Causality-based LTL Model Checking without Automata

joint work with Bernd Finkbeiner

Andrey Kupriyanov

Saarland University
Reactive Systems Group

September 5, 2014

UNIVERSITÄT
DES
SAARLANDES

Reactive
Systems

Motivation

LTL

A well-established basis for specification, verification, and synthesis of reactive programs. We consider two decision problems:

- Satisfiability/validity: $\models \varphi$
- Model checking against a program: $P \models \varphi$

Motivation

LTL

A well-established basis for specification, verification, and synthesis of reactive programs. We consider two decision problems:

- Satisfiability/validity: $\models \varphi$
- Model checking against a program: $P \models \varphi$

Automata-based LTL Model Checking

The standard way to model check a program P against an LTL property φ:

1. translate $\neg\varphi$ into a Büchi automaton A
2. check for emptiness the synchronized product of A and P

Motivation

LTL

A well-established basis for specification, verification, and synthesis of reactive programs. We consider two decision problems:

- Satisfiability/validity: $\models \varphi$
- Model checking against a program: $P \models \varphi$

Automata-based LTL Model Checking

The standard way to model check a program P against an LTL property φ:

1. translate $\neg\varphi$ into a Büchi automaton A
2. check for emptiness the synchronized product of A and P

Main problem: LTL formulas are often not small!

They describe necessary assumptions of, e.g.:

- fairness
- termination
- allowed request/response pairs

Example: individual accessibility for semaphores

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

LTL Properties

Fair scheduling: $\varphi_F \equiv \Box\Diamond(at_2 \wedge r_{free}) \implies \Box\Diamond at_3$

Termination of critical sections: $\varphi_T \equiv \Box(at_3 \implies \Diamond at_1)$

Individual **A**ccessibility: $\varphi_A \equiv \Box(at_2 \implies \Diamond at_3)$

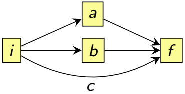
$$\varphi \equiv \bigwedge_{i \in 1..n}(\varphi_{F_i} \wedge \varphi_{T_i}) \implies \varphi_{A_1}$$

Translation of $\neg\varphi$ into a Büchi automaton: **ltl3ba**

Threads	Time (sec)	Memory (MB)	|Automaton| (MB)
2	0.005	4.2	0.002
3	0.09	5.0	0.38
4	9.6	14.7	8.6
5	1295	139	185
6	TO	X	X

Our approach

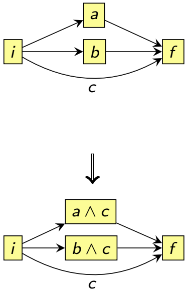
- **Proof objects: concurrent traces**
  allow to capture temporal order, constraints, independence



Our approach

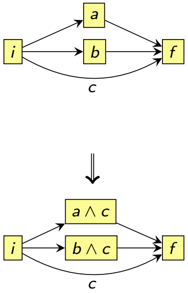
- **Proof objects: concurrent traces**
  allow to capture temporal order, constraints, independence

- **Proof rules based on causality**
  causality $\equiv$ language-preserving trace transformations



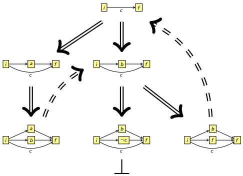
Our approach

- **Proof objects: concurrent traces**
  allow to capture temporal order, constraints, independence

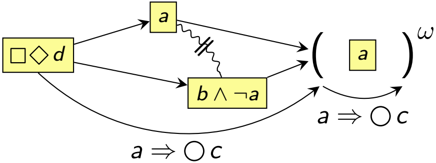


- **Proof rules based on causality**
  causality ≡ language-preserving trace transformations

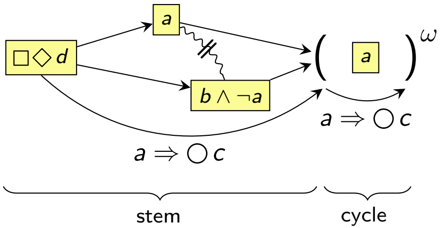
- **Proof construction: tableau search based on causal loops**
  causal loops ≡ infinitely-looping trace transformations



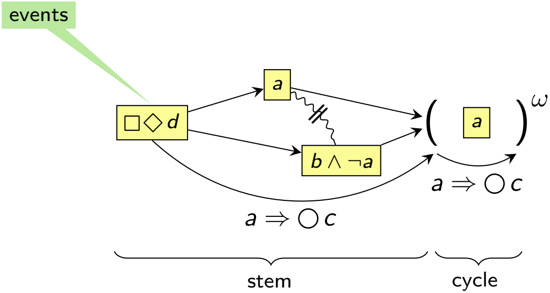
Concurrent traces



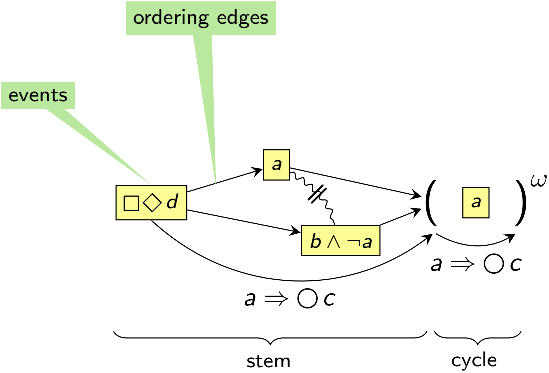
Concurrent traces



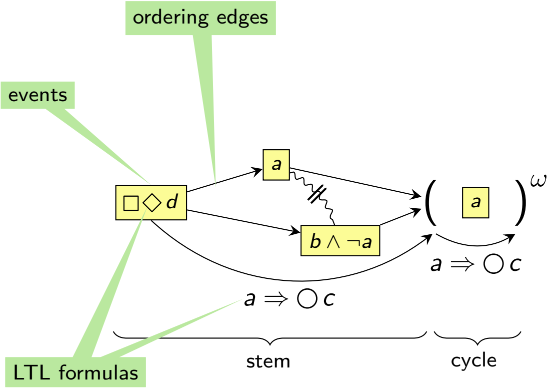
Concurrent traces



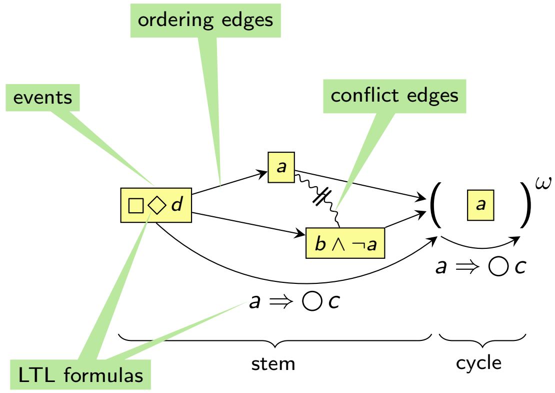
Concurrent traces



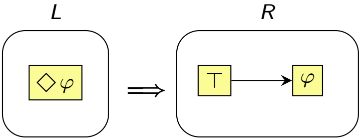
Concurrent traces



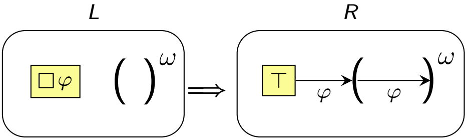
Concurrent traces



LTL proof rules

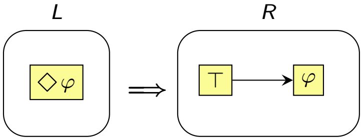


Finally

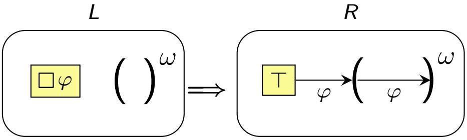


Globally

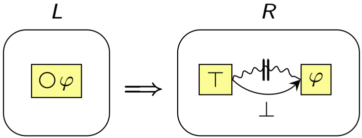
LTL proof rules



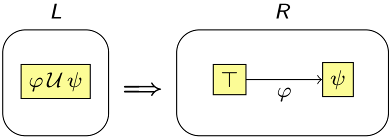
Finally



Globally

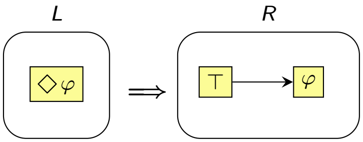


Next

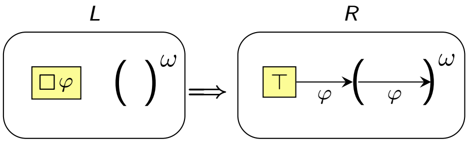


Until

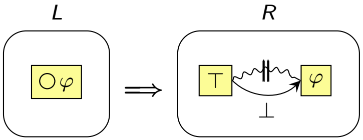
LTL proof rules



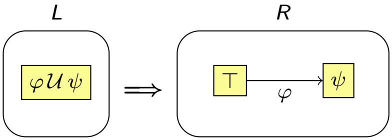
Finally



Globally



Next



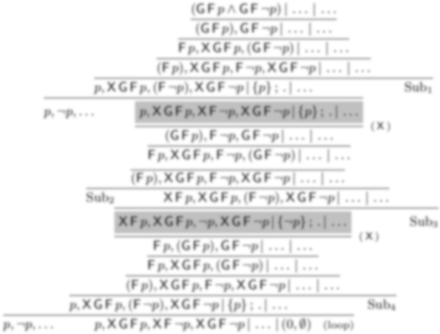
Until

Other proof rules

for safety [K., Finkbeiner, Concur 2013], and termination [K., Finkbeiner, CAV 2014]

LTL satisfiability: $\Box\Diamond p \wedge \Box\Diamond\neg p$

LTL satisfiability: $\Box\Diamond p \;\wedge\; \Box\Diamond\neg p$

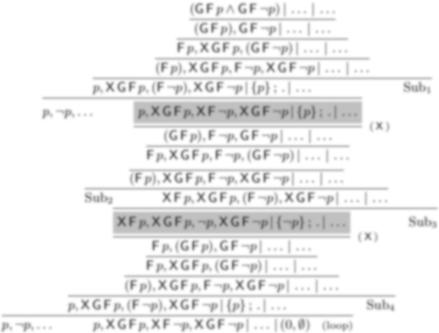

(G F p ∧ G F ¬p) | … | …
(G F p), G F ¬p | … | …
F p, X G F p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
p, X G F p, (F ¬p), X G F ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, X G F p, X F ¬p, X G F ¬p | {p} : . | …
(X)
(G F p), F ¬p, G F ¬p | … | …
F p, X G F p, F ¬p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
Sub₂
X F p, X G F p, (F ¬p), X G F ¬p | … | …
X F p, X G F p, ¬p, X G F ¬p | {¬p} : . | …
Sub₃
(X)
F p, (G F p), G F ¬p | … | …
F p, X G F p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
p, X G F p, (F ¬p), X G F ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, X G F p, X F ¬p, X G F ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \wedge \Box\Diamond\neg p$

$$\boxed{\Box\Diamond p \ \wedge\ \Box\Diamond\neg p} \longrightarrow \left(\ \boxed{\top}\ \right)^{\omega}$$


(GF $p \wedge$ GF $\neg p$) | … | …
(GF p), GF $\neg p$ | … | …
F p, XGF p, (GF $\neg p$) | … | …
(F p), XGF p, F $\neg p$, XGF $\neg p$ | … | …
p, XGF p, (F $\neg p$), XGF $\neg p$ | $\{p\}$: . | …
Sub$_1$
$p, \neg p, \ldots$
p, XGF p, XF $\neg p$, XGF $\neg p$ | $\{p\}$: . | …
(X)
(GF p), F $\neg p$, GF $\neg p$ | … | …
F p, XGF p, F $\neg p$, (GF $\neg p$) | … | …
(F p), XGF p, F $\neg p$, XGF $\neg p$ | … | …
Sub$_2$
XF p, XGF p, (F $\neg p$), XGF $\neg p$ | … | …
XF p, XGF p, $\neg p$, XGF $\neg p$ | $\{\neg p\}$: . | …
Sub$_3$
(X)
F p, (GF p), GF $\neg p$ | … | …
F p, XGF p, (GF $\neg p$) | … | …
(F p), XGF p, F $\neg p$, XGF $\neg p$ | … | …
p, XGF p, (F $\neg p$), XGF $\neg p$ | $\{p\}$: . | …
Sub$_4$
$p, \neg p, \ldots$
p, XGF p, XF $\neg p$, XGF $\neg p$ | … | $(0, \emptyset)$
(loop)

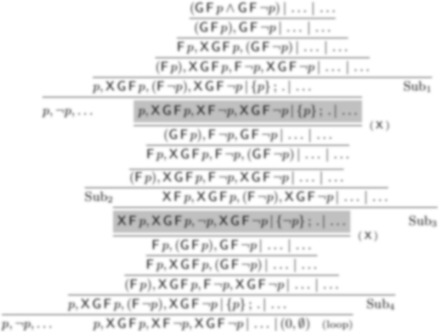
[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \land \Box\Diamond\neg p$

$$\boxed{\Box\Diamond p \land \Box\Diamond\neg p} \longrightarrow \left(\boxed{\top} \right)^{\omega}$$

$(\top)^{\omega}$

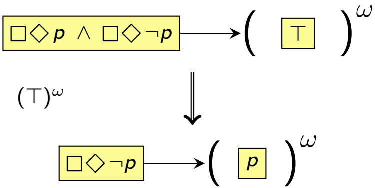


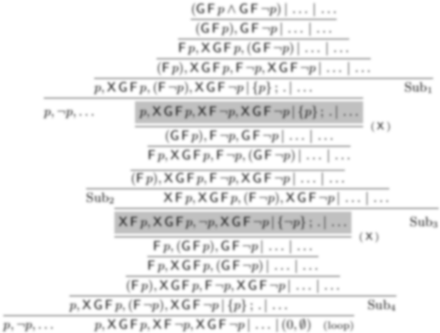
(GF p ∧ GF ¬p) | … | …
(GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} ; . | …
Sub₁
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | {p} ; . | …
(X)
(GF p), F ¬p, GF ¬p | … | …
F p, XGF p, F ¬p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
Sub₂
XF p, XGF p, (F ¬p), XGF ¬p | … | …
XF p, XGF p, ¬p, XGF ¬p | {¬p} ; . | …
Sub₃
(X)
F p, (GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} ; . | …
Sub₄
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \wedge \Box\Diamond\neg p$




(GF p ∧ GF ¬p) | … | …
(GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | {p} : . | …
(X)
(GF p), F ¬p, GF ¬p | … | …
F p, XGF p, F ¬p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
Sub₂
XF p, XGF p, (F ¬p), XGF ¬p | … | …
XF p, XGF p, ¬p, XGF ¬p | {¬p} : . | …
Sub₃
(X)
F p, (GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | … | (0, ∅)
(loop)

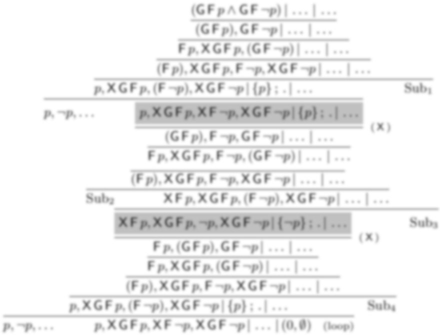
[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]
Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \land \Box\Diamond\neg p$

$$\begin{tikzcd}
\boxed{\Box\Diamond p \land \Box\Diamond\neg p} \arrow[r] \arrow[d, Rightarrow] & \left(\boxed{\top} \right)^{\omega} \\
\boxed{\Box\Diamond\neg p} \arrow[r] & \left(\boxed{p} \right)^{\omega}
\end{tikzcd}$$

$(\top)^{\omega}$

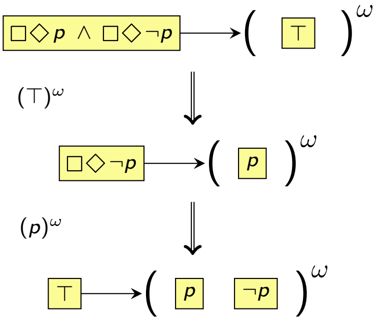
$(p)^{\omega}$

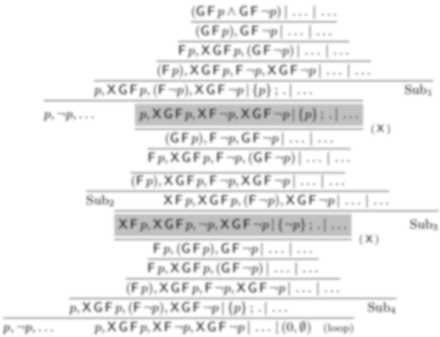

(GF p ∧ GF ¬p) | … | …
(GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | {p} : . | …
(X)
(GF p), F ¬p, GF ¬p | … | …
F p, XGF p, F ¬p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
Sub₂
XF p, XGF p, (F ¬p), XGF ¬p | … | …
XF p, XGF p, ¬p, XGF ¬p | {¬p} : . | …
Sub₃
(X)
F p, (GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**, . . .

LTL satisfiability: $\square\lozenge p \wedge \square\lozenge\neg p$

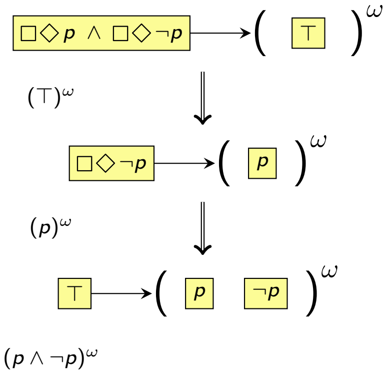



(G F p ∧ G F ¬p) | … | …
(G F p), G F ¬p | … | …
F p, X G F p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
p, X G F p, (F ¬p), X G F ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, X G F p, X F ¬p, X G F ¬p | {p} : . | …
(X)
(G F p), F ¬p, G F ¬p | … | …
F p, X G F p, F ¬p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
Sub₂
X F p, X G F p, (F ¬p), X G F ¬p | … | …
X F p, X G F p, ¬p, X G F ¬p | {¬p} : . | …
Sub₃
(X)
F p, (G F p), G F ¬p | … | …
F p, X G F p, (G F ¬p) | … | …
(F p), X G F p, F ¬p, X G F ¬p | … | …
p, X G F p, (F ¬p), X G F ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, X G F p, X F ¬p, X G F ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \ \wedge\ \Box\Diamond\neg p$



$\boxed{\Box\Diamond p \ \wedge\ \Box\Diamond\neg p} \longrightarrow \left(\ \boxed{\top}\ \right)^{\omega}$

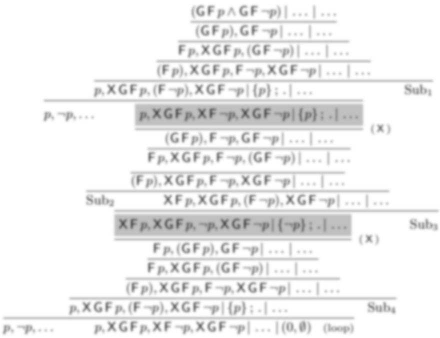
$(\top)^{\omega}$

$\boxed{\Box\Diamond\neg p} \longrightarrow \left(\ \boxed{p}\ \right)^{\omega}$

$(p)^{\omega}$

$\boxed{\top} \longrightarrow \left(\ \boxed{p}\quad \boxed{\neg p}\ \right)^{\omega}$

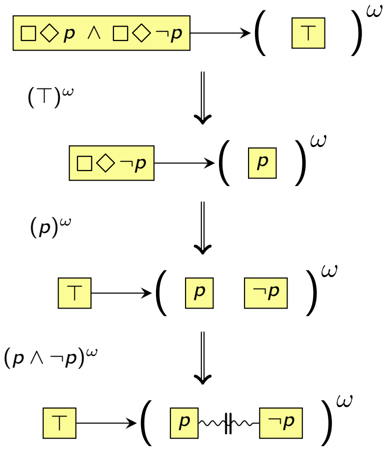
$(p \wedge \neg p)^{\omega}$

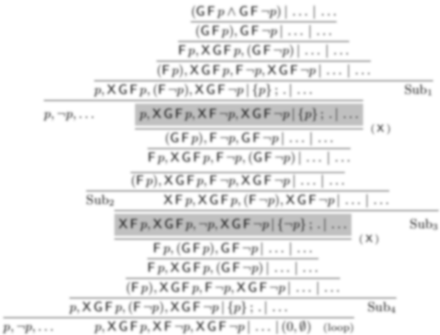

(GF p ∧ GF ¬p) | … | …
(GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | {p} : . | …
(✗)
(GF p), F ¬p, GF ¬p | … | …
F p, XGF p, F ¬p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
Sub₂
XF p, XGF p, (F ¬p), XGF ¬p | … | …
XF p, XGF p, ¬p, XGF ¬p | {¬p} : . | …
Sub₃
(✗)
F p, (GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \;\wedge\; \Box\Diamond\neg p$

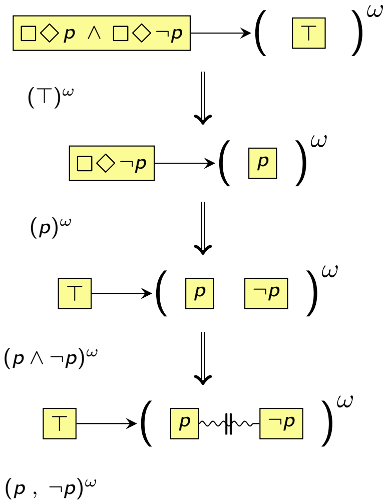


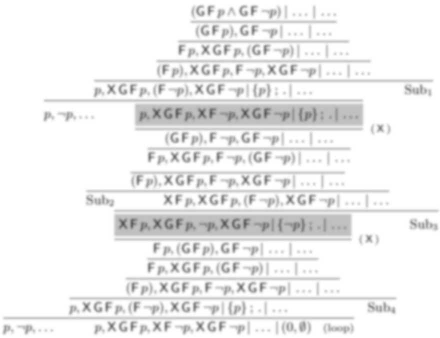

(GF p ∧ GF ¬p) | … | …
(GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₁
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | {p} : . | …
(X)
(GF p), F ¬p, GF ¬p | … | …
F p, XGF p, F ¬p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
Sub₂
XF p, XGF p, (F ¬p), XGF ¬p | … | …
XF p, XGF p, ¬p, XGF ¬p | {¬p} : . | …
Sub₃
(X)
F p, (GF p), GF ¬p | … | …
F p, XGF p, (GF ¬p) | … | …
(F p), XGF p, F ¬p, XGF ¬p | … | …
p, XGF p, (F ¬p), XGF ¬p | {p} : . | …
Sub₄
p, ¬p, …
p, XGF p, XF ¬p, XGF ¬p | … | (0, ∅)
(loop)

[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**,. . .

LTL satisfiability: $\Box\Diamond p \wedge \Box\Diamond\neg p$


$\Box\Diamond p \wedge \Box\Diamond\neg p$
$(\top)^\omega$
$(\top)^\omega$
$\Box\Diamond\neg p$
$(p)^\omega$
$(p)^\omega$
$\top$
$(p \quad \neg p)^\omega$
$(p \wedge \neg p)^\omega$
$\top$
$(p \quad \neg p)^\omega$
$(p\ ,\ \neg p)^\omega$



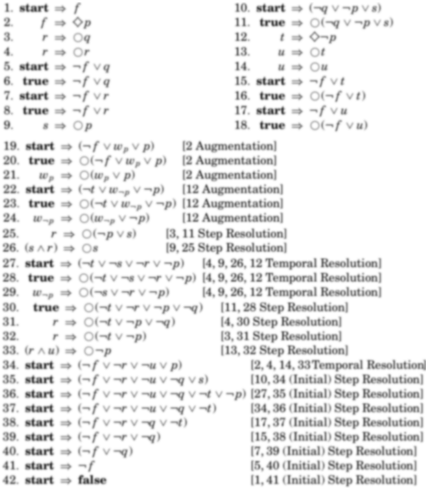
[Schwendimann, 1998,
A New One-Pass Tableau Calculus for PLTL]

Tools: **LWB**, **pltl**, **LTL Tableau**, . . .

LTL satisfiability: $\Diamond p \wedge \Box(p \implies \bigcirc p) \implies \Diamond\Box p$

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$

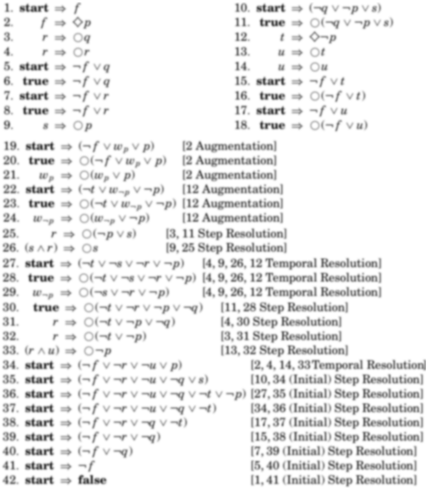


1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \vee q$
6. $\mathbf{true} \Rightarrow \neg f \vee q$
7. $\mathbf{start} \Rightarrow \neg f \vee r$
8. $\mathbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\mathbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \vee t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\mathbf{start} \Rightarrow \neg f \vee u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee u)$
19. $\mathbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33 Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$

$$\boxed{\neg\varphi} \longrightarrow \left(\; \boxed{\top} \; \right)^{\omega}$$



1. **start** $\Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. **start** $\Rightarrow \neg f \vee q$
6. **true** $\Rightarrow \neg f \vee q$
7. **start** $\Rightarrow \neg f \vee r$
8. **true** $\Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$

10. **start** $\Rightarrow (\neg q \vee \neg p \vee s)$
11. **true** $\Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. **start** $\Rightarrow \neg f \vee t$
16. **true** $\Rightarrow \bigcirc(\neg f \vee t)$
17. **start** $\Rightarrow \neg f \vee u$
18. **true** $\Rightarrow \bigcirc(\neg f \vee u)$

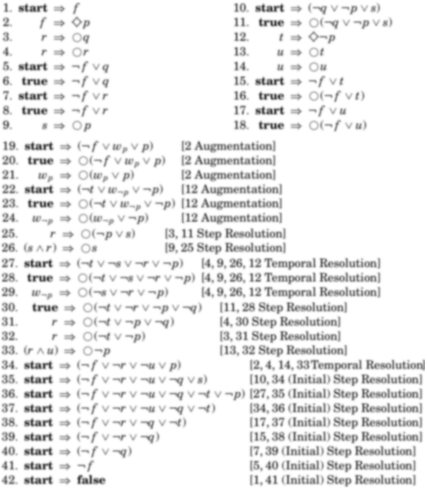
19. **start** $\Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. **true** $\Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. **start** $\Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. **true** $\Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. **start** $\Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. **true** $\Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. **true** $\Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33 Temporal Resolution]
35. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. **start** $\Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. **start** $\Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. **start** $\Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. **start** $\Rightarrow$ **false** [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$

$$\boxed{\neg\varphi} \longrightarrow \left(\boxed{\top} \right)^{\omega}$$

$(\top)^{\omega}$



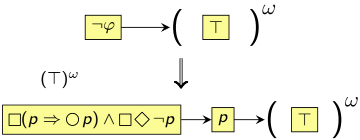
1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \vee q$
6. $\mathbf{true} \Rightarrow \neg f \vee q$
7. $\mathbf{start} \Rightarrow \neg f \vee r$
8. $\mathbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\mathbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond \neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \vee t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\mathbf{start} \Rightarrow \neg f \vee u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee u)$

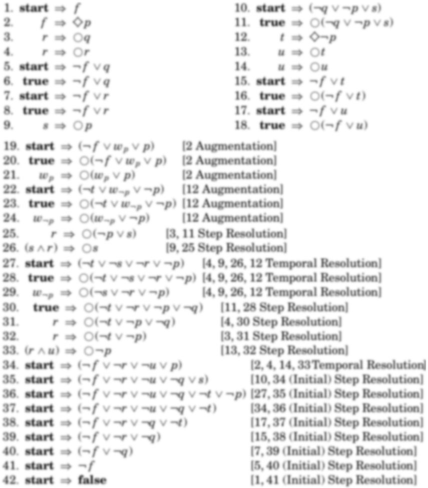
19. $\mathbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc \neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33 Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]

Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \;\equiv\; \Diamond p \,\wedge\, \Box(p \implies \bigcirc p) \,\wedge\, \Box\Diamond\neg p$

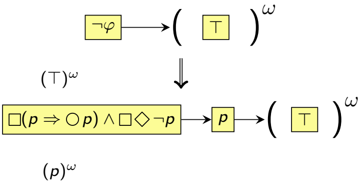


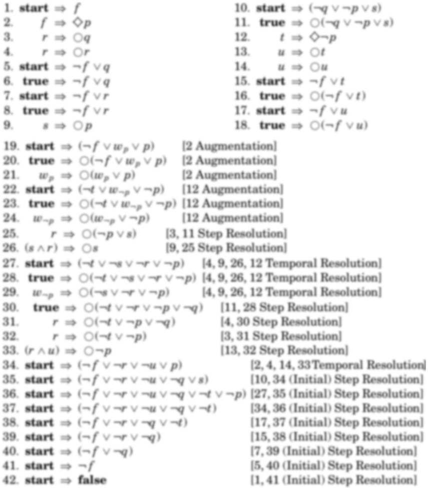


1. $\textbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\textbf{start} \Rightarrow \neg f \vee q$
6. $\textbf{true} \Rightarrow \neg f \vee q$
7. $\textbf{start} \Rightarrow \neg f \vee r$
8. $\textbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\textbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\textbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\textbf{start} \Rightarrow \neg f \vee t$
16. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\textbf{start} \Rightarrow \neg f \vee u$
18. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee u)$
19. $\textbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\textbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\textbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33Temporal Resolution]
35. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\textbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\textbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\textbf{start} \Rightarrow \textbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \Longrightarrow \bigcirc p) \wedge \Box\Diamond\neg p$

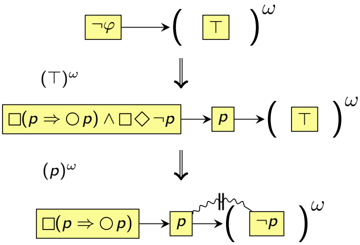


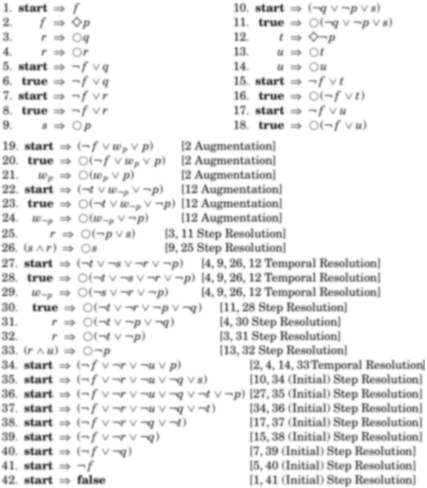


1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \vee q$
6. $\mathbf{true} \Rightarrow \neg f \vee q$
7. $\mathbf{start} \Rightarrow \neg f \vee r$
8. $\mathbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\mathbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \vee t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\mathbf{start} \Rightarrow \neg f \vee u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee u)$
19. $\mathbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33 Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$



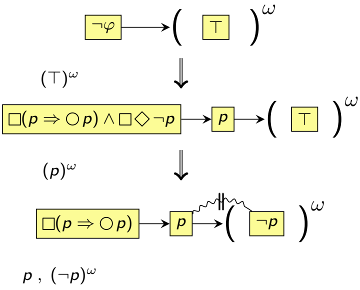


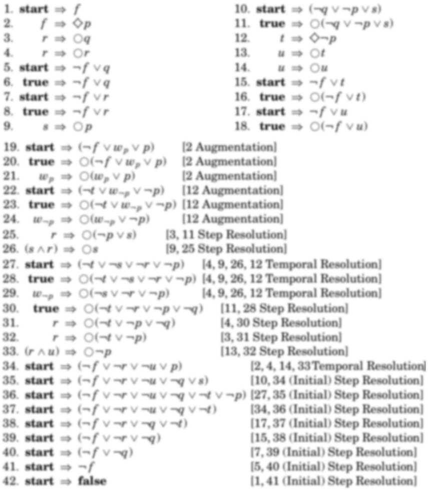
1. $\textbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\textbf{start} \Rightarrow \neg f \vee q$
6. $\textbf{true} \Rightarrow \neg f \vee q$
7. $\textbf{start} \Rightarrow \neg f \vee r$
8. $\textbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\textbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\textbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\textbf{start} \Rightarrow \neg f \vee t$
16. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\textbf{start} \Rightarrow \neg f \vee u$
18. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee u)$

19. $\textbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\textbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\textbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33Temporal Resolution]
35. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\textbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\textbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\textbf{start} \Rightarrow \textbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$



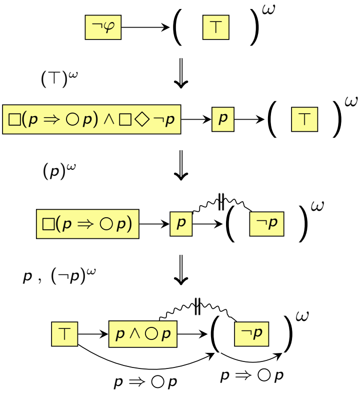


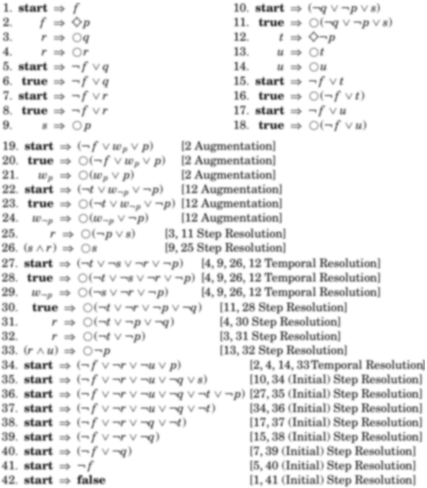
1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \vee q$
6. $\mathbf{true} \Rightarrow \neg f \vee q$
7. $\mathbf{start} \Rightarrow \neg f \vee r$
8. $\mathbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\mathbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \vee t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\mathbf{start} \Rightarrow \neg f \vee u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee u)$
19. $\mathbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]

Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \land \Box(p \implies \bigcirc p) \land \Box\Diamond\neg p$

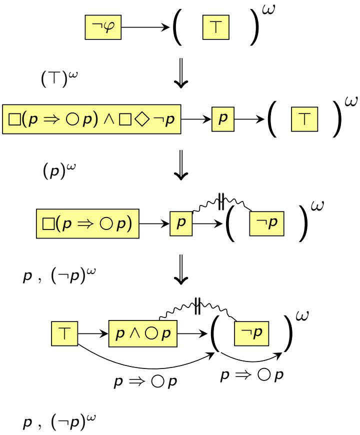


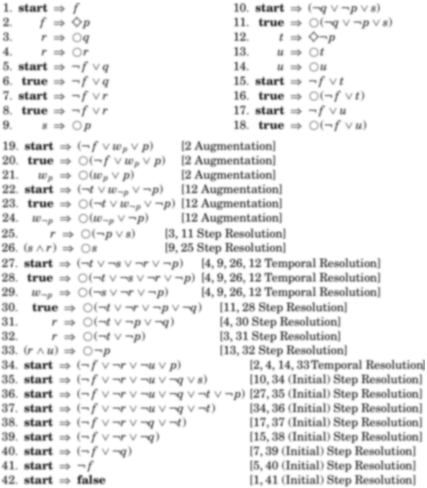


1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \lor q$
6. $\mathbf{true} \Rightarrow \neg f \lor q$
7. $\mathbf{start} \Rightarrow \neg f \lor r$
8. $\mathbf{true} \Rightarrow \neg f \lor r$
9. $s \Rightarrow \bigcirc p$
10. $\mathbf{start} \Rightarrow (\neg q \lor \neg p \lor s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \lor \neg p \lor s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \lor t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \lor t)$
17. $\mathbf{start} \Rightarrow \neg f \lor u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \lor u)$
19. $\mathbf{start} \Rightarrow (\neg f \lor w_p \lor p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \lor w_p \lor p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \lor p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \lor w_{\neg p} \lor \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \lor w_{\neg p} \lor \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \lor \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \lor s)$ [3, 11 Step Resolution]
26. $(s \land r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \lor \neg s \lor \neg r \lor \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \lor \neg r \lor \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \lor \neg r \lor \neg p \lor \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \lor \neg p \lor \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \lor \neg p)$ [3, 31 Step Resolution]
33. $(r \land u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg u \lor p)$ [2, 4, 14, 33 Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q \lor s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q \lor \neg t \lor \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q \lor \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg q \lor \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \lor \neg r \lor \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \lor \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$





1. $\mathbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\mathbf{start} \Rightarrow \neg f \vee q$
6. $\mathbf{true} \Rightarrow \neg f \vee q$
7. $\mathbf{start} \Rightarrow \neg f \vee r$
8. $\mathbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$

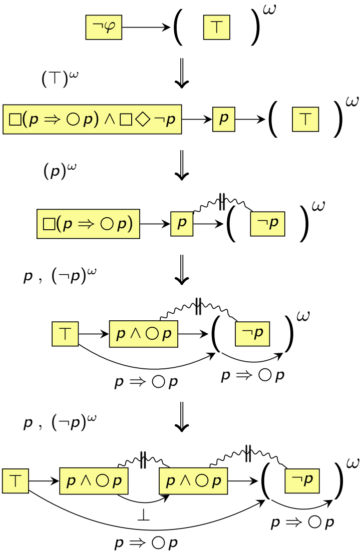
10. $\mathbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\mathbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\mathbf{start} \Rightarrow \neg f \vee t$
16. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\mathbf{start} \Rightarrow \neg f \vee u$
18. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee u)$

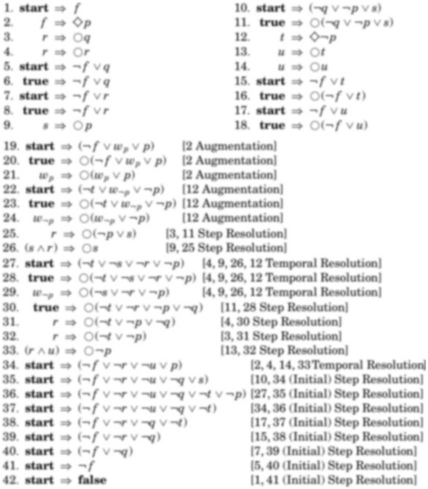
19. $\mathbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\mathbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\mathbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\mathbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\mathbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33Temporal Resolution]
35. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\mathbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\mathbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\mathbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\mathbf{start} \Rightarrow \mathbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]

Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \equiv \Diamond p \wedge \Box(p \implies \bigcirc p) \wedge \Box\Diamond\neg p$

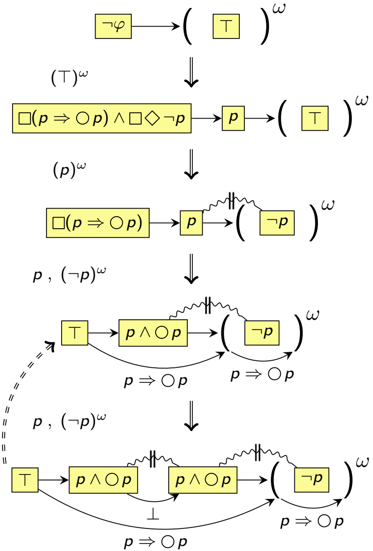


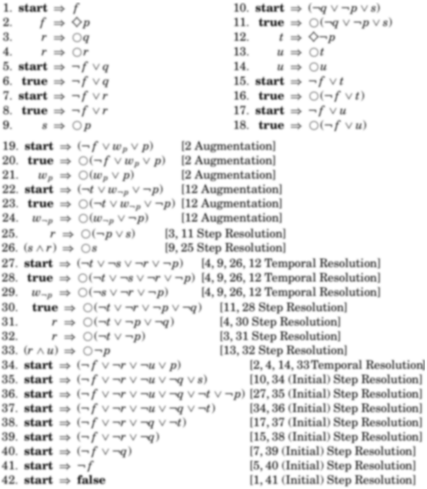


1. $\textbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\textbf{start} \Rightarrow \neg f \vee q$
6. $\textbf{true} \Rightarrow \neg f \vee q$
7. $\textbf{start} \Rightarrow \neg f \vee r$
8. $\textbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\textbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\textbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\textbf{start} \Rightarrow \neg f \vee t$
16. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\textbf{start} \Rightarrow \neg f \vee u$
18. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee u)$
19. $\textbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\textbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\textbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33 Temporal Resolution]
35. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\textbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\textbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\textbf{start} \Rightarrow \textbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL satisfiability: $\neg\varphi \;\equiv\; \Diamond p \;\wedge\; \Box(p \implies \bigcirc p) \;\wedge\; \Box\Diamond\neg p$





1. $\textbf{start} \Rightarrow f$
2. $f \Rightarrow \Diamond p$
3. $r \Rightarrow \bigcirc q$
4. $r \Rightarrow \bigcirc r$
5. $\textbf{start} \Rightarrow \neg f \vee q$
6. $\textbf{true} \Rightarrow \neg f \vee q$
7. $\textbf{start} \Rightarrow \neg f \vee r$
8. $\textbf{true} \Rightarrow \neg f \vee r$
9. $s \Rightarrow \bigcirc p$
10. $\textbf{start} \Rightarrow (\neg q \vee \neg p \vee s)$
11. $\textbf{true} \Rightarrow \bigcirc(\neg q \vee \neg p \vee s)$
12. $t \Rightarrow \Diamond\neg p$
13. $u \Rightarrow \bigcirc t$
14. $u \Rightarrow \bigcirc u$
15. $\textbf{start} \Rightarrow \neg f \vee t$
16. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee t)$
17. $\textbf{start} \Rightarrow \neg f \vee u$
18. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee u)$

19. $\textbf{start} \Rightarrow (\neg f \vee w_p \vee p)$ [2 Augmentation]
20. $\textbf{true} \Rightarrow \bigcirc(\neg f \vee w_p \vee p)$ [2 Augmentation]
21. $w_p \Rightarrow \bigcirc(w_p \vee p)$ [2 Augmentation]
22. $\textbf{start} \Rightarrow (\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
23. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee w_{\neg p} \vee \neg p)$ [12 Augmentation]
24. $w_{\neg p} \Rightarrow \bigcirc(w_{\neg p} \vee \neg p)$ [12 Augmentation]
25. $r \Rightarrow \bigcirc(\neg p \vee s)$ [3, 11 Step Resolution]
26. $(s \wedge r) \Rightarrow \bigcirc s$ [9, 25 Step Resolution]
27. $\textbf{start} \Rightarrow (\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
28. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
29. $w_{\neg p} \Rightarrow \bigcirc(\neg s \vee \neg r \vee \neg p)$ [4, 9, 26, 12 Temporal Resolution]
30. $\textbf{true} \Rightarrow \bigcirc(\neg t \vee \neg r \vee \neg p \vee \neg q)$ [11, 28 Step Resolution]
31. $r \Rightarrow \bigcirc(\neg t \vee \neg p \vee \neg q)$ [4, 30 Step Resolution]
32. $r \Rightarrow \bigcirc(\neg t \vee \neg p)$ [3, 31 Step Resolution]
33. $(r \wedge u) \Rightarrow \bigcirc\neg p$ [13, 32 Step Resolution]
34. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee p)$ [2, 4, 14, 33Temporal Resolution]
35. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee s)$ [10, 34 (Initial) Step Resolution]
36. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t \vee \neg p)$ [27, 35 (Initial) Step Resolution]
37. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg u \vee \neg q \vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q \vee \neg t)$ [17, 37 (Initial) Step Resolution]
39. $\textbf{start} \Rightarrow (\neg f \vee \neg r \vee \neg q)$ [15, 38 (Initial) Step Resolution]
40. $\textbf{start} \Rightarrow (\neg f \vee \neg q)$ [7, 39 (Initial) Step Resolution]
41. $\textbf{start} \Rightarrow \neg f$ [5, 40 (Initial) Step Resolution]
42. $\textbf{start} \Rightarrow \textbf{false}$ [1, 41 (Initial) Step Resolution]

[Fischer, Dixon, Peim, 2001,
Clausal Temporal Resolution]
Tools: **TSPASS**, **TRP++**, **TeMP**,. . .

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

LTL Properties

Fair scheduling: $\varphi_F \equiv \Box\Diamond(at_2 \wedge r_{free}) \implies \Box\Diamond at_3$

Termination of critical sections: $\varphi_T \equiv \Box(at_3 \implies \Diamond at_1)$

Individual **A**ccessibility: $\varphi_A \equiv \Box(at_2 \implies \Diamond at_3)$

$$\varphi \equiv \bigwedge_{i\in 1..n}(\varphi_{F_i} \wedge \varphi_{T_i}) \implies \varphi_{A_1}$$

Translation of $\neg\varphi$ into a Büchi automaton: **ltl3ba**

Threads	Time (sec)	Memory (MB)	|Automaton| (MB)
2	0.005	4.2	0.002
3	0.09	5.0	0.38
4	9.6	14.7	8.6
5	1295	139	185
6	TO	X	X

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$
\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}
$$

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$\begin{array}{llllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond\, at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond\, at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond\, at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond\, at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond\, at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond\, at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \land r_{free}) \implies \Box\Diamond at_{l_3} & \land & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \land r_{free}) \implies \Box\Diamond at_{m_3} & \land & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \land & \Diamond(at_{l_2} \land \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \land r_{free}) \implies \Box\Diamond at_{n_3} & \land & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond\, at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond\, at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond\, at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond\, at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond\, at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond\, at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lclclcl}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & & & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$
\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}
$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$
\begin{array}{lclcl}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond\, at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond\, at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond\, at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond\, at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond\, at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond\, at_{n_1}) & &
\end{array}
$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond\, at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond\, at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond\, at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond\, at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond\, at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond\, at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
    - Suppose, it's thread 2

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lclclcl}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & & & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
   - Suppose, it's thread 2

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond\, at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond\, at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond\, at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond\, at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond\, at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond\, at_{n_1}) & &
\end{array}$$

❶ Thread 1 stays at l_1

❷ Thread 1 moves to l_2 and stays there

❸ Someone should request and hold the resource. Who?

  - Suppose, it's thread 2
  - Thread 2 should be at m_3

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
   - Suppose, it's thread 2
   - Thread 2 should be at m_3

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$
\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}
$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
    - Suppose, it's thread 2
    - Thread 2 should be at m_3
    - Thread 2 should leave the critical section to m_1

LTL model checking

Thread 1

```
while (true) {
  $l_1$:  noncritical;
  $l_2$:  request r;
  $l_3$:  critical;
  $l_4$:  release r;
}
```

Thread 2

```
while (true) {
  $m_1$:  noncritical;
  $m_2$:  request r;
  $m_3$:  critical;
  $m_4$:  release r;
}
```

Thread 3

```
while (true) {
  $n_1$:  noncritical;
  $n_2$:  request r;
  $n_3$:  critical;
  $n_4$:  release r;
}
```

$$\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
   - Suppose, it's thread 2
   - Thread 2 should be at m_3
   - Thread 2 should leave the critical section to m_1

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$\begin{array}{lclcl} \Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\ \Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\ \Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & & \end{array}$$

❶ Thread 1 stays at l_1

❷ Thread 1 moves to l_2 and stays there

❸ Someone should request and hold the resource. Who?

- Suppose, it's thread 2
- Thread 2 should be at m_3
- Thread 2 should leave the critical section to m_1
- Thread 2 should release the resource

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$
\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}
$$

❶ Thread 1 stays at l_1

❷ Thread 1 moves to l_2 and stays there

❸ Someone should request and hold the resource. Who?

- Suppose, it's thread 2
- Thread 2 should be at m_3
- Thread 2 should leave the critical section to m_1
- Thread 2 should release the resource

- Suppose, it's thread 3
- ...

LTL model checking

Thread 1

```
while (true) {
  l1:  noncritical;
  l2:  request r;
  l3:  critical;
  l4:  release r;
}
```

Thread 2

```
while (true) {
  m1:  noncritical;
  m2:  request r;
  m3:  critical;
  m4:  release r;
}
```

Thread 3

```
while (true) {
  n1:  noncritical;
  n2:  request r;
  n3:  critical;
  n4:  release r;
}
```

$$
\begin{array}{lllll}
\Box\Diamond(at_{l_2} \wedge r_{free}) \implies \Box\Diamond at_{l_3} & \wedge & \Box(at_{l_3} \implies \Diamond at_{l_1}) & & \\
\Box\Diamond(at_{m_2} \wedge r_{free}) \implies \Box\Diamond at_{m_3} & \wedge & \Box(at_{m_3} \implies \Diamond at_{m_1}) & \wedge & \Diamond(at_{l_2} \wedge \Box\neg at_{l_3}) \\
\Box\Diamond(at_{n_2} \wedge r_{free}) \implies \Box\Diamond at_{n_3} & \wedge & \Box(at_{n_3} \implies \Diamond at_{n_1}) & &
\end{array}
$$

1. Thread 1 stays at l_1
2. Thread 1 moves to l_2 and stays there
3. Someone should request and hold the resource. Who?
   - Suppose, it's thread 2
   - Thread 2 should be at m_3
   - Thread 2 should leave the critical section to m_1
   - Thread 2 should release the resource

   - Suppose, it's thread 3
   - . . .

Conclusion

Main problem: LTL formulas are often not small!

Automata-based methods fail even to start model checking

Conclusion

Main problem: LTL formulas are often not small!

Automata-based methods fail even to start model checking

Causality-based approach to LTL model checking

- Proof objects $\Longrightarrow$ concurrent traces
- Proof rules $\Longrightarrow$ language-preserving trace transformations
- Proof construction $\Longrightarrow$ tableau-based trace search

Conclusion

Main problem: LTL formulas are often not small!

Automata-based methods fail even to start model checking

Causality-based approach to LTL model checking

- Proof objects ⟹ concurrent traces
- Proof rules ⟹ language-preserving trace transformations
- Proof construction ⟹ tableau-based trace search

Result

A method that works directly on the LTL formula and provides better scalability

Conclusion

Main problem: LTL formulas are often not small!

Automata-based methods fail even to start model checking

Causality-based approach to LTL model checking

- Proof objects $\Longrightarrow$ concurrent traces
- Proof rules $\Longrightarrow$ language-preserving trace transformations
- Proof construction $\Longrightarrow$ tableau-based trace search

Result

A method that works directly on the LTL formula and provides better scalability

Thank you for your attention!