



# A Tableau for RoBCTL\*

John M<sup>c</sup>Cabe-Dansted

University of Western Australia

September 8, 2008

## RoCTL\*

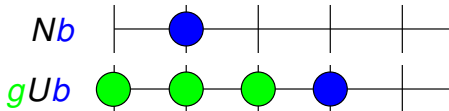
- We proposed a new logic, RoCTL\* (McCabe-Dansted et al., 2007), for modelling and verifying specifications that deal with
  - Time (extends CTL\*)
  - Obligation (what the system *should* do)
  - Robustness (what the system will do even if  $n$  failures occur, etc.)
- We motivated its use, apply to simple problems.
- We showed that RoCTL\* is decidable
- We now present a tableau based decision procedure
  - For a “bundled” variant RoBCTL\*
    - Extends tableau for BCTL\* (Reynolds, 2007)



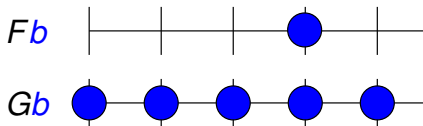
# Linear Temporal Logic (LTL)

Classical logic has two base operators  $\wedge$ ,  $\neg$

LTL has two additional base operators, Next and Until:

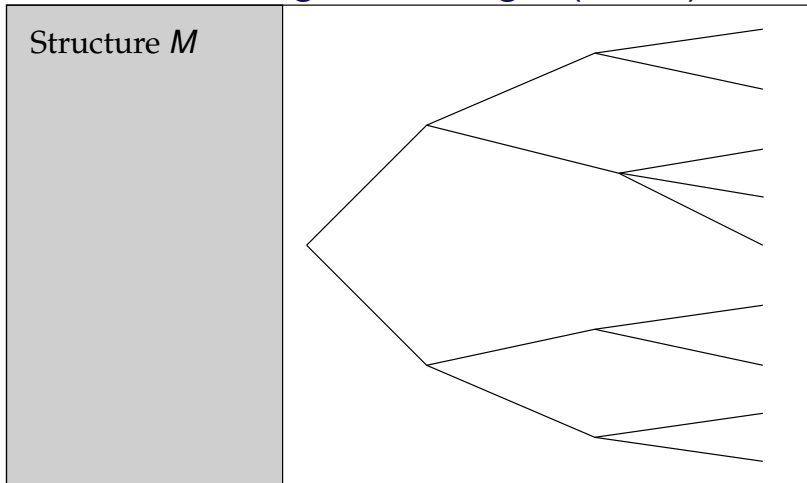


We may also define Finally and Globally in terms of Until:





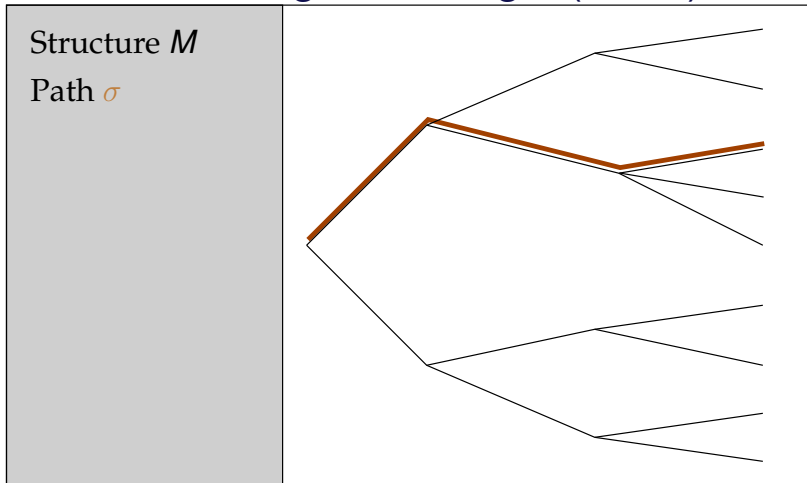
# Branching Time Logic (CTL\*)



CTL0/9

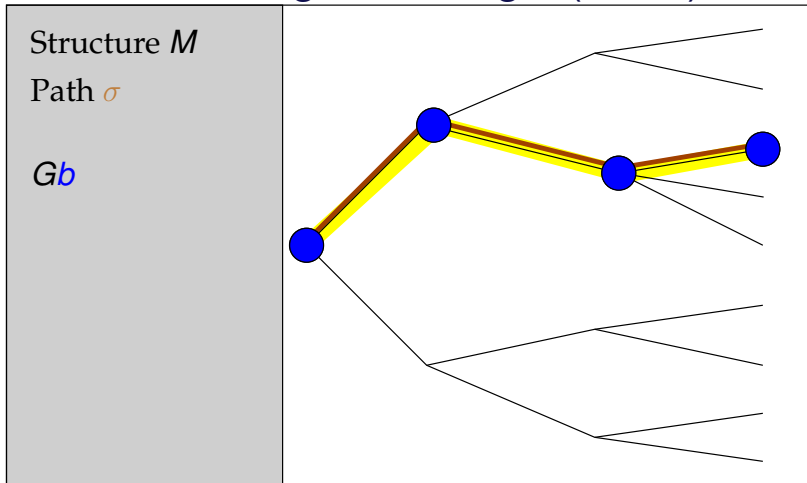


# Branching Time Logic (CTL\*)



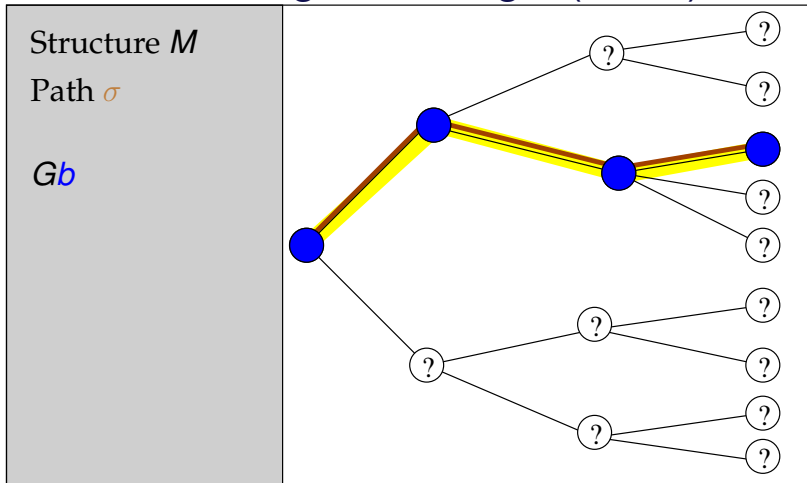


# Branching Time Logic (CTL\*)



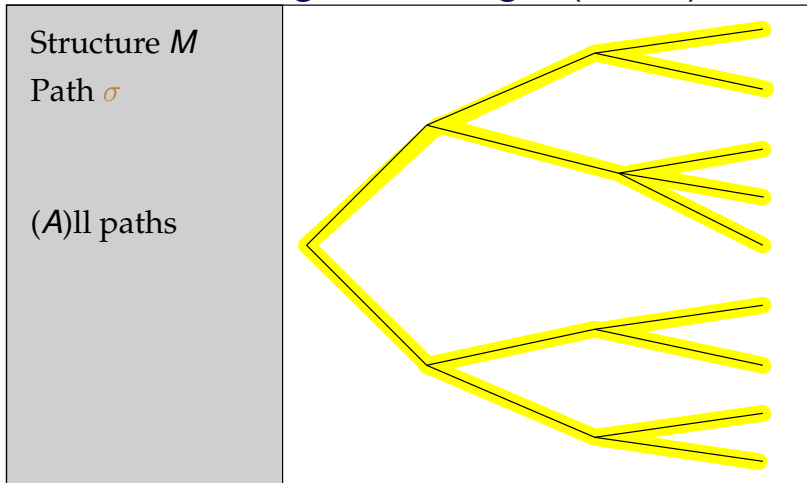


# Branching Time Logic (CTL\*)





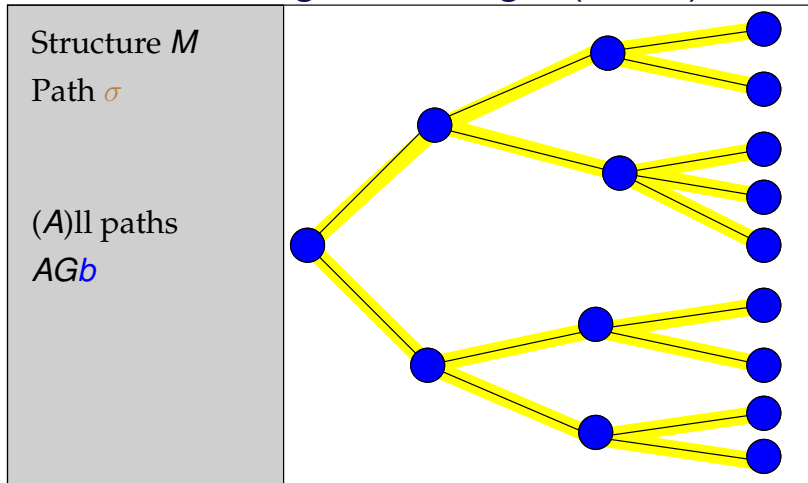
# Branching Time Logic (CTL\*)





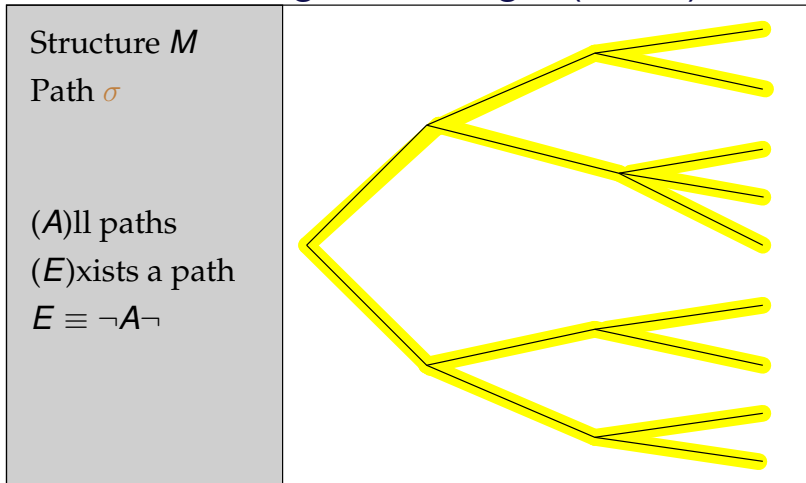


# Branching Time Logic (CTL\*)



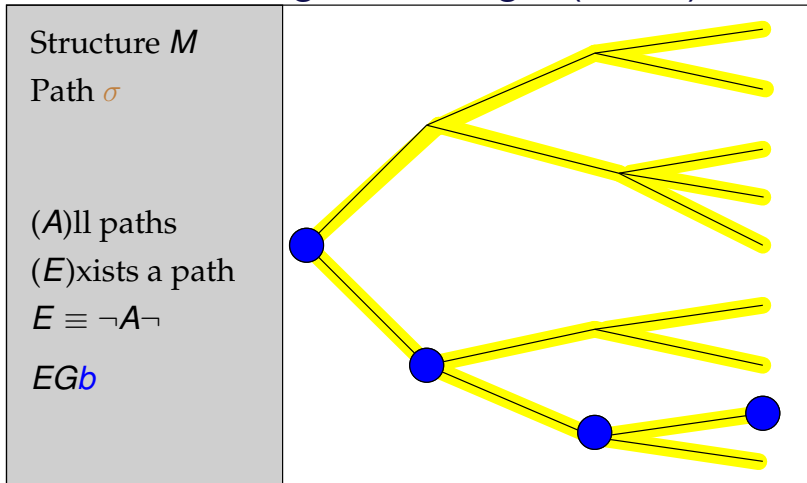


# Branching Time Logic (CTL\*)



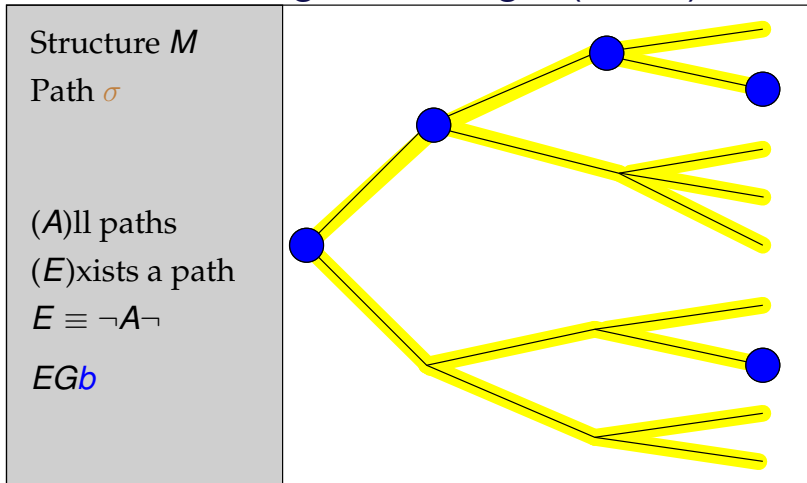


# Branching Time Logic (CTL\*)



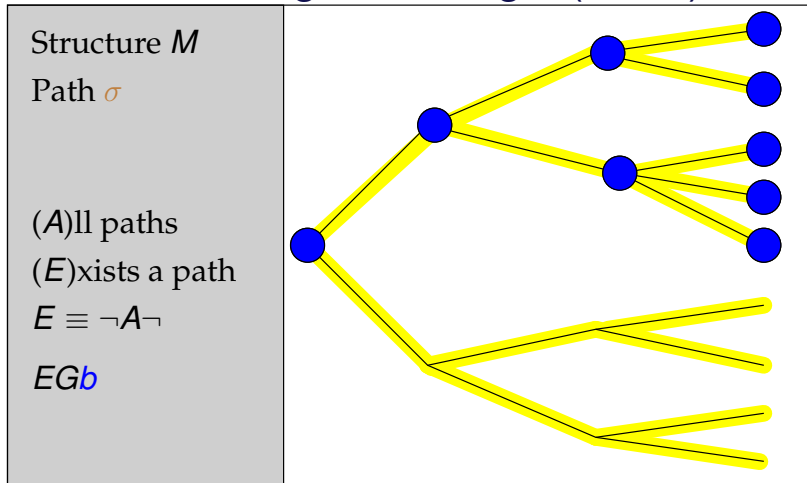


# Branching Time Logic (CTL\*)



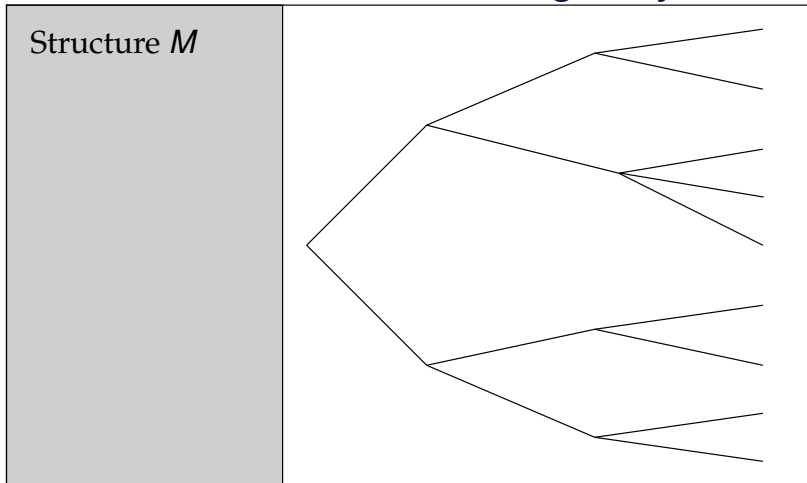


# Branching Time Logic (CTL\*)



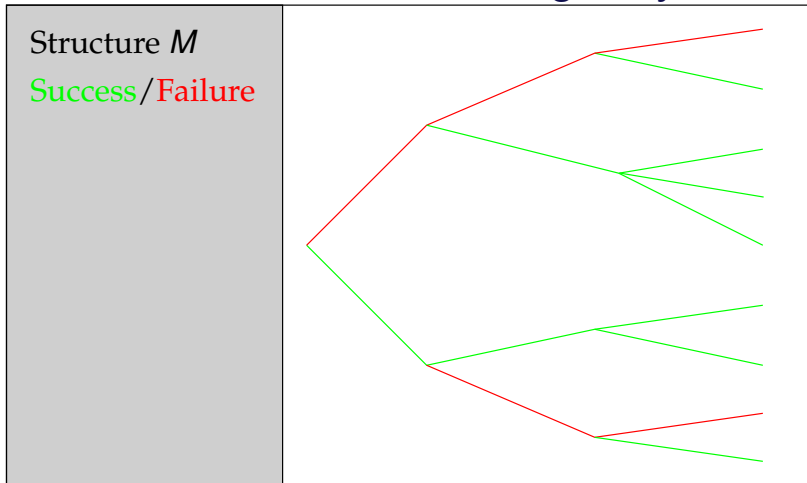


## Path Quantifier: Obligatory



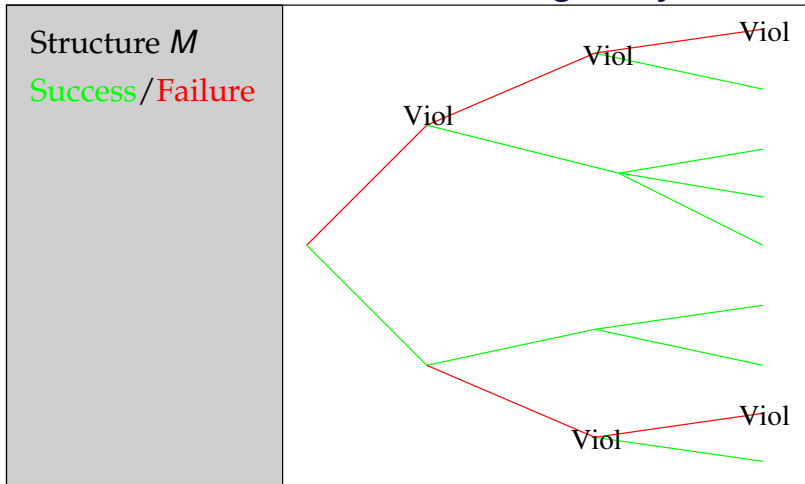


# Path Quantifier: Obligatory





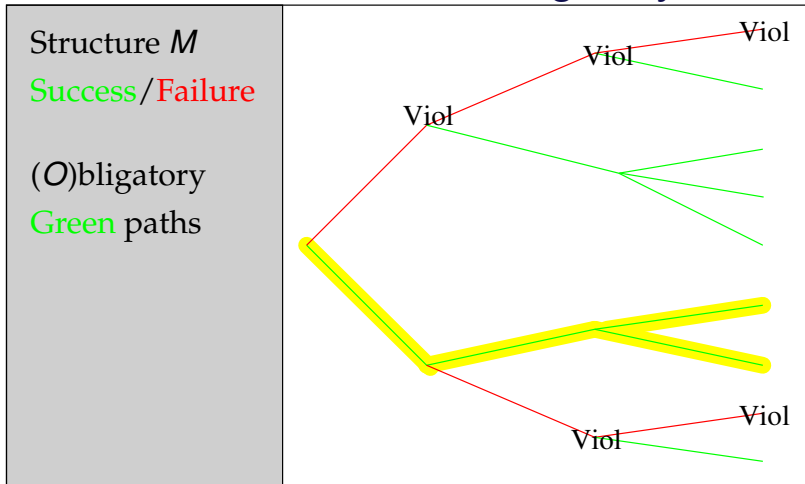
# Path Quantifier: Obligatory





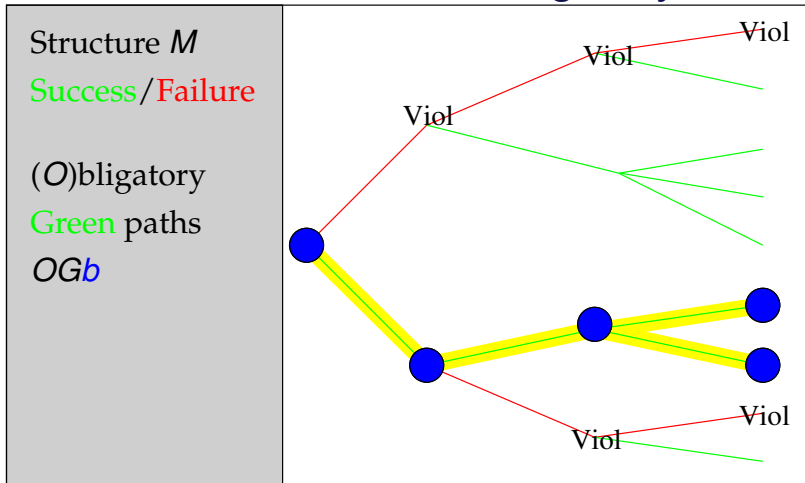


# Path Quantifier: Obligatory



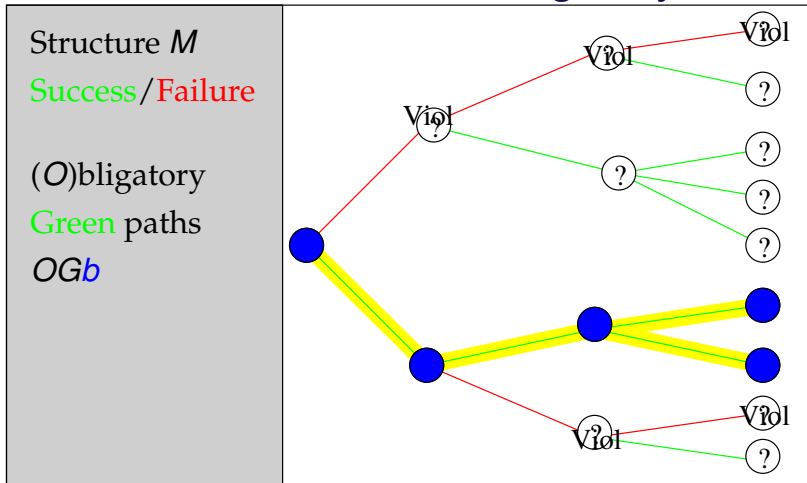


# Path Quantifier: Obligatory



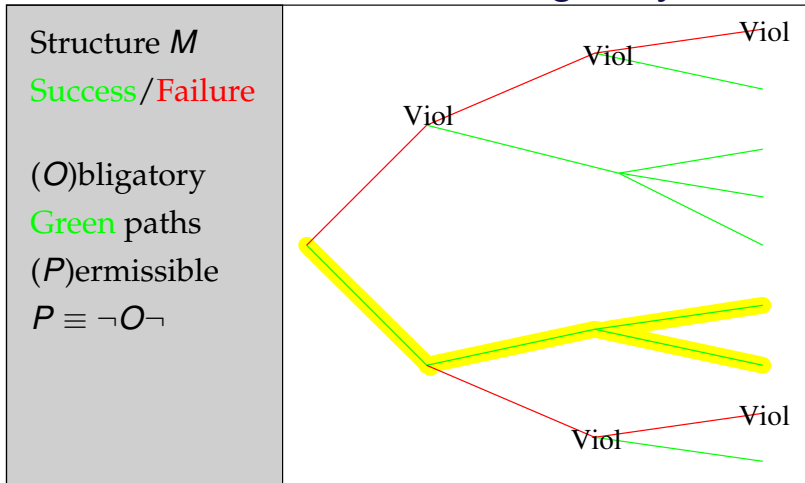


# Path Quantifier: Obligatory



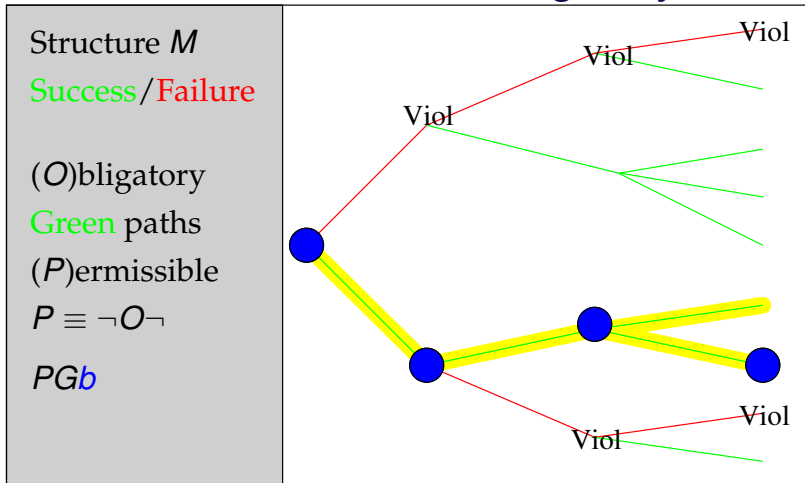


# Path Quantifier: Obligatory



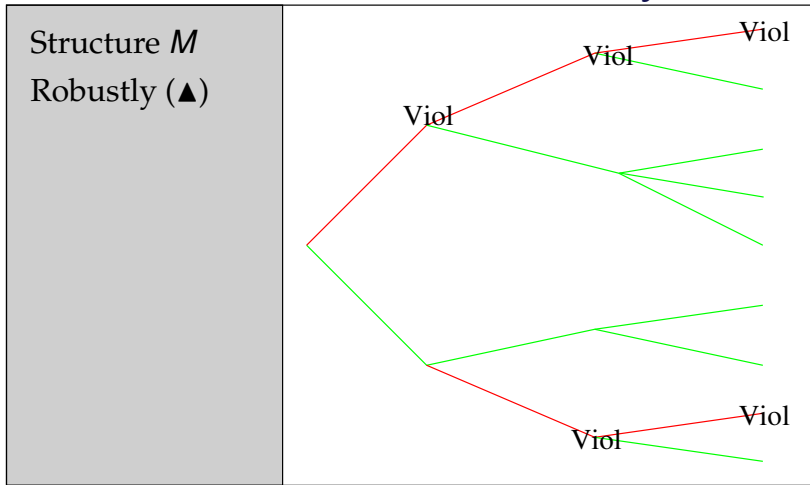


# Path Quantifier: Obligatory



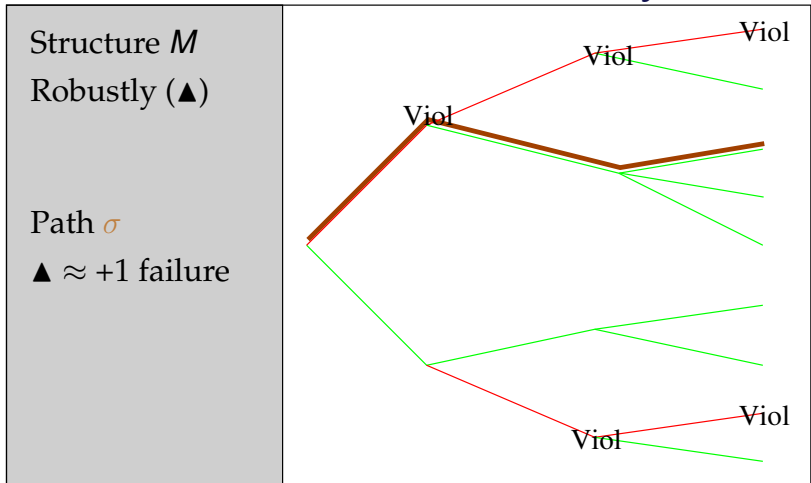


# Path Quantifier: Robustly



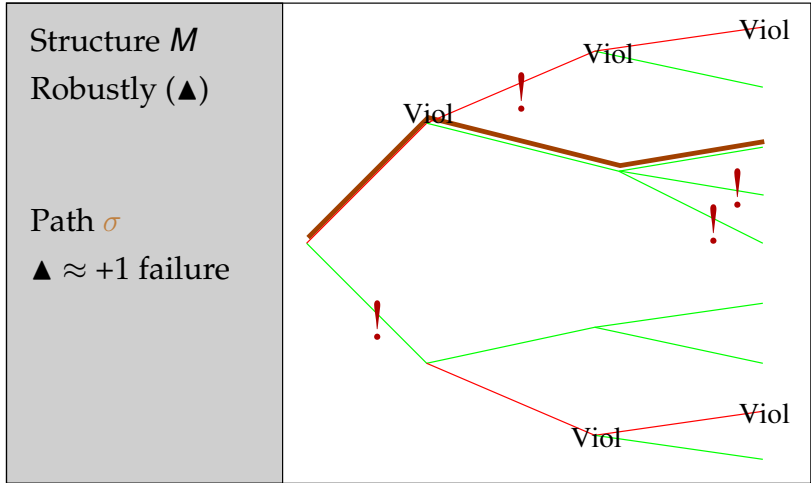


# Path Quantifier: Robustly





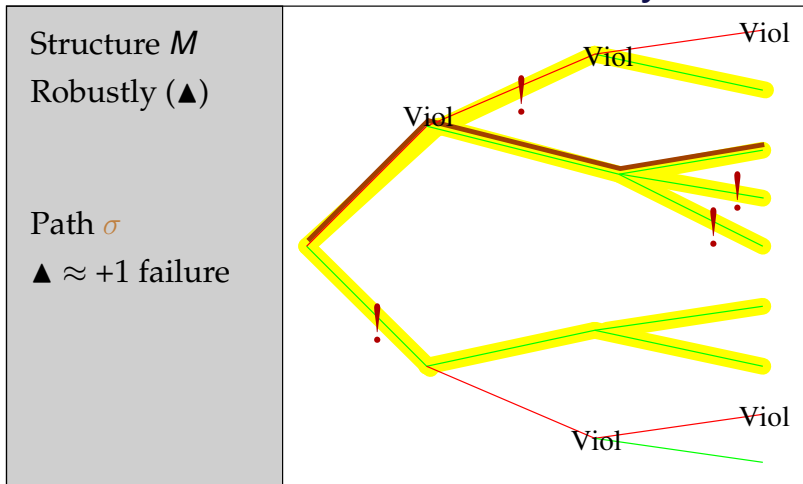
# Path Quantifier: Robustly





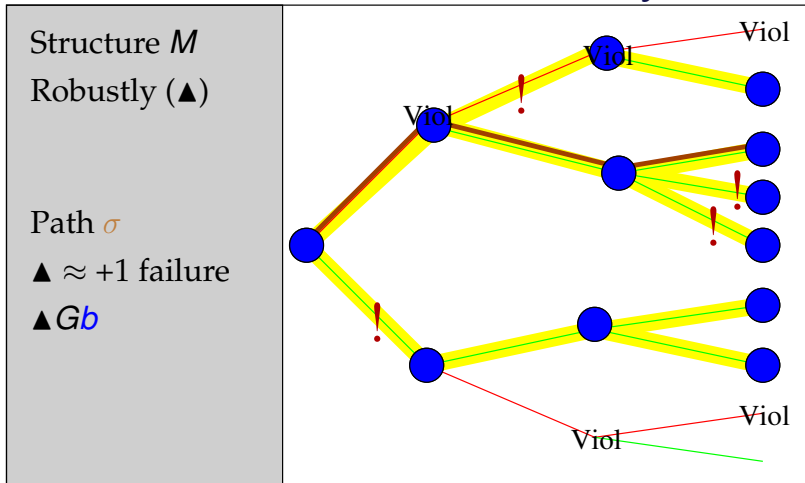


# Path Quantifier: Robustly



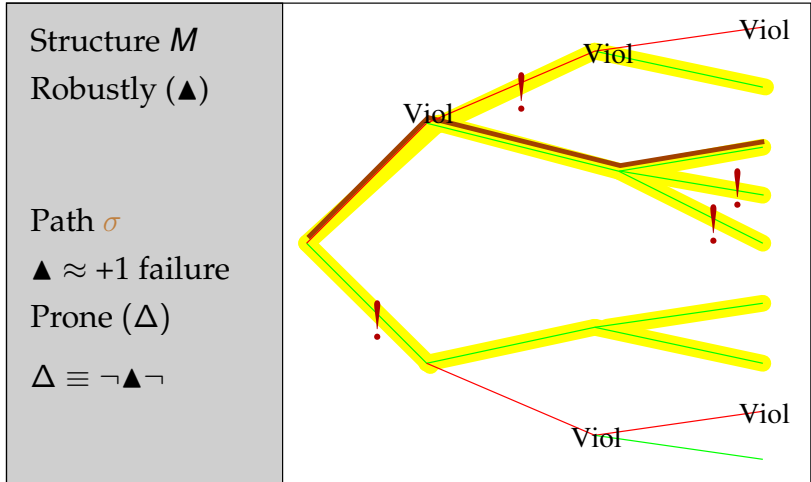


# Path Quantifier: Robustly



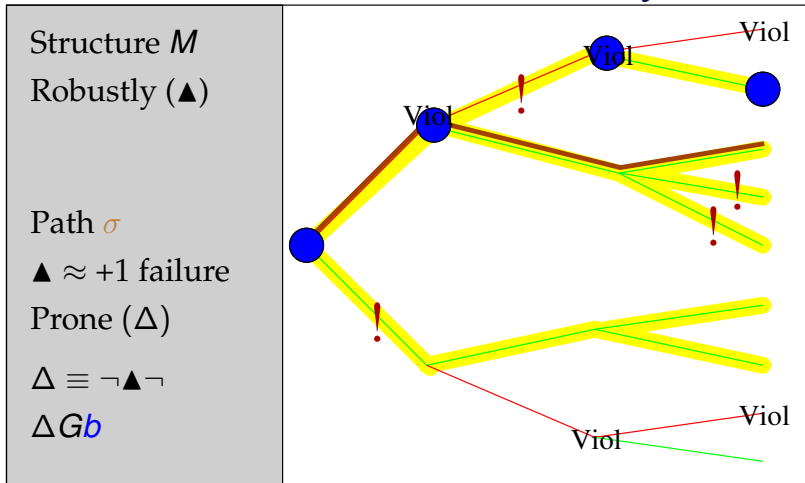


# Path Quantifier: Robustly



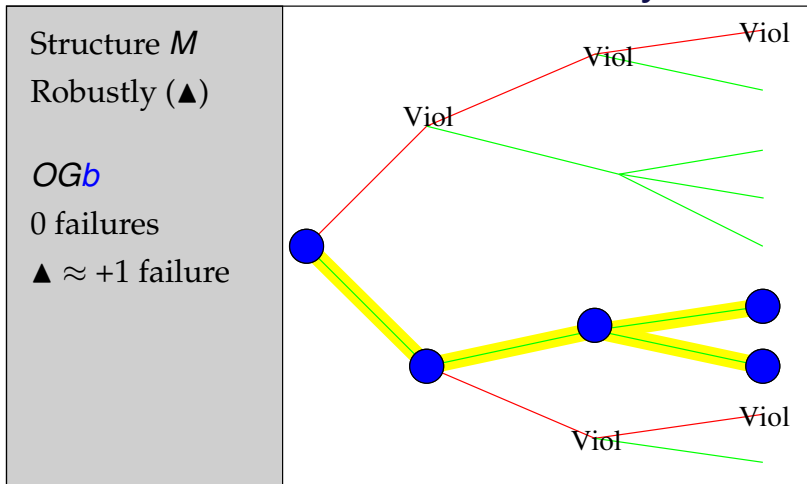


# Path Quantifier: Robustly



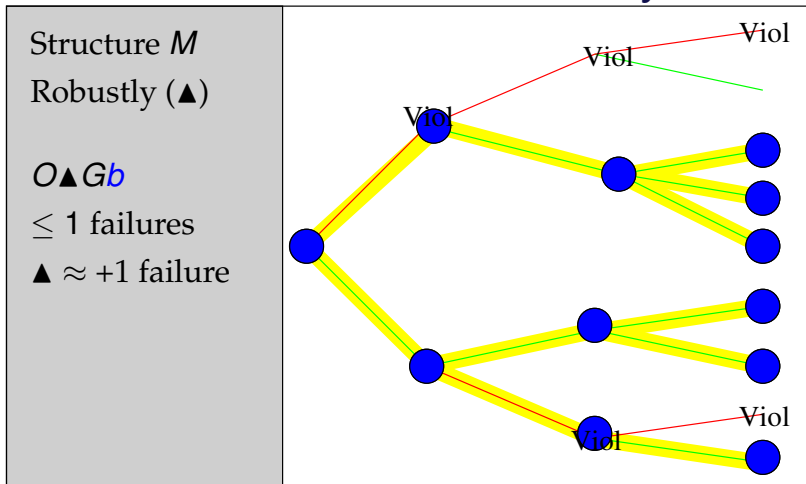


# Path Quantifier: Robustly



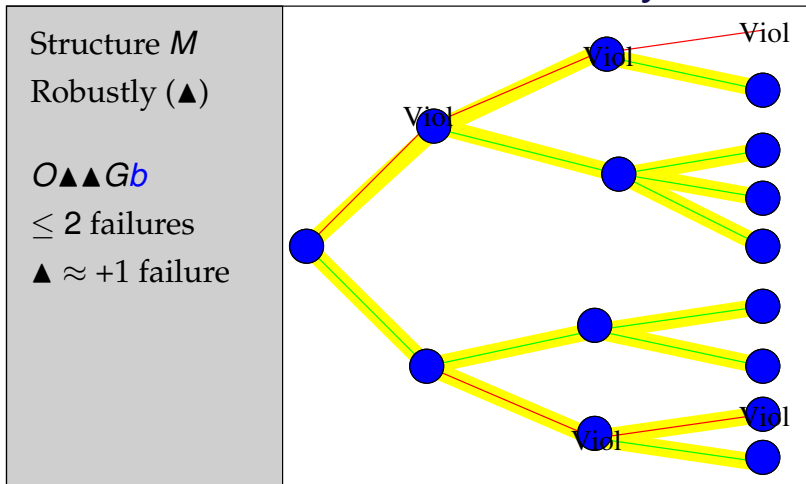


# Path Quantifier: Robustly



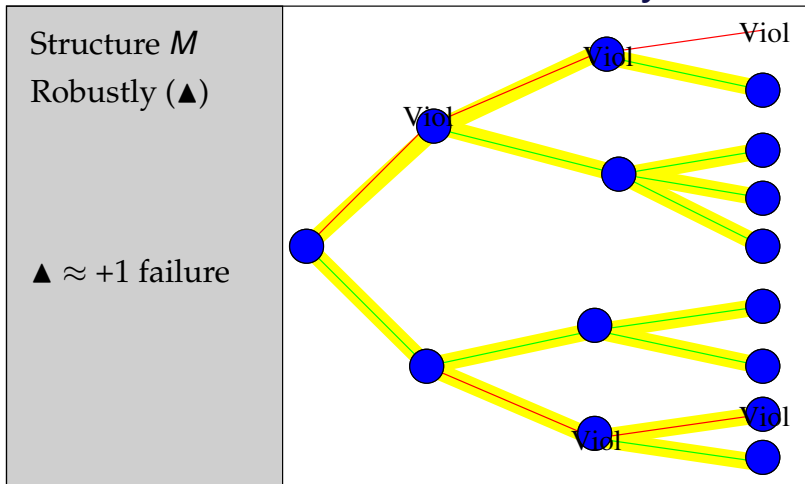


## Path Quantifier: Robustly





## Path Quantifier: Robustly







# Bundles

In (Ro)CTL\* any path through structure is allowed.

In (Ro)BCTL\* we may be limited to a bundle of paths.

- No Limit Closure axiom.

Consider a path through a maze:

- CTL\*: If you can always turn left, there is a path consisting only of left turns.
- BCTL\*: It may be case that you always have option of turning left, but all paths must have at least one right turn, eventually.



## Semantics

We limit paths to some bundle of paths  $B$

$\delta(\sigma)$ : Deviations from  $\sigma$ , for  $\tau \in B$

$\tau \in \delta(\sigma)$  iff  $\exists i$  st  $\tau_{\leq i} = \sigma$  and  $\tau_{\geq i+1}$  is failure-free

$\mathcal{F}(s)$  paths in  $B$  starting at  $s$

$\mathcal{S}(s)$  failure-free paths in  $B$  starting at  $s$

$M, \sigma \models \phi$  means  $\phi$  is true on the structure  $M$  along path  $\sigma$

$M, \sigma \models N\phi$  iff  $M, \sigma_{\geq 1} \models \phi$

$M, \sigma \models \phi U \psi$  iff  $\exists i \in \mathbb{N}$  s.t.  $M, \sigma_{\geq i} \models \psi$  and

$\forall j \in \mathbb{N} j < i \implies M, \sigma_{\geq j} \models \psi$

$M, \sigma \models A\phi$  iff  $\forall \pi \in \mathcal{F}(\sigma_0) M, \pi \models \phi$

$M, \sigma \models O\phi$  iff  $\forall \pi \in \mathcal{S}(\sigma_0) M, \pi \models \phi$

$M, \sigma \models \blacktriangle \phi$  iff  $\forall \pi \in \delta(\sigma) M, \pi \models \phi$  and  $M, \sigma \models \phi$



## Coordinated Attack Problem

General  $A$  wants to organise an attack with  $B$

$AG(s_A \rightarrow ONr_B)$ : If  $A$  sends a message,  $B$  should receive it at the next step.

$AG(\neg s_A \rightarrow \neg Nr_B)$ : If  $A$  does not send a message now,  $B$  will not receive a message at the next step.

$AG(f_A \rightarrow AGf_A)$ : Once  $A$  commits,  $A$  cannot withdraw.

$AG(f_A \rightarrow \neg s_A)$ : If  $A$  has committed to an attack, it is too late to send messages.

$A(\neg f_A Wr_A)A$  cannot commit to an attack until  $A$  has received plans from  $B$



## Coordinated Attack Protocol

For unbounded # of errors, no protocol exists, but...

Following works if one or less messages are lost.

$A(s_A W r_A)$ : General  $A$  will send plans until a response is received.

$AG(r_A \rightarrow f_A)$ : Once general  $A$  receives a response,  $A$  will commit to an attack.

$A(\neg r_B W (r_B \wedge (s_B \wedge Ns_B \wedge NNf_B)))$ : Once general  $B$  receives plans,  $B$  will send two messages to  $A$  and then commit to an attack.

Decide: is the conjunction  $\hat{\phi}$  of the above formulæ consistent under  $\text{Ro(B)CTL}^*$ ?

Decide: does  $\hat{\phi}$  imply correct behaviour even if a single failure occurs:  $\hat{\phi} \rightarrow O\blacktriangle F(f_A \wedge f_B)$



## Feeding A Cat.

We wish to ensure that a cat always has food ( $f$ ) when it is hungry ( $h$ ), even if we once forget to fill the cat bowl.

- 1  $AG(h \rightarrow \neg Nh)$ : Not hungry twice in a row.
- 2  $AG((h \vee \neg f) \rightarrow \Delta N\neg f)$ : May forget to fill empty food bowl.
- 3  $AG((\neg h \wedge f) \rightarrow Nf)$ : If the cat is not hungry the bowl will not be emptied.
- 4  $O\blacktriangle G(h \rightarrow f)$ : Even with single error, must be food whenever cat is hungry
- 5  $f$ : The cat bowl starts full.

Decide: is policy is consistent?

Decide:  $AGONf \rightarrow O\blacktriangle G(h \rightarrow f)$ : Always attempting to fill cat bowl satisfies policy.



# Overview of Tableau of BCTL\*

- Paths  $\rightarrow$  Hues
  - represents formulae that could hold together on the same path.
  - is a set of formulae
- States  $\rightarrow$  Colours
  - Many paths can start at same state
  - Colours are sets of hues

Defined in terms of closure sets, successor functions, pruning rules etc.



# Path Quantifier A

Now handling  $A$  is simple

- Require that hues  $h$  satisfy
  - (H4) if  $A\alpha \in a$  [or  $\blacktriangle\alpha \in a$ ] then  $\alpha \in a$ .
- Require that Colours  $C$  satisfy
  - (A1)  $A\alpha \in a$  iff  $A\alpha \in b$  [and  $O\alpha \in a$  iff  $O\alpha \in b$ ]
  - (C2)  $a \in C$  and  $\neg A\alpha \in a$  [or  $\neg\blacktriangle\alpha \in a$ ]  $\implies b \in C$  st.  
 $\neg\alpha \in b$

“ $A\alpha$  is in a hue of  $C$  iff  $\alpha$  is in all hues of the same colour”



## Path Quantifier $\blacktriangle$ : Like $A$ ?

We would like to require that

- “ $\blacktriangle\alpha$  is in a hue  $h$  of  $C$  iff  $\alpha$  in all hues that deviate from  $h$ ”.

What does it mean for a hue to deviate?

- Hues represent an infinite number of paths
  - Some may deviate. Some may not.
  - Discards too much information

Track deviations in hues?

- $A\Delta$ : All paths have a deviation.
- $\therefore$  A path has a deviation, which has a deviation ...
  - Have not found a finite representation.



## Path Quantifier ▲

Handle ▲ in hues rather than colours

- If ▲ $N\phi$  then
  - $N\phi$  holds on all 0/now-deviations:  $ANO\phi$  in hue.
  - ▲ $\phi$  holds on all possible successors to this hue.

In general: (R5) ▲ $\alpha \in a$  implies  $N_a^{-1}(\text{▲}\alpha)$  in temporal successor  $b$ ,

Where  $N_a^{-1}$  is a formula translation function such that:

$$\left( \bigwedge_{\psi \in a} \psi \right) \rightarrow A(\phi \leftrightarrow NN_a^{-1}(\phi))$$



## Eventualities

In BCTL\* only one type of eventuality:  $\alpha U \beta$ .

In RoBCTL\* an additional eventuality:  $\neg \blacktriangle \alpha$

Consider the colour  $C = \{\{\neg \blacktriangle Gp, Gp, p, \neg \text{Viol}, \top\}\}$

- $C$  is a valid successor to itself.
- $\neg \blacktriangle Gp \implies$  we must reach  $\neg Gp$ 
  - $C$  alone is not a valid model:
  - If  $\neg Gp$  not reachable, must prune  $C$

Note that in BCTL\* eventualities don't change

- $(\alpha U \beta)$  remains  $(\alpha U \beta)$  until reach  $\beta$

In RoBCTL\* eventualities do change

- E.g.  $\neg \blacktriangle N\phi$  becomes  $\neg \blacktriangle \phi$  at next step.



# BCTL\* Complexity

# Hues  $\approx 2^{|\mathbf{cl}\phi|}$  (powerset of formulae)

# Colours  $\approx 2^{2^{|\mathbf{cl}\phi|}}$  (powerset of powerset of formulae)

BCTL\*:  $|\mathbf{cl}\phi| \approx |\phi|$  “doubly exponential”

\* Doubly exponential best possible (like CTL\*)?

## RoBCTL\* Complexity

Again # Colours  $\approx 2^{2^{|\mathbf{cl}\phi|}}$

$|\mathbf{cl}\phi|$  not elementary, But:

- $|\mathbf{cl}\phi| \in \mathcal{O}(|\phi|)$  if  $\blacktriangle \notin \phi$
- $|\mathbf{cl}\phi| \in \mathcal{O}(2^{|\phi|})$  if  $\blacktriangle \dots U \notin \phi$
- $|\mathbf{cl}\blacktriangle^n\phi| \in \mathcal{O}(n + 2^{2^{|\mathbf{cl}\phi|}})$
- $|\mathbf{cl}\phi| \approx 2|\phi|$  for examples (Same as BCTL\*).

Informally: Extra 2-exponential blowup only on  $\blacktriangle$ ,  $U$  alternations ( $\blacktriangle^n$  OK).

- Only if not broken by an  $A$  or  $O$

Thus most interesting classes of RoBCTL\* formulae are elementary.



# RoCTL

- Double exponential complexity too hard for many purposes.
  - CTL\* itself is double exponential.
- CTL: EXPTIME
  - Find CTL like fragment of RoCTL.



## Expressivity

Is RoCTL\* more expressive than CTL\*?

We can embed in QCTL\* (CTL\* + Bisimulation quantifiers

$\exists_x \forall_x$ )

- QCTL\*  $\neq$  CTL\* (e.g. non-elementary)

Can translate  $O\phi$  into CTL\*:

$$A(GN\neg\text{Viol} \rightarrow \phi)$$

Can translate some  $\blacktriangle\phi$ , e.g.  $\blacktriangle Gp$  becomes

$$pW(E(GN\neg\text{Viol} \wedge Gp)).$$

But no full translation found.



# MarkCTL\*

We will propose and investigate MarkCTL\*

- Adds  $M$  operator and special variable  $m$ .
- Within scope of  $M$  operator,  $m$  is true iff on current path.
- Can represent  $\Delta\phi$  as  $ME(mUGN\neg\text{Viol} \wedge \phi)$

Study RoCTL\* from point of view of Hybrid logics?



# Summary

- Previously:  $\text{RoCTL}^*$  decidable by reduction to  $\text{QCTL}^*$ 
  - Novel Robustly operator
  - Decidable: Infeasible
- Presented Tableau for  $\text{RoBCTL}^*$ 
  - May be feasible to decide for some purposes?
    - (but not as feasible as  $\text{RoCTL}$ )
- Future work
  - Applications
  - Expressivity
    - Hybrid logics,  $\text{ECTL}^*$  etc.
  - Axiomatisation





# Any Questions?



# References

M<sup>c</sup>Cabe-Dansted, J. C., French, T., and Reynolds, M. A temporal logic of robustness, RoCTL\*. Technical report, UWA, 2007. <http://www.csse.uwa.edu.au/~john/papers/RoCTL07.pdf>.

Reynolds, M. A Tableau for Bundled CTL. *J Logic Computation*, 17(1):117–132, 2007.

$$N_a^{-1}(\phi U \psi) = (N_a^{-1}(\phi) \wedge (\phi U \psi)) \vee N_a^{-1}(\psi)$$

$$N_a^{-1}(\neg \phi) = \neg N_a^{-1}(\phi)$$

$$N_a^{-1}(N\phi) = \phi$$

$$N_a^{-1}(\phi \wedge \psi) = N_a^{-1}(\phi) \wedge N_a^{-1}(\psi)$$

$$N_a^{-1}(p) = \begin{cases} \perp & \text{if } p \notin a \\ \top & \text{if } p \in a \end{cases}$$

$$N_a^{-1}(A\phi) = \begin{cases} \perp & \text{if } A\phi \notin a \\ \top & \text{if } A\phi \in a \end{cases}$$

$$N_a^{-1}(O\phi) = \begin{cases} \perp & \text{if } O\phi \notin a \\ \top & \text{if } O\phi \in a \end{cases}$$

$$N_a^{-1}(\blacktriangle\phi) = \begin{cases} \perp & \text{if } ANO\exists(N_a^{-1}(\phi)) \notin a \\ \blacktriangle\exists(N_a^{-1}(\phi)) & \text{otherwise} \end{cases}$$



# Expressivity

Is RoCTL\* more expressive than CTL\*?

We can embed in QCTL\* (CTL\* + Bisimulation quantifiers

$\exists_x \forall_x$ )

- $\exists_x$ : Exists a valuation of variable  $x$
- Satisfiability of  $\exists_x \phi$  equivalent to  $\phi$
- $\neg \exists_x \phi$  not so simple.
- $\text{QCTL}^* \neq \text{CTL}^*$

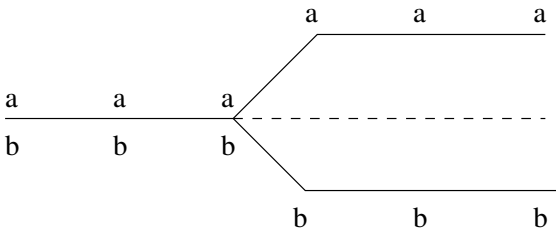
## Expressivity: No $\exists$ ?

Some formulae do not need  $\exists_x$ . E.g.:  $\blacktriangle Gp$  becomes

$$pW(E(GN\neg\text{Viol} \wedge Gp)).$$

Translation function  $f$  from RoCTL\* to CTL\* exist?

$f(\Delta(Ga \wedge Gb)) \neq f(\Delta Ga) \wedge f(\Delta Gb)$ :  $Ga$  and  $Gb$  must occur on same deviation





## Expressivity: About $\wedge$

- Push down  $\wedge$ :  $f(\Delta (Ga \wedge Gb)) = f(\Delta G(a \wedge b))$ .
- $f(aUb \wedge cUd)$ : break into stages
  - $b$  before  $d$ :  $a \wedge c$ , then  $b \wedge c$ , then  $cUd$ ; or
  - $b$  after  $d$ ; or
  - $b$  and  $d$  at same time.
- $f((aUc)Ud)$ : circular stages, no finite representation?

CONJECTURE: There exist RoBCTL\* formulae that cannot be expressed in BCTL\*. Likewise, there exist RoCTL\* formulae that cannot be expressed in CTL\*.



# Maximally Propositionally Consistent

Let  $a$  be a set of formulae.

## Definition

We say that  $a \subseteq \mathbf{cl}\phi$  is MPC iff for all  $\alpha, \beta \in a$

(M1) if  $\beta = \neg\alpha$  then  $\beta \in a$  iff  $\alpha \notin a$ ,

(M2) if  $\alpha \wedge \beta \in \mathbf{cl}\phi$  then  $(\alpha \wedge \beta) \in a \leftrightarrow (\alpha \in a \text{ and } \beta \in a)$



# Hues

A Hue represents is (roughly) a set of formulae that could hold together on some path.

## Definition (Hue)

A set  $a \subseteq \mathbf{cl}\phi$  is a hue for  $\phi$  iff

(H1)  $a$  is MPC;

(H2) if  $\alpha U \beta \in a$  then  $\alpha \in a$  or  $\beta \in a$ ;

(H3) if  $\neg(\alpha U \beta) \in a$  then  $\beta \notin a$ ; and

(H4) if  $A\alpha \in a$  or  $\blacktriangle\alpha \in a$  then  $\alpha \in a$ .