi) \\
&\Longleftrightarrow \quad \forall\, i \geqslant 1 \ \ (\pi^i \nvDash \neg\varphi \wedge \neg\psi \ \text{ or } \ \text{not } \ \forall\, j < i \ \ \pi^j \vDash \neg\psi) \\
&\Longleftrightarrow \quad \forall\, i \geqslant 1 \ \ (\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \nvDash \neg\psi)
\end{aligned}$$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$
\begin{aligned}
\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) &\iff \pi \nvDash \neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \\
&\iff \text{not } \exists\, i \geqslant 1 \;\; (\pi^i \vDash \neg\varphi \wedge \neg\psi \;\text{ and }\; \forall\, j < i \;\; \pi^j \vDash \neg\psi) \\
&\iff \forall\, i \geqslant 1 \;\; \text{not } (\pi^i \vDash \neg\varphi \wedge \neg\psi \;\text{ and }\; \forall\, j < i \;\; \pi^j \vDash \neg\psi) \\
&\iff \forall\, i \geqslant 1 \;\; (\pi^i \nvDash \neg\varphi \wedge \neg\psi \;\text{ or }\; \text{not } \forall\, j < i \;\; \pi^j \vDash \neg\psi) \\
&\iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \nvDash \neg\psi) \\
&\iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \vDash \psi)
\end{aligned}
$$

Theorem

$$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Theorem

$\varphi \mathsf{U} \psi \equiv \neg(\neg\psi \mathsf{U} (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \psi$

$$\pi \vDash \neg(\neg\psi \mathsf{U} (\neg\varphi \wedge \neg\psi)) \iff \forall i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \vDash \psi)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \,\mathsf{U}\, \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \, \mathsf{U} \, \psi$ and consider smallest m such that $\pi^m \vDash \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\; \text{or} \;\; \exists\, j < i \;\; \pi^j \vDash \psi)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \, \mathsf{U} \, \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F} \, \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \;\; \left(\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \, \mathsf{U} \, \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F}\,\psi$ and $\pi^i \vDash \varphi$ for all $i < m$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \vDash \psi)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \,\mathsf{U}\, \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F}\,\psi$ and $\pi^i \vDash \varphi$ for all $i < m$
- consider $i \geqslant 1$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \, \mathsf{U} \, \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F} \, \psi$ and $\pi^i \vDash \varphi$ for all $i < m$
- consider $i \geqslant 1$
  - if $i > m$ then $\exists\, j < i \ \ \pi^j \vDash \psi$

Theorem

$\varphi \mathsf{U} \psi \equiv \neg(\neg\psi \mathsf{U} (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \psi$

$$\pi \vDash \neg(\neg\psi \mathsf{U} (\neg\varphi \wedge \neg\psi)) \iff \forall i \geqslant 1 \ (\pi^i \vDash \varphi \vee \psi \text{ or } \exists j < i \ \pi^j \vDash \psi)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \mathsf{U} \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F} \psi$ and $\pi^i \vDash \varphi$ for all $i < m$
- consider $i \geqslant 1$
  - if $i > m$ then $\exists j < i \ \pi^j \vDash \psi$ and if $i \leqslant m$ then $\pi^i \vDash \varphi \vee \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \;\; (\pi^i \vDash \varphi \vee \psi \;\; \text{or} \;\; \exists\, j < i \;\; \pi^j \vDash \psi)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \varphi \, \mathsf{U} \, \psi$ and consider smallest m such that $\pi^m \vDash \psi$
- $\pi \vDash \mathsf{F}\, \psi$ and $\pi^i \vDash \varphi$ for all $i < m$
- consider $i \geqslant 1$
  - if $i > m$ then $\exists\, j < i \;\; \pi^j \vDash \psi$ and if $i \leqslant m$ then $\pi^i \vDash \varphi \vee \psi$
- $\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi))$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \; \left(\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists\, j < i \;\; \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$
- there exists smallest m such that $\pi^m \vDash \psi$

Theorem

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$
- there exists smallest m such that $\pi^m \vDash \psi$
- if $i < m$ then $\pi^i \vDash \neg\psi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall\, i \geqslant 1 \ \left(\pi^i \vDash \varphi \vee \psi \ \text{ or } \ \exists\, j < i \ \ \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$
- there exists smallest m such that $\pi^m \vDash \psi$
- if $i < m$ then $\pi^i \vDash \neg\psi$ and hence $\pi^i \vDash \varphi$

Theorem

$\varphi \, \mathsf{U} \, \psi \equiv \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$

$$\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \iff \forall \, i \geqslant 1 \; \left(\pi^i \vDash \varphi \vee \psi \;\text{ or }\; \exists \, j < i \;\; \pi^j \vDash \psi\right)$$

Proof

- consider arbitrary path $\pi = s_1 \to s_2 \to s_3 \to \cdots$ in arbitrary model $\mathcal{M}$
- suppose $\pi \vDash \neg(\neg\psi \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F} \, \psi$
- there exists smallest m such that $\pi^m \vDash \psi$
- if $i < m$ then $\pi^i \vDash \neg\psi$ and hence $\pi^i \vDash \varphi$
- $\pi \vDash \varphi \, \mathsf{U} \, \psi$

Outline

Mutual Exclusion

- concurrent processes sharing resource

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code
- at most one process can be in its critical section at any time

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code
- at most one process can be in its critical section at any time

desired:

protocol for determining which process is allowed to enter its critical section at which time

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code
- at most one process can be in its critical section at any time

desired:

protocol for determining which process is allowed to enter its critical section at which time

expected properties:

safety only one process is in its critical section at any time

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code
- at most one process can be in its critical section at any time

desired:

protocol for determining which process is allowed to enter its critical section at which time

expected properties:

safety	only one process is in its critical section at any time
liveness	whenever process requests to enter its critical section, it will eventually be permitted to do so

Mutual Exclusion

- concurrent processes sharing resource
- identify critical sections (including access to shared resource) in each process' code
- at most one process can be in its critical section at any time

desired:

protocol for determining which process is allowed to enter its critical section at which time

expected properties:

safety	only one process is in its critical section at any time
liveness	whenever process requests to enter its critical section, it will eventually be permitted to do so
non-blocking	each process can always request to enter its critical section

Mutual Exclusion

- two processes have three states each:

  (n) non–critical state

Mutual Exclusion

- two processes have three states each:

  (n) non–critical state   (t) trying to enter critical state

Mutual Exclusion

- two processes have three states each:

  (n) non–critical state   (t) trying to enter critical state   (c) critical state

Mutual Exclusion

- two processes have three states each:

  (n) non−critical state   (t) trying to enter critical state   (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$

Mutual Exclusion

- two processes have three states each:

  (n) non−critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$

- asynchronous interleaving

Mutual Exclusion (first modeling attempt)

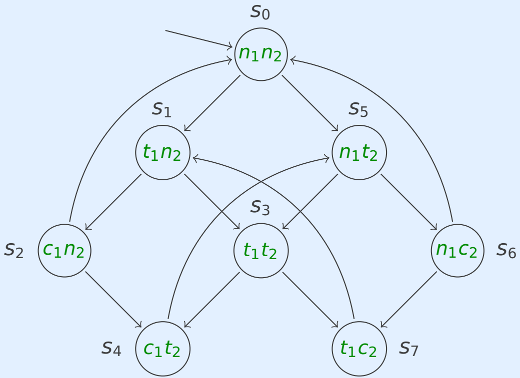
- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$

- asynchronous interleaving

- model (protocol):

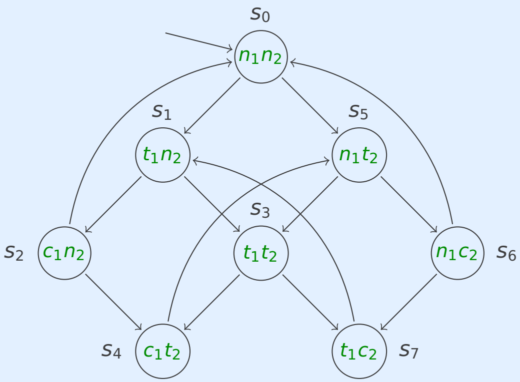


Mutual Exclusion (first modeling attempt)

- two processes have three states each:

  (n) non–critical state   (t) trying to enter critical state   (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots \quad (n_i t_i c_i)^\omega$
- asynchronous interleaving
- model (protocol):
- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$

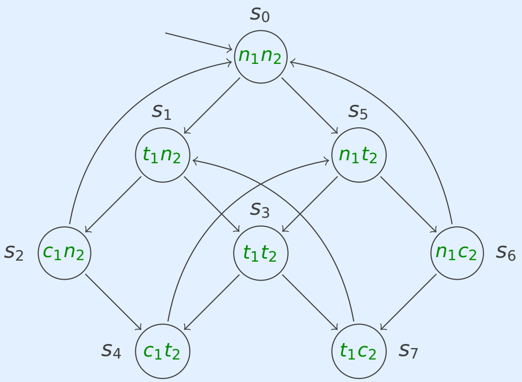


Mutual Exclusion (first modeling attempt)

- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$
- asynchronous interleaving
- model (protocol):
- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓

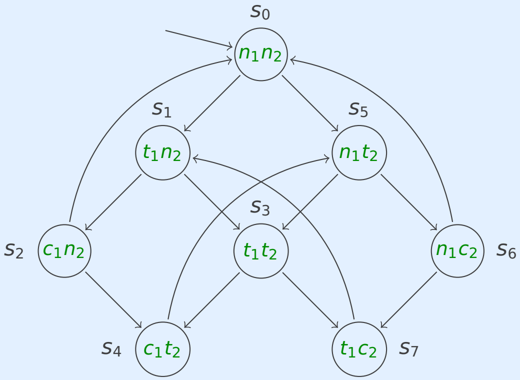


Mutual Exclusion (first modeling attempt)

- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i\, t_i\, c_i)^\omega$
- asynchronous interleaving
- model (protocol):
- safety: $\mathrm{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathrm{G}\,(t_1 \to \mathrm{F}\,c_1)$

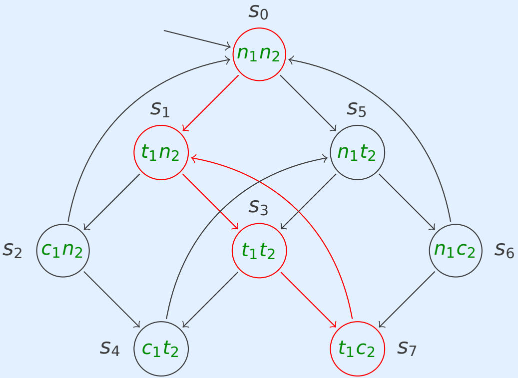


Mutual Exclusion (first modeling attempt)

- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$
- asynchronous interleaving
- model (protocol):



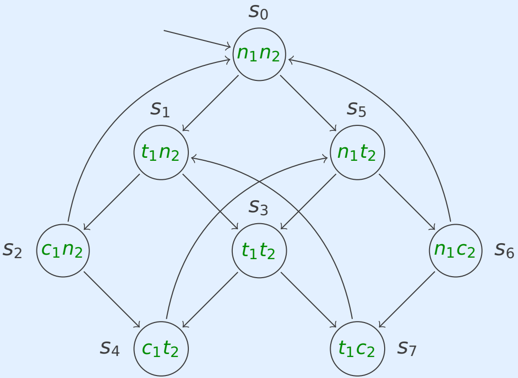
- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathsf{G}\,(t_1 \to \mathsf{F}\, c_1)$ ✗

Mutual Exclusion (first modeling attempt)

- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

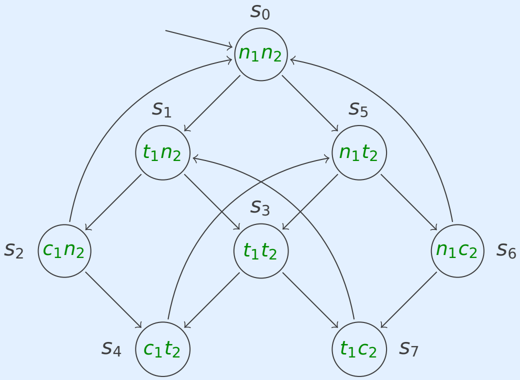
- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i t_i c_i)^\omega$
- asynchronous interleaving
- model (protocol):
- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathsf{G}\,(t_1 \to \mathsf{F}\,c_1)$ ✗
- non–blocking holds but is not expressible in LTL



- two processes have three states each:

  (n) non–critical state (t) trying to enter critical state (c) critical state

- each process undergoes transitions in cycle $n_i \to t_i \to c_i \to n_i \to \cdots$ $(n_i\, t_i\, c_i)^\omega$
- asynchronous interleaving
- model (protocol):

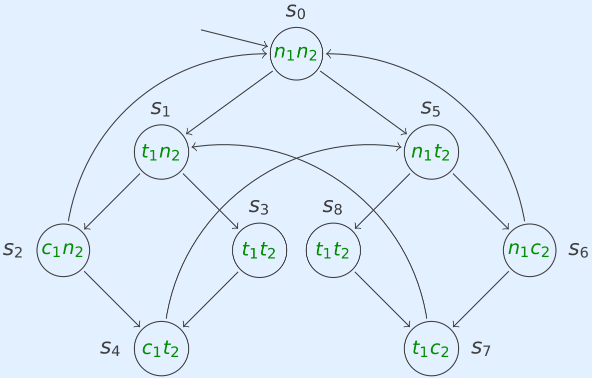


- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathsf{G}\,(t_1 \to \mathsf{F}\, c_1)$ ✗
- non–blocking holds but is not expressible in LTL

  $\mathsf{AG}(n_1 \to \mathsf{EX}\, t_1)$ in CTL

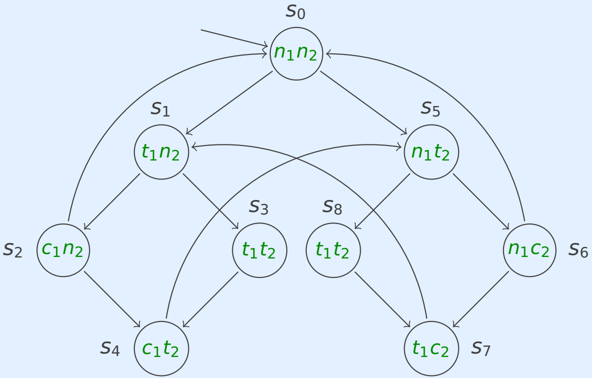
Mutual Exclusion (second modeling attempt)

- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$
- liveness: $\mathsf{G}\,(t_1 \rightarrow \mathsf{F}\,c_1)$



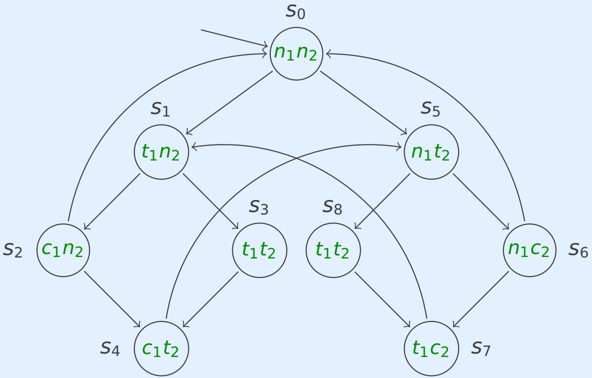
Mutual Exclusion (second modeling attempt)

- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathsf{G}\,(t_1 \rightarrow \mathsf{F}\,c_1)$ ✓



Mutual Exclusion (second modeling attempt)

- safety: $\mathsf{G}\,\neg(c_1 \wedge c_2)$ ✓
- liveness: $\mathsf{G}\,(t_1 \rightarrow \mathsf{F}\,c_1)$ ✓



NuSMV (New Symbolic Model Verifier)

provides language for describing models and checks satisfaction of LTL and CTL formulas

Mutual Exclusion Protocol in NuSMV

```
MODULE main
VAR
  pr1 : process prc ( pr2.st, turn, FALSE ) ;
  pr2 : process prc ( pr1.st, turn, TRUE ) ;
  turn : boolean ;
ASSIGN
  init ( turn ) := FALSE ;

LTLSPEC G ! (( pr1.st = c ) & ( pr2.st = c ))   -- safety
LTLSPEC G (( pr1.st = t ) -> F ( pr1.st = c ))  -- liveness
LTLSPEC G (( pr2.st = t ) -> F ( pr2.st = c ))  -- liveness

MODULE prc ( other-st, turn, myturn )
VAR st : { n, t, c } ;
ASSIGN
  init ( st ) := n ;
  next ( st ) := case
    ( st = n )                        : { n, t } ;
    ( st = t ) & ( other-st = n )     : c ;
    ( st = t ) & ( other-st = t )     : c ;
    ( st = c )                        : st ;
    TRUE                              : st ;
  esac ;
  next ( turn ) := case
    turn = myturn & st = c            : ! turn ;
    TRUE                              : turn ;
  esac ;

FAIRNESS running
FAIRNESS ! ( st = c )
```

Outline

Huth and Ryan

- Section 3.1
- Section 3.2
- Section 3.3
- Section 3.7
- Section 6.3

Huth and Ryan

- Section 3.1
- Section 3.2
- Section 3.3
- Section 3.7
- Section 6.3

Model Checking Tools

- NuSMV
- Spin

Important Concepts

- $[\![\varphi]\!]$
- F
- fixed point
- G
- greatest fixed point
- Knaster–Tarski
- least fixed point
- linear–time temporal logic
- liveness
- LTL
- non–blocking
- path
- $\text{pre}_\forall$
- $\text{pre}_\exists$
- R
- safety
- symbolic model checking
- U
- W
- X

Important Concepts

- $[\![\varphi]\!]$
- F
- fixed point
- G
- greatest fixed point
- Knaster–Tarski
- least fixed point
- linear–time temporal logic
- liveness
- LTL
- non–blocking
- path
- $\text{pre}_\forall$
- $\text{pre}_\exists$
- R
- safety
- symbolic model checking
- U
- W
- X

homework for May 28