

---

# Modal and Temporal Logics

Colin Stirling  
School of Informatics  
University of Edinburgh

July 26, 2003

# Computational Properties

- **Satisfiability Problem:** “Given a modal  $\mu$ -calculus formula  $\Phi$ , is  $\Phi$  satisfiable?” is **EXPTIME**-complete.
- **Tree Model Property** If  $\Phi$  is satisfiable then  $\Phi$  is satisfiable in a transition system/Kripke model that is a (regular) infinite tree.
- **Finite Model Property** If  $\Phi$  is satisfiable then  $\Phi$  is satisfiable in a finite transition system/Kripke model.
- **Model Checking Problem** “Given a finite model, a state  $E$  and closed  $\Phi$ , does  $E \models \Phi$  ?” Its exact complexity is a long standing **OPEN** problem.

Best known upper bound is **NP  $\cap$  co-NP**

# Why Model Checking is Complex

- Problem: understanding alternations of fixed points

$$\mu Y_1. \nu Z_1. \dots, \mu Y_n. \nu Z_n. \Phi(Y_1, \dots, Y_n, Z_1, \dots, Z_n)$$

- In terms of expressive power, there is a strict alternation depth hierarchy
- Nice subset of modal  $\mu$ -calculus: alternation free  $\mu$ -calculus (AM).

$\Phi \in \text{AM}$  provided that if  $\mu Y. \Psi_1$  and  $\nu Z. \Psi_2$  are subformulas of  $\Phi$  then  $Y$  is not free in  $\Psi_2$  and  $Z$  is not free in  $\Psi_1$

- AM contains CTL (but not CTL\*). Model checking AM is **P-complete**

# Games

- A game account of  $E \models \Phi$  ( $\Phi$  closed and in normal form)
- $G(E, \Phi)$  is played by **R (the refuter)** and **V (the verifier)**
- **R attempts to show that  $E \not\models \Phi$  and V aims to frustrate R.**
- A play of  $G(E_0, \Phi_0)$  is a sequence of the form

$$(E_0, \Phi_0) \dots (E_n, \Phi_n) \dots,$$

where each  $\Phi_i$  is a subformula of  $\Phi_0$

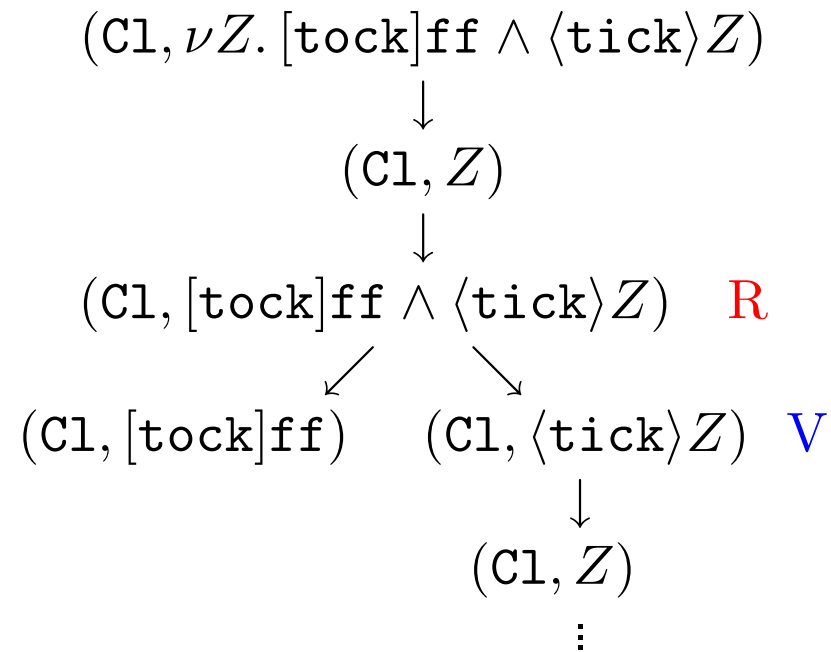
## Rules of play

If part of a play is  $(E_0, \Phi_0) \dots (E_j, \Phi_j)$ , then the next move is by cases on  $\Phi_j$

- $\Phi_j = \Psi_1 \wedge \Psi_2$ : **R** chooses  $\Psi_i = \Phi_{j+1}$  and  $E_{j+1} = E_j$
- $\Phi_j = \Psi_1 \vee \Psi_2$ : **V** chooses  $\Psi_i = \Phi_{j+1}$  and  $E_{j+1} = E_j$
- $\Phi_j = [K]\Psi$ : **R** chooses  $E_j \xrightarrow{a} E_{j+1}$  with  $a \in K$  and  $\Phi_{j+1} = \Psi$
- $\Phi_j = \langle K \rangle \Psi$ : **V** chooses  $E_j \xrightarrow{a} E_{j+1}$  with  $a \in K$  and  $\Phi_{j+1} = \Psi$
- $\Phi_j = \sigma Z. \Psi$ :  $\Phi_{j+1} = Z$  and  $E_{j+1} = E_j$
- $\Phi_j = Z$ : if  $Z$  identifies  $\sigma Z. \Psi$ , then  $\Phi_{j+1} = \Psi$  and  $E_{j+1} = E_j$

# Example

$G(C1, \nu Z. [\text{tock}]ff \wedge \langle \text{tick} \rangle Z)$



## When R wins a play

1. The play is  $(E_0, \Phi_0) \dots (E_n, \Phi_n)$  and
  - $\Phi_n = \text{ff}$ , or
  - $\Phi_n = \langle K \rangle \Psi$  and  $\{F : E_n \xrightarrow{a} F \text{ and } a \in K\} = \emptyset$
2. The play  $(E_0, \Phi_0) \dots (E_n, \Phi_n) \dots$  has infinite length and the outermost fixed point variable  $X$ , which occurs infinitely often is a **least fixed point**,  $\mu X. \Psi$

## When V wins a play

1. The play is  $(E_0, \Phi_0) \dots (E_n, \Phi_n)$  and
  - $\Phi_n = \text{tt}$ , or
  - $\Phi_n = [K]\Psi$  and  $\{F : E_n \xrightarrow{a} F \text{ and } a \in K\} = \emptyset$
2. The play  $(E_0, \Phi_0) \dots (E_n, \Phi_n) \dots$  has infinite length and the outermost fixed point variable  $X$ , which occurs infinitely often is a **greatest fixed point**,  $\nu X. \Psi$



# Strategies

A strategy for a player is a family of rules telling the player how to move. A history-free strategy, depends only on current position.

For player R

- at position  $(E, \Phi_1 \wedge \Phi_2)$  choose  $(E, \Phi_i)$  where  $i = 1$  or  $i = 2$
- at position  $(E, [K]\Phi)$  choose  $(F, \Phi)$  where  $E \xrightarrow{a} F$  and  $a \in K$

For player V

- at position  $(E, \Phi_1 \vee \Phi_2)$  choose  $(E, \Phi_i)$  where  $i = 1$  or  $i = 2$
- at position  $(E, \langle K \rangle \Phi)$  choose  $(F, \Phi)$  where  $E \xrightarrow{a} F$  and  $a \in K$

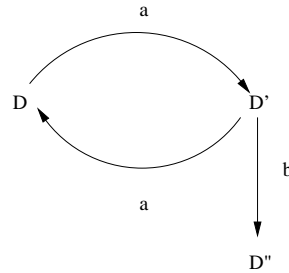
# Winning Strategies

- A player uses the strategy  $\pi$  in a play provided all her moves in the play obey the rules in  $\pi$ .
- The strategy  $\pi$  is winning if the player wins every play in which she uses  $\pi$ .

## Proposition

1.  $E \models \Phi$  iff  $V$  has a history-free winning strategy for  $G(E, \Phi)$
2.  $E \not\models \Phi$  iff  $R$  has a history-free winning strategy for  $G(E, \Phi)$

## Example

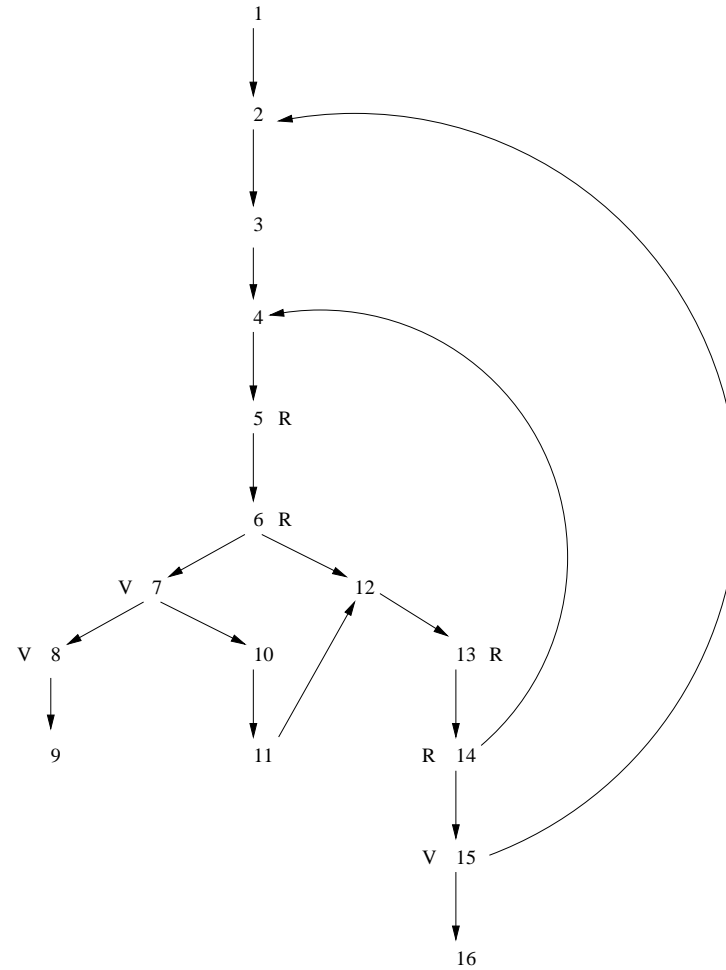


$D \not\models \Psi$

$$\Psi = \mu Y. \nu Z. [a](((\langle b \rangle \text{tt} \vee Y) \wedge Z))$$

The refuter has a winning strategy for  $G(D, \Psi)$

# Game Graph



## Positions

- |   |  |
|---|--|
| 1 : $(D, \mu Y. \nu Z. [a]((\langle b \rangle \mathbf{tt} \vee Y) \wedge Z))$ | 9 : $(D'', \mathbf{tt})$   |
| 2 : $(D, Y)$  | 10 : $(D', Y)$   |
| 3 : $(D, \nu Z. [a]((\langle b \rangle \mathbf{tt} \vee Y) \wedge Z))$        | 11 : $(D', \nu Z. [a]((\langle b \rangle \mathbf{tt} \vee Y) \wedge Z))$ |
| 4 : $(D, Z)$  | 12 : $(D', Z)$   |
| 5 : $(D, [a]((\langle b \rangle \mathbf{tt} \vee Y) \wedge Z))$               | 13 : $(D', [a]((\langle b \rangle \mathbf{tt} \vee Y) \wedge Z))$        |
| 6 : $(D', (\langle b \rangle \mathbf{tt} \vee Y) \wedge Z)$                   | 14 : $(D, (\langle b \rangle \mathbf{tt} \vee Y) \wedge Z)$              |
| 7 : $(D', \langle b \rangle \mathbf{tt} \vee Y)$                              | 15 : $(D, \langle b \rangle \mathbf{tt} \vee Y)$                         |
| 8 : $(D', \langle b \rangle \mathbf{tt})$                                     | 16 : $(D, \langle b \rangle \mathbf{tt})$                                |

R's winning strategy: at 6 choose 12 and at 14 choose 15

# Model Checking

- **Model Checking Problem** “Given a finite model, a state  $E$  and closed  $\Phi$ , does  $E \models \Phi$ ?”
- Equivalent to solving the game problem: does  $V$  have a winning strategy for the finite game  $G(E, \Phi)$
- **Why in  $\mathbf{NP} \cap \mathbf{co-NP}$ ?** Guess a strategy: easy to check if it is winning in  $O(n^2)$  time. Therefore in **NP**. Games are closed under complement: so, also in **co-NP**.
- Abstract to an equivalent but simpler graph game

# Parity Games

A parity game is a directed graph  $G = (N, \rightarrow, L)$

- $N$  is a finite subset of  $\mathbb{N}$
- $\rightarrow$  is a total edge relation:  $\forall i. \exists j. i \rightarrow j$
- $L$  labels each vertex with R or with V:  $L(i)$  tells us which player is responsible for moving from vertex  $i$ .



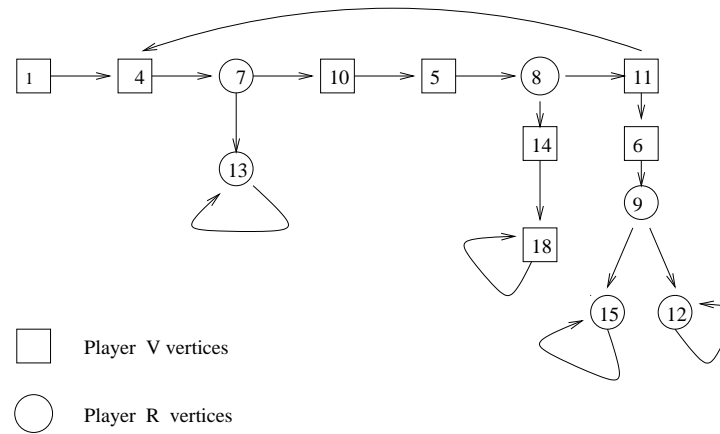
## Playing and Winning

1. A play of  $G$  is an infinite sequence of vertices  $i_0, i_1, \dots$  where  $i_0$  is least vertex in  $N$ 
  - if  $L(i_j) = R$  then  $R$  chooses an edge  $i_j \rightarrow i_{j+1}$
  - if  $L(i_j) = V$  then  $V$  chooses an edge  $i_j \rightarrow i_{j+1}$
2. Winner of a play: the label of the least  $i$  that occurs infinitely often in the play.
3. A history-free strategy for a player is a family of rules telling the player how to move that only depends only on current position

# Determinization

- A player uses the strategy  $\pi$  in a play provided all her moves in the play obey the rules in  $\pi$ .
- The strategy  $\pi$  is winning if the player wins every play in which she uses  $\pi$ .
- **Proposition** For any parity game  $G$  one of players wins  $G$  with a history free winning strategy **Prove this later**
- **Proposition** Any game  $G(E, \Phi)$  can be transformed into an equivalent parity game  $G$  whose size is linear in  $G(E, \Phi)$

# Example



## Force Sets: $X \subseteq N$

$$\text{Force}_P^0(X) = X \text{ for } P \in \{R, V\}$$

$$\begin{aligned} \text{Force}_R^{i+1}(X) &= \text{Force}_R^i(X) \\ &\cup \{j : L(j) = R \text{ and } \exists k \in \text{Force}_R^i(X). j \rightarrow k\} \\ &\cup \{j : L(j) = V \text{ and } \forall k. \text{ if } j \rightarrow k \text{ then } k \in \text{Force}_R^i(X)\} \end{aligned}$$

$$\begin{aligned} \text{Force}_V^{i+1}(X) &= \text{Force}_V^i(X) \\ &\cup \{j : L(j) = V \text{ and } \exists k \in \text{Force}_V^i(X). j \rightarrow k\} \\ &\cup \{j : L(j) = R \text{ and } \forall k. \text{ if } j \rightarrow k \text{ then } k \in \text{Force}_V^i(X)\} \end{aligned}$$

$$\text{Force}_P(X) = \bigcup \{\text{Force}_P^i(X) : i \geq 0\} \text{ for } P \in \{R, V\}.$$

## Determinization

- if  $G$  is a parity game let  $G(i)$  be the game that starts from vertex  $i$
- **Proposition** For any parity game  $G$  and vertex  $i$ , one of the players has a history-free winning strategy for  $G(i)$

**Proof:** Let  $G = (N, \rightarrow, L)$  be a parity game. The proof is by induction on  $|N|$ . The base case is when  $|N| = 0$  and the result holds. For the inductive step, let  $|N| > 0$  and assume that  $k$  is the least vertex in  $N$ . Let  $X$  be the set  $\text{Force}_{L(k)}(\{k\})$ . If  $X = N$ , then player  $L(k)$  has a history-free winning strategy for  $G(i)$  for each  $i \in N$ , by forcing play infinitely often through vertex  $k$ . Otherwise,  $X \neq N$ .  $G' = G - X$  is a subgame. The size of  $N'$  is strictly smaller than the size of  $N$ . Therefore, by the induction hypothesis, partition  $N'$  into  $W'_R$ , the vertices won by R, and  $W'_V$ , the vertices won by V.

## Lots of Other Topics

- Automata and games
- Symbolic model checking
- Compositional model checking (Game Semantics)
- Model checking infinite-state systems: when decidable
- Tractable first-order temporal logic (monodic fragments)
- Tractable fragments of first-order logic + fixed points (guarded fragments)
- :::: ... ::::