universität innsbruck

26S lecture 10

# Logic

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

## Outline





### 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 $f(x_1, \ldots, x_n) = \overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$
- 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 $\varphi$ in state $s \in S$ of model $\mathcal{M} = (S, \to, L)$ is defined by induction on $\varphi$

## Definition

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

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

for all models $\mathcal{M} = (S, \to, L)$ 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 $\mathcal{M} = (S, \to, L)$ and CTL formula $\varphi$

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

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

- $p$: label $s$ $\iff$ $p \in L(s)$ — $\neg\varphi$: label $s$ $\iff$ $s$ is not labelled with $\varphi$
- $\varphi \wedge \psi$: label $s$ $\iff$ $s$ is labelled with both $\varphi$ and $\psi$
- $\mathsf{EX}\,\varphi$: label $s$ $\iff$ $t$ is labelled with $\varphi$ for some $t$ with $s \to t$
- $\mathsf{EG}\,\varphi$:
  ① label every $s$ that is labelled with $\varphi$
  ② remove label from $s$ $\iff$ $t$ is not labelled with $\mathsf{EG}\,\varphi$ for all $t$ with $s \to t$
  ③ repeat ② until no change
- $\mathsf{E}[\varphi\,\mathsf{U}\,\psi]$: label $s$ $\iff$
  ① $s$ is labelled with $\psi$
  ② $s$ is labelled with $\varphi$ and $t$ with $\mathsf{E}[\varphi\,\mathsf{U}\,\psi]$ for some $t$ with $s \to t$
  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



# Outline

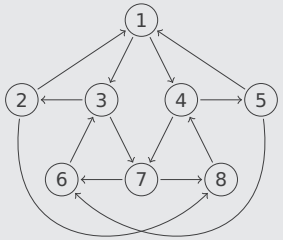
symbolic model checking = (CTL) model checking with BDDs

## Questions

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



## Example




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

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

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

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

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

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

- 8 states require 3 boolean variables

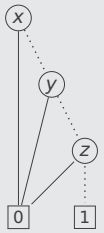
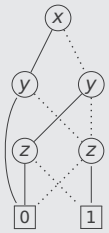
| state | $x$ | $y$ | $z$ | | state | $x$ | $y$ | $z$ | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | $\bar{x}\bar{y}\bar{z}$ | 5 | 1 | 0 | 0 | $x\bar{y}\bar{z}$ |
| 2 | 0 | 0 | 1 | $\bar{x}\bar{y}z$ | 6 | 1 | 0 | 1 | $x\bar{y}z$ |
| 3 | 0 | 1 | 0 | $\bar{x}y\bar{z}$ | 7 | 1 | 1 | 0 |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



## 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 | $\{1\}$ | $\{1,2\}$ | $\varnothing$ | $\{2,3,6\}$ |
|---|---|---|---|---|
| boolean function | $\bar{x}\bar{y}\bar{z}$ | $\bar{x}\bar{y}$ | 0 | $\bar{y}z + \bar{x}y\bar{z}$ |
| reduced OBDD |  |  |  |  |





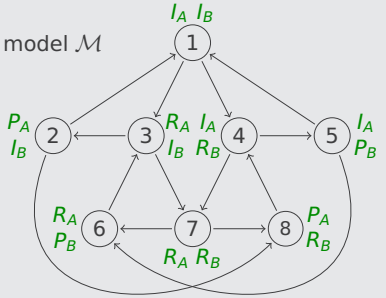
## Example (cont'd)

| 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 | $xyz$ |

transition relation

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

model $\mathcal{M}$




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

## Definition

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

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

## Lemma

$$[\![\top]\!] = S \qquad [\![p]\!] = \{s \in S \mid p \in L(s)\}$$
$$[\![\bot]\!] = \varnothing \qquad [\![\mathsf{AX}\,\varphi]\!] = \mathrm{pre}_\forall([\![\varphi]\!])$$
$$[\![\neg\varphi]\!] = S - [\![\varphi]\!] \qquad [\![\mathsf{EX}\,\varphi]\!] = \mathrm{pre}_\exists([\![\varphi]\!])$$
$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$
$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$
$$[\![\varphi \to \psi]\!] = (S - [\![\varphi]\!]) \cup [\![\psi]\!] \qquad \mathrm{pre}_\forall(X) = S - \mathrm{pre}_\exists(S - X)$$



## Symbolic Model Checking Operations

| required operations | | BDD representation |
|---|---|---|
| complement | $S - X$ | $\mathrm{apply}(\oplus, B_S, B_X)$ |
| union | $X \cup Y$ | $\mathrm{apply}(+, B_X, B_Y)$ |
| intersection | $X \cap Y$ | $\mathrm{apply}(\cdot, B_X, B_Y)$ |
| | $\mathrm{pre}_\exists(X)$ | $\mathrm{exists}(x'_1, \cdots (\mathrm{exists}(x'_n, \mathrm{apply}(\cdot, B_\to, \underbrace{B_{X'}}))) \cdots)$ |

replace $x_1, \ldots, x_n$ by $x'_1, \ldots, x'_n$ in $B_X$

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



## Lemma

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

## Remark

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

## Theorem (Knaster–Tarski)

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

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



## Theorem (Knaster–Tarski)

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

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

see overlay version of slides

## Definition

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

## Example

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

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

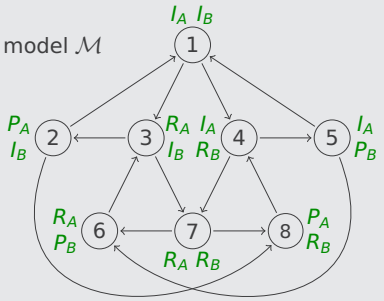
$F^2_{\mathsf{AF}}(X) = F_{\mathsf{AF}}(F_{\mathsf{AF}}(X)) = \{1,2,3\} \cup \{6\}$

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

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

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

model $\mathcal{M}$






## Definition

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

## Example

$\varphi = P_A \vee I_B$

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

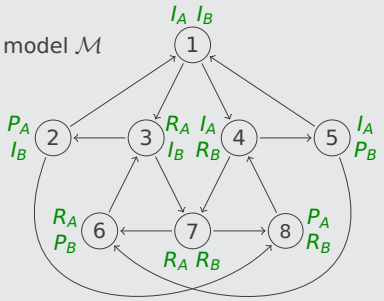
$F_{\mathsf{EG}}(X) = [\![\varphi]\!] = \{1,2,3,8\}$

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

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

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

model $\mathcal{M}$






## Definition

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

## Lemma

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

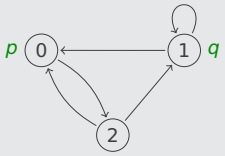
## Algorithm

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



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

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




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

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

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

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

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

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

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

## Outline





Particify with session ID **6893 6178**

### 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





### 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

  according to following BNF grammar:

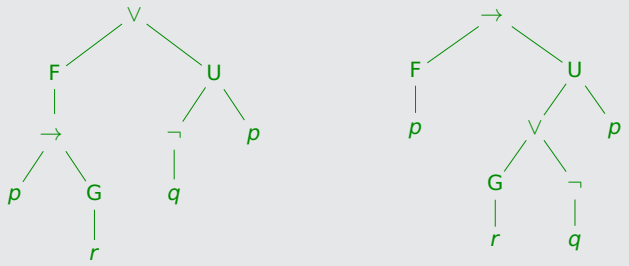
$$\varphi ::= \bot \mid \top \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid (\mathsf{X}\,\varphi) \mid (\mathsf{F}\,\varphi) \mid (\mathsf{G}\,\varphi) \mid (\varphi\,\mathsf{U}\,\varphi) \mid (\varphi\,\mathsf{W}\,\varphi)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

- 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 $\mathsf{F}(p \to \mathsf{G}\, r) \vee \neg q \,\mathsf{U}\, p$ $\qquad$ $\mathsf{F}\, p \to (\mathsf{G}\, r \vee \neg q)\,\mathsf{U}\, p$

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 $s_1 \to s_2 \to \cdots$
- $\forall$ 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 $\varphi$ with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$

$$\pi \vDash \varphi$$

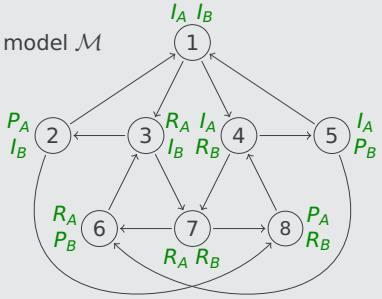
is defined by induction on $\varphi$:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\pi \vDash \top$ | | $\pi \nvDash \bot$ | | $\pi \vDash \varphi \wedge \psi$ | $\iff$ | $\pi \vDash \varphi$ and | $\pi \vDash \psi$ |
| $\pi \vDash p$ | $\iff$ | $p \in L(s_1)$ | | $\pi \vDash \varphi \vee \psi$ | $\iff$ | $\pi \vDash \varphi$ or | $\pi \vDash \psi$ |
| $\pi \vDash \neg\varphi$ | $\iff$ | $\pi \nvDash \varphi$ | | $\pi \vDash \varphi \to \psi$ | $\iff$ | $\pi \nvDash \varphi$ or | $\pi \vDash \psi$ |



## Example

model $\mathcal{M}$




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

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

special notation for infinite paths:

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

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

## Definition

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

$$\pi \vDash \varphi$$

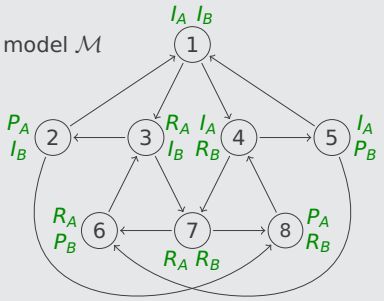
is defined by induction on $\varphi$:

$$\begin{aligned}
\pi &\vDash \mathsf{X}\,\varphi && \iff && \pi^2 \vDash \varphi \\
\pi &\vDash \mathsf{F}\,\varphi && \iff && \exists\, i \geqslant 1 \quad \pi^i \vDash \varphi \\
\pi &\vDash \mathsf{G}\,\varphi && \iff && \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi \\
\pi &\vDash \varphi\,\mathsf{U}\,\psi && \iff && \exists\, i \geqslant 1 \quad \pi^i \vDash \psi \quad \text{and} \quad \forall\, j < i \quad \pi^j \vDash \varphi \\
\pi &\vDash \varphi\,\mathsf{W}\,\psi && \iff && (\exists\, i \geqslant 1 \quad \pi^i \vDash \psi \quad \text{and} \quad \forall\, j < i \quad \pi^j \vDash \varphi) \quad \text{or} \quad \forall\, i \geqslant 1 \quad \pi^i \vDash \varphi \\
\pi &\vDash \varphi\,\mathsf{R}\,\psi && \iff && (\exists\, i \geqslant 1 \quad \pi^i \vDash \varphi \quad \text{and} \quad \forall\, j \leqslant i \quad \pi^j \vDash \psi) \quad \text{or} \quad \forall\, i \geqslant 1 \quad \pi^i \vDash \psi
\end{aligned}$$



## Example

model $\mathcal{M}$




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

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

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

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



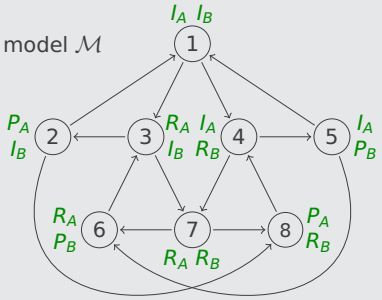
## Definition

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

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

## Example

model $\mathcal{M}$




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

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

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

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



## Definition

LTL formulas $\varphi$ and $\psi$ are semantically equivalent ($\varphi \equiv \psi$) if

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

$\forall$ paths $\pi$ in $\mathcal{M}$

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

## Theorem

$$\begin{aligned}
\neg\mathsf{X}\,\varphi &\equiv \mathsf{X}\,\neg\varphi & \qquad \varphi\,\mathsf{U}\,\psi &\equiv \neg(\neg\psi\,\mathsf{U}\,(\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi \\
\neg\mathsf{F}\,\varphi &\equiv \mathsf{G}\,\neg\varphi & \qquad \mathsf{F}\,(\varphi \vee \psi) &\equiv \mathsf{F}\,\varphi \vee \mathsf{F}\,\psi \\
\neg\mathsf{G}\,\varphi &\equiv \mathsf{F}\,\neg\varphi & \qquad \mathsf{G}\,(\varphi \wedge \psi) &\equiv \mathsf{G}\,\varphi \wedge \mathsf{G}\,\psi \\
\neg(\varphi\,\mathsf{U}\,\psi) &\equiv \neg\varphi\,\mathsf{R}\,\neg\psi & \qquad \mathsf{F}\,\varphi &\equiv \top\,\mathsf{U}\,\varphi \\
\neg(\varphi\,\mathsf{R}\,\psi) &\equiv \neg\varphi\,\mathsf{U}\,\neg\psi & \qquad \mathsf{G}\,\varphi &\equiv \bot\,\mathsf{R}\,\varphi \\
\varphi\,\mathsf{U}\,\psi &\equiv \varphi\,\mathsf{W}\,\psi \wedge \mathsf{F}\,\psi & \qquad \varphi\,\mathsf{W}\,\psi &\equiv \psi\,\mathsf{R}\,(\varphi \vee \psi) \\
\varphi\,\mathsf{W}\,\psi &\equiv \varphi\,\mathsf{U}\,\psi \vee \mathsf{G}\,\varphi & \qquad \varphi\,\mathsf{R}\,\psi &\equiv \psi\,\mathsf{W}\,(\varphi \wedge \psi)
\end{aligned}$$

**Theorem**

$\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\psi \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\, \psi$

see overlay version for proof



## Outline





**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

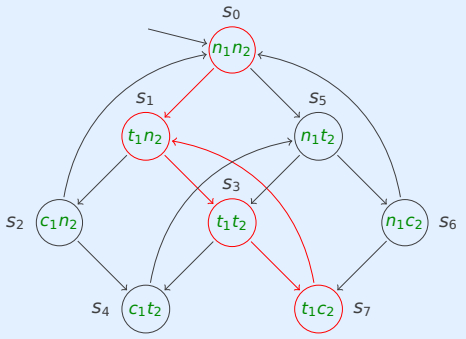
expected properties:

| | |
|---|---|
| **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 |



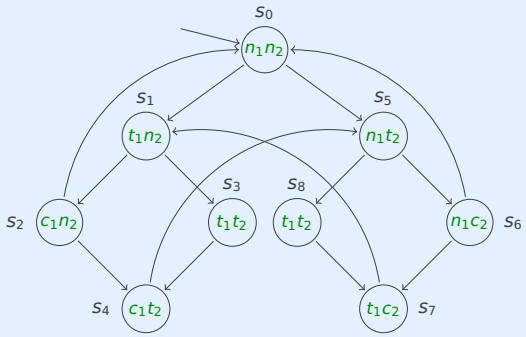
**Mutual Exclusion (first modeling attempt)**

- 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: $\mathsf{G}\neg(c_1 \wedge c_2)$ ✓
- 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: $\mathsf{G}\,(t_1 \rightarrow \mathsf{F}\,c_1)$ ✓




## 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

## 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

homework for May 28