Causality-based LTL Model Checking without Automata joint work with Bernd Finkbeiner

Andrey Kupriyanov

Saarland University Reactive Systems Group

September 5, 2014





Motivation		
•0		

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			
00	000	00	

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 :

- $\bullet \text{ translate } \neg \varphi \text{ into a Büchi automaton } A$
- \boldsymbol{O} check for emptiness the synchronized product of A and P

Motivation		
•0		

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 :

- $\bullet \text{ translate } \neg \varphi \text{ into a Büchi automaton } A$
- \boldsymbol{O} 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

Motivation		
00		

Example: individual accessibility for semaphores

Threa	d 1	Thread	2	Thread	13
while	(true) {	while	(true) {	while	(true) {
$I_1:$	noncritical;	m_1 :	noncritical;	n_1 :	noncritical;
l_2 :	request r;	m_2 :	request r;	n_2 :	request r;
<i>I</i> ₃ :	critical;	<i>m</i> ₃ :	critical;	<i>n</i> ₃ :	critical;
$I_4:$	release r;	$m_4:$	release r;	n ₄ :	release r;
}		}		}	

LTL Properties

Fair scheduling: Termination of critical sections: $\varphi_T \equiv \Box(at_3 \Longrightarrow \diamondsuit at_1)$ Individual Accessibility:

 $\varphi_F \equiv \Box \diamondsuit (at_2 \land r_{free}) \implies \Box \diamondsuit at_3$ $\varphi_A \equiv \Box(at_2 \Longrightarrow \diamondsuit at_3)$

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

Translation of $\neg \varphi$ into a Büchi automaton: **Itl3ba**

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	то	X	Х

Causality-based Proofs		
000		

Our approach

• Proof objects: concurrent traces

allow to capture temporal order, constraints, independence



Causality-based Proofs		
000		

Our approach

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

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



C

Causality-based Proofs		
000		

Our approach

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

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

• Proof construction: tableau search based on causal loops causal loops \equiv infinitely-looping trace transformations







Causality-based Proofs		
000		



Causality-based Proofs		
000		



Causality-based Proofs		
000		



Causality-based Proofs		
000		



Causality-based Proofs		
000		



Causality-based Proofs ○●○		



Causality-based Proofs		
000		

LTL proof rules



Finally

Globally

Causality-based Proofs		
000		

LTL proof rules



Finally

Globally



Causality-based Proofs		
000		

LTL proof rules



Finally

Globally



Other proof rules

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

	LTL Satisfiability	
	••	

	LTL Satisfiability	
	•0	



[Schwendimann, 1998,

	LTL Satisfiability	
	0	

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



[Schwendimann, 1998,

	LTL Satisfiability	
	0	



 $(\top)^{\omega}$



[Schwendimann, 1998,

	LTL Satisfiability	
	0	





[Schwendimann, 1998,

	LTL Satisfiability	
	0	



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



[Schwendimann, 1998,

	LTL Satisfiability	
	0	





Schwendimann, 1998,

	LTL Satisfiability	
	0	



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



Schwendimann, 1998,

	LTL Satisfiability	
	0	



	$\frac{(GF p \land GF \neg p) \dots \dots}{(GF p), GF \neg p \dots \dots}$ $\overline{F p, XGF p, (GF \neg p) \dots \dots}$ $\overline{F p, XGF p, (GF \neg p) \dots \dots \dots}$	
$\overline{p, X}$	$(F_p), X_{G}_{F_p}, F_{\neg p}, X_{G}_{F_{\neg p}} \{p\}; . \dots$	Sub ₁
$p, \neg p, \ldots$	$p, X G F p, X F \neg p, X G F \neg p \{p\}; . $	
	$\frac{(GFp),F\neg p,GF\neg p \dots \dots}{Fp,XGFp,F\neg p,(GF\neg p) \dots \dots}$ (X)	
Sub ₂	$ \begin{array}{c} \hline (Fp), XGFp, F\neg p, XGF\neg p \mid \ldots \mid \ldots \\ \\ XFp, XGFp, (F\neg p), XGF\neg p \mid \ldots \mid \ldots \end{array} $	
	$X F p, X G F p, \neg p, X G F \neg p \{\neg p\}; . $	Sub;
	$\frac{Fp, (GFp), GF\neg p \dots \dots}{Fp XGFp (GF\neg p) \dots \dots}$ (X)	
	$\frac{(F_p), X G F_p, (G F_p) \dots \dots}{(F_p), X G F_p, F \neg p, X G F \neg p \dots \dots}$	
p, X G F	$p, (F \neg p), X G F \neg p \mid \{p\}; . \dots$ Sub ₄	
$p, \neg p, \dots \qquad p, X$	$(GF_p, XF \neg p, XGF \neg p \dots (0, \emptyset) \text{ (loop)})$	

[Schwendimann, 1998,

	LTL Satisfiability	
	0	



	$\frac{(GFp \land GF\neg p) \dots \dots}{(GFp), GF\neg p \dots \dots}$ $\overline{Fp, XGFp, (GF\neg p) \dots \dots}$ $\overline{Fp, XGFp, CF\neg p \dots \dots}$	
	$(Fp), XGFp, F\neg p, XGF \neg p \dots \dots$	Sub ₁
$p, \neg p, \dots$	$p, X \subseteq F p, X F \neg p, X \subseteq F \neg p \mid \{p\}; . $	
	$\frac{(GFp), F \neg p, GF \neg p \dots \dots}{Fp, XGFp, F \neg p, (GF \neg p) \dots \dots}$ (X)	
Sul	$ \overline{(Fp),XGFp,F\neg p,XGF\neg p \ldots \ldots} } $ $ b_2 \qquad XFp,XGFp,(F\neg p),XGF\neg p \ldots \ldots} $	
	$X F p, X G F p, \neg p, X G F \neg p \{\neg p\}; . $	Sub;
	F_{p} , (GF _p), GF _{¬p} (X)	
	$F p, X G F p, (G F \neg p) \mid \ldots \mid \ldots$	
	$(F p), X G F p, F \neg p, X G F \neg p \mid \ldots \mid \ldots$	_
p, X G	$F p$, $(F \neg p)$, $X G F \neg p \{p\}$; . Sub	4
$p, \neg p, \dots p$	$X G F p, X F \neg p, X G F \neg p \dots (0, \emptyset)$ (loop)	

[Schwendimann, 1998,

	LTL Satisfiability	
	00	

LTL satisfiability: $\Diamond p \land \Box(p \Longrightarrow \bigcirc p) \Longrightarrow \Diamond \Box p$

		LTL Satisfiability	
00	000	00	

	LTL Satisfiability	
	00	

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

	LTL Satisfiability	
	00	

 $\xrightarrow{\neg \varphi} (\Box)^{\omega}$

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

	LTL Satisfiability	
	00	

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

 $(\top)^{\omega}$

1. start $\Rightarrow f$	10. start $\Rightarrow (\neg q \lor \neg p \lor s)$
2. $f \Rightarrow \Diamond p$	11. true $\Rightarrow \bigcirc (\neg q \lor \neg p \lor s)$
3. $r \Rightarrow \bigcirc q$	12. $t \Rightarrow \Diamond \neg p$
4. $r \Rightarrow \bigcirc r$	13. $u \Rightarrow \bigcirc t$
5. start $\Rightarrow \neg f \lor q$	14. $u \Rightarrow \bigcirc u$
6. true $\Rightarrow \neg f \lor q$	15. start $\Rightarrow \neg f \lor t$
7. start $\Rightarrow \neg f \lor r$	16. true $\Rightarrow \bigcirc (\neg f \lor t)$
8. true $\Rightarrow \neg f \lor r$	17. start $\Rightarrow \neg f \lor u$
9. $s \Rightarrow \bigcirc p$	18. true $\Rightarrow \bigcirc (\neg f \lor u)$
19. start $\Rightarrow (\neg f \lor w \lor p)$	[2 Augmentation]
20. true $\Rightarrow \bigcirc (\neg f \lor w_{-} \lor p)$	[2 Augmentation]
21. $w_n \Rightarrow \bigcirc (w_n \lor p)$	[2 Augmentation]
22. start $\Rightarrow (\neg t \lor w_{\neg n} \lor \neg p)$	[12 Augmentation]
23. 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. $(s \wedge r) \Rightarrow \bigcirc s$ [9,	25 Step Resolution]
27. start $\Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p)$	[4, 9, 26, 12 Temporal Resolution]
28. 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. true $\Rightarrow \bigcirc (\neg t \lor \neg r \lor \neg p \lor$	¬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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor p)$	[2, 4, 14, 33 Temporal Resolution
35. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q$	(10, 34 (Initial) Step Resolution)
36. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q)$	$q \lor \neg t \lor \neg p$) [27, 35 (Initial) Step Resolution
37. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q$	$(v \neg t)$ [34, 36 (Initial) Step Resolution
38. start $\Rightarrow (\neg f \lor \neg r \lor \neg q \lor \neg t)$	 [17, 37 (Initial) Step Resolution
39. start $\Rightarrow (\neg f \lor \neg r \lor \neg q)$	[15, 38 (Initial) Step Resolution
40. start $\Rightarrow (\neg f \lor \neg q)$	[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]

	LTL Satisfiability	
	00	



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

	LTL Satisfiability	
	00	



 $(p)^{\omega}$

1. start $\Rightarrow f$ 2. $f \Rightarrow \Diamond p$ 3. $r \Rightarrow \bigcirc q$ 4. $r \Rightarrow \bigcirc r$ 5. start $\Rightarrow \neg f \lor q$ 6. true $\Rightarrow \neg f \lor q$ 7. start $\Rightarrow \neg f \lor r$ 8. true $\Rightarrow \neg f \lor r$	10. start $\Rightarrow (\neg q \lor \neg p \lor s)$ 11. true $\Rightarrow \bigcirc (\neg q \lor \neg p \lor s)$ 12. $t \Rightarrow \circlearrowright \neg p$ 13. $u \Rightarrow \circlearrowright t$ 14. $u \Rightarrow \bigcirc t$ 15. start $\Rightarrow \neg f \lor t$ 16. true $\Rightarrow \bigcirc (\neg f \lor t)$ 17. start $\Rightarrow \neg f \lor u$
9. $s \Rightarrow \bigcirc p$ 19. $start \Rightarrow (\neg f \lor w_p \lor p)$ 20. $true \Rightarrow \bigcirc (\neg f \lor w_p \lor p)$ 21. $w_p \Rightarrow \bigcirc w_p \lor p$ 22. $start \Rightarrow (\neg t \lor w_{-p} \lor \neg p)$ 23. $true \Rightarrow \bigcirc (\neg t \lor w_{-p} \lor \neg p)$ 24. $w_{-p} \Rightarrow \bigcirc (w_{-p} \lor \neg p)$ 25. $r \Rightarrow \bigcirc (\neg p \lor s)$ [3,	18. true ⇒ ○(¬f ∨ u) [2 Augmentation] [2 Augmentation] [2 Augmentation] [12 Augmentation] [12 Augmentation] [12 Augmentation] 11 Step Resolution]
26. $(s \land r) \Rightarrow \bigcirc s$ [9, 27. start $\Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p$ 28. true $\Rightarrow \bigcirc (\neg t \lor \neg s \lor \neg r \lor \neg p$ 29. $w_{\neg p} \Rightarrow \bigcirc (\neg s \lor \neg r \lor \neg p)$ 30. true $\Rightarrow \bigcirc (\neg t \lor \neg r \lor \neg p \lor$ 31. $r \Rightarrow \bigcirc (\neg t \lor \neg p)$	25 Step Resolution] [4, 9, 26, 12 Temporal Resolution] ¬p) [4, 9, 26, 12 Temporal Resolution] [4, 9, 26, 12 Temporal Resolution] [4, 30 Step Resolution] [3, 31 Step Resolution]
$\begin{array}{cccc} 3. & r & \ldots & 0 & r \\ 3. & (r , u) \Rightarrow & 0 & \neg p \\ 34. & \operatorname{start} \Rightarrow & (-f \lor \neg r \lor \neg u \lor \gamma \\ 35. & \operatorname{start} \Rightarrow & (-f \lor \neg r \lor \neg u \lor \gamma \\ 36. & \operatorname{start} \Rightarrow & (-f \lor \neg r \lor \neg u \lor \gamma \\ 38. & \operatorname{start} \Rightarrow & (-f \lor \neg r \lor \neg q) \\ 40. & \operatorname{start} \Rightarrow & (-f \lor \neg r \lor \gamma \\ 41. & \operatorname{start} \Rightarrow & \neg f \\ 42. & \operatorname{start} \Rightarrow & -f \\ 42. & \operatorname{start} \Rightarrow & -f \\ 43. & \operatorname{start} \Rightarrow & -f \\ 44. & \operatorname{start} $	[13, 32 Step Resolution] [13, 32 Step Resolution] (2, 4, 14, 33 Temporal Resolution] $q \lor s$ $q \lor t \lor -p$) [27, 35 (Initial) Step Resolution] $q \lor t \lor -p$) [27, 35 (Initial) Step Resolution] (17, 37 (Initial) Step Resolution] (15, 38 (Initial) Step Resolution] (7, 39 (Initial) Step Resolution] (7, 39 (Initial) Step Resolution] (5, 40 (Initial) Step Resolution] (2, 40 (Initial) Step Resolution]
the start of table	(a) as (minin) over nesonation)

[Fischer, Dixon, Peim, 2001,

Clausal Temporal Resolution]

	LTL Satisfiability	
	00	



1. start $\Rightarrow f$	10. start $\Rightarrow (\neg q \lor \neg p \lor s)$
2. $f \Rightarrow \Diamond p$	11. true $\Rightarrow \bigcirc (\neg q \lor \neg p \lor s)$
3. $r \Rightarrow \bigcirc q$	12. $t \Rightarrow \Diamond \neg p$
4. $r \Rightarrow \bigcirc r$	13. $u \Rightarrow \bigcirc t$
5. start $\Rightarrow \neg f \lor q$	14. $u \Rightarrow \bigcirc u$
6. true $\Rightarrow \neg f \lor q$	15. start $\Rightarrow \neg f \lor t$
7. start $\Rightarrow \neg f \lor r$	16. true $\Rightarrow \bigcirc (\neg f \lor t)$
8. true $\Rightarrow \neg f \lor r$	17. start $\Rightarrow \neg f \lor u$
9. $s \Rightarrow \bigcirc p$	18. true $\Rightarrow \bigcirc (\neg f \lor u)$
19. start $\Rightarrow (\neg f \lor w_n \lor p)$	[2 Augmentation]
20. true $\Rightarrow \bigcirc (\neg f \lor w_n \lor p)$	[2 Augmentation]
21. $w_n \Rightarrow \bigcirc (w_n \lor p)$	[2 Augmentation]
22. start $\Rightarrow (\neg t \lor w_{\neg p} \lor \neg p)$	[12 Augmentation]
23. 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. start $\Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p$	[4, 9, 26, 12 Temporal Resolution]
28. true $\Rightarrow \bigcirc (\neg t \lor \neg s \lor \neg r \lor \cdot$	¬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. 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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor p)$	 [2, 4, 14, 33 Temporal Resolution
35. start \Rightarrow ($\neg f \lor \neg r \lor \neg u \lor \neg$	$q \lor s$ [10, 34 (Initial) Step Resolution
36. 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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg$	$q \lor \neg t$) [34, 36 (Initial) Step Resolution
38. start $\Rightarrow (\neg f \lor \neg r \lor \neg q \lor \neg$	(17, 37 (Initial) Step Resolution
39. start $\Rightarrow (\neg f \lor \neg r \lor \neg q)$	[15, 38 (Initial) Step Resolution
40. start $\Rightarrow (\neg f \lor \neg q)$	[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]

	LTL Satisfiability	
	00	



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

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

	LTL Satisfiability	
	00	



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

	LTL Satisfiability	
	00	



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

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

	LTL Satisfiability	
	00	



1. start $\Rightarrow f$	10. start $\Rightarrow (\neg q \lor \neg p \lor s)$
2. $f \Rightarrow \Diamond p$	11. true $\Rightarrow \bigcirc (\neg q \lor \neg p \lor s)$
3. $r \Rightarrow \bigcirc q$	12. $t \Rightarrow \Diamond \neg p$
4. $r \Rightarrow \bigcirc r$	13. $u \Rightarrow \bigcirc t$
5. start $\Rightarrow \neg f \lor q$	14. $u \Rightarrow \bigcirc u$
6. true $\Rightarrow \neg f \lor q$	15. start $\Rightarrow \neg f \lor t$
7. start $\Rightarrow \neg f \lor r$	16. true $\Rightarrow \bigcirc (\neg f \lor t)$
8. true $\Rightarrow \neg f \lor r$	17. start $\Rightarrow \neg f \lor u$
9. $s \Rightarrow \bigcirc p$	18. true $\Rightarrow \bigcirc (\neg f \lor u)$
19. start $\Rightarrow (\neg f \lor w_p \lor p)$ [2.1]	Augmentation]
20. true $\Rightarrow \bigcirc (\neg f \lor w_p \lor p)$ [2]	Augmentation]
21. $w_p \Rightarrow \bigcirc (w_p \lor p)$ [24]	Augmentation]
22. start $\Rightarrow (\neg t \lor w_{\neg p} \lor \neg p)$ [12]	Augmentation]
23. 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. start $\Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p)$	[4, 9, 26, 12 Temporal Resolution]
28. 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. 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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor p)$	[2, 4, 14, 33 Temporal Resolution]
35. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q \lor)$	s) [10, 34 (Initial) Step Resolution]
36. 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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q \lor$	¬t) [34, 36 (Initial) Step Resolution]
38. start $\Rightarrow (\neg f \lor \neg r \lor \neg q \lor \neg t)$	[17, 37 (Initial) Step Resolution]
39. start $\Rightarrow (\neg f \lor \neg r \lor \neg q)$	[15, 38 (Initial) Step Resolution]
40. start $\Rightarrow (\neg f \lor \neg q)$	[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	
	00	



1. start $\Rightarrow f$	10. start $\Rightarrow (\neg q \lor \neg p \lor s)$
2. $f \Rightarrow \Diamond p$	11. true $\Rightarrow \bigcirc (\neg q \lor \neg p \lor s)$
3. $r \Rightarrow \bigcirc q$	12. $t \Rightarrow \Diamond \neg p$
4. $r \Rightarrow \bigcirc r$	13. $u \Rightarrow \bigcirc t$
5. start $\Rightarrow \neg f \lor q$	14. $u \Rightarrow \bigcirc u$
6. true $\Rightarrow \neg f \lor q$	15. start $\Rightarrow \neg f \lor t$
7. start $\Rightarrow \neg f \lor r$	16. true $\Rightarrow \bigcirc (\neg f \lor t)$
8. true $\Rightarrow \neg f \lor r$	17. start $\Rightarrow \neg f \lor u$
9. $s \Rightarrow \bigcirc p$	18. true $\Rightarrow \bigcirc (\neg f \lor u)$
19. start $\Rightarrow (\neg f \lor w_p \lor p)$	2 Augmentation]
20. true $\Rightarrow \bigcirc (\neg f \lor w_p \lor p)$	2 Augmentation]
21. $w_p \Rightarrow \bigcirc (w_p \lor p)$	2 Augmentation]
22. start $\Rightarrow (\neg t \lor w_{\neg p} \lor \neg p)$	12 Augmentation]
23. 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, 1]	11 Step Resolution]
26. $(s \land r) \Rightarrow \bigcirc s$ [9, 2	25 Step Resolution]
27. start $\Rightarrow (\neg t \lor \neg s \lor \neg r \lor \neg p)$	[4, 9, 26, 12 Temporal Resolution]
28. 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. true $\Rightarrow \bigcirc (\neg t \lor \neg r \lor \neg p \lor $	¬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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor p)$	[2, 4, 14, 33 Temporal Resolution
35. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q$	∨ s) [10, 34 (Initial) Step Resolution]
36. 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. start $\Rightarrow (\neg f \lor \neg r \lor \neg u \lor \neg q$	$(\vee \neg t)$ [34, 36 (Initial) Step Resolution]
38. start \Rightarrow $(\neg f \lor \neg r \lor \neg q \lor \neg t)$) [17, 37 (Initial) Step Resolution]
39. start $\Rightarrow (\neg f \lor \neg r \lor \neg q)$	[15, 38 (Initial) Step Resolution]
40. start $\Rightarrow (\neg f \lor \neg q)$	[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 Model Checking	
00	000	00		

Thread 1	Thread 2	Thread 3
while (true) {	while (true) {	while (true) {
l_1 : noncritical;	<pre>m1: noncritical;</pre>	<pre>n₁: noncritical;</pre>
I ₂ : request r;	m ₂ : request r;	n ₂ : request r;
I ₃ : critical;	<pre>m₃: critical;</pre>	n ₃ : critical;
l_4 : release r;	m4: release r;	<pre>n₄: release r;</pre>
}	}	}

LTL Properties

Fair scheduling: Termination of critical sections: Individual Accessibility:

$$\begin{array}{l}\varphi_{F} \equiv \Box \diamondsuit (at_{2} \land r_{free}) \Longrightarrow \Box \diamondsuit at_{3}\\ \varphi_{T} \equiv \Box (at_{3} \Longrightarrow \diamondsuit at_{1})\\ \varphi_{A} \equiv \Box (at_{2} \Longrightarrow \diamondsuit at_{3})\end{array}$$

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

Translation of $\neg \varphi$ into a Büchi automaton: **Itl3ba**

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	то	X	Х

	LTL Model Checking	
	•	

Thread	d 1	Thread 2	Thread 3
while <i>l</i> ₁ : <i>l</i> ₂ : <i>l</i> ₃ : <i>l</i> ₄ : }	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) { m1: noncritical; m2: request r; m3: critical; m4: release r; }</pre>	<pre>while (true) { n1: noncritical; n2: request r; n3: critical; n4: release r; }</pre>

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

	LTL Model Checking	
	•	

Thread	11	Thread 2	Thread 3
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ : }	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) { m1: noncritical; m2: request r; m3: critical; m4: release r; }</pre>	<pre>while (true) { n1: noncritical; n2: request r; n3: critical; n4: release r; }</pre>
J		J	J

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

 $\bullet \ \ {\rm Thread} \ \ 1 \ {\rm stays} \ {\rm at} \ \ I_1$

	LTL Model Checking	
	•	

Thread	d 1	Thread 2		Thread	13
while <i>l</i> ₁ : <i>l</i> ₂ : <i>l</i> ₃ : <i>l</i> ₄ : }	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (tru m1: no m2: re m3: cr m4: re }</pre>	<pre>le) { ncritical; quest r; itical; lease r;</pre>	<pre>while n1: n2: n3: n4: }</pre>	<pre>(true) { noncritical; request r; critical; release r;</pre>
,		J		J	

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

 $\bullet \ \ {\rm Thread} \ \ 1 \ {\rm stays} \ {\rm at} \ \ I_1$

Motivation	Causality-based Proofs	LTL Satisfiability	LTL Model Checking	
00	000	00	●	

Thread	d 1	Thread	2	Thread	13
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while (<i>m</i> ₁ : <i>m</i> ₂ : <i>m</i> ₃ : <i>m</i> ₄ :	<pre>true) { noncritical; request r; critical; release r;</pre>	while n1: n2: n3: n4:	<pre>(true) { noncritical; request r; critical; release r;</pre>
}		}		}	

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

• Thread 1 stays at I_1

2 Thread 1 moves to I_2 and stays there

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Thread	11	Thread	2	Thread	3
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while <i>m</i> ₁ : <i>m</i> ₂ : <i>m</i> ₃ : <i>m</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while n ₁ : n ₂ : n ₃ : n ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>
}		}		}	

$$\begin{array}{c} \bigcirc \left(\mathsf{at}_{l_2} \wedge \mathsf{r}_{\mathsf{free}} \right) \implies \bigcirc \diamond \mathsf{at}_{l_3} & \wedge & \square \left(\mathsf{at}_{l_3} \implies \diamondsuit \mathsf{at}_{l_1} \right) \\ \square \diamondsuit \left(\mathsf{at}_{m_2} \wedge \mathsf{r}_{\mathsf{free}} \right) \implies \square \diamondsuit \mathsf{at}_{m_3} & \wedge & \square \left(\mathsf{at}_{m_3} \implies \diamondsuit \mathsf{at}_{m_1} \right) & \wedge & \diamondsuit \left(\mathsf{at}_{l_2} \wedge \square \neg \mathsf{at}_{l_3} \right) \\ \square \diamondsuit \left(\mathsf{at}_{n_2} \wedge \mathsf{r}_{\mathsf{free}} \right) \implies \square \diamondsuit \mathsf{at}_{n_3} & \wedge & \square \left(\mathsf{at}_{n_3} \implies \diamondsuit \mathsf{at}_{n_1} \right) \end{array}$$

• Thread 1 stays at I_1

2 Thread 1 moves to I_2 and stays there

	LTL Model Checking	

Threa	d 1	Thread	2	Thread	13
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while (m1: m2: m3: m4:	<pre>(true) { noncritical; request r; critical; release r;</pre>	while n ₁ : n ₂ : n ₃ : n ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>
}		}		}	

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

- Thread 1 stays at I_1
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Thread	d 1	Thread	2	Thread	13
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while (<i>m</i> ₁ : <i>m</i> ₂ : <i>m</i> ₃ : <i>m</i> ₄ :	<pre>true) { noncritical; request r; critical; release r;</pre>	while n1: n2: n3: n4:	<pre>(true) { noncritical; request r; critical; release r;</pre>
}		}		}	

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

- Thread 1 stays at I_1
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Threa	d 1	Thread	2	Thread	13
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	while <i>m</i> ₁ : <i>m</i> ₂ : <i>m</i> ₃ : <i>m</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r:</pre>	while n ₁ : n ₂ : n ₃ : n ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>
}		}		}	

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

- Thread 1 stays at I_1
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2

	LTL Model Checking	

Thread	d 1	Thread 2	Thread 3	
while <i>l</i> ₁ : <i>l</i> ₂ : <i>l</i> ₃ : <i>l</i> ₄ : }	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) m1: noncr m2: reque m3: criti m4: relea }</pre>	<pre>{ while (true) { ritical; n1: noncritic est r; n2: request r ical; n3: critical; ase r; n4: release r }</pre>	cal; ;; ; ;;
,		,	,	

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Thread	d 1	Thread 2	Thread 3
while <i>l</i> ₁ : <i>l</i> ₂ : <i>l</i> ₃ : <i>l</i> ₄ : }	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) { m1: noncritical, m2: request r; m3: critical; m4: release r; }</pre>	<pre>while (true) { n₁: noncritical; n₂: request r; n₃: critical; n₄: release r; }</pre>
J		J	J

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃

	LTL Model Checking	

Threa	d 1	Thread 2	Thread 3
while l_1 :	<pre>(true) { noncritical;</pre>	while (true) { m_1 : noncritication	<pre>while (true) { al; n₁: noncritical;</pre>
I ₂ : I ₃ : I ₄ :	request r; critical; release r;	<pre>m2: request r m3: critical; m4: release r</pre>	<pre>; n₂: request r; n₃: critical; ; n₄: release r;</pre>
}		}	}

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

- $\bullet \ \ {\rm Thread} \ \ 1 \ {\rm stays} \ {\rm at} \ \ I_1$
- **2** Thread 1 moves to l_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃

	LTL Model Checking	

Threa	d 1	Thread 2	Thread 3
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r:</pre>	<pre>while (true) { m1: noncritical; m2: request r; m3: critical; m.: release r:</pre>	<pre>while (true) { n1: noncritical; n2: request r; n3: critical; n. release r;</pre>
}	1010000 1,	}	}

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃
 - Thread 2 should leave the critical section to m1

	LTL Model Checking	

Thread	11	Thread 2	Thread 3
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) { m1: noncritical; m2: request r; m3: critical; m4: release r; </pre>	<pre>while (true) { n1: noncritical; n2: request r; n3: critical; n4: release r; </pre>
}		}	}

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃
 - Thread 2 should leave the critical section to m1

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Thread	11	Thread 2	Thread 3
while <i>I</i> ₁ : <i>I</i> ₂ : <i>I</i> ₃ : <i>I</i> ₄ :	<pre>(true) { noncritical; request r; critical; release r;</pre>	<pre>while (true) { m1: noncritical; m2: request r; m3: critical; m4: release r; </pre>	<pre>while (true) { n1: noncritical; n2: request r; n3: critical; n4: release r; </pre>
}		}	}

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to I_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃
 - Thread 2 should leave the critical section to m₁
 - Thread 2 should release the resource

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Threa	d 1	Thread 2	Thread 3	
while /1:	<pre>(true) { noncritical:</pre>	<pre>while (true) { m1: noncrit;</pre>	while (true) { ical: n1: noncritic	al:
l_2 :	request r;	m2: request	r; n ₂ : request r	;
I3 : I₄ :	critical; release r;	m3: critical m4: release	l; n ₃ : critical; r; n ₄ : release r	;
}	·	}	}	

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to l_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃
 - Thread 2 should leave the critical section to m₁
 - Thread 2 should release the resource
 - Suppose, it's thread 3
 - ...

Motivation 00	Causality-based Proofs 000	LTL Satisfiability 00	LTL Model Checking	

Threa	d 1	Thread 2	Thread 3	
while /1:	<pre>(true) { noncritical:</pre>	<pre>while (true) { m1: noncrit;</pre>	while (true) { ical: n1: noncritic	al:
l_2 :	request r;	m2: request	r; n ₂ : request r	;
I3 : I₄ :	<pre>critical; release r;</pre>	m3: critical m4: release	l; n ₃ : critical; r; n ₄ : release r	;
}	·	}	}	

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

- $\bullet \ \ \, \text{Thread} \ \, 1 \ \, \text{stays at} \ \, l_1$
- **2** Thread 1 moves to l_2 and stays there
- Someone should request and hold the resource. Who?
 - Suppose, it's thread 2
 - Thread 2 should be at m₃
 - Thread 2 should leave the critical section to m₁
 - Thread 2 should release the resource
 - Suppose, it's thread 3
 - ...

Causality-based Proofs		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 \implies concurrent traces
- Proof rules \implies language-preserving trace transformations
- Proof construction \implies 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 \implies concurrent traces
- Proof rules \implies language-preserving trace transformations
- Proof construction \implies 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 \implies concurrent traces
- Proof rules \implies language-preserving trace transformations
- Proof construction \implies tableau-based trace search

Result

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

Thank you for your attention!