

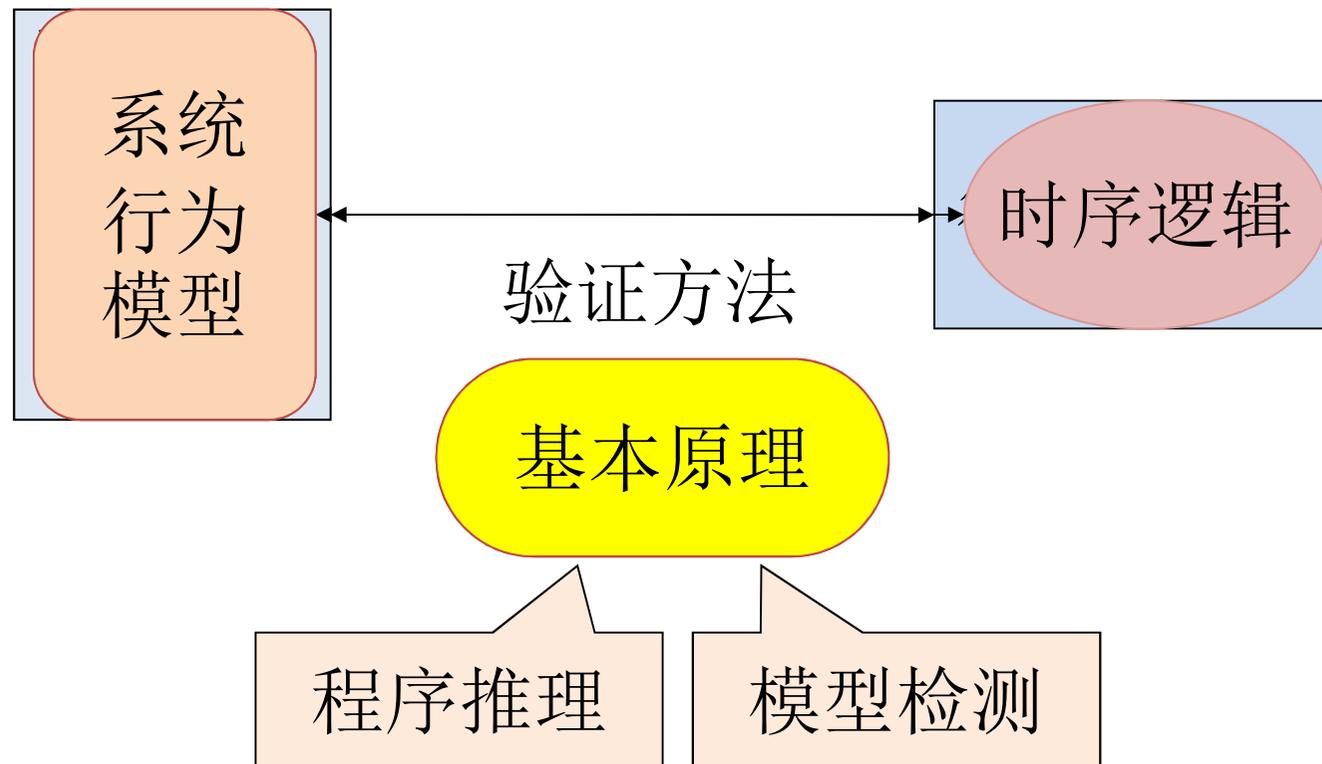
# Linear Temporal Logic (II)

中国科学院软件研究所  
计算机科学国家重点实验室

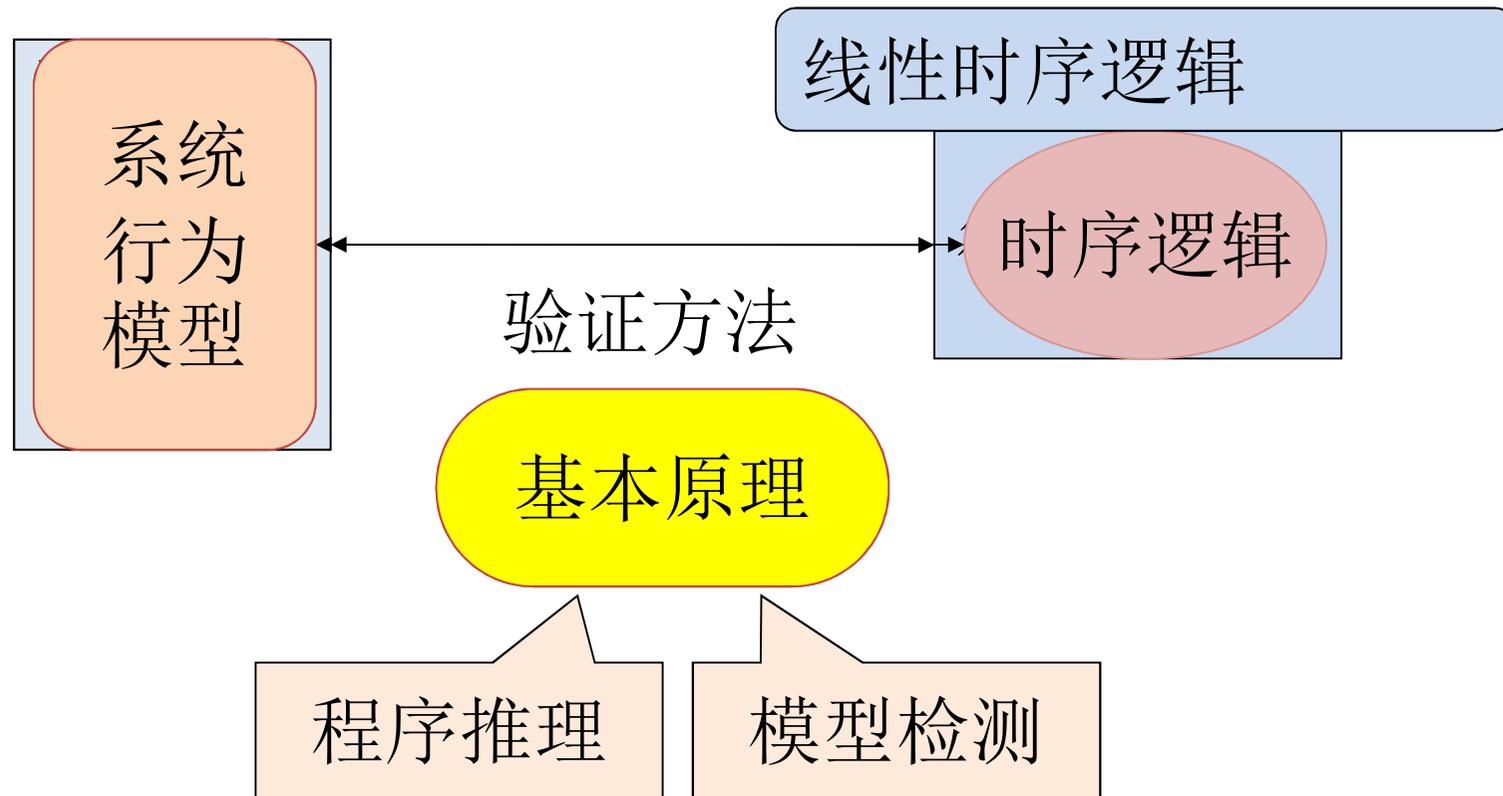
张文辉

<http://lcs.ios.ac.cn/~zwh/>

# 课程内容



# 课程内容



# Contents

- Bounded Semantics of PLTL
- Automata Representation of PLTL Formulas
- First Order LTL

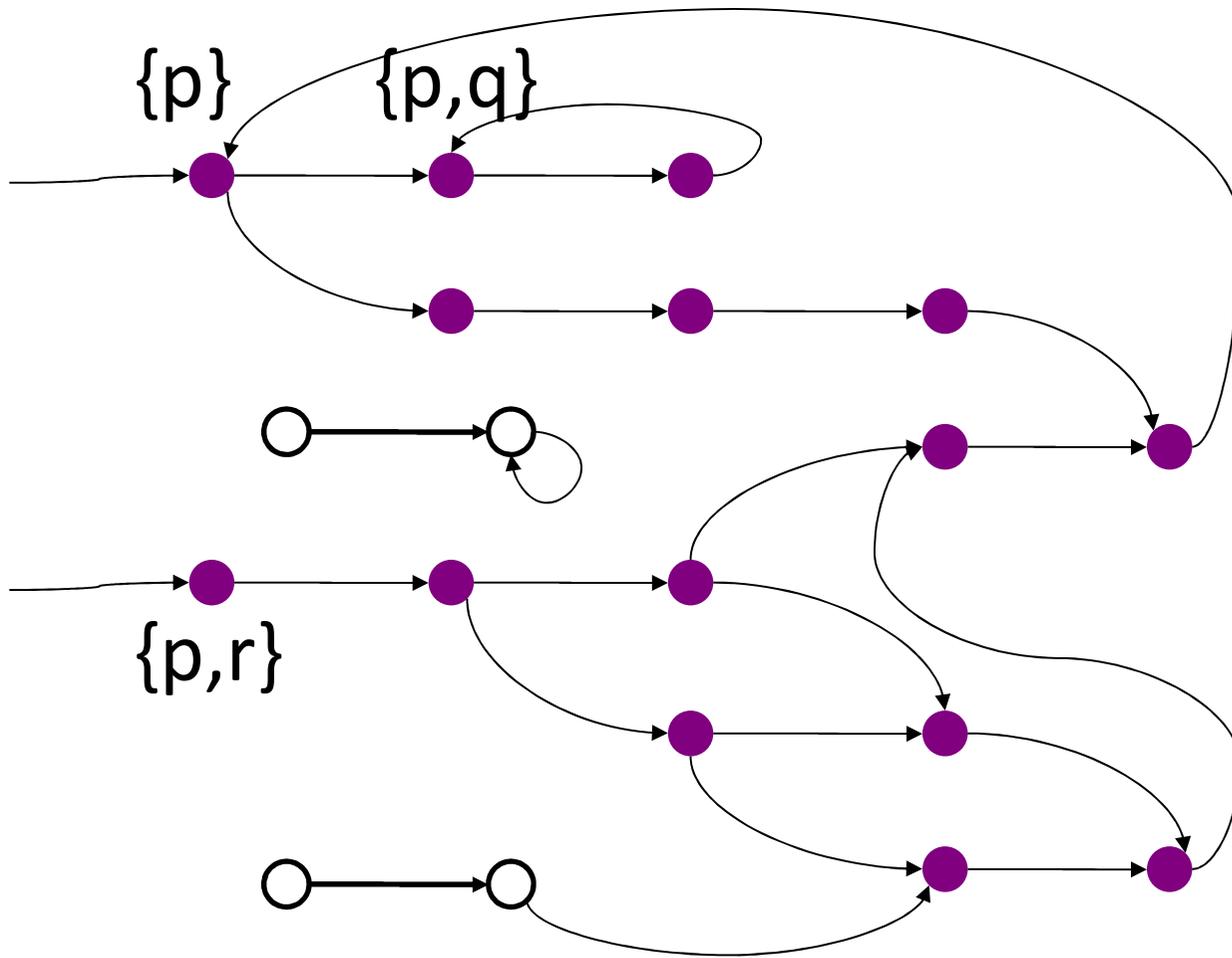
# (I) Bounded Semantics of PLTL

$$M \models \varphi$$

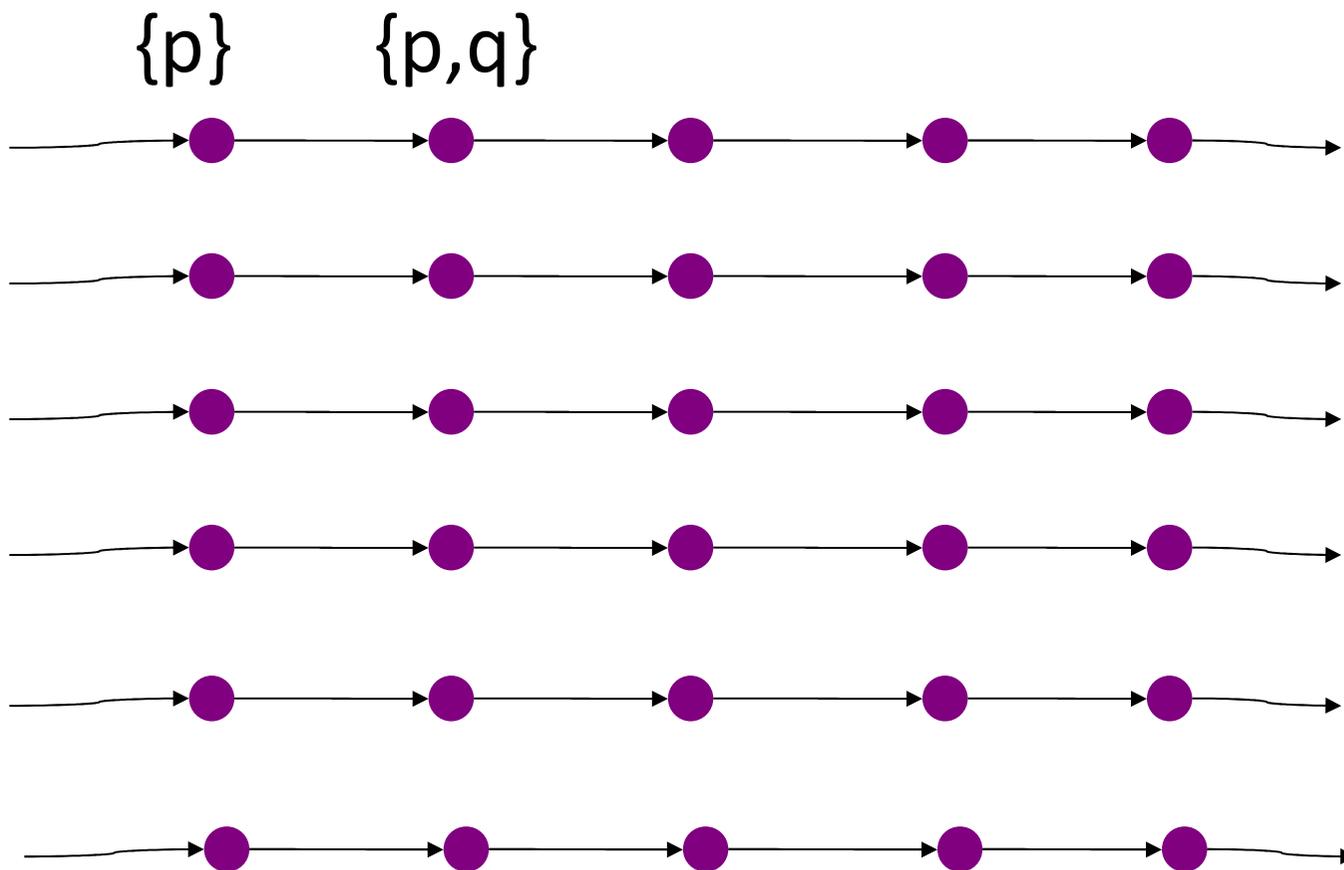
语义上牵涉无穷路径

考虑有穷路径

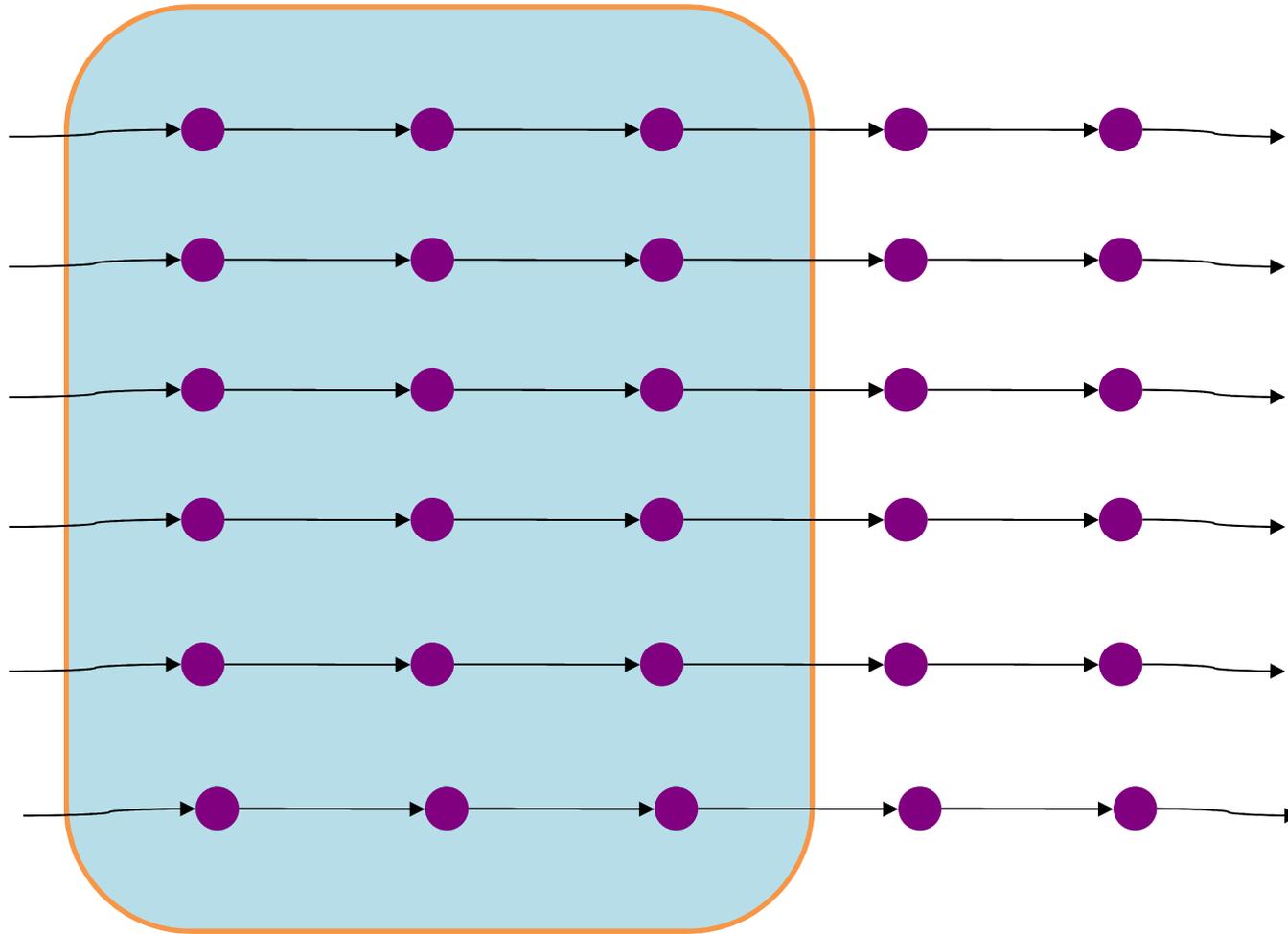
# Kripke 结构



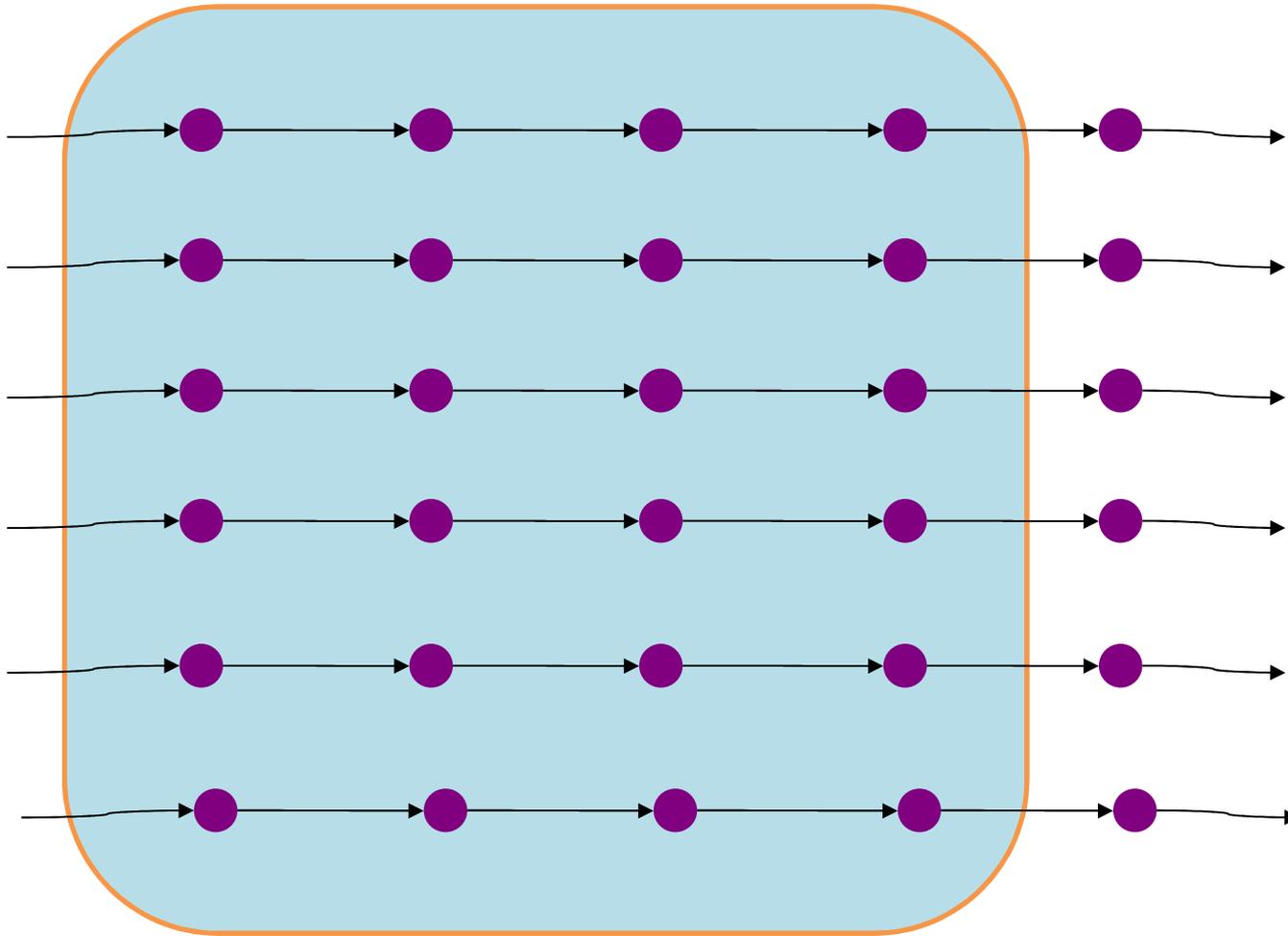
# 无穷路径



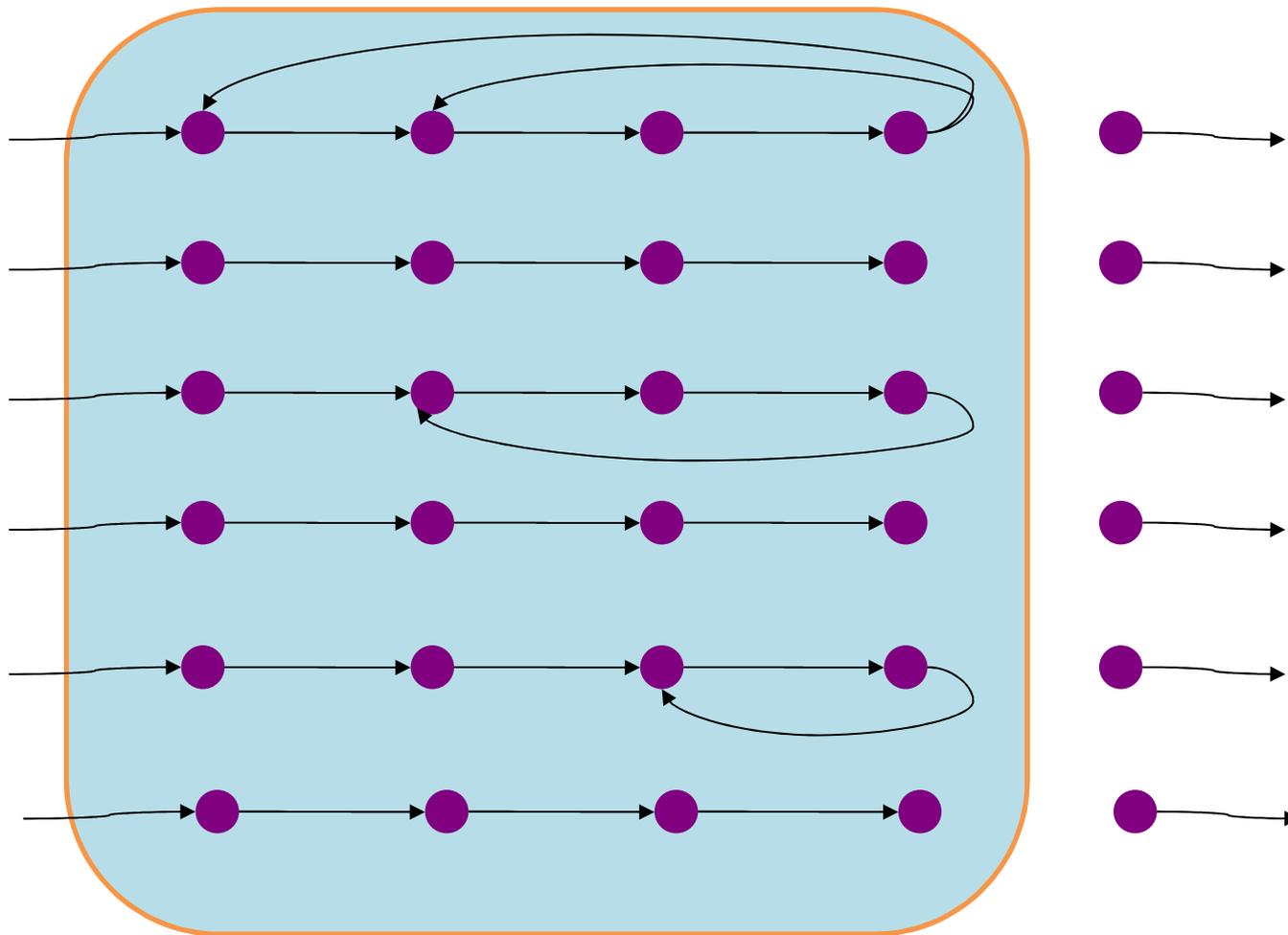
# 有穷路径



# 有穷路径



# 有穷路径



# LTL

k路径 $\pi$  : 长度为k+1的路径。

(k,l)环 $\pi$  : k路径 且  $R(\pi_k, \pi_l)$ 成立。

存在 计算 $\pi$ 使得  $M, \pi \models \phi$

当且仅当存在l起点的 (k,l)环 $\pi'$ 使得

$M, \pi_0' \dots \pi_{l-1}' (\pi_l' \dots \pi_k')^\omega \models \phi$  且  $k \leq |M| \times 2^{|\phi|}$ .

$M \not\models \phi$

当且仅当存在l起点的 (k,l)环 $\pi$ 使得

$M, \pi_0 \dots \pi_{l-1} (\pi_l \dots \pi_k)^\omega \models \neg \phi$

# LTL

考虑NNF-LTL:

$$\Phi ::= p \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg p \mid X \Phi \mid G\Phi \mid \Phi U \Phi$$

# (正常)语义: $M, \pi \models \phi$

$M, \pi \models p,$	if $p \in AP$ and $p \in L(\pi_0)$
$M, \pi \models \neg\phi,$	if $M, \pi \not\models \phi$
$M, \pi \models \phi \vee \psi,$	if $M, \pi \models \phi$ or $M, \pi \models \psi$
$M, \pi \models \phi \wedge \psi,$	if $M, \pi \models \phi$ and $M, \pi \models \psi$
$M, \pi \models X\phi,$	if $M, \pi^1 \models \phi$
$M, \pi \models \phi U \psi,$	if $\exists i \geq 0, M, \pi^i \models \psi$ and $\forall j < i, M, \pi^j \models \phi$
$M, \pi \models G\psi,$	if $\forall i \geq 0, M, \pi^i \models \psi$

# Existential Model Checking Problem

$M \models_E \phi$ , if there a computation  $\pi$  such that  $M, \pi \models \phi$

---

Given  $M$  and  $\phi$ .

$M \models_E \neg\phi$ , iff

$M \not\models \phi$

限界语义:  $M, \pi \models_k \phi$

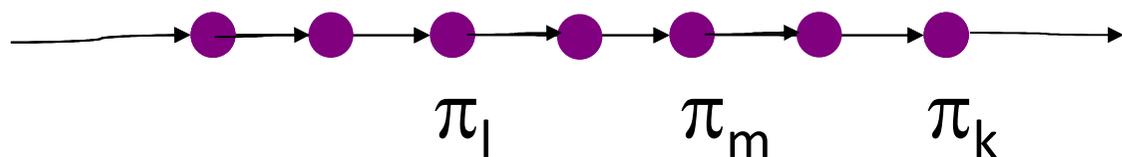
k-path:

$$\pi = \pi_0 \dots \pi_k$$

# 限界语义(non-loop): $M, \pi \models_k \phi$

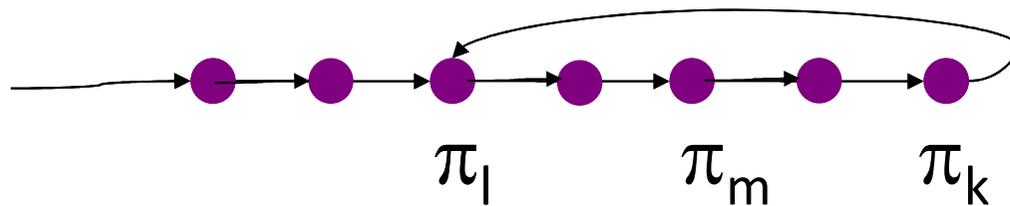
$M, \pi \models_k^m p,$	if $p \in AP$ and $p \in L(\pi_m)$
$M, \pi \models_k^m \neg p,$	if $p \in AP$ and $p \notin L(\pi_m)$
$M, \pi \models_k^m \phi \vee \psi,$	if $M, \pi \models_k^m \phi$ or $M, \pi \models_k^m \psi$
$M, \pi \models_k^m \phi \wedge \psi,$	if $M, \pi \models_k^m \phi$ and $M, \pi \models_k^m \psi$
$M, \pi \models_k^m X \phi,$	if $k \geq m+1$ and $M, \pi \models_k^{m+1} \phi$
$M, \pi \models_k^m \phi U \psi,$	if $\exists m \leq i \leq k, M, \pi \models_k^i \psi$ and $\forall m \leq j < i, M, \pi \models_k^j \phi$
$M, \pi \models_k^m G \psi,$	if false

$M, \pi \models_{k,-1} \phi$  if  $M, \pi \models_k^0 \phi$



限界语义(loop):  $M, \pi \models_k \phi$

(k,l)-loop:  $\pi = \pi_0 \dots \pi_{l-1} (\pi_l \dots \pi_k)^\omega$

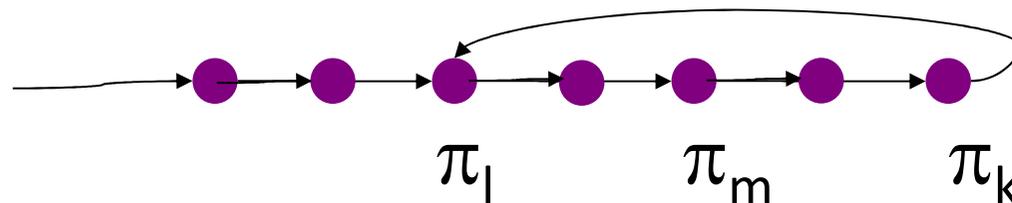


# 限界语义(loop): $M, \pi \models_k \phi$

$M, \pi \models_k^{l,m} p,$	if $p \in AP$ and $p \in L(\pi_m)$
$M, \pi \models_k^{l,m} \neg p,$	if $p \in AP$ and $p \notin L(\pi_m)$
$M, \pi \models_k^{l,m} \phi \vee \psi,$	if $M, \pi \models_k^{l,m} \phi$ or $M, \pi \models_k^{l,m} \psi$
$M, \pi \models_k^{l,m} \phi \wedge \psi,$	if $M, \pi \models_k^{l,m} \phi$ and $M, \pi \models_k^{l,m} \psi$
$M, \pi \models_k^{l,m} X \phi,$	if $k \geq m+1$ and $M, \pi \models_k^{l,m+1} \phi,$ or $k=m$ and $M, \pi \models_k^{l,l} \phi$
$M, \pi \models_k^{l,m} \phi U \psi,$	if $\exists m \leq i \leq k, M, \pi \models_k^{l,i} \psi$ and $\forall m \leq j < i, M, \pi \models_k^{l,j} \phi,$ or $\forall m \leq j \leq k, M, \pi \models_k^{l,j} \phi$ and $\exists l \leq i < m, M, \pi \models_k^{l,i} \psi$ and $\forall l \leq j < i, M, \pi \models_k^{l,j} \phi$
$M, \pi \models_k^{l,m} G \psi,$	if $\forall \min(l,m) \leq i \leq k, M, \pi \models_k^{l,i} \psi$

-----

$M, \pi \models_{k,l} \phi$  if  $M, \pi \models_k^{l,0} \phi$



# 限界语义: $M, \pi \models_k \phi$

## DEFINITION

$M, \pi \models_k \phi$ , if  $M, \pi \models_{k,-1} \phi$  or  $M, \pi \models_{k,l} \phi$  for some  $l \in \{0, \dots, k\}$

## DEFINITION

$M \models_{E,k} \phi$ , if  $M, \pi \models_k \phi$  for some computation  $\pi$ .

## LEMMA (Soundness)

If  $M \models_{E,k} \phi$ , then  $M \models_E \phi$ .

## LEMMA (Completeness)

If  $M \models_E \phi$ , then  $M \models_{E,k} \phi$  for some  $k \geq 0$ .

# 限界语义

## THEOREM

$M \models_E \phi$  iff

there is  $k \geq 0$  such that  $M \models_{E,k} \phi$

## Corollary

$M \not\models \phi$  iff

there is  $k \geq 0$  such that  $M \models_{E,k} \neg\phi$

# 完备阈值

$k$  是  $M \models \varphi$  的完备阈值，当且仅当

若  $M \not\models_{E,k} \neg\varphi$ ，则对  $k' \geq k$ ， $M \not\models_{E,k'} \neg\varphi$

设  $lct$  是  $M \models \varphi$  的最小完备阈值：

若  $b \geq lct$  且  $M \not\models_{E,b} \neg\varphi$ ，则  $M \models \varphi$ 。

(小模型定理)

最小完备阈值

(least completeness threshold  $\leq |M| * 2^{|\varphi|}$ )

# 限界模型检测

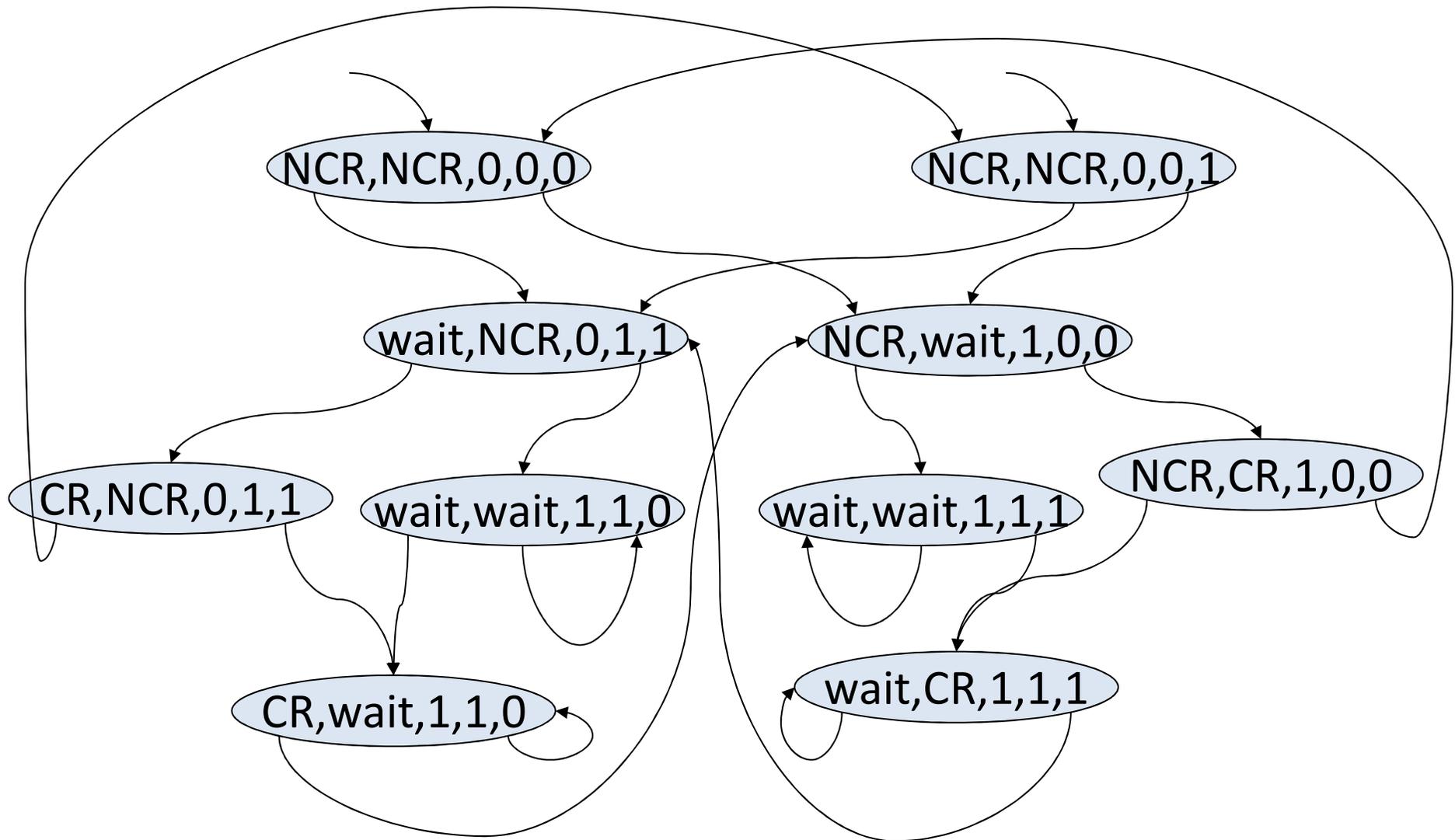
## (Bounded Model Checking)

Let  $b$  be a completeness threshold for  $M \models \varphi$  or infinity.

1.  $k=0$ ;
2. if  $M \models_{E,k} \neg\varphi$ , then report  $M \not\models \varphi$ ;
3. if  $k=b$ , then report  $M \models \varphi$ ;
4.  $k=k+1$ ; goto step 2;



# Example: $F(a=CR \text{ or } b=CR)$ ?



E.g.  $G(a \neq CR \text{ and } b \neq CR)$  ?

# Example: $\phi = F(a=CR \text{ or } b=CR)$

Q:  $M \models F(a=CR \text{ or } b=CR) ?$

Negation:  $M \models_E \neg F(a=CR \text{ or } b=CR) ?$

$M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$  for some  $k$  ?

$M, \pi \models_k G(a \neq CR \text{ and } b \neq CR)$  for some  $k$  and computation  $\pi$

$k=0$ : (NCR,NCR,0,0,0),.....

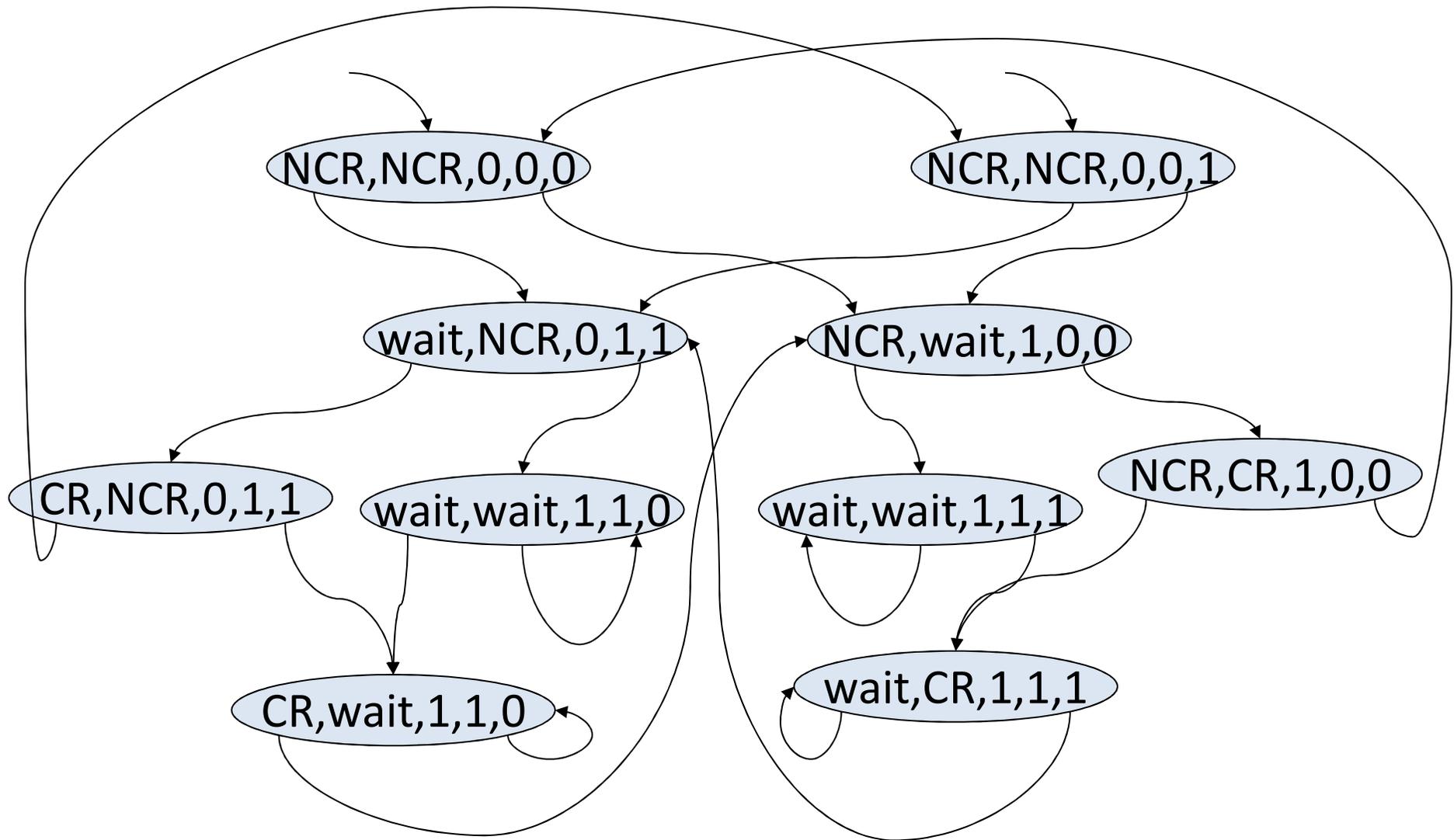
$k=1$ : (NCR,NCR,0,0,0)(wait,NCR,0,1,1),.....

$k=2$ : (NCR,NCR,0,0,0)(wait,NCR,0,1,1)(wait,wait,1,1,0),.....

Since  $M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$  holds for  $k=2$ ,

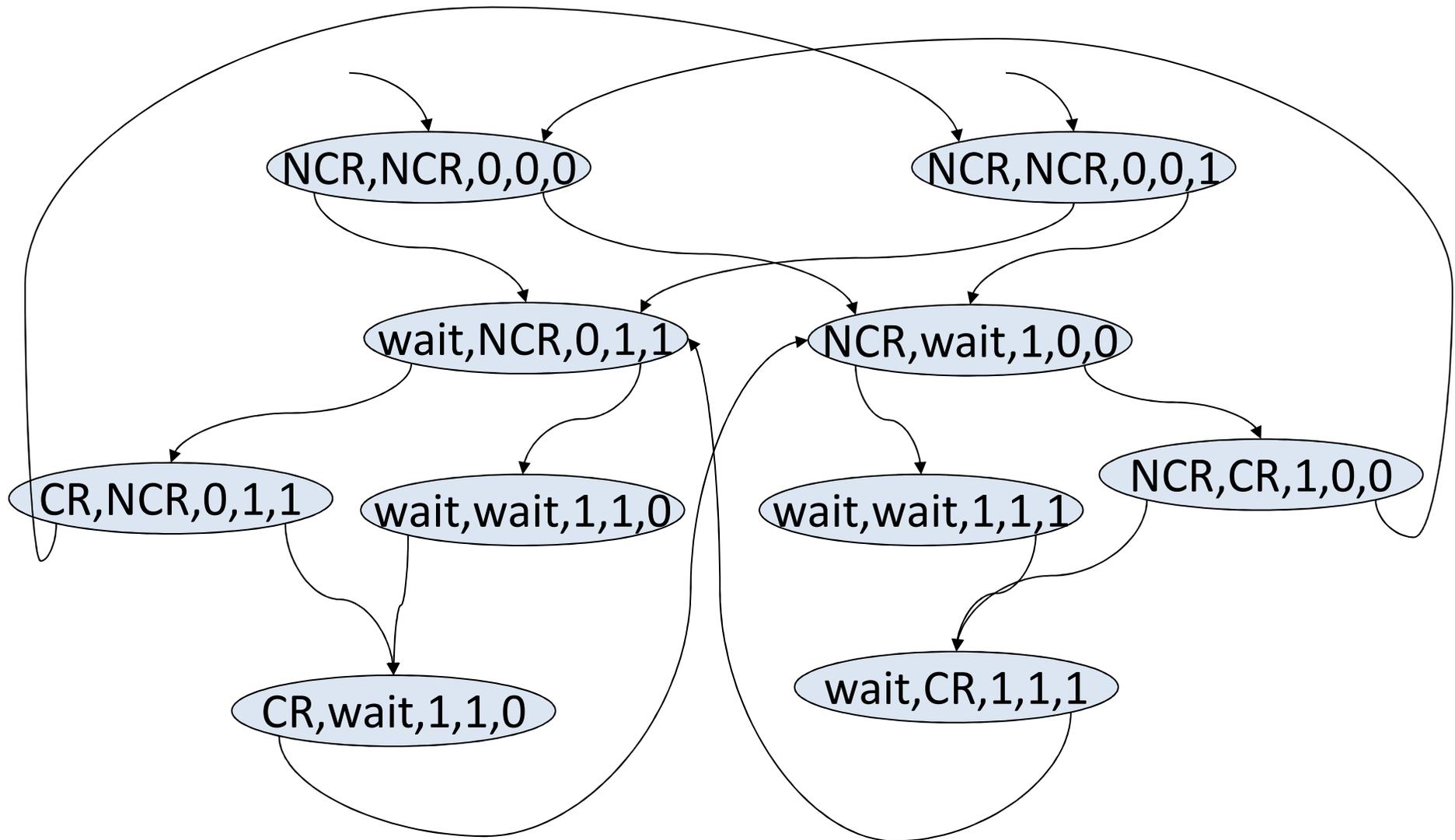
we have that  $M \models F(a=CR \text{ or } b=CR)$  does not hold.

# Example: $F(a=CR \text{ or } b=CR)$ ?



E..  $G(a \neq CR \text{ and } b \neq CR)$  ? ok

# Example: $F(a=CR \text{ or } b=CR)$ ?



E..  $G(a \neq CR \text{ and } b \neq CR)$  ?

# Example: $\phi = F(a=CR \text{ or } b=CR)$

Q:  $M \models F(a=CR \text{ or } b=CR)$  ?

Negation:  $M \models_E \neg F(a=CR \text{ or } b=CR)$  ?

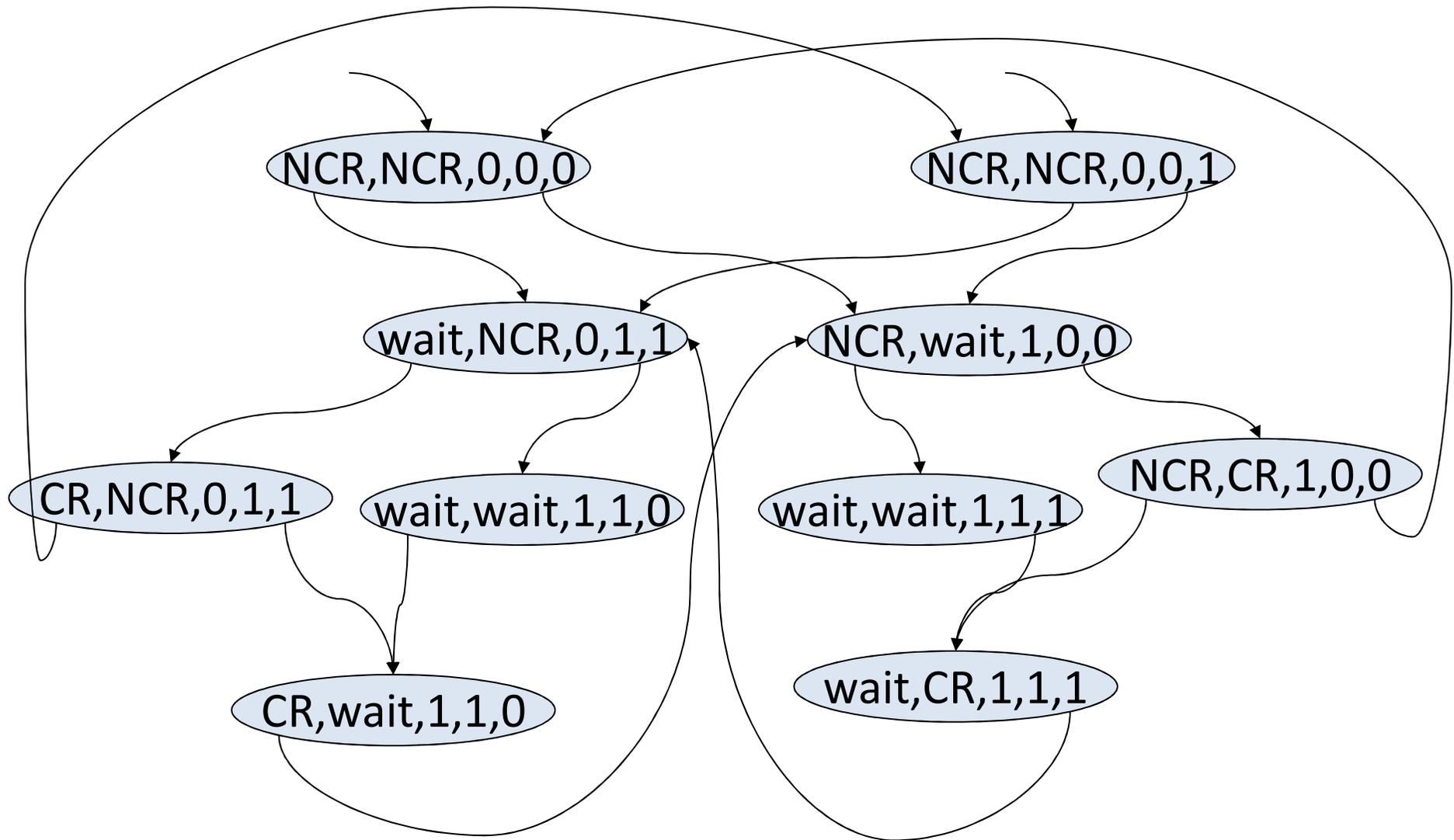
$M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$  for some  $k$  ?

$M, \pi \models_k G(a \neq CR \text{ and } b \neq CR)$  for some  $k$  and computation  $\pi$  ?

Check  $M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$  for  $k = 0, 1, 2, \dots, |M| * 2^{|\phi|}$

Since  $M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$  does not hold for  $k = |M| * 2^{|\phi|}$ ,  
we have  $M \models F(a=CR \text{ or } b=CR)$ .

# Example: $F(a=CR \text{ or } b=CR)$ ?



E..  $G(a \neq CR \text{ and } b \neq CR)$ ?  $lct()$ ?

## (II) Automata Representation of PLTL

# PLTL $\rightarrow$ $\omega$ -Automata

Let AP be given.

Let  $\phi$  over AP be given.

Construct a GBA A such that

$$\langle S, \zeta, L \rangle \models \phi \text{ iff } L(\zeta) \in L(A)$$

$$L(\zeta) \in (2^{AP})^\omega$$

# Example

$G p$

$p \cup q$

$p \cup (q \cup r)$

# Example

$G \ p$

$AP = \{p\}$

$\langle \Sigma, S, \Delta, I, F \rangle$

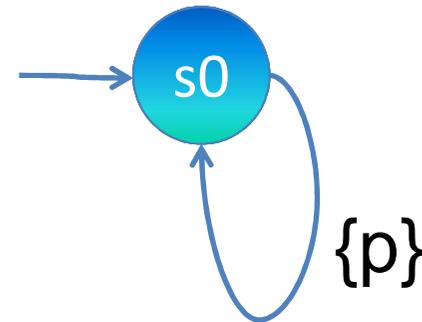
$\Sigma = \{ \{\}, \{p\} \}$

$S = \{s_0\}$

$\Delta = \{ (s_0, \{p\}, s_0) \}$

$I = \{s_0\}$

$F = \{s_0\}$



# Example

$p \cup q$

$AP = \{p, q\}$

$\langle \Sigma, S, \Delta, I, F \rangle$

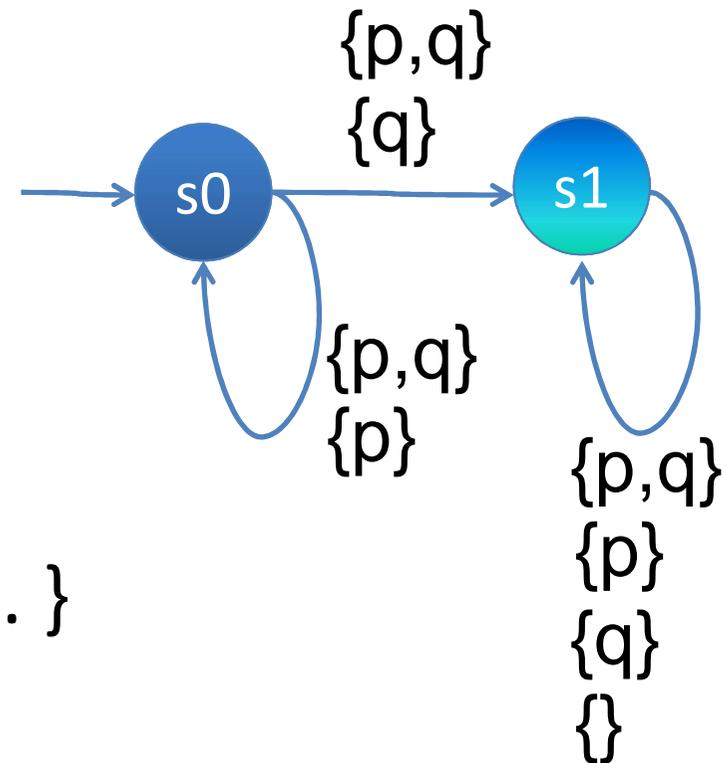
$\Sigma = \{ \{\}, \{p\}, \{q\}, \{p, q\} \}$

$S = \{s_0, s_1\}$

$\Delta = \{ (s_0, \{p\}, s_0), (s_0, \{p, q\}, s_0), \dots \}$

$I = \{s_0\}$

$F = \{s_1\}$



# Example

$p \cup q$

$AP = \{p, q\}$

$\langle \Sigma, S, \Delta, I, F \rangle$

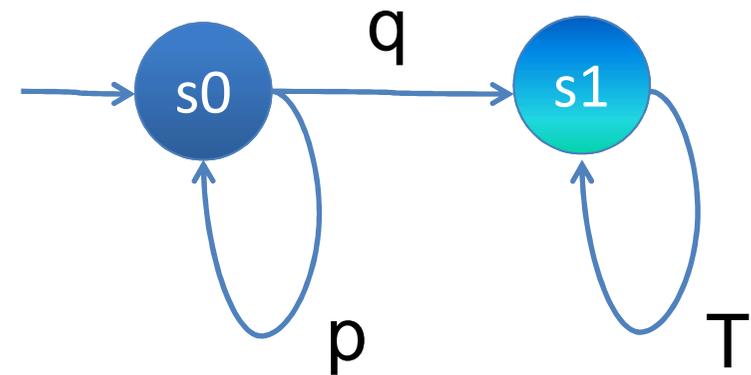
$\Sigma = \{ \{\}, \{p\}, \{q\}, \{p, q\} \}$

$S = \{s_0, s_1\}$

$\Delta = \{ (s_0, \{p\}, s_0), (s_0, \{p, q\}, s_0), \dots \}$

$I = \{s_0\}$

$F = \{s_1\}$



# Example

$p \cup (q \cup r) ?$

$p \cup (q \cup r)$



# PLTL $\rightarrow$ $\omega$ -Automata

Only consider NNF formulas with

literals,

disjunction, conjunction,

X, U, R

$\Phi ::= p \mid \neg p \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid X \Phi \mid \Phi R \Phi \mid \Phi U \Phi$

# PLTL $\rightarrow$ $\omega$ -Automata

Let  $\phi$  be a PLTL formula over AP.

Construct a GBA  $A = \langle S, \Sigma, \Delta, I, F \rangle$  such that  
 $\langle S, \zeta, L \rangle \models \phi$  iff  $L(\zeta) \in L(A)$

$$(1) \Sigma = 2^{AP}$$

$$(2) S, I, \Delta, F = ?$$

# PLTL $\rightarrow$ $\omega$ -Automata

$\varphi \rightarrow$

initial node

$$s = [\varepsilon; \varphi; \emptyset; \emptyset]$$

$s = [a; \emptyset; c; d] \rightarrow$

new node

$$s' = [s; d; \emptyset; \emptyset]$$

Meaning of  $[a; b; c; d]$

# PLTL $\rightarrow$ $\omega$ -Automata

$s=[a; p, \varphi; c; d]$  where  $p$  is a literal

Replace by

$s'=[a; \varphi; p, c; d]$

# PLTL $\rightarrow$ $\omega$ -Automata

$$s = [a; \varphi_0 \vee \varphi_1, \varphi; c; d]$$

Replace by

$$s' = [a; \varphi_0, \varphi; \varphi_0 \vee \varphi_1, c; d]$$

$$s'' = [a; \varphi_1, \varphi; \varphi_0 \vee \varphi_1, c; d]$$

# PLTL $\rightarrow$ $\omega$ -Automata

$s = [a; \varphi_0 \wedge \varphi_1, \varphi; c; d]$

Replace by

$s' = [a; \varphi_0, \varphi_1, \varphi; \varphi_0 \wedge \varphi_1, c; d]$

# PLTL $\rightarrow$ $\omega$ -Automata

$s = [a; X\varphi_1, \varphi; c; d]$

Replace by

$s' = [a; \varphi; X\varphi_1, c; \varphi_1, d]$

# PLTL $\rightarrow$ $\omega$ -Automata

$$s = [a; \varphi_0 \cup \varphi_1, \varphi; c; d]$$

Replace by

$$s' = [a; \varphi_1 \vee (\varphi_0 \wedge X(\varphi_0 \cup \varphi_1)), \varphi; \varphi_0 \cup \varphi_1, c; d]$$

Or equivalently, by,

$$s1 = [a; \varphi_1, \varphi; \varphi_0 \cup \varphi_1, c; d]$$

$$s2 = [a; \varphi_0, \varphi; \varphi_0 \cup \varphi_1, c; d, (\varphi_0 \cup \varphi_1)]$$

# PLTL $\rightarrow$ $\omega$ -Automata

$$s = [a; \varphi_0 R \varphi_1, \varphi; c; d]$$

Replace by

$$s' = [a; \varphi_1 \wedge (\varphi_0 \vee X(\varphi_0 R \varphi_1)), \varphi; \varphi_0 R \varphi_1, c; d]$$

Or equivalently, by,

$$s1 = [a; \varphi_1, \varphi_0, \varphi; \varphi_0 R \varphi_1, c; d]$$

$$s2 = [a; \varphi_1, \varphi; \varphi_0 R \varphi_1, c; d, (\varphi_0 R \varphi_1)]$$

# PLTL $\rightarrow$ $\omega$ -Automata

$s=[a; \emptyset; c; d]$

$s'=[a'; \emptyset; c; d]$

Replace by

$s''=[a, a'; \emptyset; c; d]$

# PLTL $\rightarrow$ $\omega$ -Automata

$s=[a; \emptyset; c; d]$

$s'=[a'; \emptyset; c; d]$

Replace by

$s''=[a, a'; \emptyset; c; d]$

$s=[a; b; c; d]$

$s'=[a'; b; c; d]$

Replace by

$s''=[a, a'; b; c; d]$

Generally,

merge equivalent nodes

# PLTL $\rightarrow$ $\omega$ -Automata

$s = [a; \emptyset; c; d]$

$s \in I$  iff  $\varepsilon \in a$

# PLTL $\rightarrow$ $\omega$ -Automata

$$\Sigma = 2^{AP}$$

$$s = [a; \emptyset; c; d]$$

$$s' = [a'; \emptyset; c'; d']$$

Define  $\Delta$  as follow:

$$(s, \sigma, s') \in \Delta \text{ iff } s \in a' \text{ and } \sigma \models s$$

# PLTL $\rightarrow$ $\omega$ -Automata

Let  $f(\varphi_0 \cup \varphi_1) = \{ s \mid \varphi_0 \cup \varphi_1 \in s.c \rightarrow \varphi_1 \in s.c \}$

$F = \{ f(\varphi_0 \cup \varphi_1) \mid \varphi_0 \cup \varphi_1 \text{ is a sub-formula of } \varphi \}$

# PLTL $\rightarrow$ $\omega$ -Automata

## Theorem

Let  $A = \langle \Sigma, S, \Delta, I, F \rangle$  be a GBA as constructed.

Then  $\langle S, \zeta, L \rangle \models \phi$  iff  $L(\zeta) \in L(A)$ .

# Example

$G p$

$p \cup q$

$p \cup (q \cup r)$

# 1

New

1	$\varepsilon$	$pU(qUr)$		
---	---------------	-----------	--	--

Replaced by

11	$\varepsilon$	$qUr$	$pU(qUr)$	
12	$\varepsilon$	$p$	$pU(qUr)$	$pU(qUr)$

Replaced by

111	$\varepsilon$	$r$	$pU(qUr),qUr$	
112	$\varepsilon$	$q$	$pU(qUr),qUr$	$qUr$
12'	$\varepsilon$		$pU(qUr),p$	$pU(qUr)$

# 1

Replaced by

111'	$\varepsilon$		$pU(qUr),qUr,r$	
112'	$\varepsilon$		$pU(qUr),qUr,q$	$qUr$
12'	$\varepsilon$		$pU(qUr),p$	$pU(qUr)$

# 2, 3, 4

New

2	111			
3	112	qUr		
4	12	pU(qUr)		

Replaced by

2	111			
31	112	r	qUr	
32	112	q	qUr	qUr
4=1	12	pU(qUr)		

# 2, 3

Remain

2	111			
31	112	r	qUr	
32	112	q	qUr	qUr

Replaced by

2	111			
31'	112		qUr,r	
32'	112		qUr,q	qUr

# 5, 6, 7

New

5=2	2			
6=2	31			
7=3	32	qUr		

# Summary: 1

111	$\varepsilon$		$pU(qUr),qUr,r$	
112	$\varepsilon$		$pU(qUr),qUr,q$	$qUr$
12	$\varepsilon$		$pU(qUr),p$	$pU(qUr)$

# Summary: 1, 4

111	$\varepsilon, 12$		$pU(qUr), qUr, r$	
112	$\varepsilon, 12$		$pU(qUr), qUr, q$	$qUr$
12	$\varepsilon, 12$		$pU(qUr), p$	$pU(qUr)$

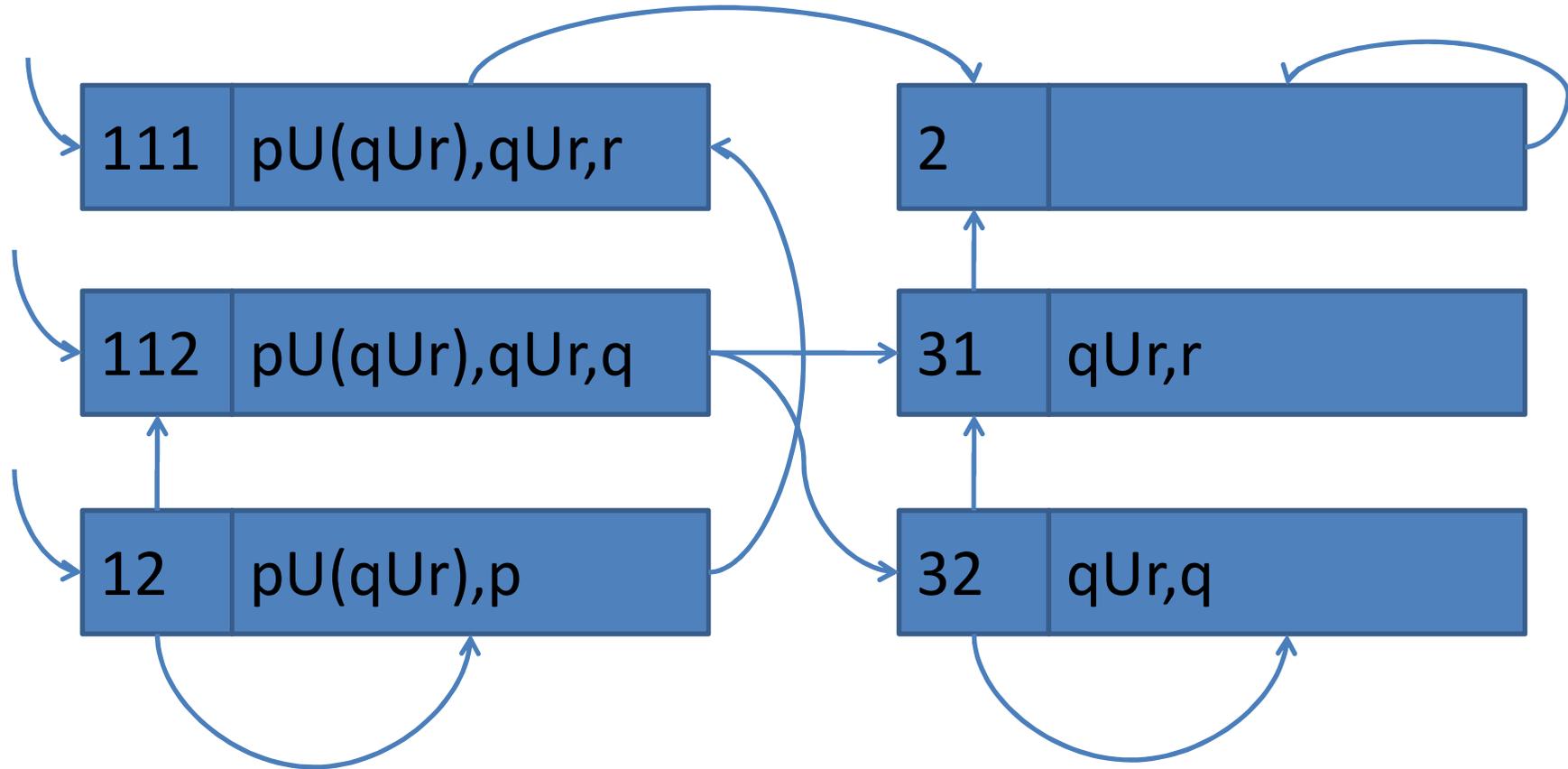
# Summary: 1, 2, 3, 4

111	$\varepsilon, 12$		$pU(qUr), qUr, r$	
112	$\varepsilon, 12$		$pU(qUr), qUr, q$	$qUr$
12	$\varepsilon, 12$		$pU(qUr), p$	$pU(qUr)$
2	111			
31	112		$qUr, r$	
32	112		$qUr, q$	$qUr$

# Summary: 1, 2, 3, 4, 5, 6, 7

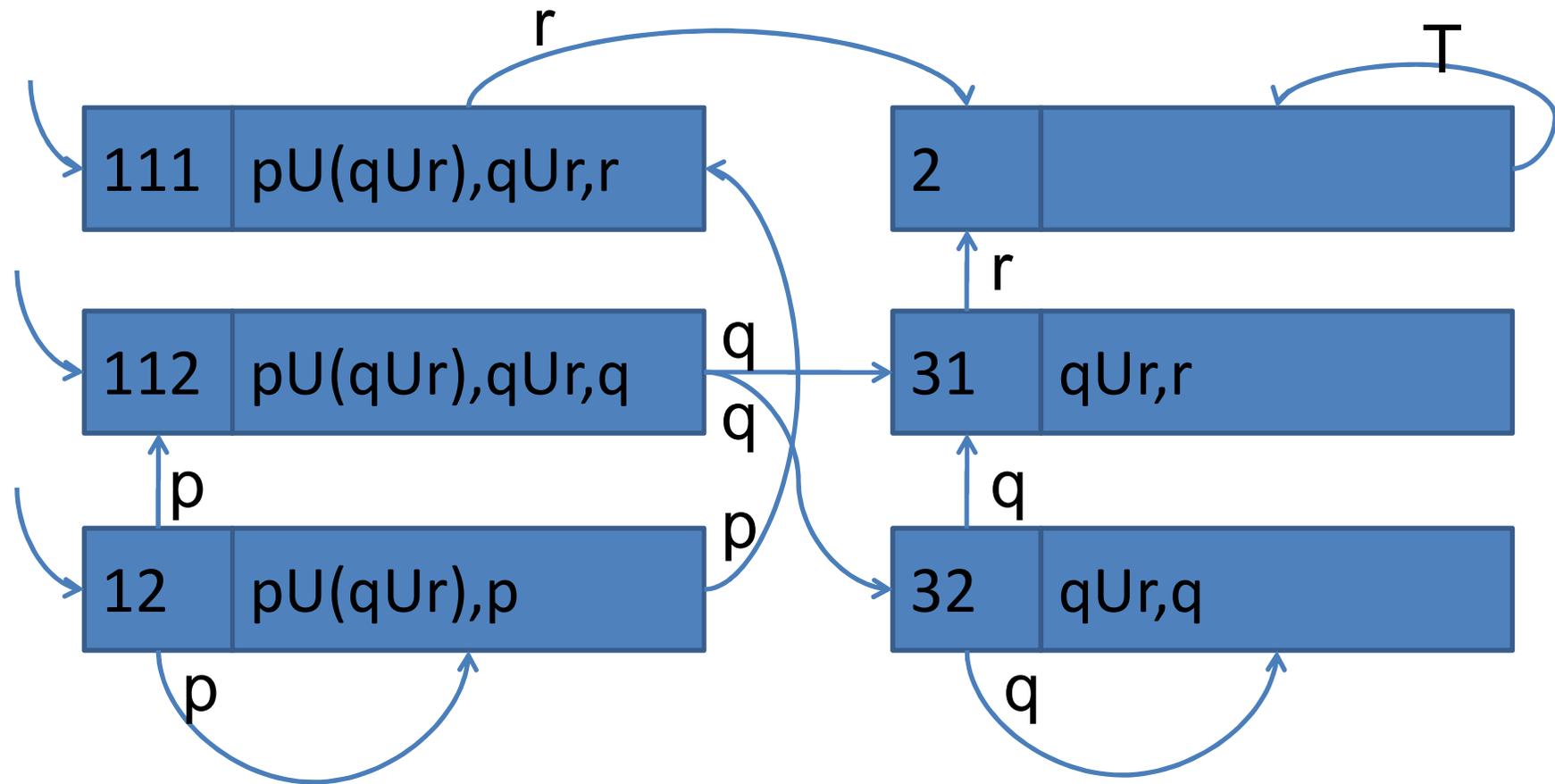
111	$\varepsilon, 12$		$pU(qUr), qUr, r$	
112	$\varepsilon, 12$		$pU(qUr), qUr, q$	$qUr$
12	$\varepsilon, 12$		$pU(qUr), p$	$pU(qUr)$
2	111, 2, 31			
31	112, 32		$qUr, r$	
32	112, 32		$qUr, q$	$qUr$

# 自动机



$$F = \{ \{111, 112, 2, 31, 32\}, \{12, 111, 31, 2\} \}$$

# 自动机



$$F = \{ \{111, 112, 2, 31, 32\}, \{12, 111, 31, 2\} \}$$

# 自动机

p: {q,p,r}, {q,p}, {p,r}, {p}

q: {q,p,r}, {q,p}, {q,r}, {q}

r: {q,p,r}, {r,p}, {q,r}, {r}

T: {q,p,r}, {q,p}, {p,r}, {p}, {q,r}, {q}, {r}, {}

$A=(\Sigma, S, \Delta, I, F)$

# 自动机

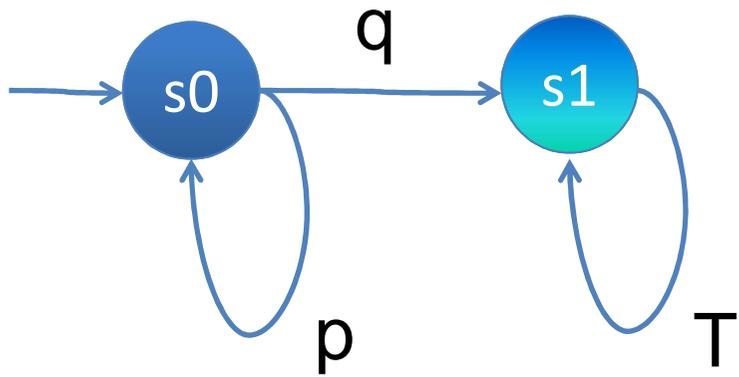
Let  $\varphi = pU(qUr)$ .

Let  $A = (\Sigma, S, \Delta, I, F)$  where

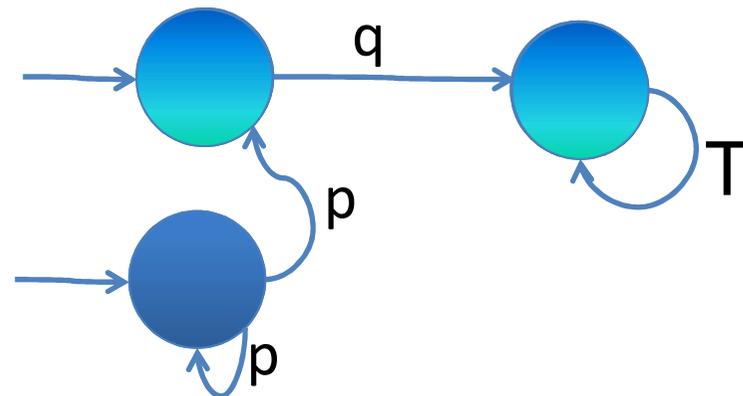
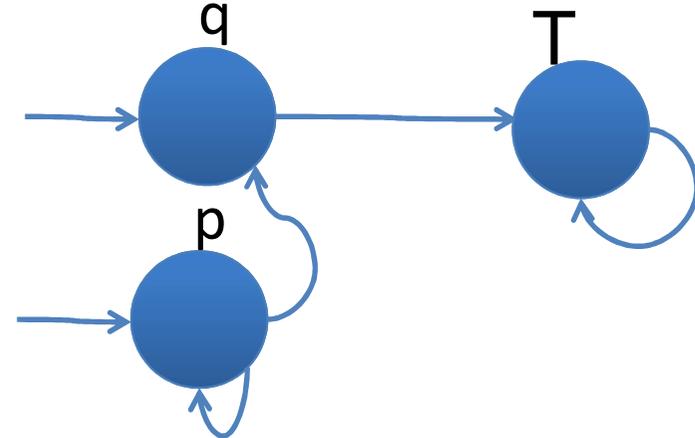
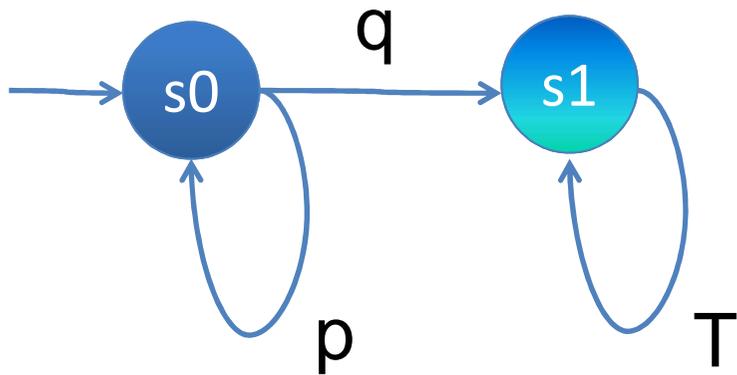
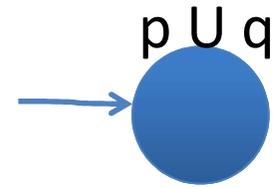
- $\Sigma = 2^{\{p,q,r\}}$
- $S = \{ 111, 112, 12, 2, 31, 32 \}$
- $\Delta = \{$ 
  - $(111, \{r\}, 2), (111, \{p, r\}, 2),$
  - $(111, \{q, r\}, 2), (111, \{p, q, r\}, 2), \dots$ $\}$
- $I = \{ 111, 112, 12 \}$
- $F = \{ \{111, 112, 2, 31, 32\}, \{12, 111, 31, 2\} \}$

Then  $\langle S, \zeta, L \rangle \models \varphi$  iff  $L(\zeta) \in L(A)$

# Example $(p \cup q)$



# Example (p U q)



# Automata-based Model Checking

$$M \models \varphi$$

$$L(A_M) \subseteq [[\varphi]]$$

$$L(A_M) \subseteq L(A_\varphi)$$

$$L(A_M) \cap L(\neg A_\varphi) = \emptyset$$

$$L(A_M \cap \neg A_\varphi) = \emptyset$$

$$L(A_M \cap A_{\neg\varphi}) = \emptyset$$

# (III) First Order Linear Temporal Logic

# Syntax of FOLTL

Let  $B=(F,P)$  be a base for a first order logic.

Let WFF be the set of well-formed formulas.

Definition

Let  $p$  range over formulas over WFF.

The set  $\Phi$  of FOLTL formulas is defined as follows.

$$\Phi ::= p \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg \Phi \mid \\ X \Phi \mid G \Phi \mid F \Phi \mid \Phi R \Phi \mid \Phi U \Phi$$

# Semantics

# Semantics

Let  $B=(F,P)$  be a base for a first order logic.

Let the interpretation  $I=(D,I_0)$  of  $B=(F,P)$  be given.

Let  $\Sigma$  be the set of assignments.

$$\sigma: X \rightarrow D$$

$\zeta \in \Sigma^\omega$  : A sequence of states

$\zeta$  is called a model.

# Semantics: $\zeta \models \phi$

$\zeta \models \phi$  is defined as follows:

$\zeta \models p$ ,                   if  $p \in \text{WFF}$  and  $\zeta_0 \models_1 p$

$\zeta \models \neg\phi$ ,                if  $\zeta \not\models \phi$

$\zeta \models \phi \vee \psi$ ,           if  $\zeta \models \phi$  or  $\zeta \models \psi$

$\zeta \models \phi \wedge \psi$ ,           if  $\zeta \models \phi$  and  $\zeta \models \psi$

$\zeta \models X\phi$ ,                if  $\zeta^1 \models \phi$

$\zeta \models F\phi$ ,                if  $\exists i \geq 0, \zeta^i \models \phi$

$\zeta \models G\phi$ ,                if  $\forall i \geq 0, \zeta^i \models \phi$

$\zeta \models \phi U \psi$ ,            if  $\exists i \geq 0, \zeta^i \models \psi$  and  $\forall 0 \leq j < i, \zeta^j \models \phi$

$\zeta \models \phi R \psi$ ,            if  $\forall i \geq 0, (\forall 0 \leq j < i, \zeta^j \not\models \phi) \rightarrow \zeta^i \models \psi$

# Satisfiability

# Satisfiability and Validity

## Definition

A formula  $\phi$  is satisfiable, if there is a model  $\zeta$  such that  $\zeta \models \phi$ .

## Definition

A formula  $\phi$  is valid, if for every model  $\zeta$ ,  $\zeta \models \phi$  holds.

# Equivalences

# Equivalences

## Definition

A formula  $\phi$  is equivalent to a formula  $\psi$ , if for all models  $\zeta$ , ( $\zeta \models \phi$  iff  $\zeta \models \psi$ ).

# FOLTL Proof Rules

# Proof Rules (for G/R)

$$\frac{\vdash \varphi}{\vdash G\varphi}$$

# Proof Rules (for G/R)

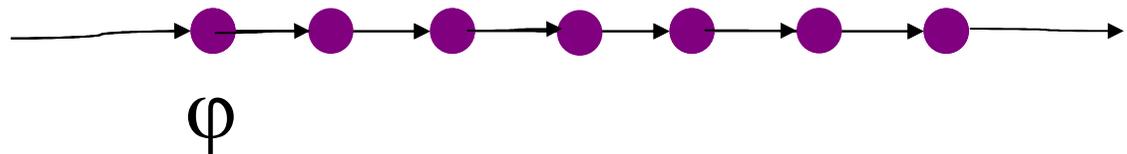
$\varphi \Rightarrow \psi$  denotes  $G(\varphi \rightarrow \psi)$

$$\varphi \Rightarrow \varphi$$

$$\varphi \wedge \neg \psi \Rightarrow X \varphi$$

-----

$$\varphi \Rightarrow (\psi R \varphi)$$



# Proof Rules (for G/R)

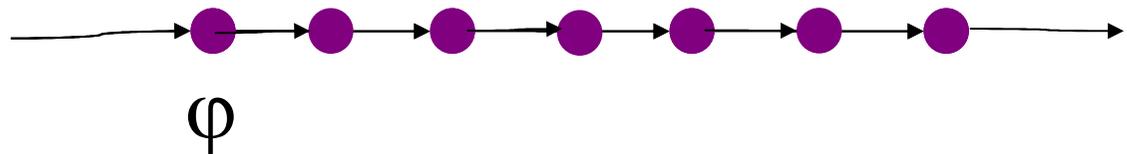
$\varphi \Rightarrow \psi$  denotes  $G(\varphi \rightarrow \psi)$

$$\varphi \Rightarrow \varphi$$

$$\varphi \Rightarrow X \varphi$$

-----

$$\varphi \Rightarrow G \varphi$$



# Proof Rules (for G/R)

$\varphi \Rightarrow \psi$  denotes  $G(\varphi \rightarrow \psi)$

$$\varphi \Rightarrow \phi'$$

$$\phi' \wedge \neg \psi \Rightarrow X \phi'$$

$$\phi' \Rightarrow \phi$$

-----

$$\varphi \Rightarrow (\psi R \phi)$$

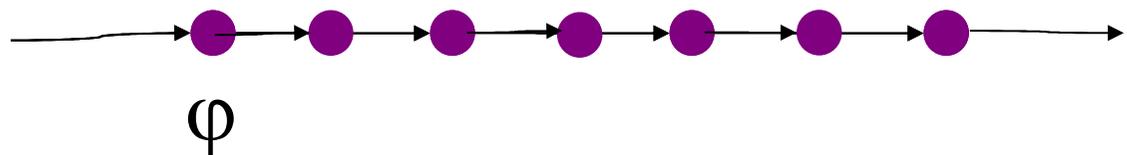
$$\varphi \Rightarrow \phi'$$

$$\phi' \Rightarrow X \phi'$$

$$\phi' \Rightarrow \phi$$

-----

$$\varphi \Rightarrow G \phi$$



# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a - 2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models G(\text{even}(a))$

# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a-2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models G(\text{even}(a))$

$\varphi \Rightarrow \phi'$

$\phi' \Rightarrow X \phi'$

$\phi' \Rightarrow \phi$

-----

$\varphi \Rightarrow G \phi$

$\varphi = \Theta$

$\phi = \text{even}(a)$

$\phi' ?$

$\Theta \Rightarrow G(\text{even}(a))$

# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a-2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models G(\text{even}(a))$

$\varphi \Rightarrow \phi'$

$\phi' \Rightarrow \neg \phi'$

$\phi' \Rightarrow \phi$

-----

$\varphi \Rightarrow G\phi$

$\varphi = \Theta$

$\phi = \text{even}(a)$

$\phi' = \phi$

$\Theta \Rightarrow G(\text{even}(a))$

# Proof Rules (for F/U)

$$\varphi \Rightarrow \psi$$

-----

$$\varphi \Rightarrow (\varphi \cup \psi)$$

$$\varphi \Rightarrow X\psi$$

-----

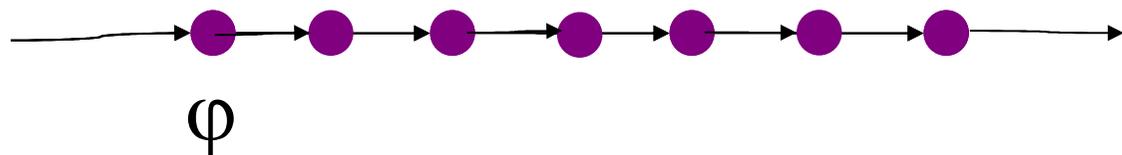
$$\varphi \Rightarrow (\varphi \cup \psi)$$

$$\varphi \Rightarrow \varphi_0$$

$$\varphi \Rightarrow X\psi$$

-----

$$\varphi \Rightarrow (\varphi_0 \cup \psi)$$



# Proof Rules (for F/U)

关于集合的基本概念:

偏序(partial order, 自反、传递、非对称)

完全偏序(complete partial order, 链有上界)

完全偏序(带最小元)

完全格

线性序(linear order, total order)

良基序(well-founded order)

良序 (well-order)

# Proof Rules (for F/U)

良基序(well-founded order):

$(W, \leq)$

严格下降链  $w_0 > w_1 > w_2 > \dots$

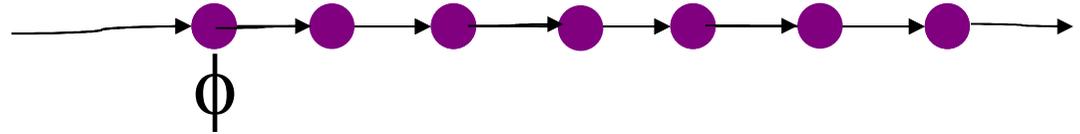
定义:

若 $W$ 的任意子集都有极小元, 则称 $W$ 为良基集合

定理:

$W$ 是良基集合 当且仅当  $W$ 没有无穷严格下降链

# Proof Rules (for F/U)



$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow \phi_0 U (\psi \vee (\phi \wedge t < v))$$

-----

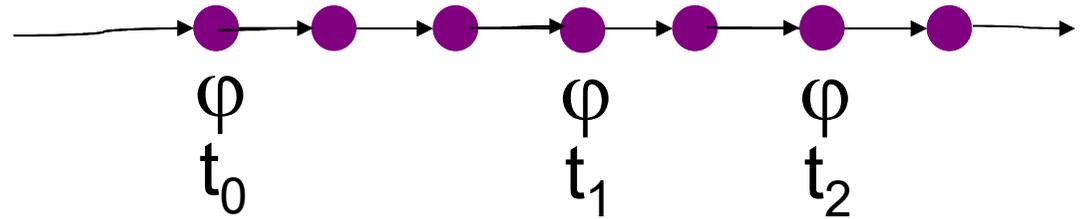
$$\phi \Rightarrow (\phi_0 U \psi)$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)



$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow \phi_0 \mathbf{U}(\psi \vee (\phi \wedge t < v))$$

-----

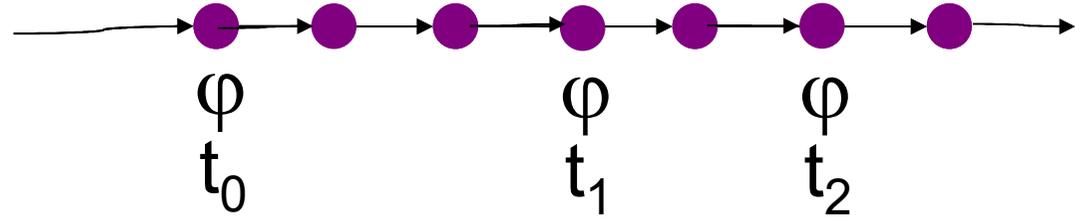
$$\phi \Rightarrow (\phi_0 \mathbf{U} \psi)$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)



$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow \phi_0 U (\psi \vee (\phi \wedge t < v))$$

-----

$$\phi \Rightarrow (\phi_0 U \psi)$$

$$I(w(t/x))(\sigma) = \text{true}$$

$$\rightarrow I(w)(\sigma[x/I(t)\sigma]) = \text{true}$$

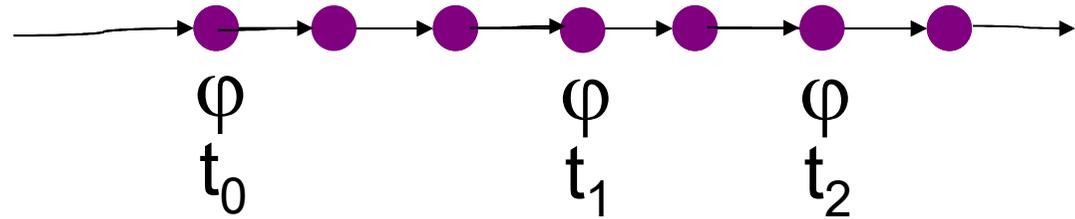
$$\rightarrow I(t)(\sigma) \in W$$

$v$  为变量,  $t$  为项,  $\leq$  为二元谓词符号;

$w$  为一元谓词公式, 其变量为  $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)



$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow \phi_0 \mathbf{U} (\psi \vee (\phi \wedge t < v))$$

-----

$$\phi \Rightarrow (\phi_0 \mathbf{U} \psi)$$

$$\phi \Rightarrow \phi_0$$

$$\phi \Rightarrow \mathbf{X} \psi$$

-----

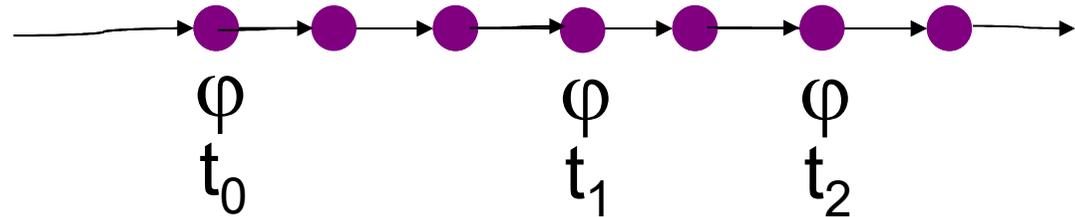
$$\phi \Rightarrow (\phi_0 \mathbf{U} \psi)$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)



$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow \phi_0 \wedge w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow X(\psi \vee (\phi \wedge t < v))$$

-----

$$\phi \Rightarrow (\phi_0 \cup \psi)$$

$$\phi \Rightarrow \phi_0$$

$$\phi \Rightarrow X\psi$$

-----

$$\phi \Rightarrow (\phi_0 \cup \psi)$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)

$$\frac{\varphi \Rightarrow \psi}{\varphi \Rightarrow \mathbf{F}\psi}$$

$$\frac{\varphi \Rightarrow \mathbf{X}\psi}{\varphi \Rightarrow \mathbf{F}\psi}$$

# Proof Rules (for F/U)

$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow F(\psi \vee (\phi \wedge t \leq v))$$

-----

$$\phi \Rightarrow F\psi$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Proof Rules (for F/U)

$$\phi \Rightarrow (\psi \vee \phi)$$

$$\phi \Rightarrow w(t/x)$$

$$(\phi \wedge t=v) \Rightarrow X(\psi \vee (\phi \wedge t \leq v))$$

-----

$$\phi \Rightarrow F\psi$$

$v$ 为变量,  $t$ 为项,  $\leq$  为二元谓词符号;

$w$ 为一元谓词公式, 其变量为 $x$ ;

$W = (\{\sigma(x) \mid I(w)(\sigma) = \text{true}\}, I_0(\leq))$  为良基集合

# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a - 2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models F(a \leq 2)$

# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a-2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models F(a \leq 2)$

$\phi \Rightarrow (\psi \vee \varphi)$

$\varphi \Rightarrow w(t/x)$

$(\varphi \wedge t = v) \Rightarrow X(\psi \vee (\varphi \wedge t < v))$

-----

$\phi \Rightarrow F\psi$

$\phi = \Theta, \psi = (a \leq 2)$

$\varphi? \quad t? \quad w? \quad W?$

$\Theta \Rightarrow F(a \leq 2)$

# Example

$M = \langle T, \Theta \rangle$

$T: \quad \{ a > 2 \rightarrow (a) := (a-2),$   
 $\quad \quad a \leq 2 \rightarrow (a) := (a)$   
 $\quad \quad \}$

$\Theta: \quad (a = 100 \vee a = 200)$

$I: \quad (\text{Int}, I_0)$

$M \models F(a \leq 2)$

$\phi \Rightarrow (\psi \vee \varphi)$

$\varphi \Rightarrow w(t/x)$

$(\varphi \wedge t = v) \Rightarrow X(\psi \vee (\varphi \wedge t < v))$

-----

$\phi \Rightarrow F\psi$

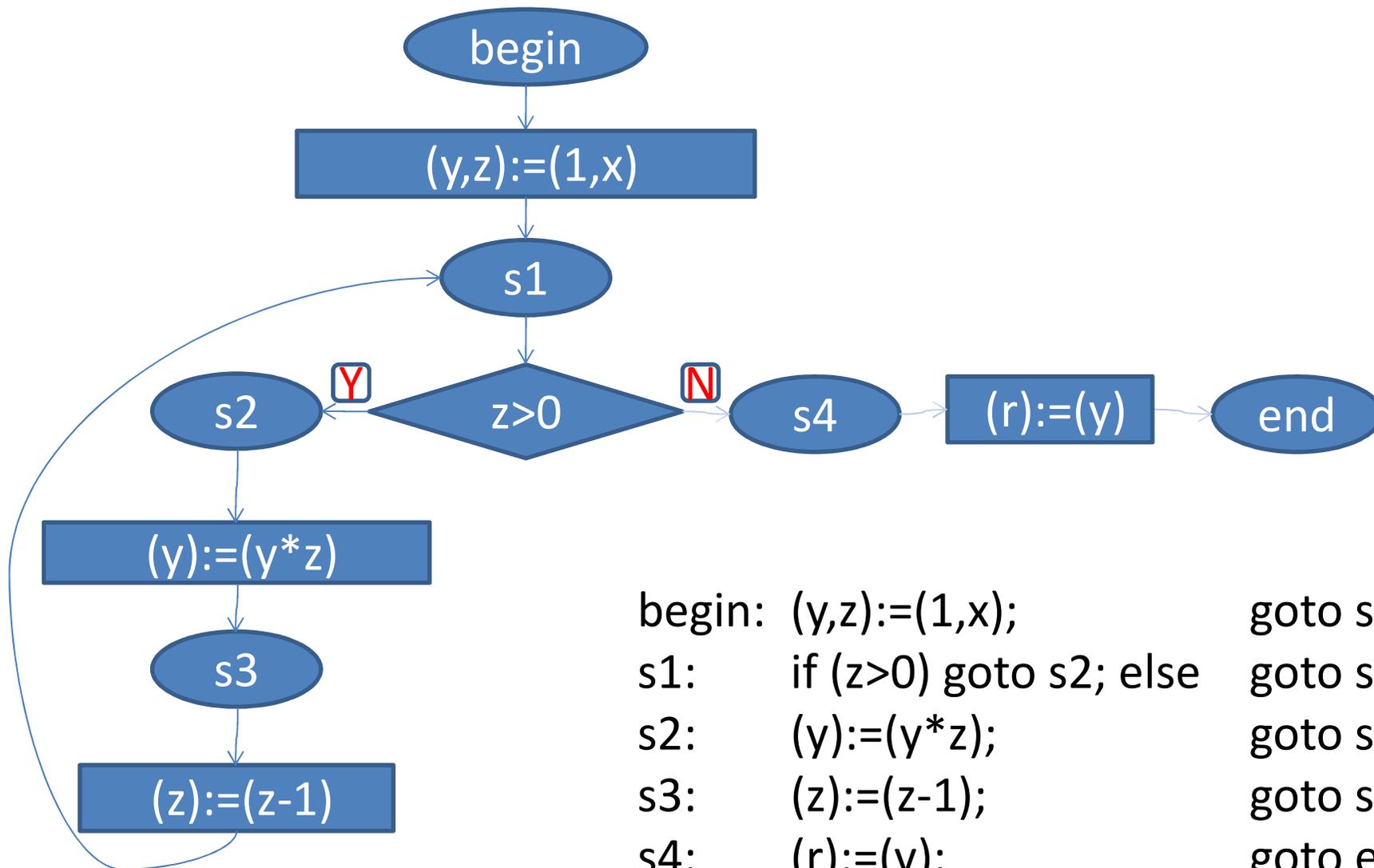
$\phi = \Theta, \psi = (a \leq 2)$

$\varphi = (a > 2), t = a, w = (x > 2)$

$W = \{3, 4, 5, \dots\}$

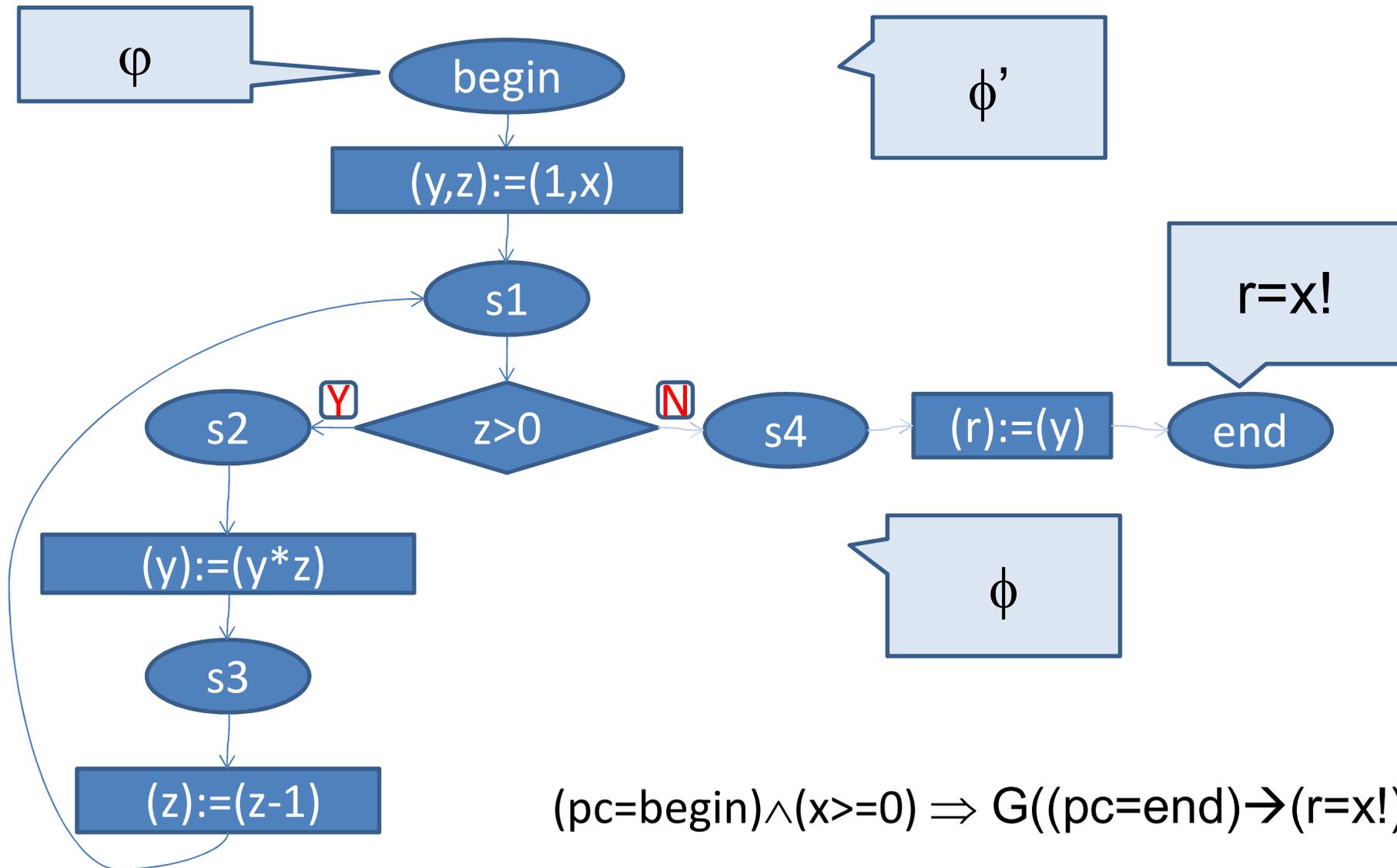
$\Theta \Rightarrow F(a \leq 2)$

# Example

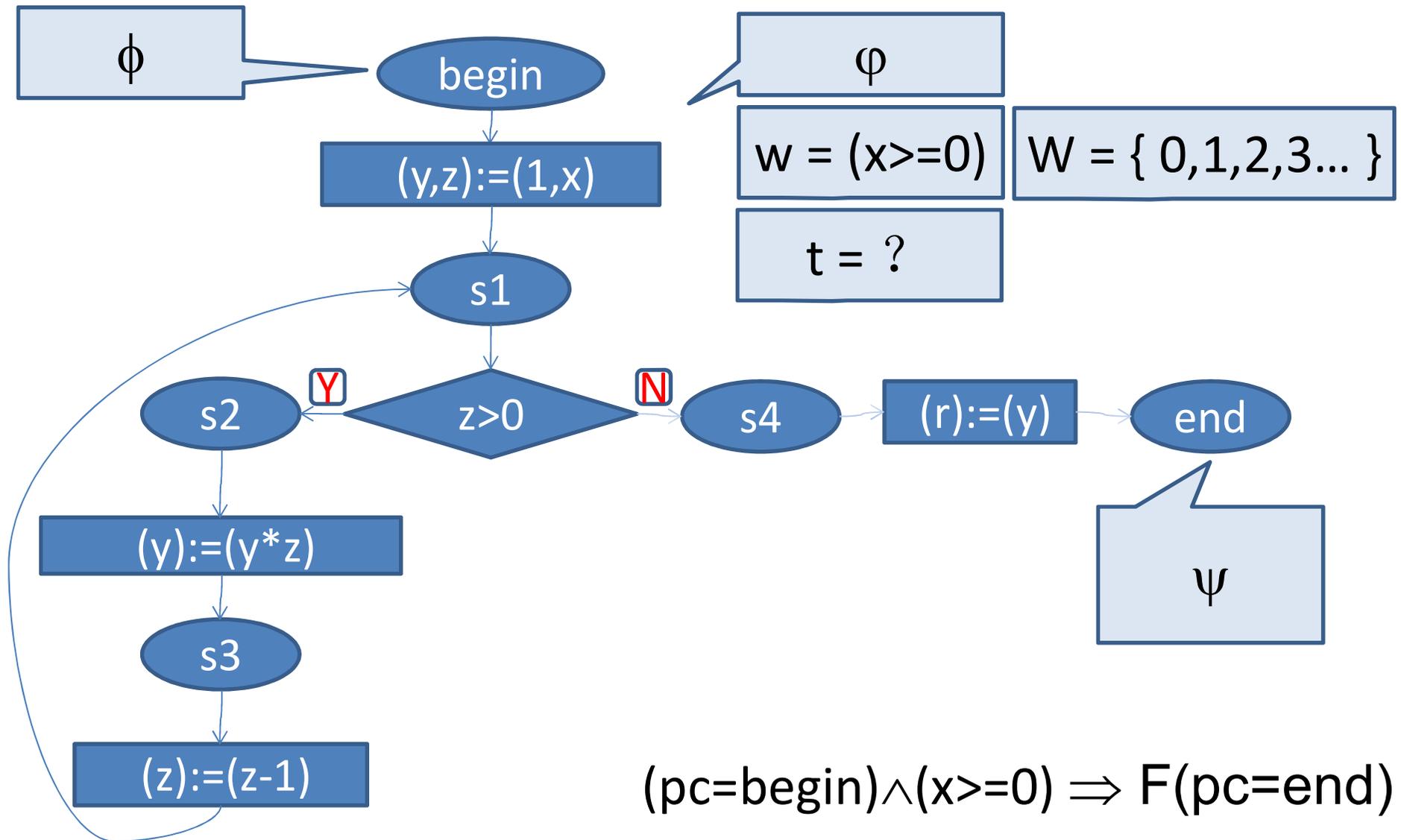


begin:	(y,z):=(1,x);	goto s1;
s1:	if (z>0) goto s2; else	goto s4;
s2:	(y):=(y*z);	goto s3;
s3:	(z):=(z-1);	goto s1;
s4:	(r):=(y);	goto end;

# Example



# Example



$$(pc = \text{begin}) \wedge (x \geq 0) \Rightarrow F(pc = \text{end})$$

$$\phi \Rightarrow F\psi$$

# Applications of FOLTL

# FOLTL as a Specification Language

System Models:	First Order Models (M)
System Specifications:	Formulas of FOLTL ( $\varphi$ )

Verification of correctness

Solving the verification problem:  $M \models \varphi$

# FOLTL as a Specification Language

System Models: GTS ( $M = \langle T, \Theta \rangle$ )

System Specifications: Formulas of FOLTL ( $\varphi$ )

Verification of correctness

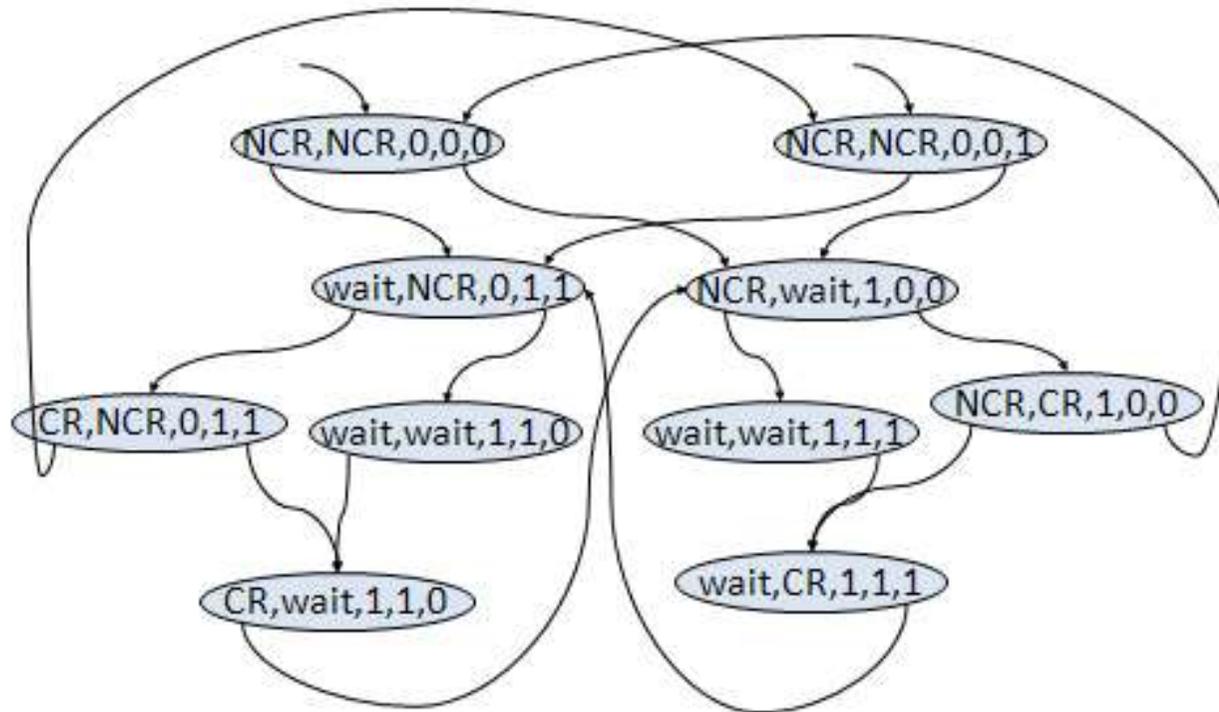
Solving the verification problem:  $M \models \varphi$

## (IV) Summary

- Bounded Semantics of PLTL
- Automata Representation of PLTL Formulas
- First Order LTL

# 练习1

给定Kripke结构如下(其中标号函数符合状态显示的内容)。



用限界语义证明(a)不成立并说明(b)成立。

$$(a) M \models (a=NCR \vee a=wait) \cup a=CR$$

$$(b) M \models (a=NCR \vee a=wait) \cup (a=CR \text{ or } b=CR)$$

## 练习2

- (a) 构造与公式  $(p \vee (q \cup r))$  等价的自动机。
- (b) 构造与公式  $(\exists p \wedge (q \cap r))$  等价的自动机。