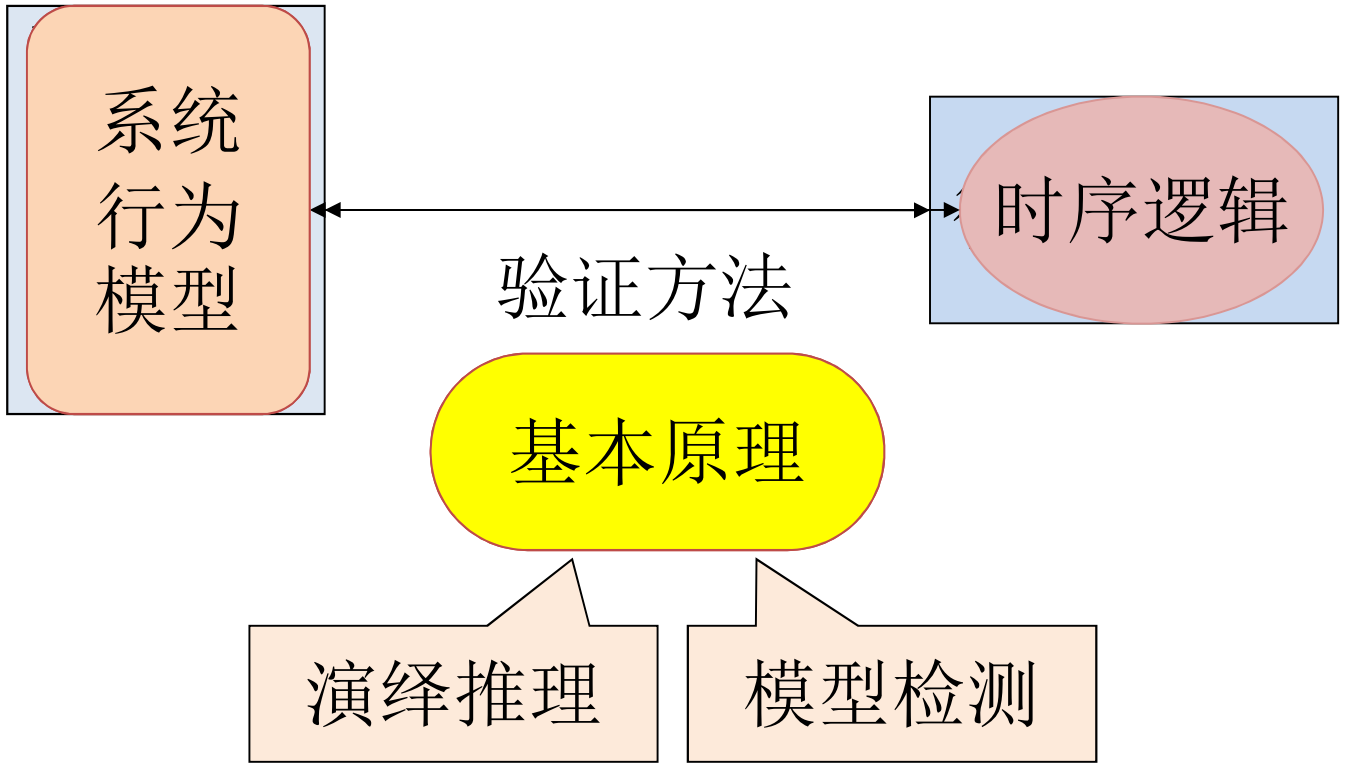
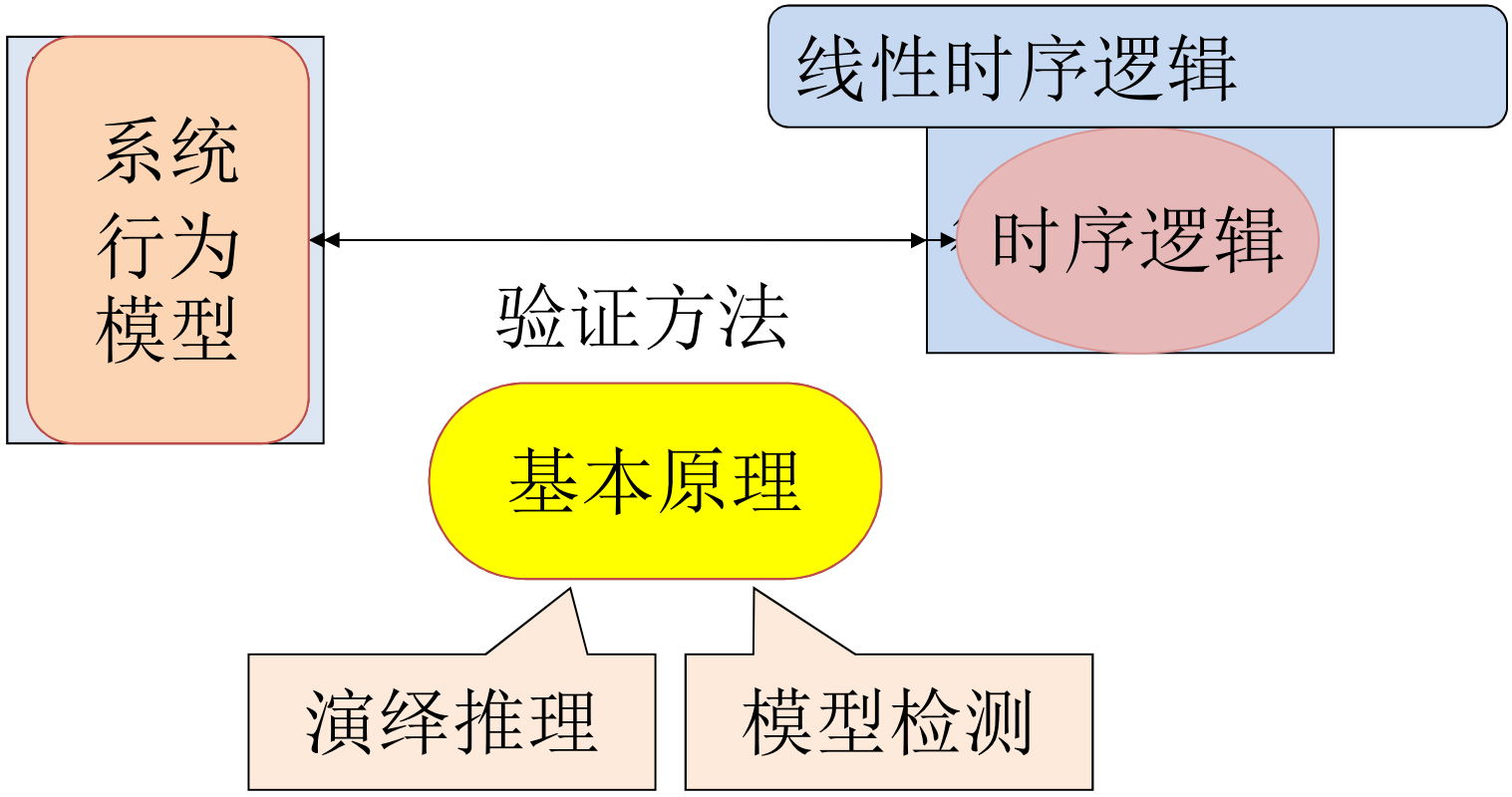
Linear Temporal Logic (II)

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

(Part I)

- Propositional Linear Temporal Logic (PLTL)
- Fixpoint Representation of PLTL Formulas
- νTL

Further Questions:

- Verification, i.e., determine whether $M \models \phi$
  - Based on the semantics
  - Based on language (behavior) inclusion, $[[M]] \subseteq [[\phi]]$
- Expressiveness of the logic
  - Propositional → first order

Contents

(Part I)

- Propositional Linear Temporal Logic (PLTL)
- Fixpoint Representation of PLTL Formulas
- νTL

(Part II)

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

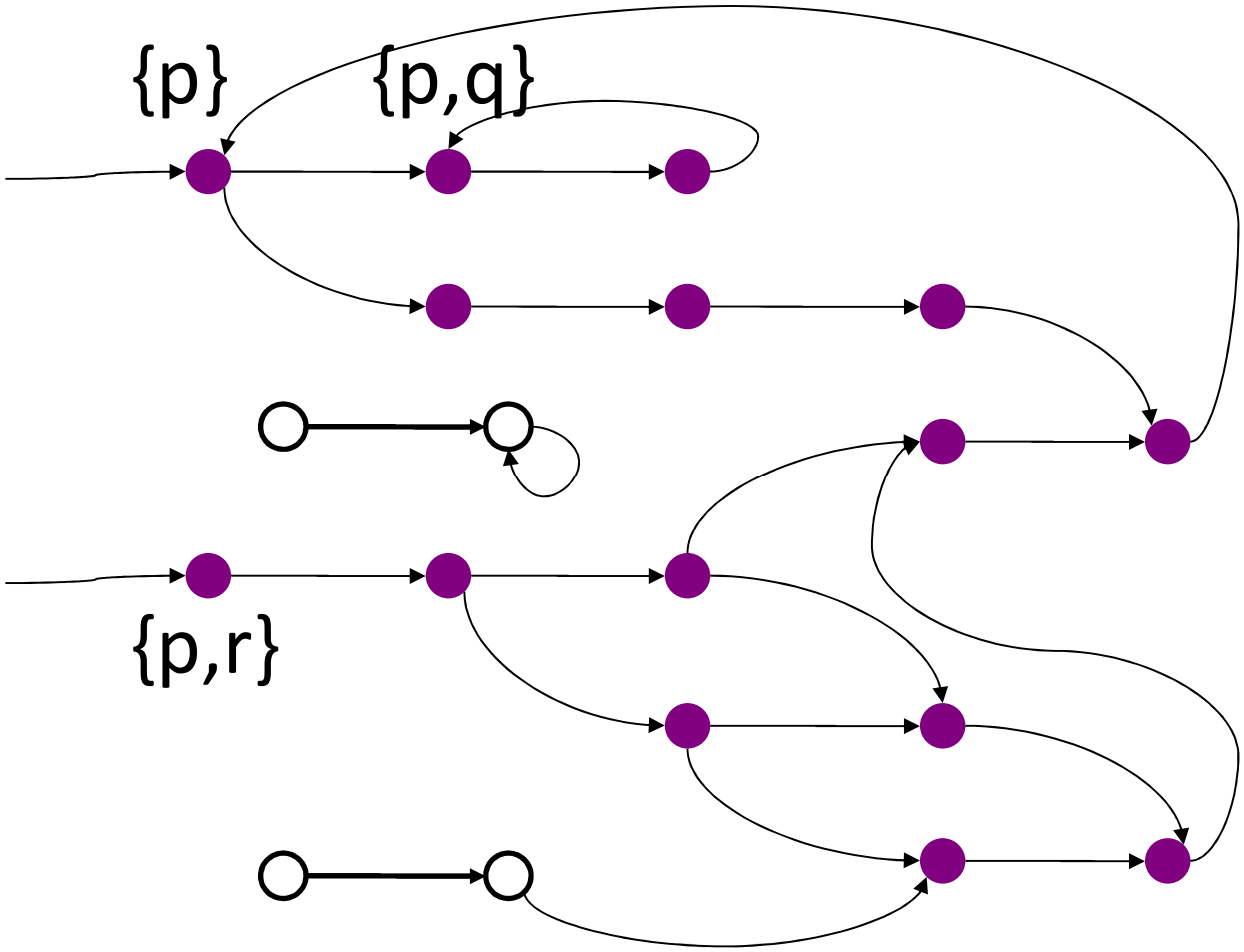
(I) Bounded Semantics of PLTL

$M \models \varphi$

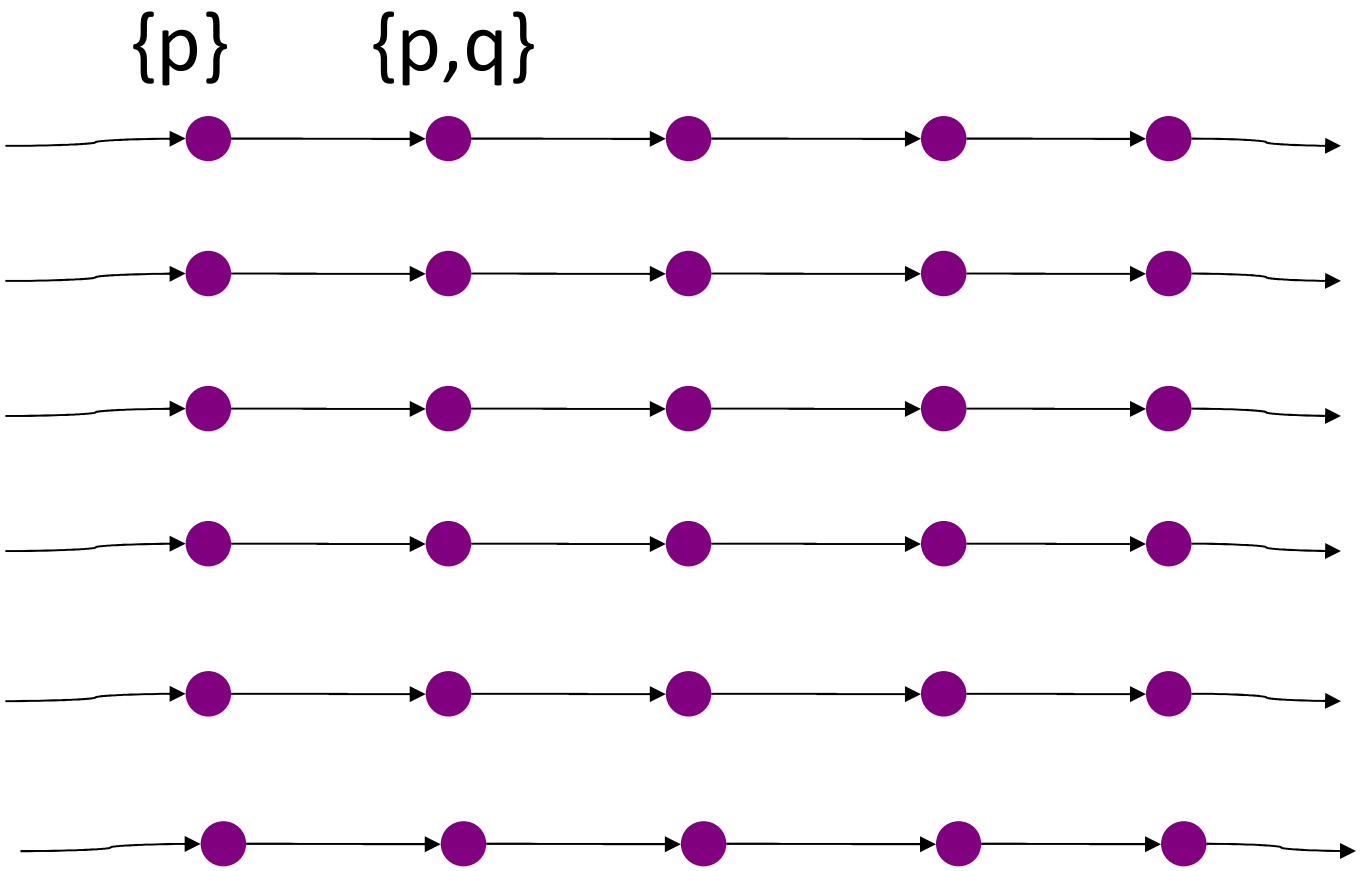
语义上牵涉无穷路径

考虑有穷路径

Kripke 结构 (S,R,I,L)



无穷路径



LTL

考虑NNF-LTL：

Φ == p | $\Phi \wedge \Phi$ | $\Phi \vee \Phi$ | $\neg$p | X Φ | GΦ | Φ U Φ

语义：$M,\pi \models \phi$

线性结构下的语义：$\langle S,\zeta,L\rangle \models \phi$ or $\zeta \models \phi$

Kripke结构下的语义：

$M,\pi \models p$, if $p \in AP$ and $p \in L(\pi_0)$

$M,\pi \models \neg p$, if $M,\pi \not\models p$

$M,\pi \models \phi \vee \psi$, if $M,\pi \models \phi$ or $M,\pi \models \psi$

$M,\pi \models \phi \wedge \psi$, if $M,\pi \models \phi$ and $M,\pi \models \psi$

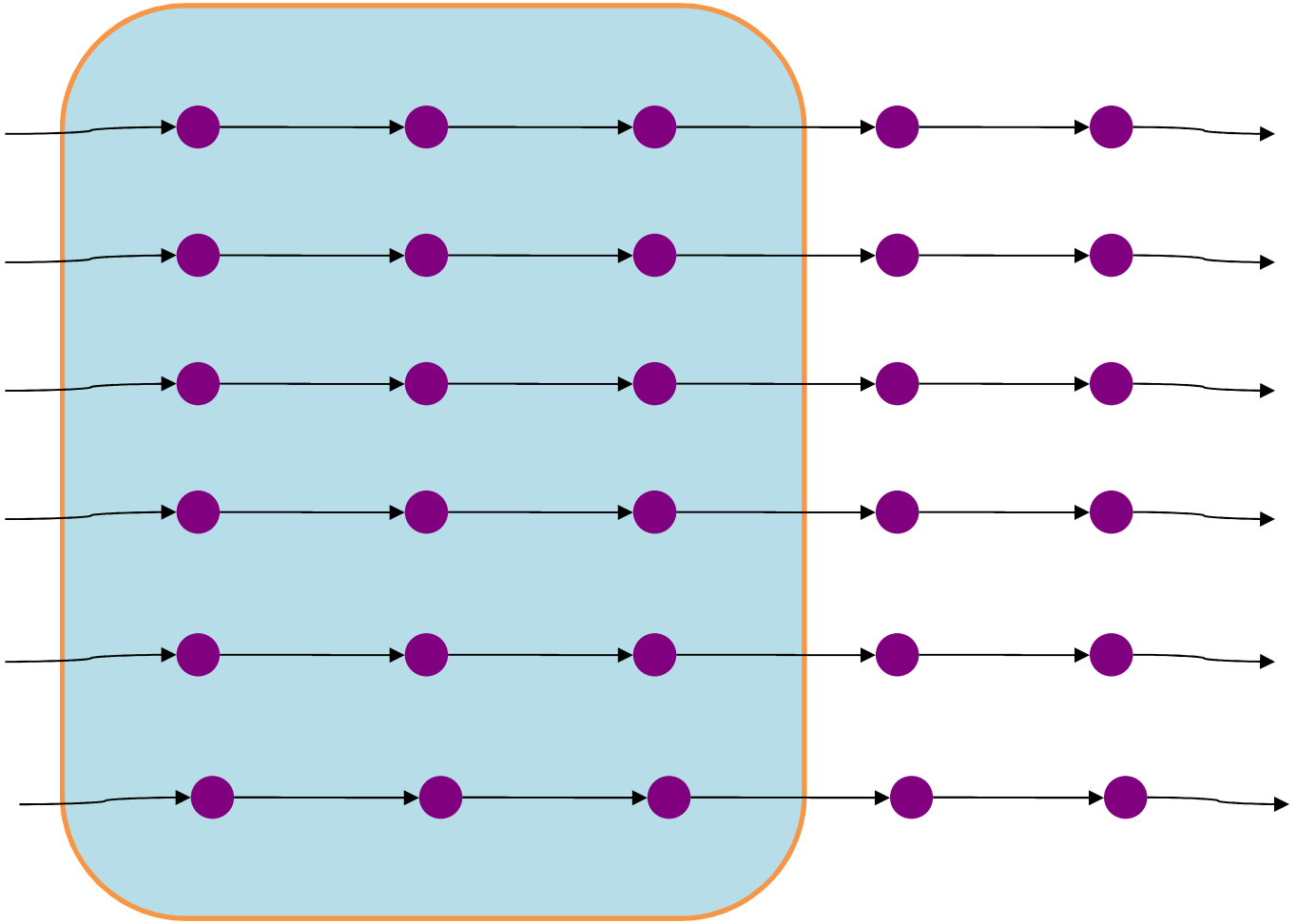
$M,\pi \models X\,\phi$, if $M,\pi^1 \models \phi$

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

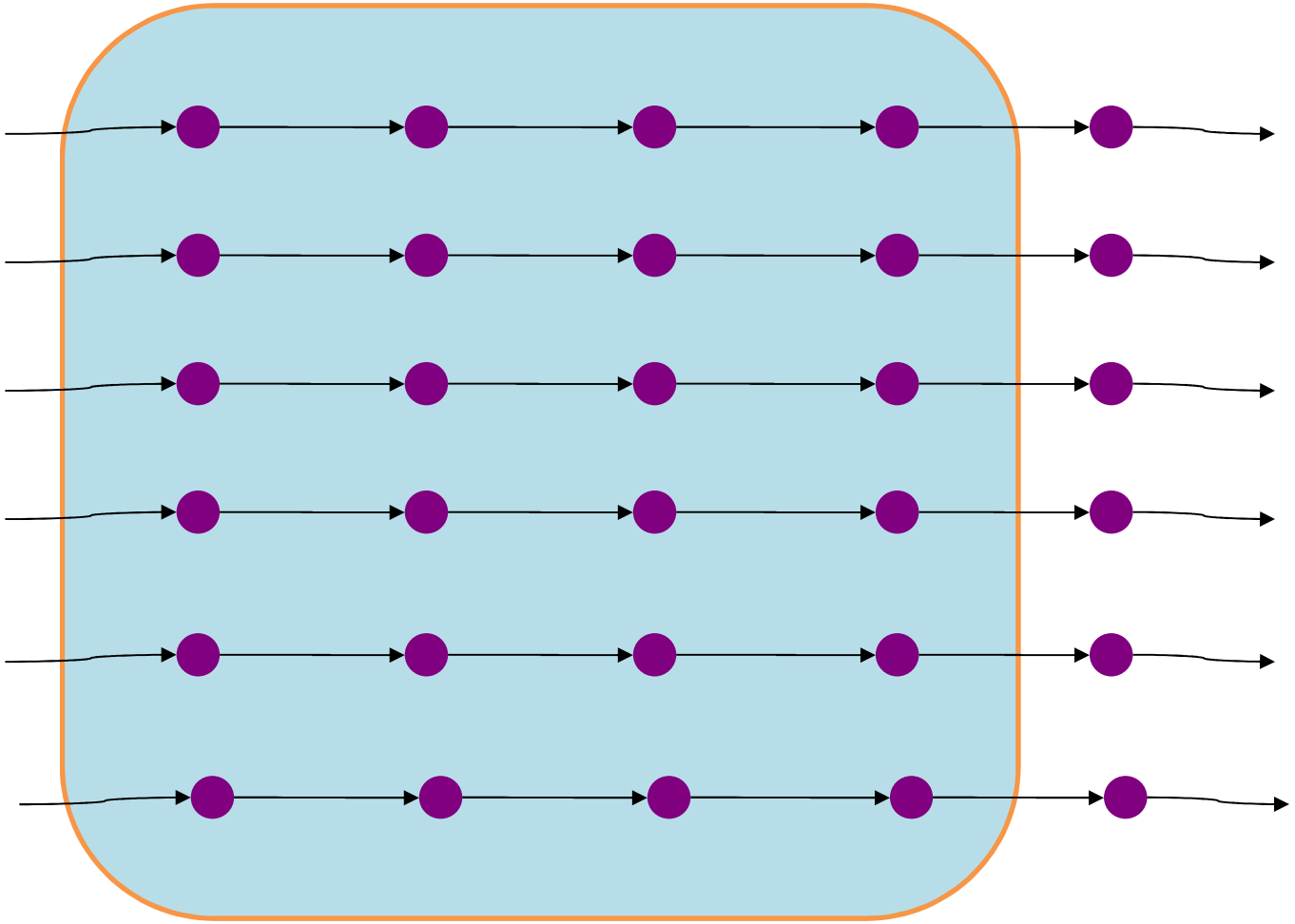
$M,\pi \models G\psi$, if $\forall i \geq 0$, $M,\pi^i \models \psi$

$M \models \phi$, if $M,\pi \models \phi$ for every computation π.

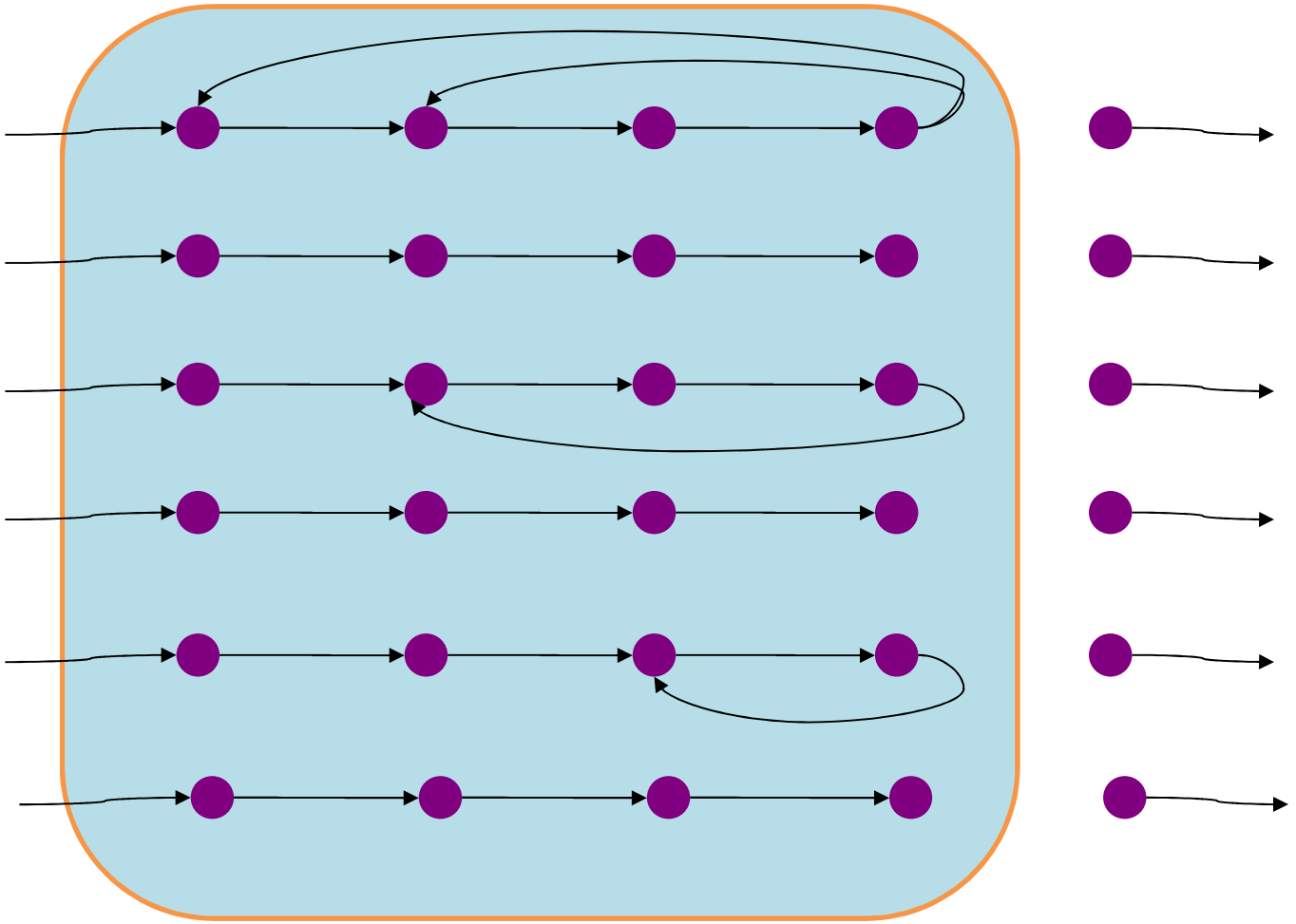
有穷路径



有穷路径



有穷路径



LTL

k路径π：　　长度为k+1的路径。

(k,l)环π：　　k路径 且 $R(\pi_k, \pi_l)$成立。

若π是计算且$M,\pi \models \phi$

则存在计算π'且存在l,k其中$k \leq |M| \times 2^{|\phi|}$

使得$\pi' = \pi_0' \ldots \pi_{l-1}' (\pi_l' \ldots \pi_k')^{\omega}$且$M, \pi' \models \phi$.

$M \not\models \phi$

当且仅当

存在l起点的 (k,l)环π使得$M, \pi_0 \ldots \pi_{l-1} (\pi_l \ldots \pi_k)^{\omega} \models \neg\phi$

Existential Satisfiability

DEFINITION:

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

Given M and ϕ.

$M \not\models \phi$ iff $M \models_E \neg\phi$

iff there is a (k,l)-loop starting from I

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

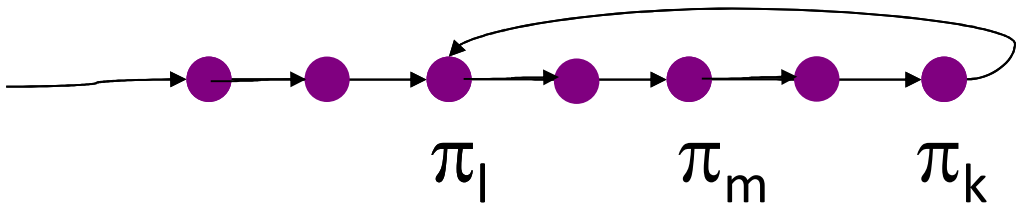
限界语义： $M, \pi \models_k \phi$

k-path: $\pi = \pi_0 \ldots \pi_k$

限界语义(loop)： $M, \pi \models_{k,l} \phi$

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

i.e., k-path: $\pi_0 \ldots \pi_{l-1}\pi_l \ldots \pi_k$ and $R(\pi_k,\pi_l)$



限界语义(loop)： $M, \pi \models_{k,l} \phi$

$M,\pi \models_k^{l,m} p$, 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 $M,\pi \models_k^{l,l} \phi$

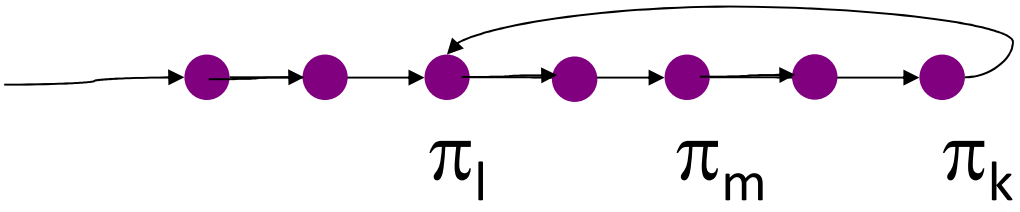
$M,\pi \models_k^{l,m} \phi U \psi$, if $\exists m \leq i \leq k$, $M,\pi \models_k^{l,i} \psi$ and $\forall m \leq j < i$, $M,\pi \models_k^{l,j} \phi$,

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(loop)： $M, \pi \models_{k,l} \phi$

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

$M,\pi \models_{k,l} \phi$
iff
$M,\pi \models \phi$

$M,\pi \models_{k,l} \phi$ for some (k,l) ➔ there is a π' such that $M, \pi' \models \phi$
$M,\pi \models \phi$ ➔ there are some (k,l) and π' such that $M, \pi' \models_{k,l} \phi$

限界语义(non-loop)： $M, \pi \models_{k,-1} \phi$

$M,\pi \models_k^m p$, 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 $M,\pi \models_k^m \psi$

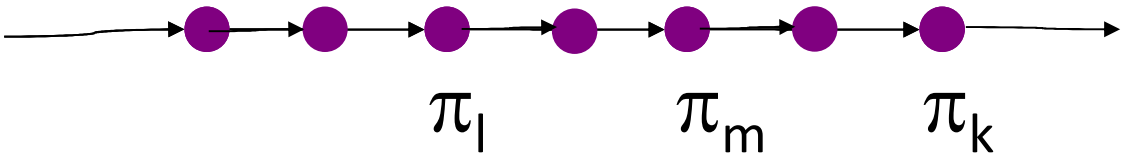
$M,\pi \models_k^m \phi \wedge \psi$, if $M,\pi \models_k^m \phi$ and $M,\pi \models_k^m \psi$

$M,\pi \models_k^m X\phi$, 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(non-loop)： $M, \pi \models_{k,-1} \phi$

$M,\pi \models_{k,-1} \phi$ for some k ➔ there is a π' such that $M, \pi' \models \phi$

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 $l \in \{0,\ldots,k\}$

DEFINITION

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

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,φ)的完备阈值，当且仅当
若$M \not\models_{E,k} \neg\varphi$，则对$k' \geq k$，$M \not\models_{E,k'} \neg\varphi$

记(M,φ)的最小完备阈值为 lct(M,φ)：
若 $b \geq lct(M,\varphi)$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)

BMC(M,φ,b):

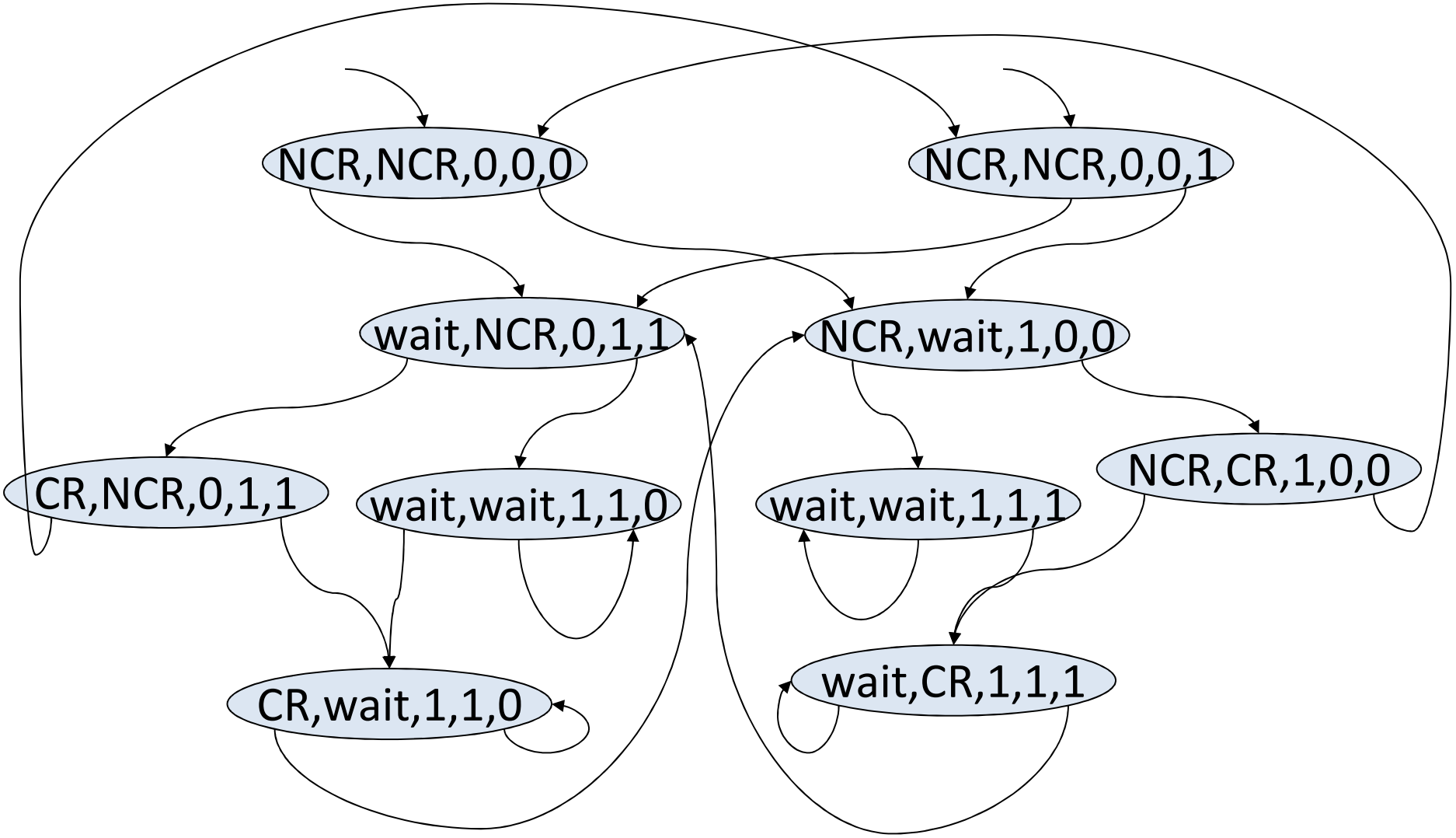
1. k=0;
2. if $M|=_{E,k} \neg\varphi$, then report unsat;
3. if k=b, then report done;
4. k=k+1; goto step 2;

If BMC(M,φ,b) returns unsat, then $M \not\models \varphi$;

If $b \geq lct(M,\varphi)$, then BMC(M,φ,b) returns unsat iff $M \not\models \varphi$.

例子

Example: F(a=CR or b=CR)?



E..G(a!=CR and b!=CR) ?

Example: ϕ = F(a=CR 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 ?

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

k=0: **(**NCR,NCR,0,0,0),……

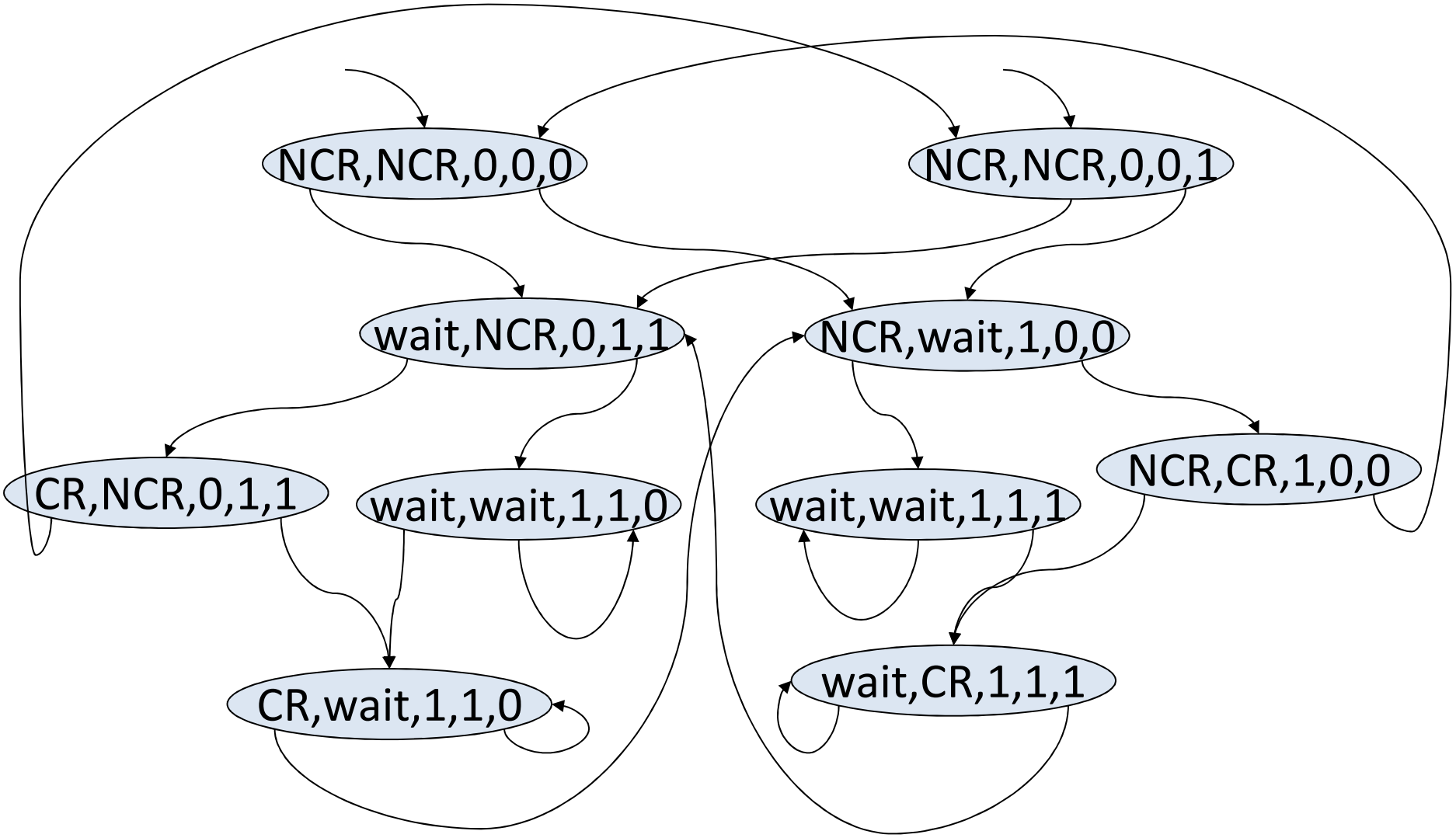
k=1: (NCR,NCR,0,0,0)(wait,NCR,0,1,1),……

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,

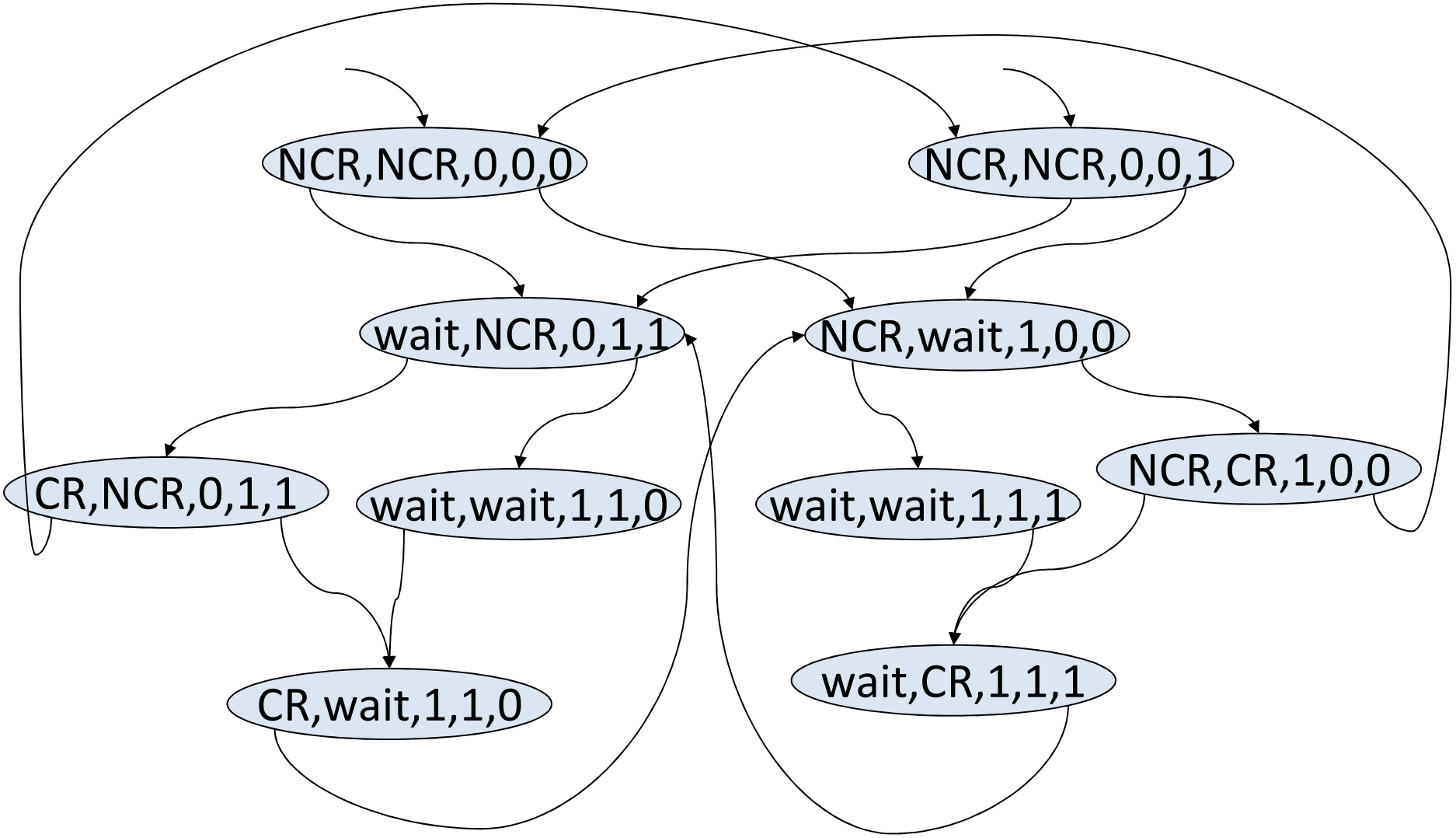
we have that $M \models F(a=CR \text{ or } b=CR)$ does not hold.

Example: F(a=CR or b=CR)?



E..G(a!=CR and b!=CR) ? ok

Example: F(a=CR or b=CR)?



E..G(a!=CR and b!=CR) ?

Example: ϕ = F(a=CR or b=CR)

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

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

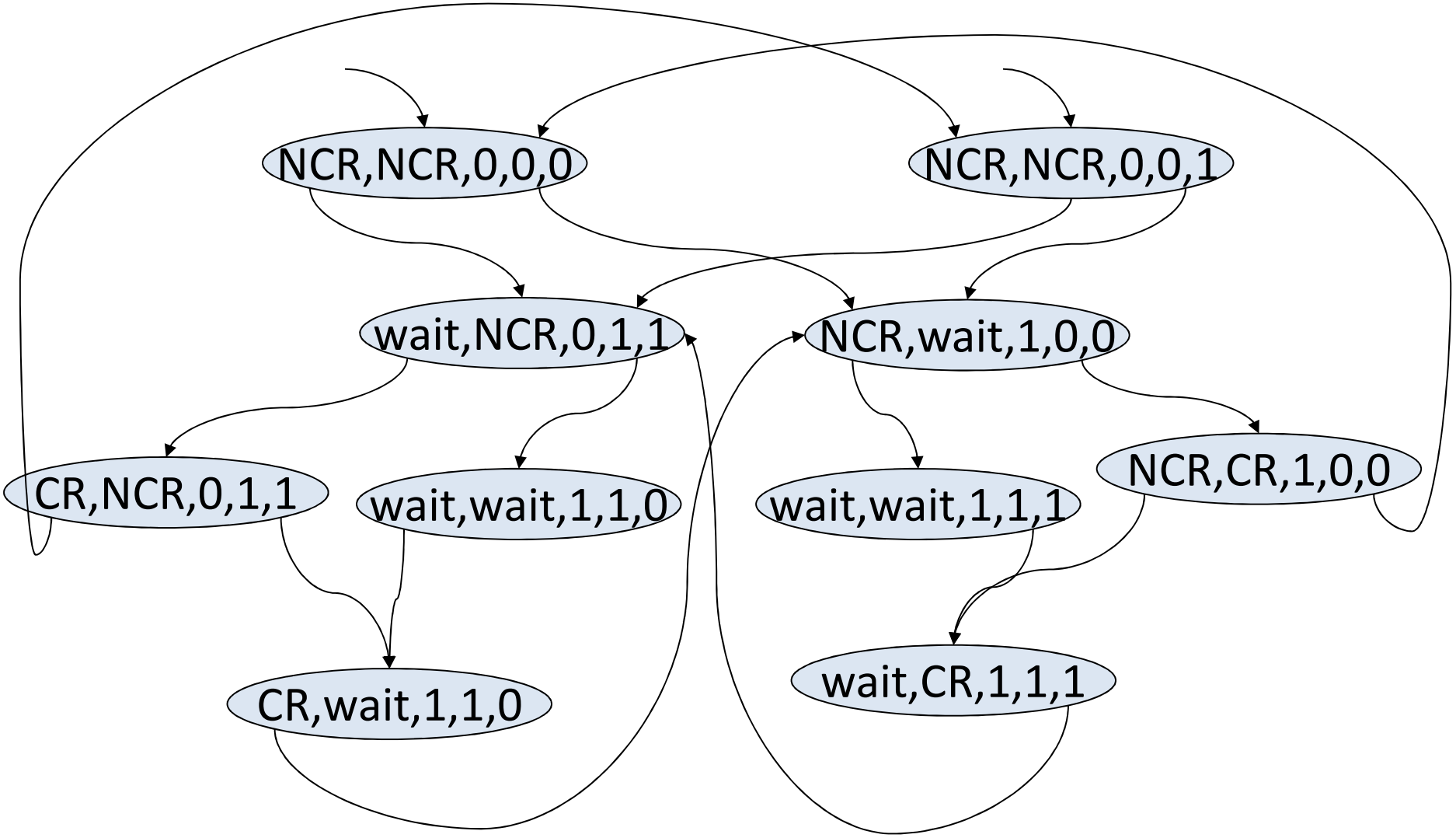
$M \models_{E,k} \neg F(a=CR \text{ or } b=CR)$ for some k ?

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

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

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

Example: F(a=CR or b=CR)?



E..G(a!=CR and b!=CR)? lct()?

(II) Automata Representation of PLTL

$M \models \varphi$

$M \rightarrow$ Automaton

$\varphi \rightarrow$ Automaton

Language inclusion

Language emptiness

Emptiness of fair Kripke structures

PLTL → ω-Automata

Let AP be given.

Let ϕ over AP be given.

Construct a GBA A such that

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

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

Example

G p

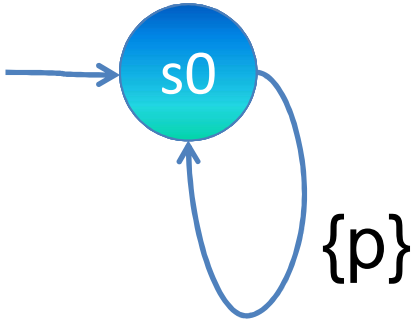
p U q

p U (q U r)

Example

G p

AP={p}



<Σ,S,Δ,I,F>

Σ ={ {}, {p} }

S = {s0}

Δ = { (s0,{p},s0) }

I = {s0}

F = {s0}

Example

p U q

AP={p,q}

<Σ,S,Δ,I,F>

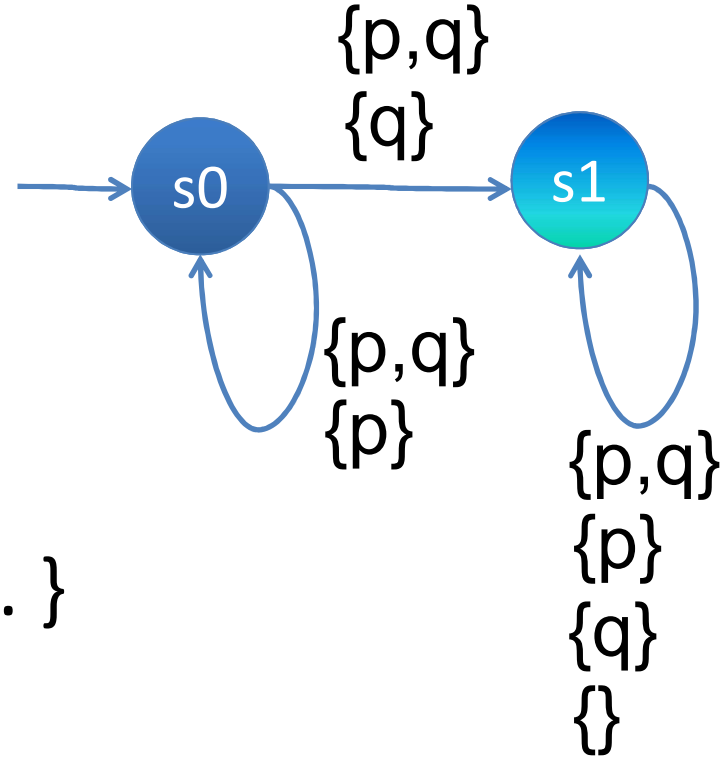
Σ ={ {}, {p}, {q}, {p,q} }

S = {s0,s1}

Δ = { (s0,{p},s0), (s0,{p,q},s0), … }

I = {s0}

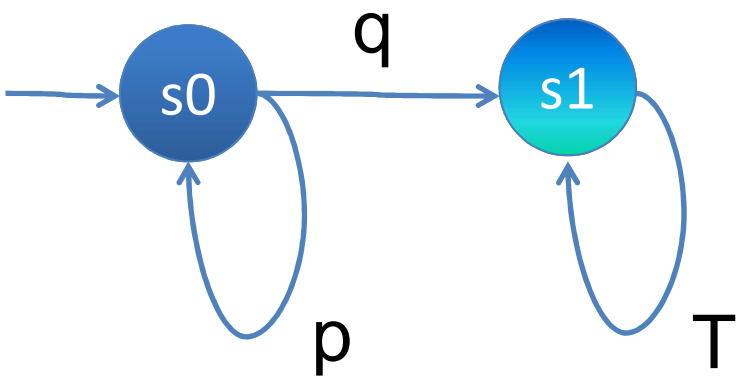
F = {s1}



Example

p U q

AP={p,q}



<Σ,S,Δ,I,F>

Σ ={ {}, {p}, {q}, {p,q} }

S = {s0,s1}

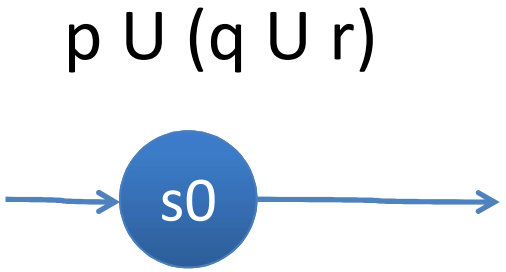
Δ = { (s0,{p},s0), (s0,{p,q},s0), … }

I = {s0}

F = {s1}

Example

p U (q U r) ?



PLTL → ω-Automata

Only consider NNF formulas with

literals,

disjunction, conjunction,

X, U, R

Φ == p | $\neg$p | $\Phi \wedge \Phi$ | $\Phi \vee \Phi$ | X Φ | Φ R Φ | Φ U Φ

PLTL → ω-Automata

Let φ be a PLTL formula over AP.

Construct a GBA A=<S,Σ,Δ,I,F> such that

<S,ζ,L> |= ϕ iff L(ζ)∈ ***L***(A)

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

(2)S,I,Δ,F = ?

PLTL → ω-Automata

$\varphi \rightarrow$

initial node

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

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

new node

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

Meaning of [a; b; c; d]

PLTL → ω-Automata

s=[a; p,φ; c; d] where p is a literal

Replace by

s'=[a; φ; p,c; d]

PLTL → ω-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 → ω-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 → ω-Automata

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

Replace by

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

PLTL → ω-Automata

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

Replace by

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

Or equivalently, by,

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

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

PLTL → ω-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 → ω-Automata

s=[a; ∅; c; d]

s'=[a'; ∅; c; d]

Replace by

s''=[a,a'; ∅; c; d]

PLTL → ω-Automata

s=[a; ∅; c; d]

s’=[a’; ∅; c; d]

Replace by

s’’=[a,a’; ∅; 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 → ω-Automata

s=[a; ∅; c; d]

$s \in l$ iff $\varepsilon \in a$

PLTL → ω-Automata

$\Sigma = 2^{AP}$

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

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

Define Δ as follow:

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

PLTL → ω-Automata

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

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

PLTL → ω-Automata

Theorem

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

Then $<S,\zeta,L> \models \phi$ iff $L(\zeta) \in \boldsymbol{L}(A)$.

Example

G p

p U q

p U (q U r)

例子

1

New

1	ε	pU(qUr)		

Replaced by

11	ε	qUr	pU(qUr)	
12	ε	p	pU(qUr)	pU(qUr)

Replaced by

111	ε	r	pU(qUr),qUr	
112	ε	q	pU(qUr),qUr	qUr
12’	ε		pU(qUr),p	pU(qUr)

1

Replaced by

111’	ε		pU(qUr),qUr,r	
112’	ε		pU(qUr),qUr,q	qUr
12’	ε		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	ε		pU(qUr),qUr,r	
112	ε		pU(qUr),qUr,q	qUr
12	ε		pU(qUr),p	pU(qUr)

Summary: 1, 4

111	ε,12		pU(qUr),qUr,r	
112	ε,12		pU(qUr),qUr,q	qUr
12	ε,12		pU(qUr),p	pU(qUr)

Summary: 1, 2, 3, 4

111	ε,12		pU(qUr),qUr,r	
112	ε,12		pU(qUr),qUr,q	qUr
12	ε,12		pU(qUr),p	pU(qUr)

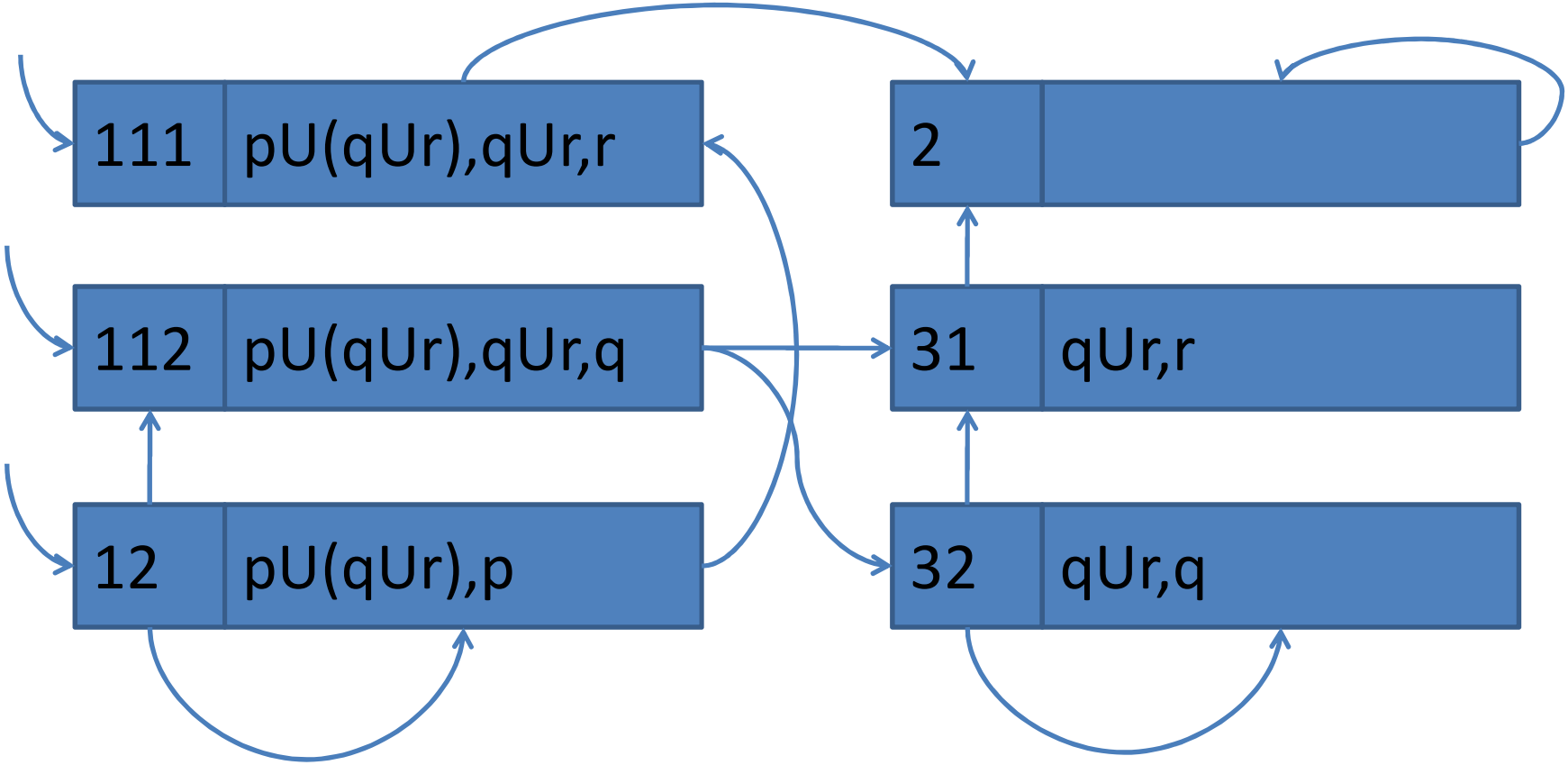
2	111			
31	112		qUr,r	
32	112		qUr,q	qUr

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

111	ε,12		pU(qUr),qUr,r	
112	ε,12		pU(qUr),qUr,q	qUr
12	ε,12		pU(qUr),p	pU(qUr)

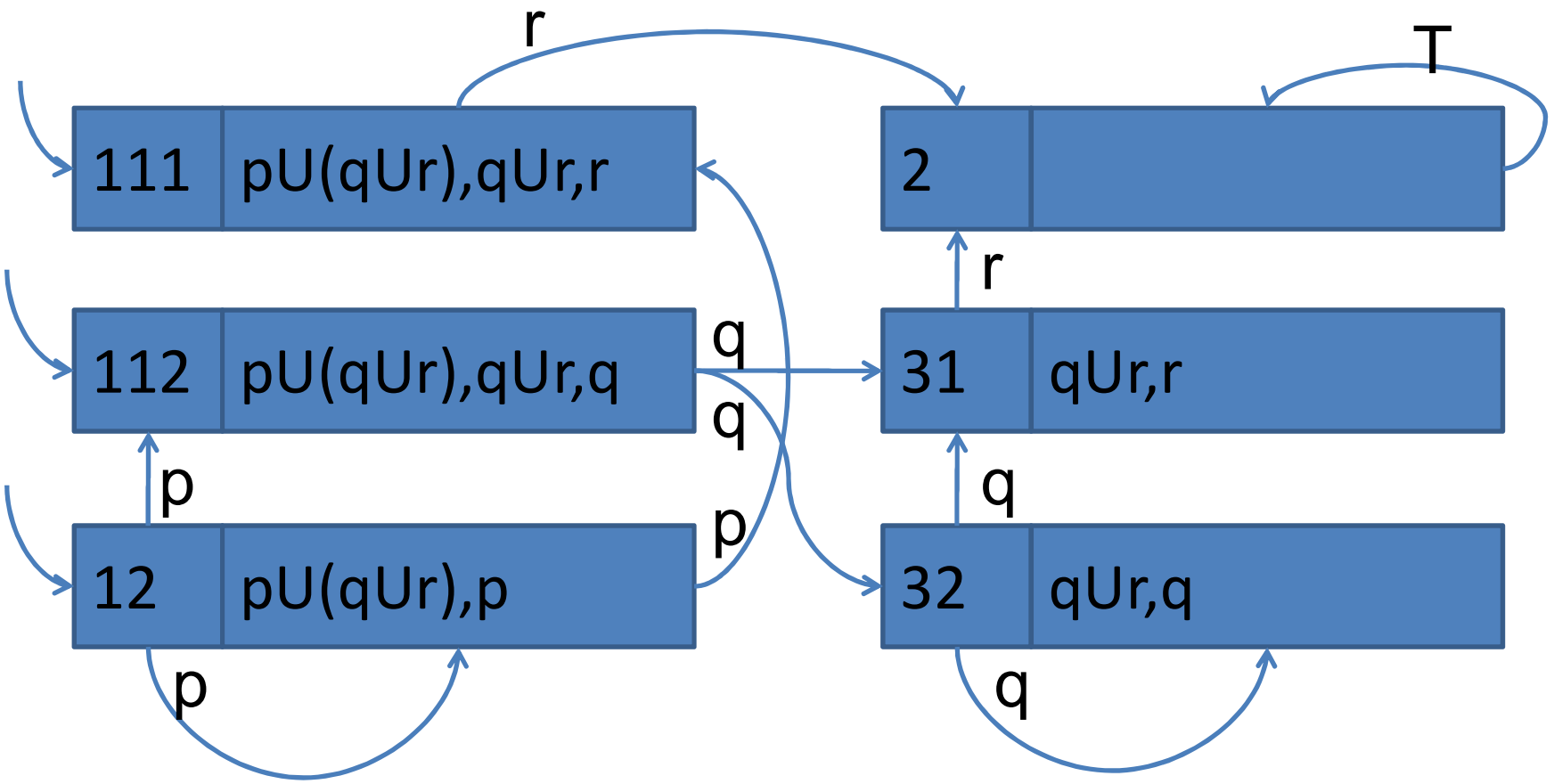
2	111,2,31			
31	112,32		qUr,r	
32	112,32		qUr,q	qUr

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

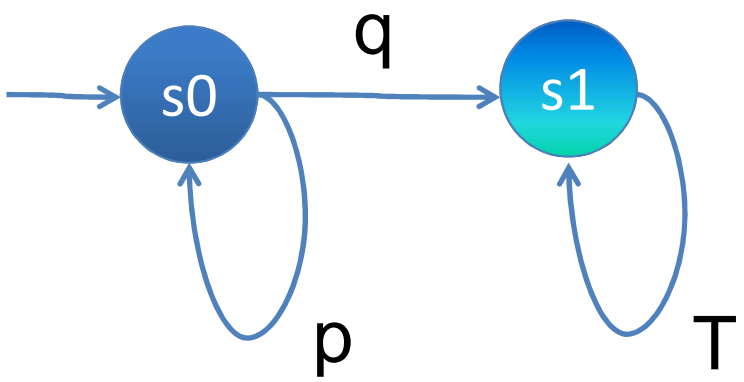
Let φ = pU(qUr).

Let A = (Σ,S,Δ,I,F) where

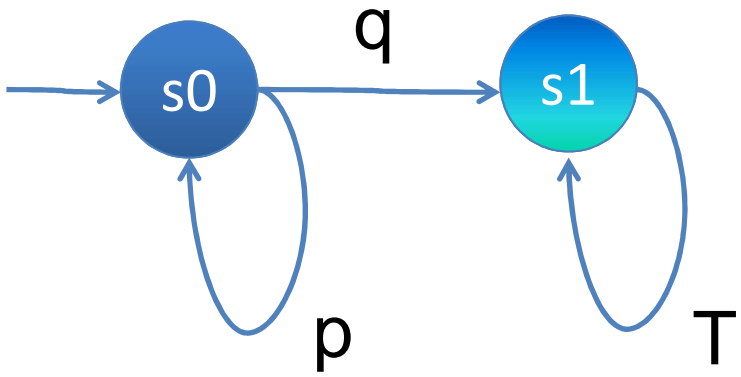
- $\Sigma = 2^{\{p,q,r\}}$
- S = { 111,112,12,2,31,32 }
- Δ = {
  (111,{r},2), (111,{p,r},2),
  (111,{q,r},2), (111,{p,q,r},2),……
  }
- I = { 111,112,12 }
- F={ {111,112,2,31,32}, {12,111,31,2} }

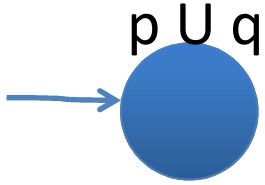
Then <S,ζ,L> |= φ iff L(ζ)$\in$ ***L***(A)

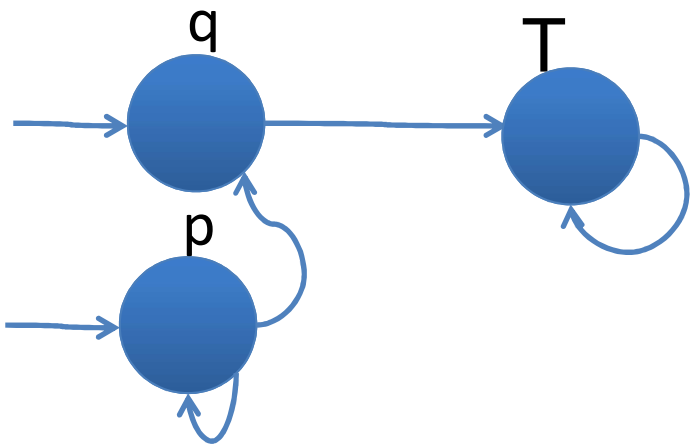
Example (p U q)

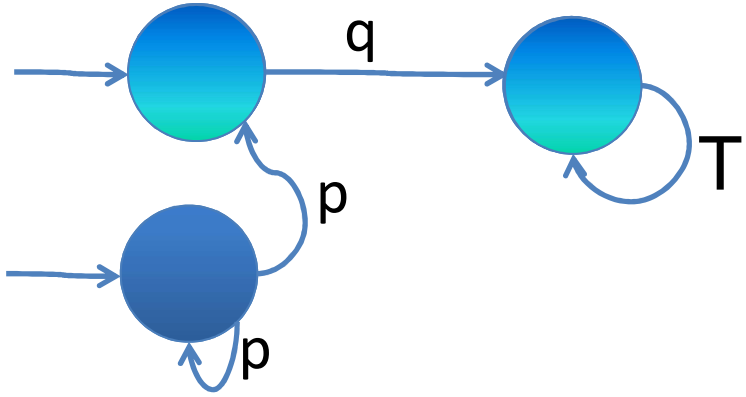


Example (p U q)









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 Φ 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 Σ be the set of assignments.

$$\sigma: X \rightarrow D$$

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

ζ is called a model.

Semantics: $\zeta \models \phi$

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

$\zeta \models p$, if $p \in WFF$ and $\zeta_0 \models_l p$

$\zeta \models \neg\phi$, 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 ϕ is satisfiable, if there is a model ζ such that $\zeta \models \phi$.

Definition

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

Equivalences

Equivalences

Definition

A formula ϕ is equivalent to a formula ψ, if for every model ζ, ($\zeta \models \phi$ iff $\zeta \models \psi$).

FOLTL Proof Rules

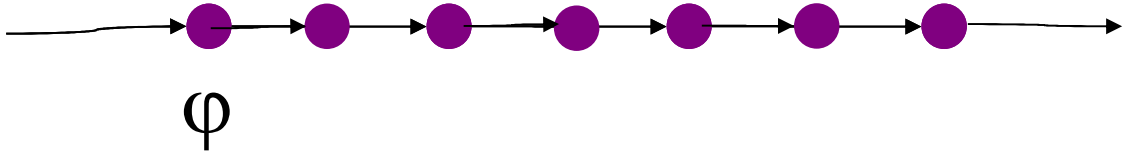
Generalization

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

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

Proof Rules (for F/U)

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



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)：

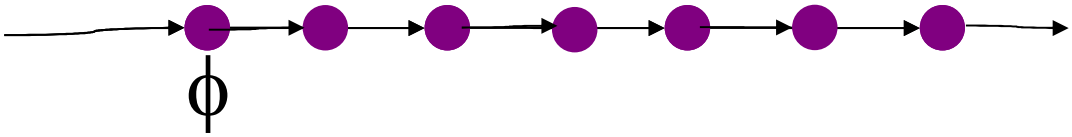
(W,≤)

严格下降链 w0 > w1 > w2 > ……

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)



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

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

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

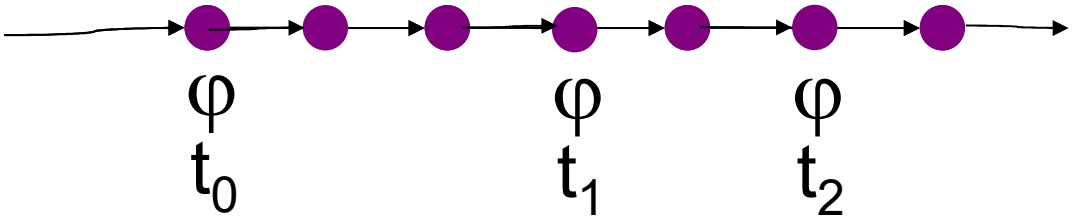
$\phi \Rightarrow F\psi$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

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

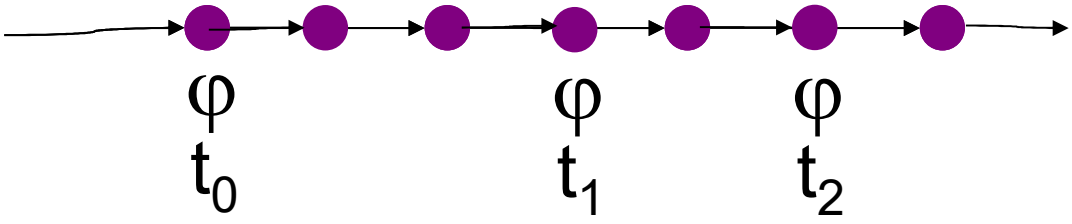
$\phi \Rightarrow F\psi$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

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

$\phi \Rightarrow F\psi$

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

➔ $I(w)(\sigma[x/I(t)\sigma])=true$

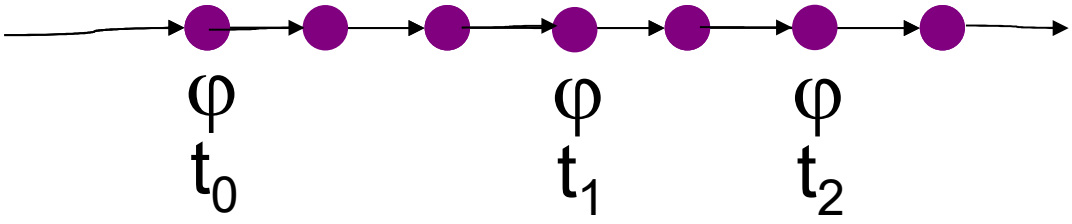
➔ $I(t)(\sigma) \in W$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

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

$\phi \Rightarrow F\psi$

$\varphi \Rightarrow X\psi$

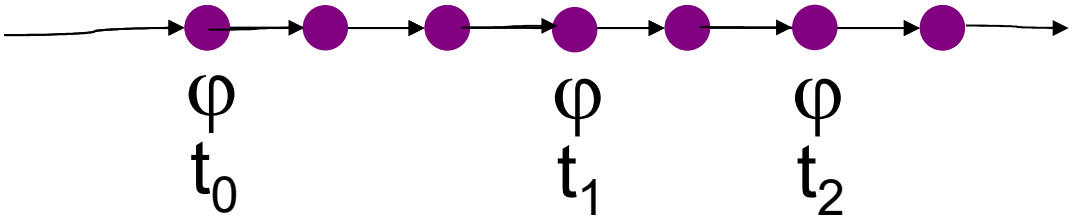
$\varphi \Rightarrow F\psi$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

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

$\phi \Rightarrow F\psi$

$\varphi \Rightarrow X\psi$

$\varphi \Rightarrow F\psi$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Example

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

T: { a>2 → (a):=(a-2),
a<=2 → (a):=(a)
}

Θ: (a=100$\vee$a=200)

I: (Int,I_0)

M |= F(a<=2)

Example

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

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

Θ: $(a=100 \vee a=200)$

I: (Int, I_0)

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

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

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

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

$\phi \Rightarrow F\psi$

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

φ? t? w? W?

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

Example

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

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

Θ: $(a=100 \vee a=200)$

I: (Int, I_0)

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

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

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

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

$\phi \Rightarrow F\psi$

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

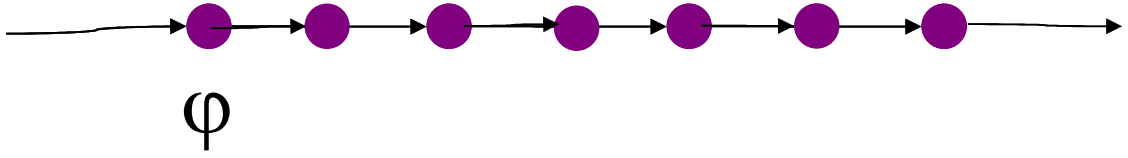
$\varphi = (a>2)$, $t=a$, $w = (x>2)$

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

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

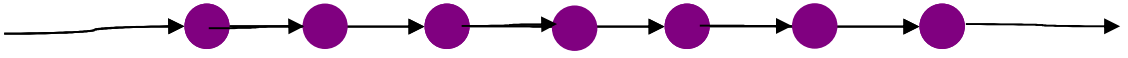
Proof Rules (for F/U)

$$\frac{\varphi \Rightarrow \psi}{\varphi \Rightarrow (\varphi U \psi)} \qquad \frac{\varphi \Rightarrow X\psi}{\varphi \Rightarrow (\varphi U \psi)}$$



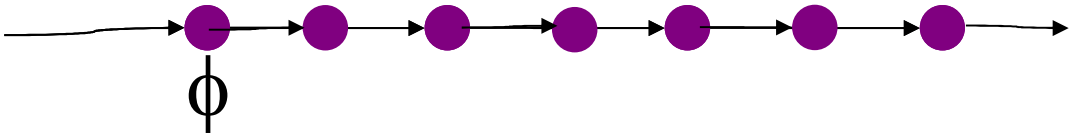
Proof Rules (for F/U)

$$\frac{\varphi \Rightarrow \psi}{\varphi \Rightarrow (\varphi_0 \mathsf{U} \psi)} \qquad \frac{\varphi \Rightarrow \varphi_0 \quad \varphi \Rightarrow \mathsf{X}\psi}{\varphi \Rightarrow (\varphi_0 \mathsf{U} \psi)}$$



φ

Proof Rules (for F/U)



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

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

$(\varphi \wedge t=v) \Rightarrow \varphi_0 U(\psi \vee (\varphi \wedge t<v))$

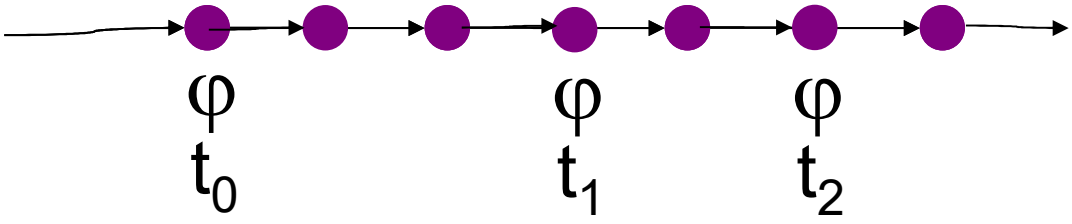
$\phi \Rightarrow (\varphi_0 U \psi)$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

$(\varphi \wedge t=v) \Rightarrow \varphi_0 U(\psi \vee (\varphi \wedge t<v))$

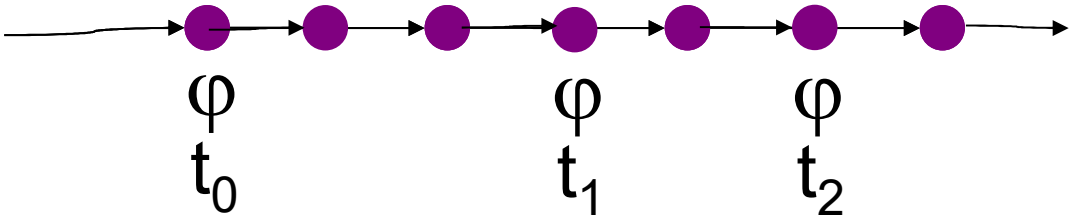
$\phi \Rightarrow (\varphi_0 U \psi)$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

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

$(\varphi \wedge t=v) \Rightarrow \varphi_0 U(\psi \vee (\varphi \wedge t<v))$

$\phi \Rightarrow (\varphi_0 U \psi)$

$\varphi \Rightarrow \varphi_0$

$\varphi \Rightarrow X\psi$

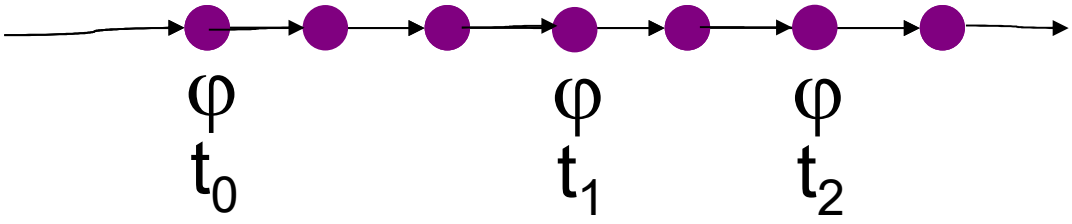
$\varphi \Rightarrow (\varphi_0 U \psi)$

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

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

Proof Rules (for F/U)



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

$\varphi \Rightarrow \varphi_0 \wedge w(t/x)$

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

$\phi \Rightarrow (\varphi_0 U \psi)$

$\varphi \Rightarrow \varphi_0$

$\varphi \Rightarrow X\psi$

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

v为变量, t为项, ≤ 为二元谓词符号;

w为一元谓词公式, 其变量为x;

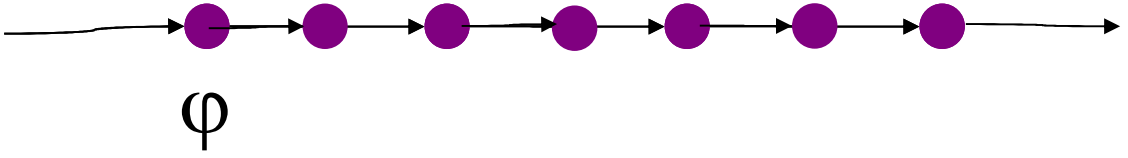
$W=(\{\sigma(x) \mid I(w)(\sigma)=true\}, I_0(\leq))$ 为良基集合

Proof Rules (for G/R)

$$\varphi \Rightarrow \phi$$

$$\phi \Rightarrow \mathsf{X}\, \phi$$

$$\varphi \Rightarrow \mathsf{G}\, \phi$$



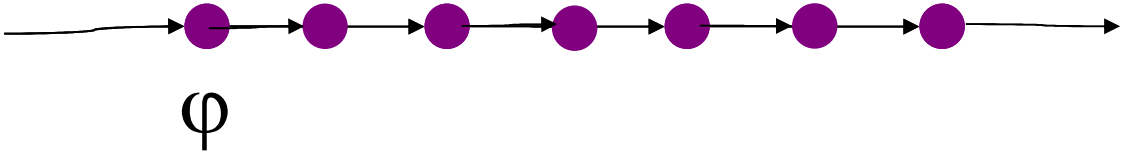
Proof Rules (for G/R)

$$\varphi \Rightarrow \phi'$$

$$\phi' \Rightarrow \mathsf{X}\, \phi'$$

$$\phi' \Rightarrow \phi$$

$$\varphi \Rightarrow \mathsf{G}\, \phi$$



Example

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

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

Θ: $(a=100 \vee a=200)$

I: (Int, I_0)

$M \models G(even(a))$

Example

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

T: { a>2 → (a):=(a-2),
a<=2 → (a):=(a)
}

Θ: $(a=100 \vee a=200)$

I: (Int, I_0)

$M \models G(even(a))$

$\varphi \Rightarrow \phi'$

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

$\phi' \Rightarrow \phi$

$\varphi \Rightarrow G\, \phi$

$\varphi = \Theta$

$\phi = even(a)$

ϕ' ?

$\Theta \Rightarrow G(even(a))$

Example

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

T: { a>2 → (a):=(a-2),
a<=2 → (a):=(a)
}

Θ: $(a=100 \vee a=200)$

I: (Int, I_0)

$M \models G(even(a))$

$\varphi \Rightarrow \phi'$

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

$\phi' \Rightarrow \phi$

$\varphi \Rightarrow G\,\phi$

$\varphi = \Theta$

$\phi = even(a)$

$\phi' = \phi$

$\Theta \Rightarrow G(even(a))$

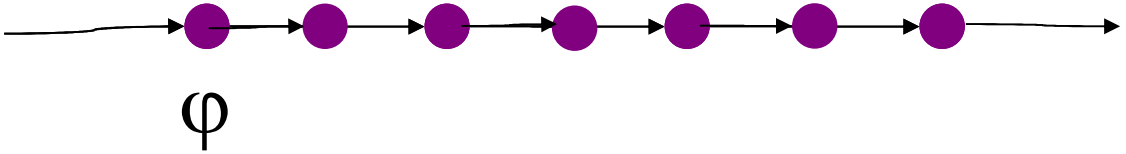
Proof Rules (for G/R)

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

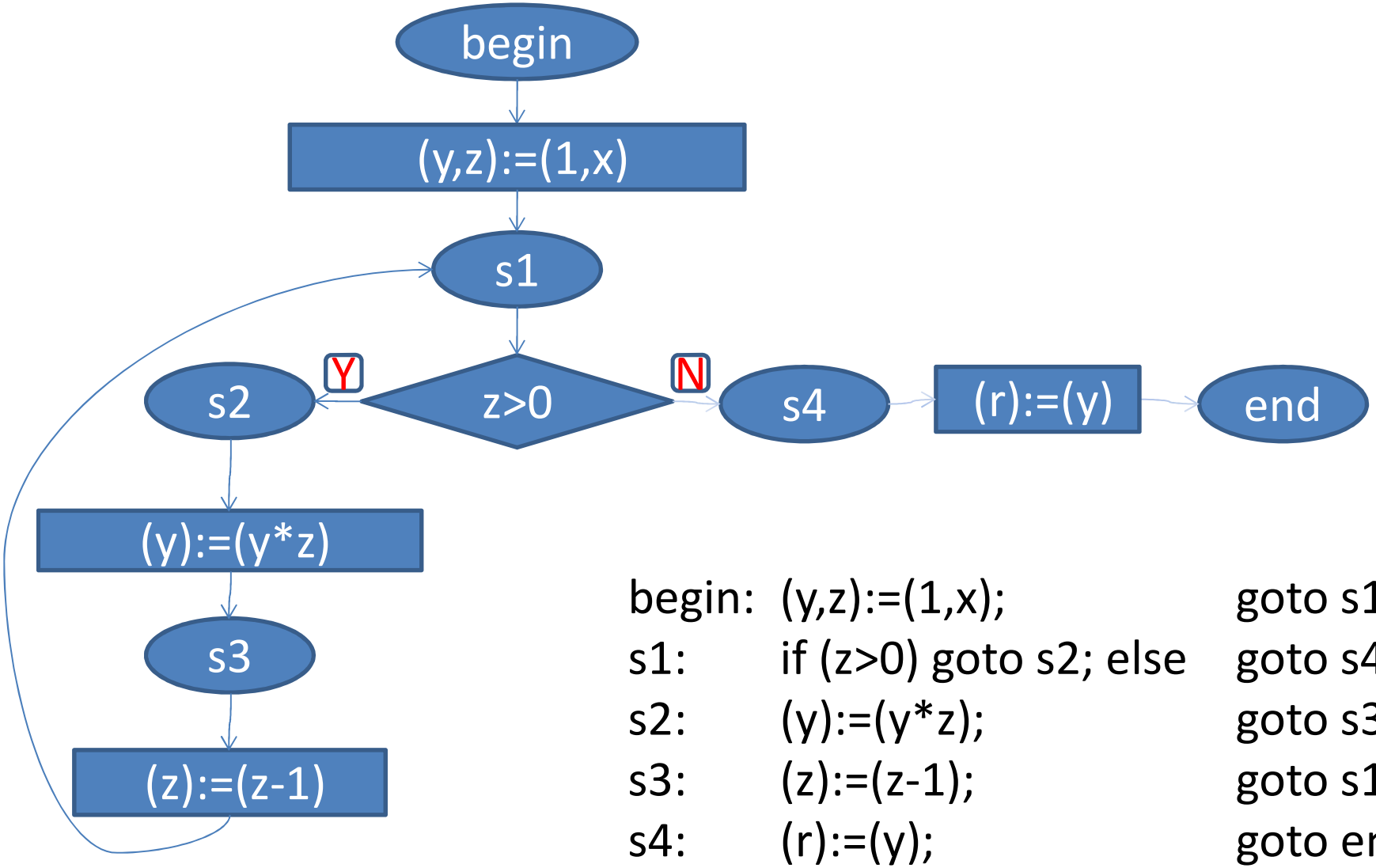
$$\varphi \Rightarrow (\psi R\ \phi)$$

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

$$\varphi \Rightarrow G\ \phi$$

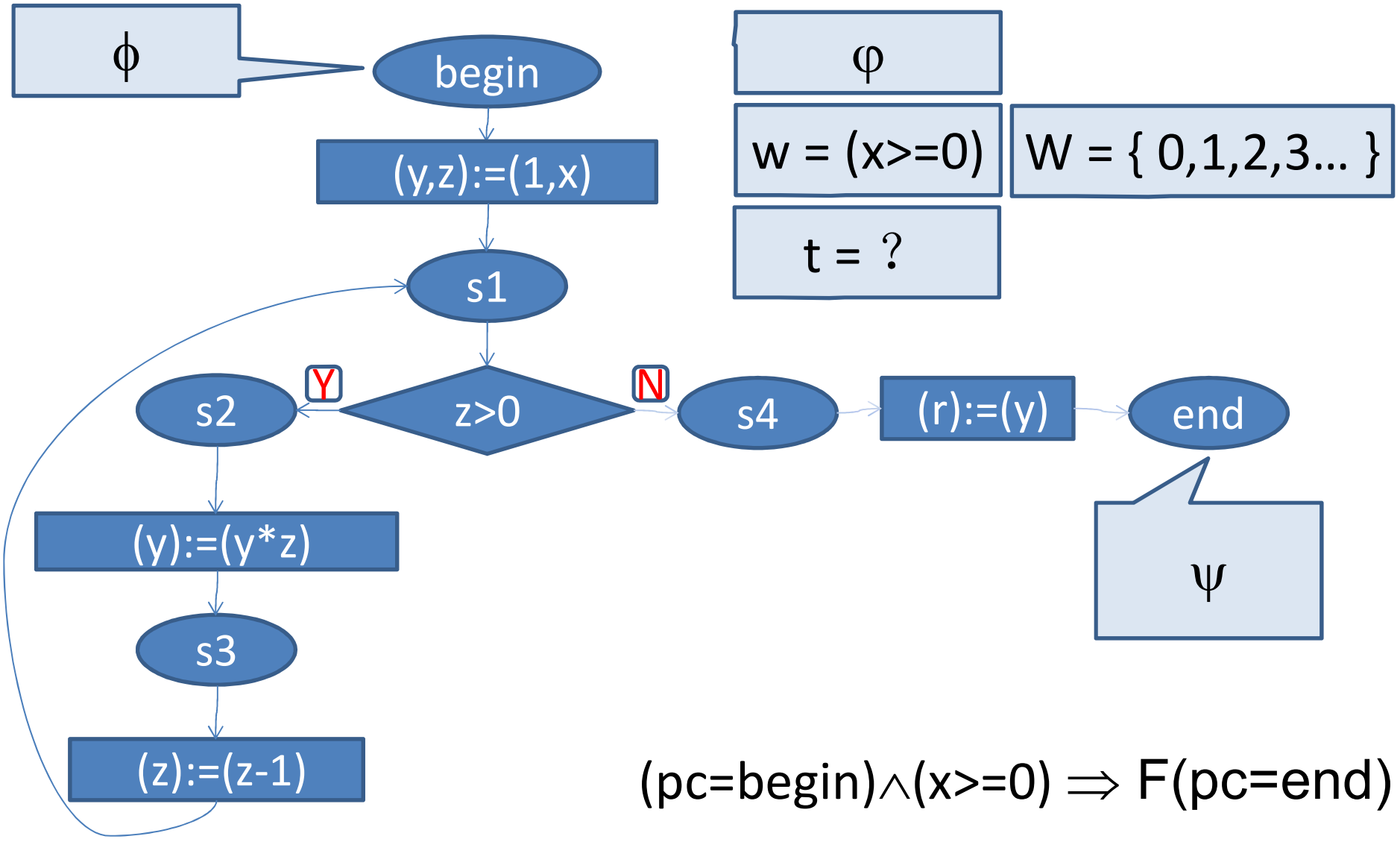


Ex: Termination and Partial Correctness




```
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;
```

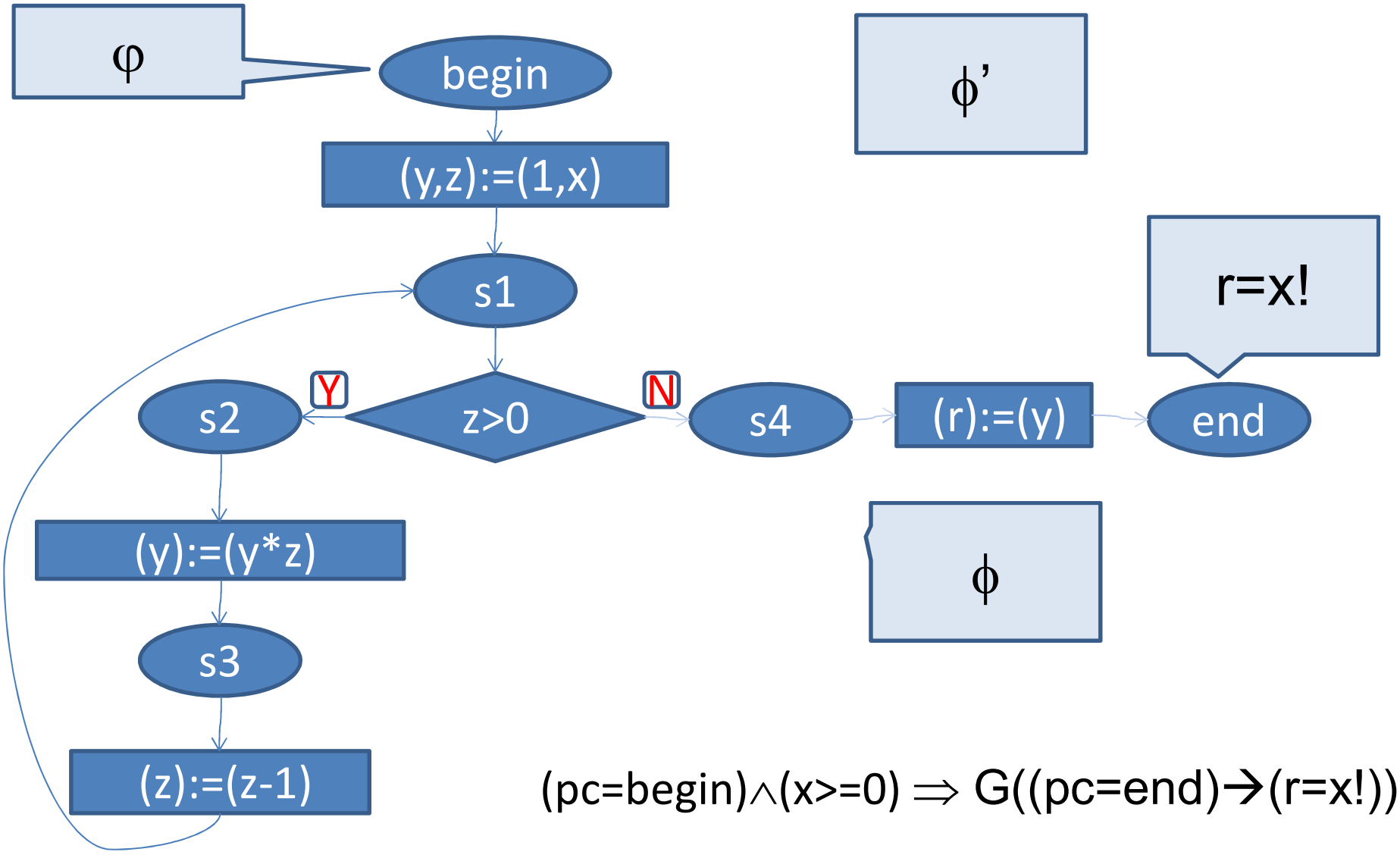
Example



$(pc=begin) \wedge (x>=0) \Rightarrow F(pc=end)$

$\phi \Rightarrow F\psi$

Example



$(pc=begin) \wedge (x>=0) \Rightarrow G((pc=end) \rightarrow (r=x!))$

$\varphi \Rightarrow G\ \phi$

Applications of FOLTL

FOLTL as a Specification Language

System Models: First Order Models (M)

System Specifications: Formulas of FOLTL (φ)

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 (φ)

Verification of correctness

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

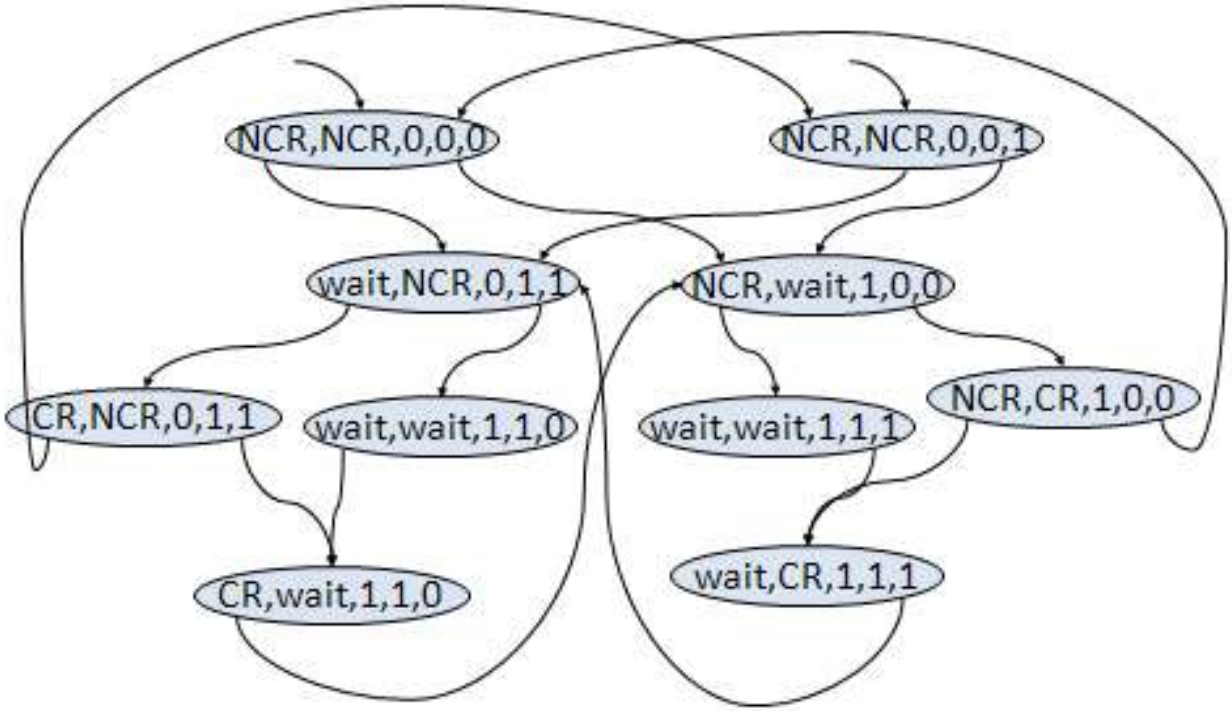
EX

(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 |= ((a=NCR ∨a=wait) U a=CR)

(b) M |= ((a=NCR ∨a=wait) U (a=CR or b=CR))

练习2

(a) 构造与公式 $(p \vee (q \ U \ r))$ 等价的自动机。
(b) 构造与公式 $(Xp \wedge (q \ R \ r))$ 等价的自动机。