

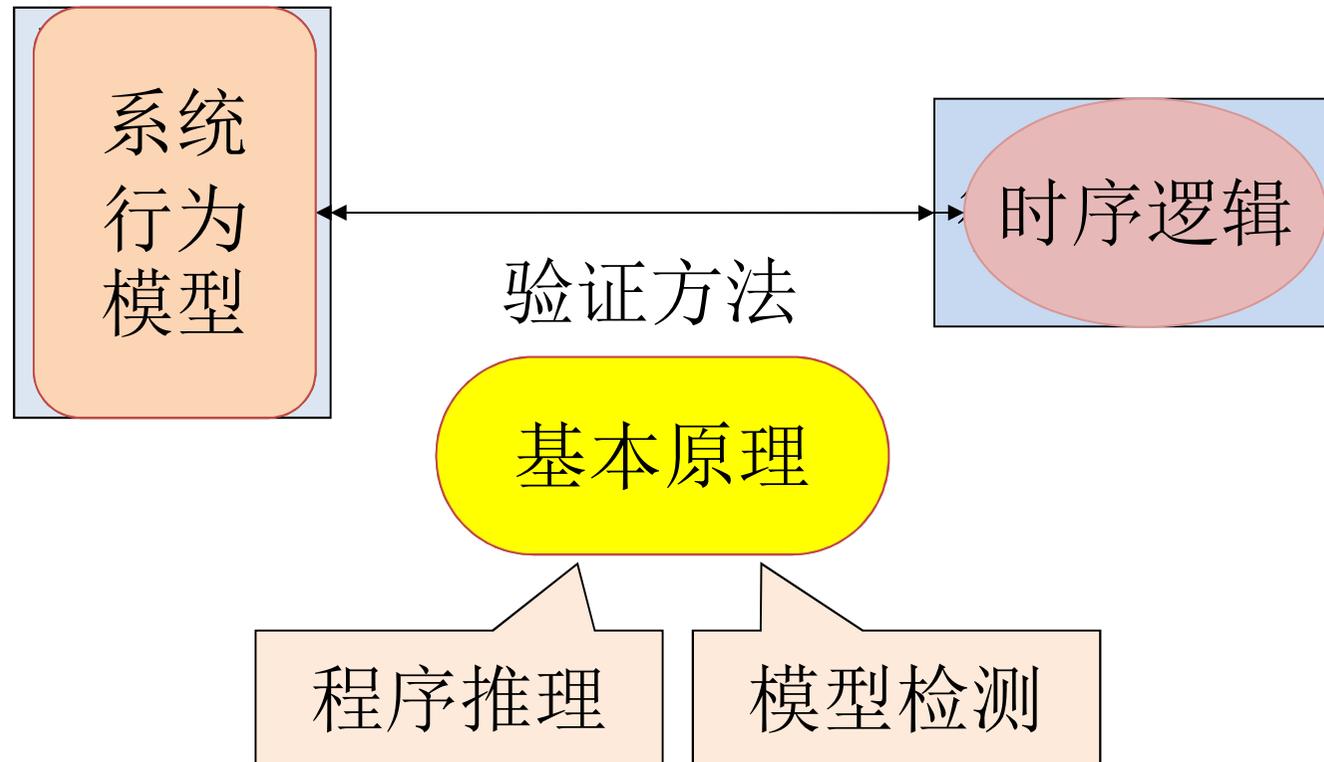
Branching Time Temporal Logics

中国科学院软件研究所
计算机科学国家重点实验室

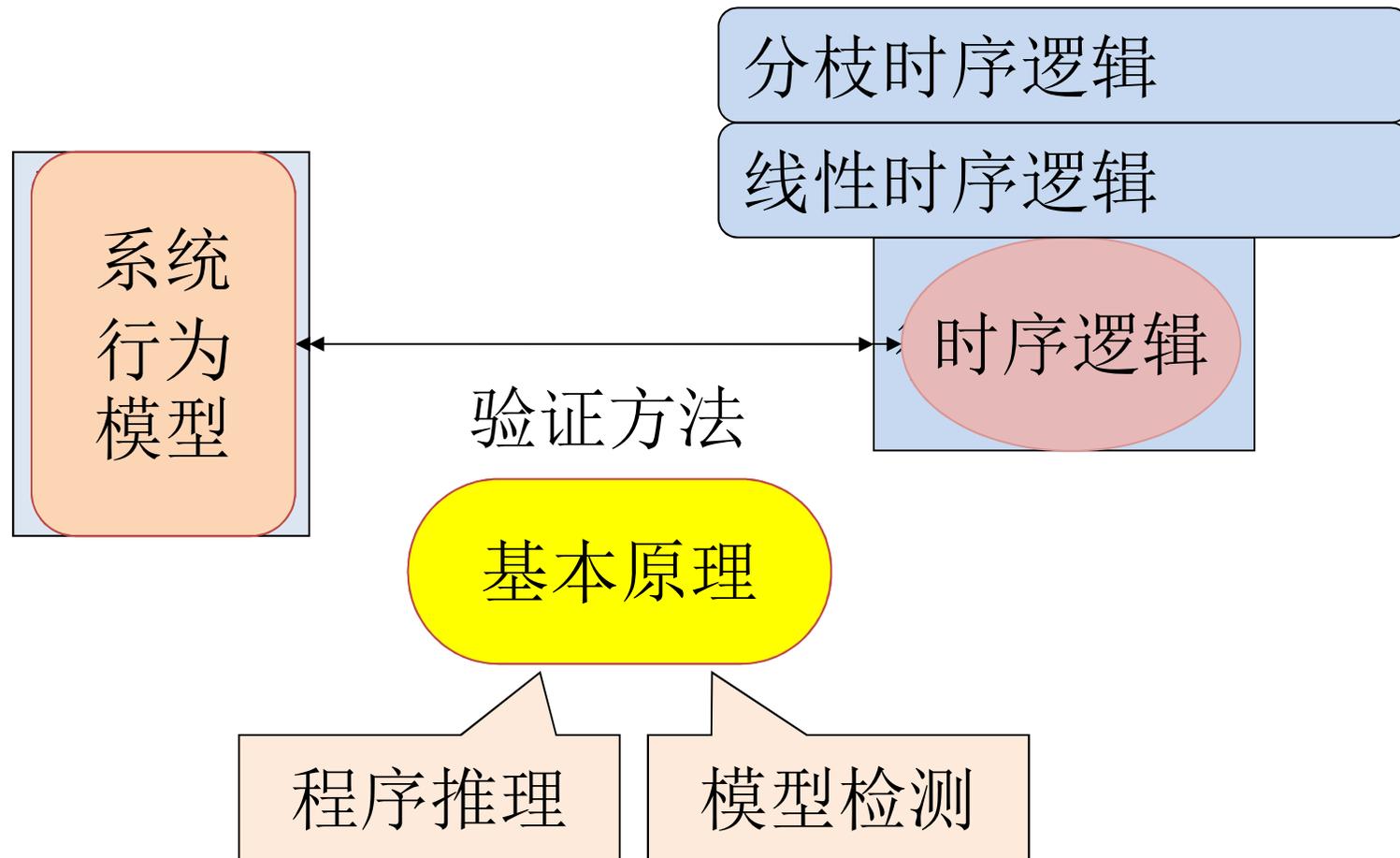
张文辉

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

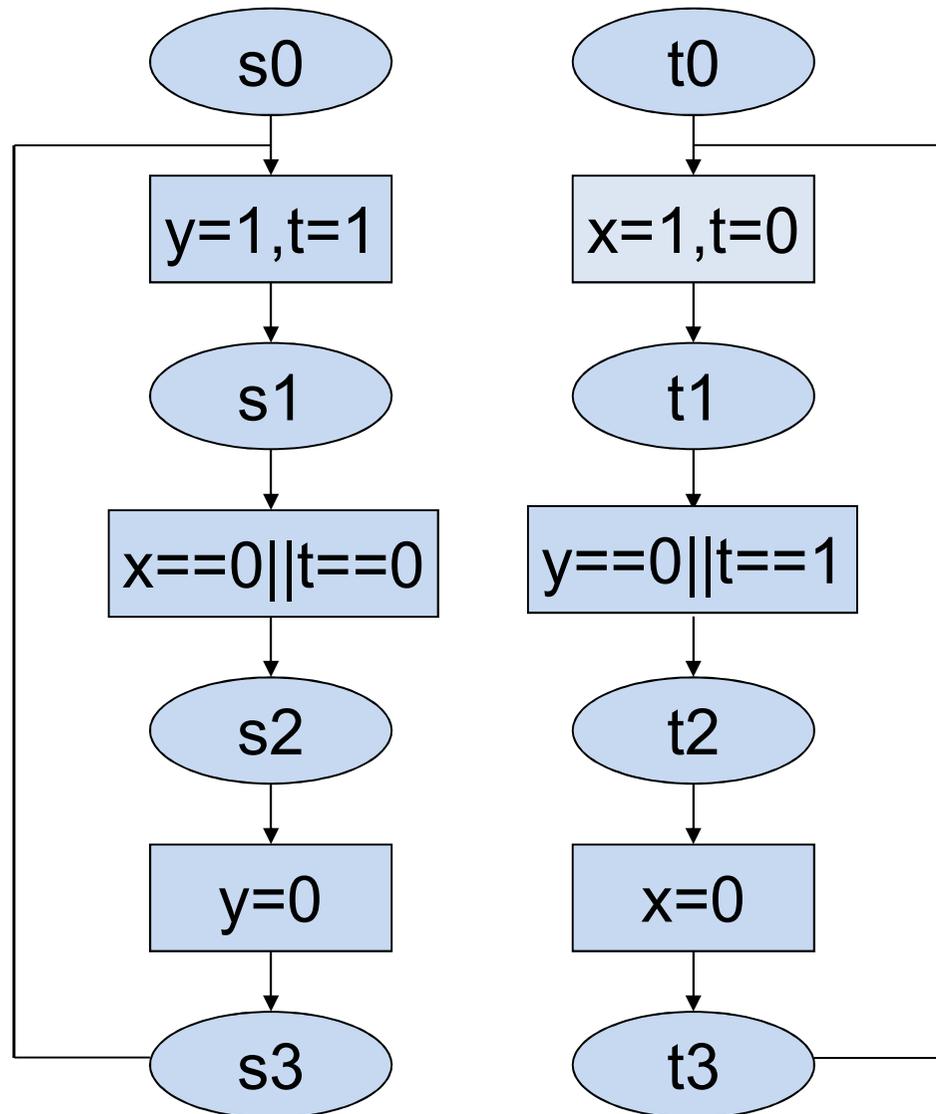
课程内容



课程内容



Example



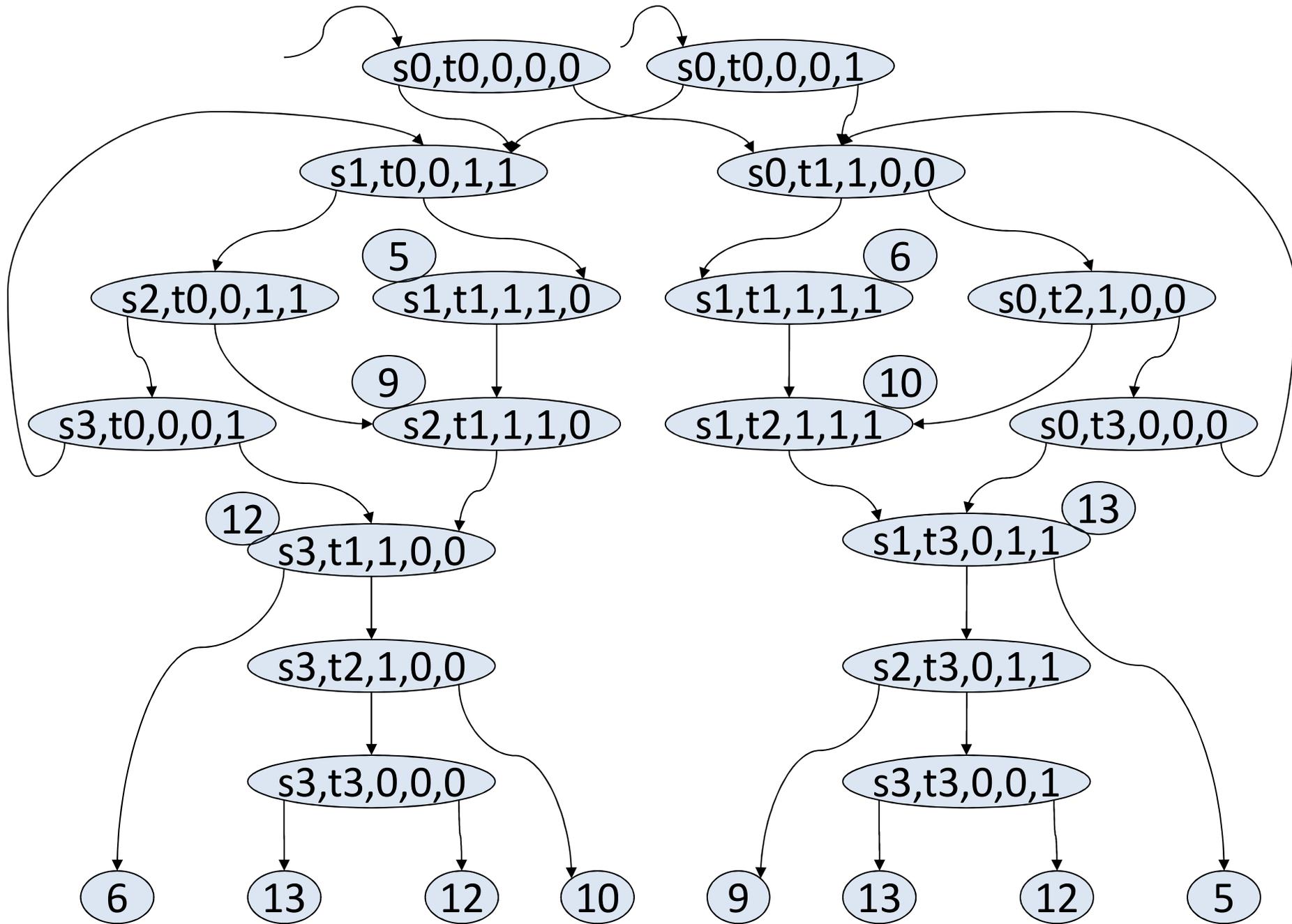
Initial States

s0

t0

x=0

y=0



Examples of Properties

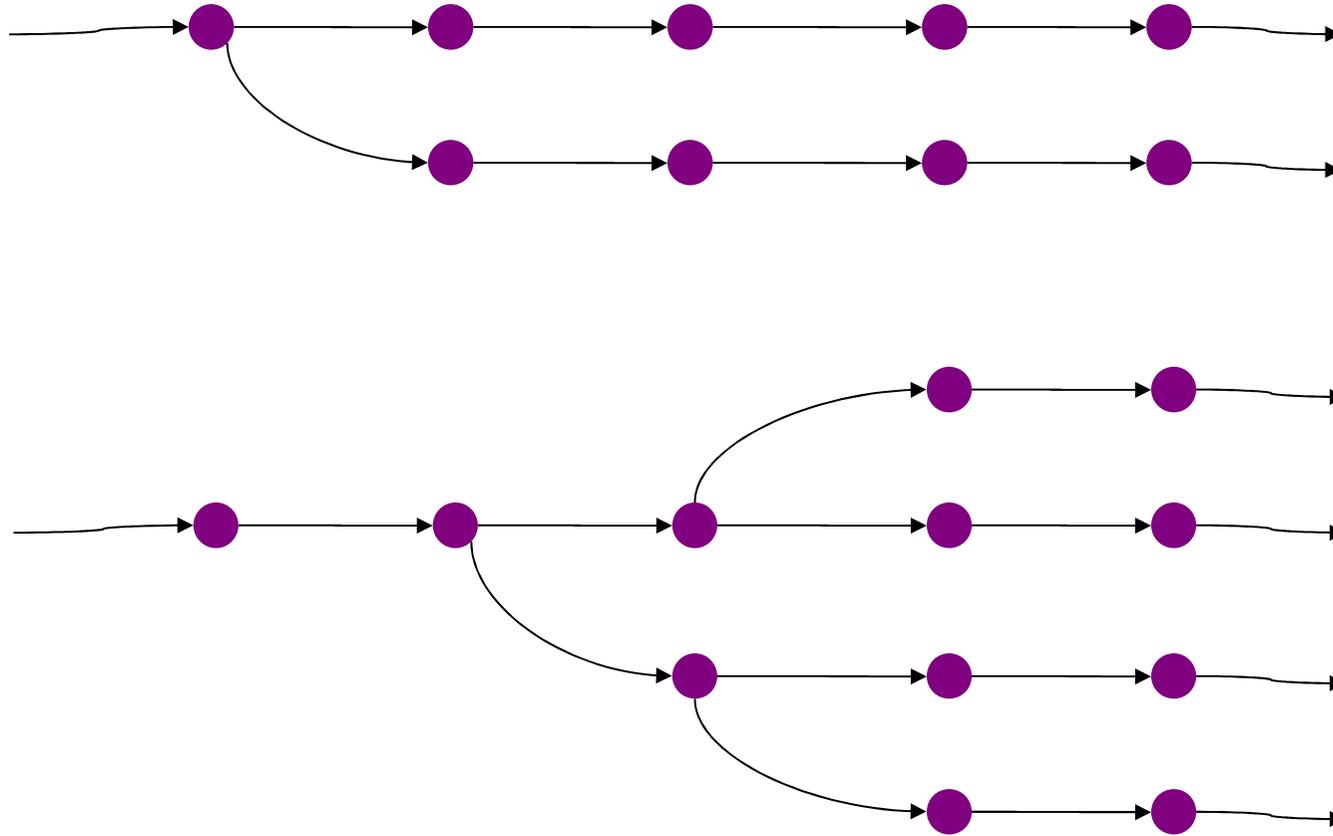
- Safety
- Inevitability
- Response
- Immediate Response
- Priority
- First Come – First Served
- Globally Exists a Branch such that $F(a=s^2)$

Contents

- Computation Tree Logic (CTL)
- Bounded Semantics of CTL
- Fixpoint Representation of CTL Formulas
- μ -Calculus

(I) Computation Tree Logic (CTL)

Tree Structures



Path Quantifiers: A, E

Examples of Properties

- Safety: $AG (\!(a=s2 \wedge b=t2)\!)$
- Inevitability $AF (a=s2 \vee b=t2)$
- Response $AG (a=s1 \rightarrow AF (a=s2))$
- Imm. Response $AG (a=s1 \rightarrow AX (a=s2))$
- Priority $AG (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow A(a=s2 \ R \ b \neq t2))$
- FCFS $AG (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow A(b \neq t2 \ U \ a=s2))$
- GE.. $AG (EF(a=s2))$

Syntax of CTL

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of CTL formulas is defined as follows.

$$\begin{aligned} \Phi ::= & p \quad | \quad \Phi \wedge \Phi \quad | \quad \Phi \vee \Phi \quad | \quad \neg \Phi \quad | \\ & AX \Phi \quad | \quad AG \Phi \quad | \quad AF \Phi \quad | \quad A(\Phi R \Phi) \quad | \quad A(\Phi U \Phi) \quad | \\ & EX \Phi \quad | \quad EG \Phi \quad | \quad EF \Phi \quad | \quad E(\Phi R \Phi) \quad | \quad E(\Phi U \Phi) \end{aligned}$$

Examples of Properties

- Safety: $AG (\!(a=s2 \wedge b=t2)\!)$
- Inevitability $AF (a=s2 \vee b=t2)$
- Response $AG (a=s1 \rightarrow AF (a=s2))$
- Imm. Response $AG (a=s1 \rightarrow AX (a=s2))$
- Priority $AG (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow A(a=s2 \ R \ b \neq t2))$
- FCFS $AG (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow A(b \neq t2 \ U \ a=s2))$
- GE.. $AG (EF(a=s2))$

Proposition Symbols

Let AP be the set of proposition symbols $\{p_0, p_1, \dots, p_{13}\}$ with the following meaning:

$p_0 \equiv (x = 0)$	$p_1 \equiv (x = 1)$
$p_2 \equiv (y = 0)$	$p_3 \equiv (y = 1)$
$p_4 \equiv (t = 0)$	$p_5 \equiv (t = 1)$
$p_{6+i} \equiv (a = s_i)$	$p_{10+i} \equiv (b = t_i)$

$$i \in \{0, 1, 2, 3\}$$

Examples of Properties

- Safety: $AG (\neg(p8 \wedge p12))$
- Inevitability $AF (p8 \vee p12)$
- Response $AG (p7 \rightarrow AF p8)$
- Imm. Response $AG (p7 \rightarrow AX p8)$
- Priority $AG (p7 \wedge \neg p11 \wedge \neg p12 \rightarrow A(p8 R \neg p12))$
- FCFS $AG (p7 \wedge \neg p11 \wedge \neg p12 \rightarrow A(\neg p12 U p8))$
- GE... $AG (EF (p8))$

Semantics

Kripke Structures

Let $K = \langle S, R, I, L \rangle$ be a Kripke structure.

- S : A finite set of states
- $R \subseteq S \times S$: A total transition relation
- $I \subseteq S$: A set of initial states
- $L: S \rightarrow 2^{AP}$ is a labeling function

Semantics: $M \models \phi$

A CTL formula may be interpreted on a Kripke structure.

(1) Define $M, s \models \phi$ for a state s

(2) Define $M \models \phi$ as follows:

$M \models \phi$ if $M, s \models \phi$ for every initial state s .

Semantics: $M, u \models \phi$

Definition

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

$M, u \models \neg\phi,$ if $M, u \not\models \phi$

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

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

$M, u \models A \psi,$ if for every path π of $u,$ ($M, \pi \models \psi$)

$M, u \models E \psi,$ if there is a path π of $u,$ ($M, \pi \models \psi$)

Semantics: $M, \pi \models \psi$

Definition

$M, \pi \models X \phi$, if $M, \pi_1 \models \phi$

$M, \pi \models F \phi$, if $\exists i \geq 0, (M, \pi_i \models \phi)$

$M, \pi \models G \phi$, if $\forall i \geq 0, (M, \pi_i \models \phi)$

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

$M, \pi \models \phi R \psi$, if $\forall i \geq 0, (\forall 0 \leq j < i, M, \pi_j \not\models \phi) \rightarrow M, \pi_i \models \psi$

Satisfiability and Validity

Satisfiability and Validity

Definition

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

Definition

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

Satisfiability and Validity Checking

The complexities of CTL satisfiability and validity checking are EXPTIME-complete.

Equivalences

Equivalences

Definition

A formula ϕ is equivalent to a formula ψ , if for every model M , $(M \models \phi \text{ iff } M \models \psi)$.

Examples of Equivalences

$$EX \phi \equiv \neg AX \neg \phi$$

$$E(\phi R \psi) \equiv E(\psi U (\phi \wedge \psi)) \vee EG \psi$$

These equivalences can be proved by applying the semantics.

Dual Operators and the Negation Normal Form (NNF)

Dual Operators

$EX \phi$	$\equiv \neg AX \neg \phi$
$EG \phi$	$\equiv \neg AF \neg \phi$
$E(\phi R \psi)$	$\equiv \neg A(\neg \phi U \neg \psi)$
$EF \phi$	$\equiv \neg AG \neg \phi$
$E(\phi U \psi)$	$\equiv \neg A(\neg \phi R \neg \psi)$

NNF

Definition

A formula is in NNF, if the negation symbol is only applied to atomic formulas.

Every formula is equivalent to a formula in NNF.

Recursive Equations

Operators R and U

$$E(\phi R \psi) \equiv \psi \wedge (\phi \vee EX E(\phi R \psi))$$

$$E(\phi U \psi) \equiv \psi \vee (\phi \wedge EX E(\phi U \psi))$$

$$A(\phi R \psi) \equiv \psi \wedge (\phi \vee AX A(\phi R \psi))$$

$$A(\phi U \psi) \equiv \psi \vee (\phi \wedge AX A(\phi U \psi))$$

Operators G and F

Let $p_0 \in AP$ be given.

Let \perp denote $(p_0 \wedge \neg p_0)$

Then

$$EG \psi \equiv E(\perp R \psi)$$

$$EF \psi \equiv E(\neg \perp U \psi)$$

Minimal Complete Set of Temporal Operators

Minimal Complete Set

EX,EF,EG,ER,EU

ER is expressible by EU and EG

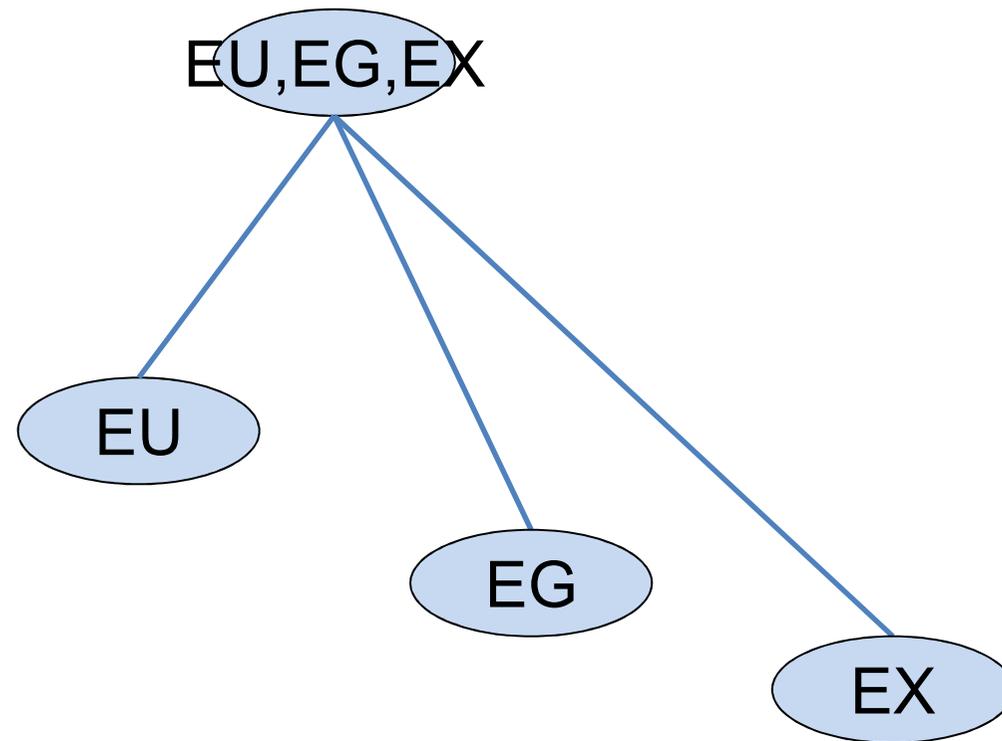
EF is expressible by EU

Then {EX,EU,EG} is a complete set.

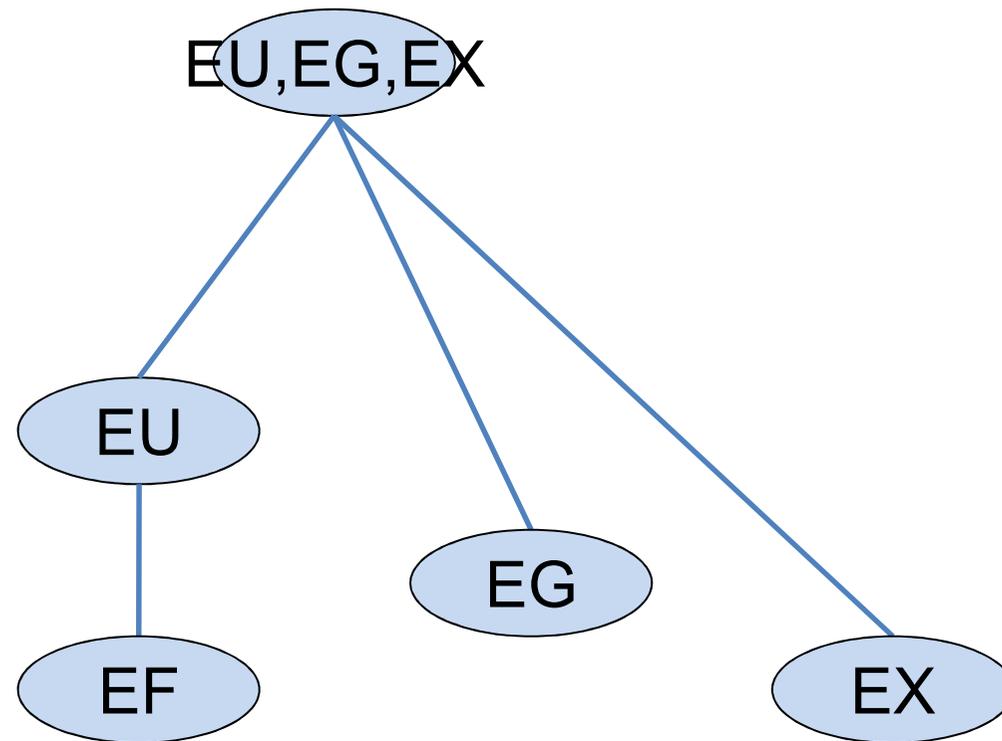
{EX,EU,EG} is also a minimal complete set.

Expressivity

Expressivity of Subsets of CTL



Expressivity of Subsets of CTL



CTL Proof System

Proof System for {EX,EU,EG,EF,AX,AU,AG,AF}

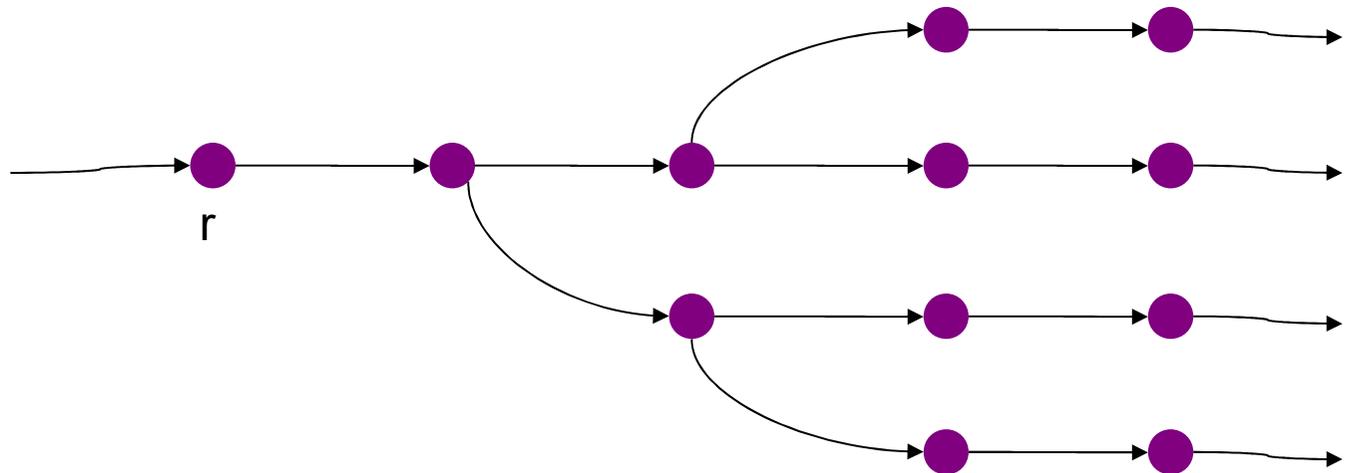
- Axioms for temporal logics formulas
- Proof rules for temporal formulas
- Propositional proof system

Axioms for Temporal Logics Formulas

- $EFp \leftrightarrow E(\neg\perp \cup p)$
- $AGp \leftrightarrow \neg EF\neg p$
- $AFp \leftrightarrow A(\neg\perp \cup p)$
- $EGp \leftrightarrow \neg AF\neg p$
- $EX(p \vee q) \leftrightarrow EXp \vee EXq$
- $AXp \leftrightarrow \neg EX\neg p$
- $E(p \cup q) \leftrightarrow (q \vee (p \wedge EXE(p \cup q)))$
- $A(p \cup q) \leftrightarrow (q \vee (p \wedge AXA(p \cup q)))$
- $EX\neg\perp \wedge AX\neg\perp$

Axioms for Temporal Logics Formulas

- $AG(r \rightarrow (\neg q \wedge EXr)) \rightarrow (r \rightarrow \neg A(p \cup q))$
- $AG(r \rightarrow (\neg q \wedge EXr)) \rightarrow (r \rightarrow \neg AFq)$
- $AG(r \rightarrow (\neg q \wedge (p \rightarrow AXr))) \rightarrow (r \rightarrow \neg E(p \cup q))$
- $AG(r \rightarrow (\neg q \wedge AXr)) \rightarrow (r \rightarrow \neg EFq)$
- $AG(p \rightarrow q) \rightarrow (EXp \rightarrow EXq)$



Proof Rule (Generalization)

$$\frac{\vdash p}{\vdash AGp}$$

Propositional proof system

- Axioms: all tautologies are axioms
- Proof Rule (MP):

$$\frac{\begin{array}{cc} \vdash p \rightarrow q & \vdash p \end{array}}{\vdash q}$$

Proof System

The proof system is sound and complete.

Applications of CTL

CTL as a Specification Language

System Models: Kripke Structures (K)

System Specifications: Formulas of CTL (φ)

Verification of correctness

Solving the model checking problem: $K \models \varphi$

Model Checking

Model Checking

Definition

Given a model K and a formula ϕ .

The model checking problem is the problem of checking whether $K \models \phi$ holds.

Model Checking

The complexity of model checking is P-complete.



On CTL*

The set Φ of CTL* formulas is defined as follows.

$$\begin{aligned} \Phi ::= & p \quad | \quad \Phi \wedge \Phi \quad | \quad \Phi \vee \Phi \quad | \quad \neg \Phi \quad | \\ & X \Phi \quad | \quad G \Phi \quad | \quad F \Phi \quad | \quad (\Phi R \Phi) \quad | \quad (\Phi U \Phi) \quad | \\ & E \Phi \quad | \quad A \Phi \end{aligned}$$

CTL: every path quantifier of $\{E, A\}$

must be followed by one of X, G, F, R, U

CTL* is more expressive than CTL

(II) CTL限界语义

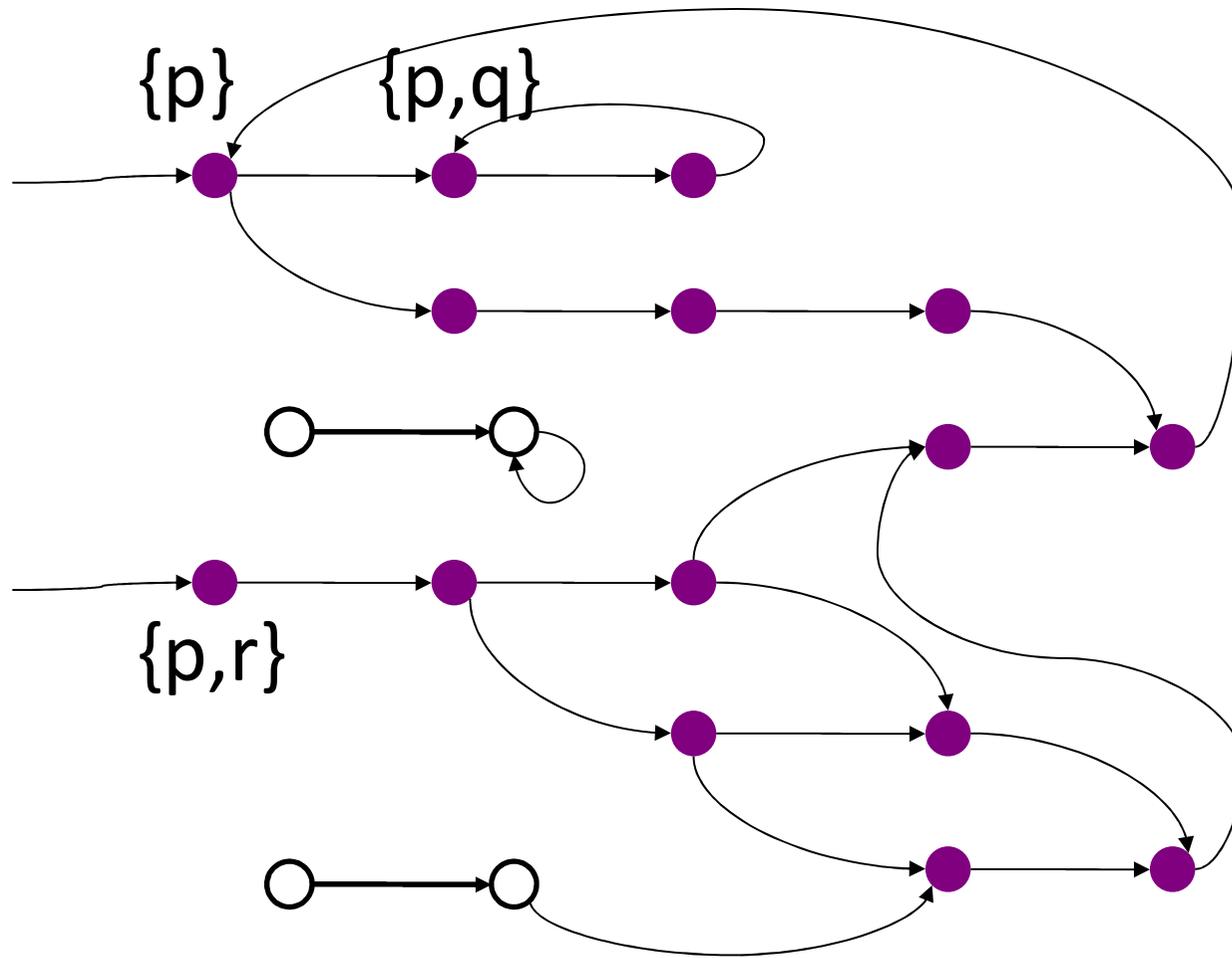
CTL语义

$$M \models \varphi$$

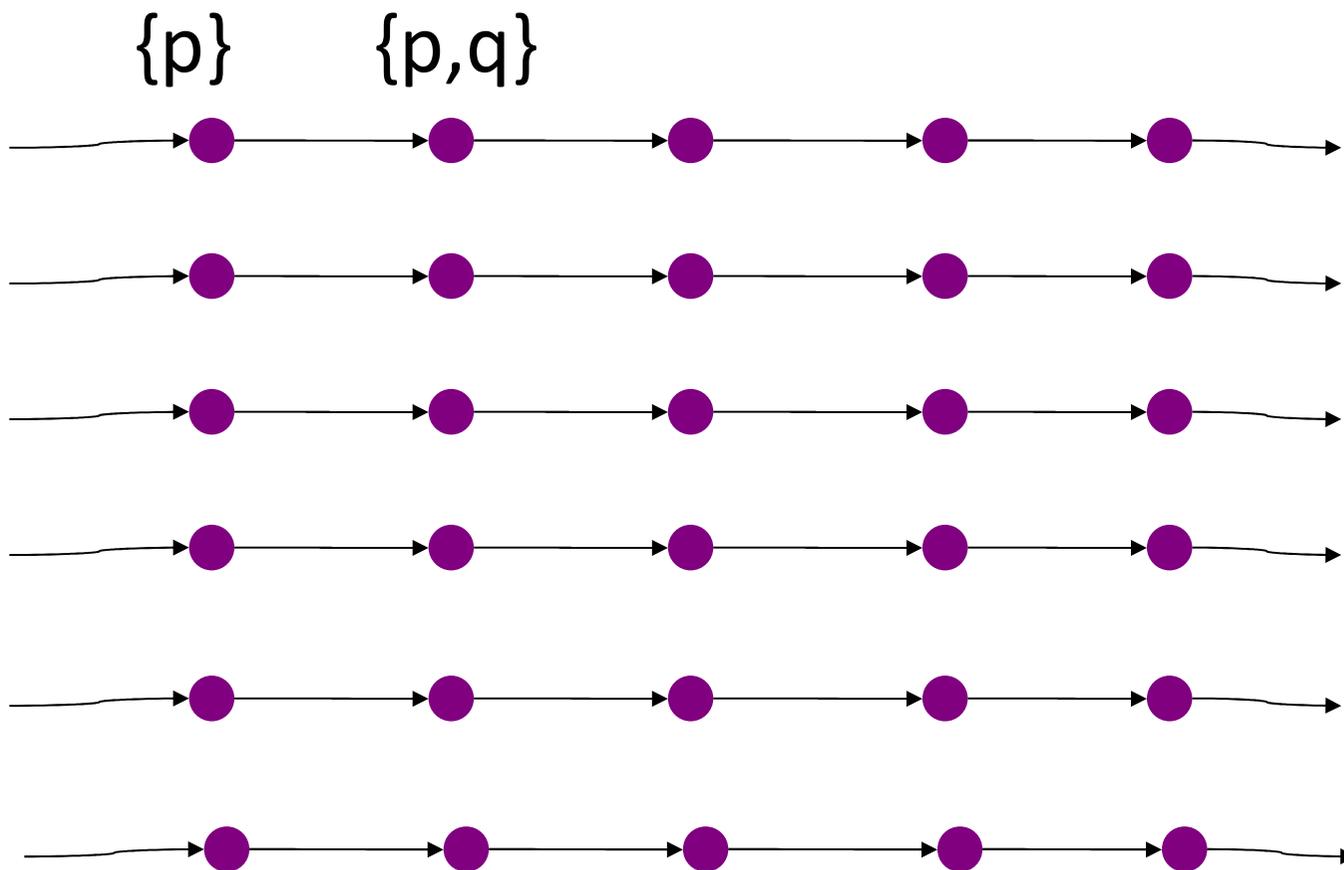
语义上牵涉无穷路径

考虑有穷路径

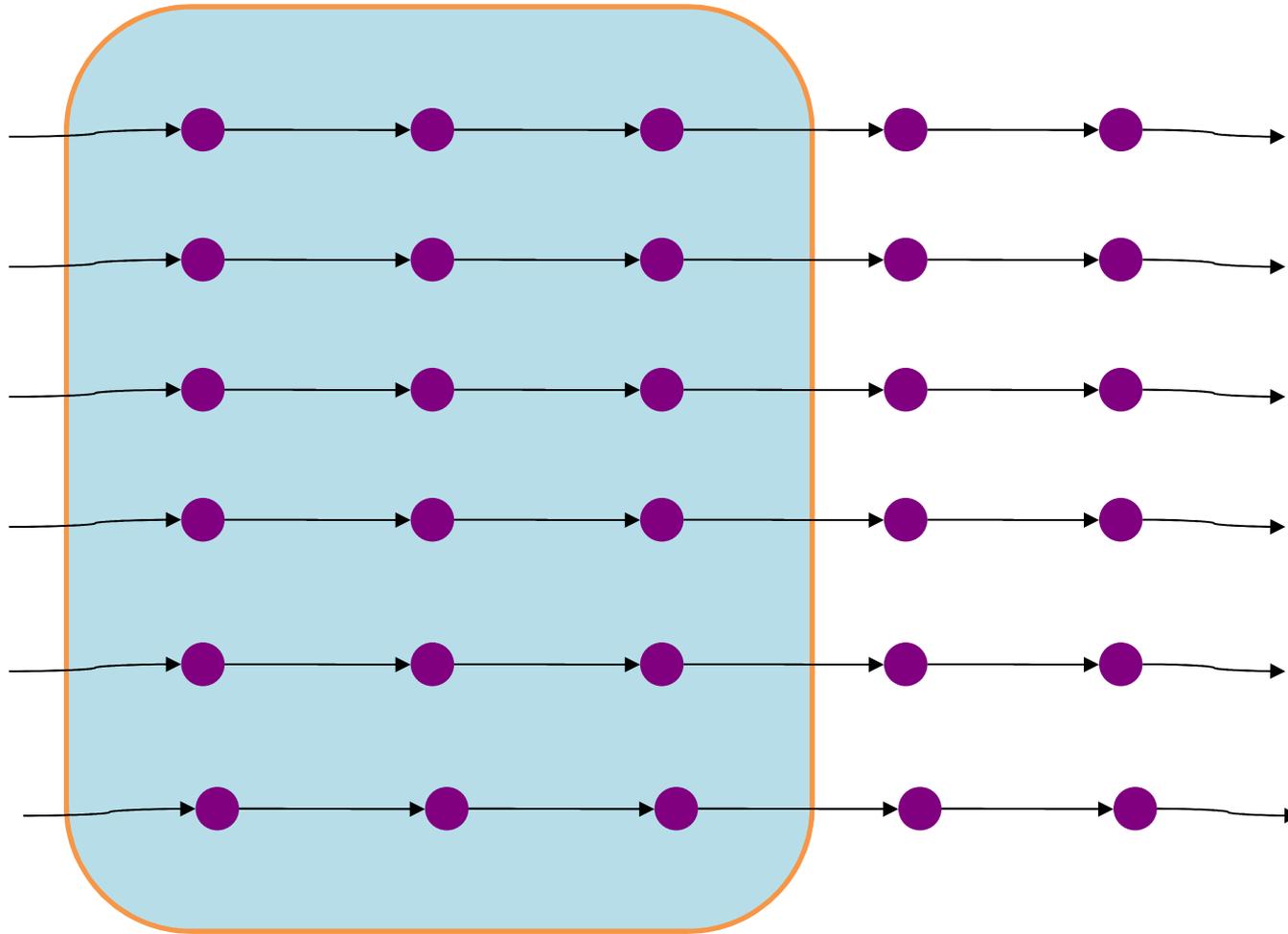
Kripke 结构



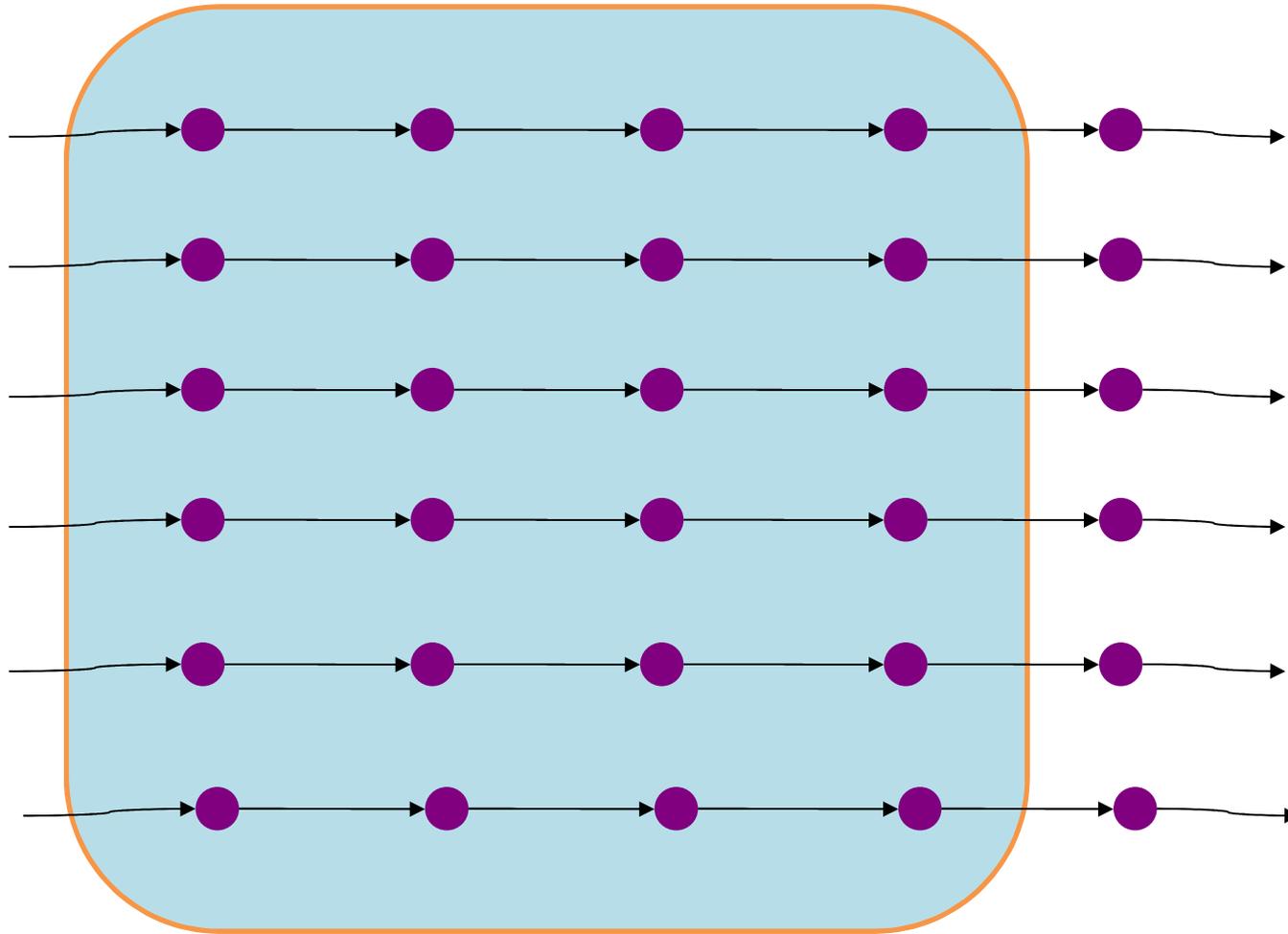
无穷路径



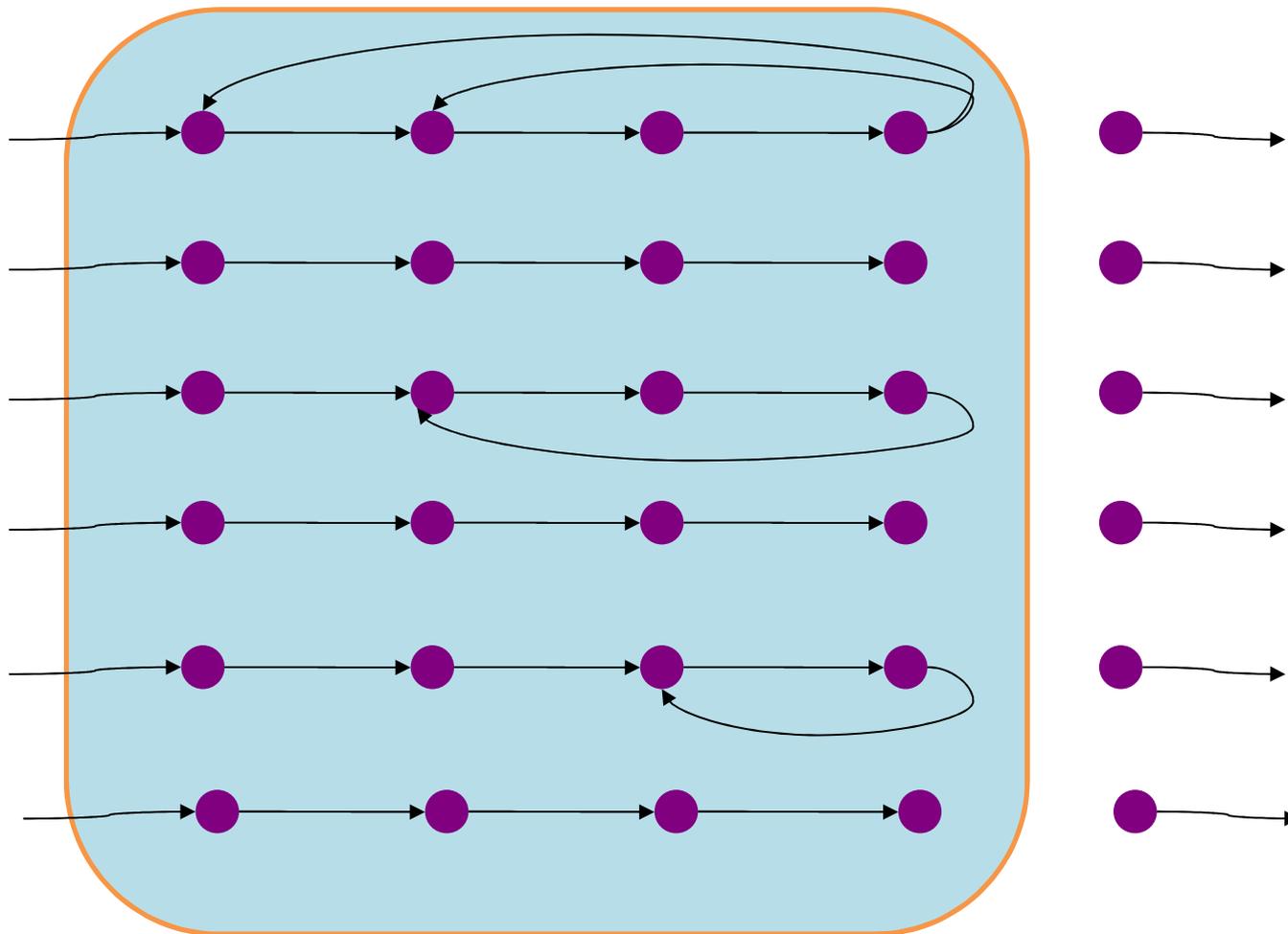
有穷路径



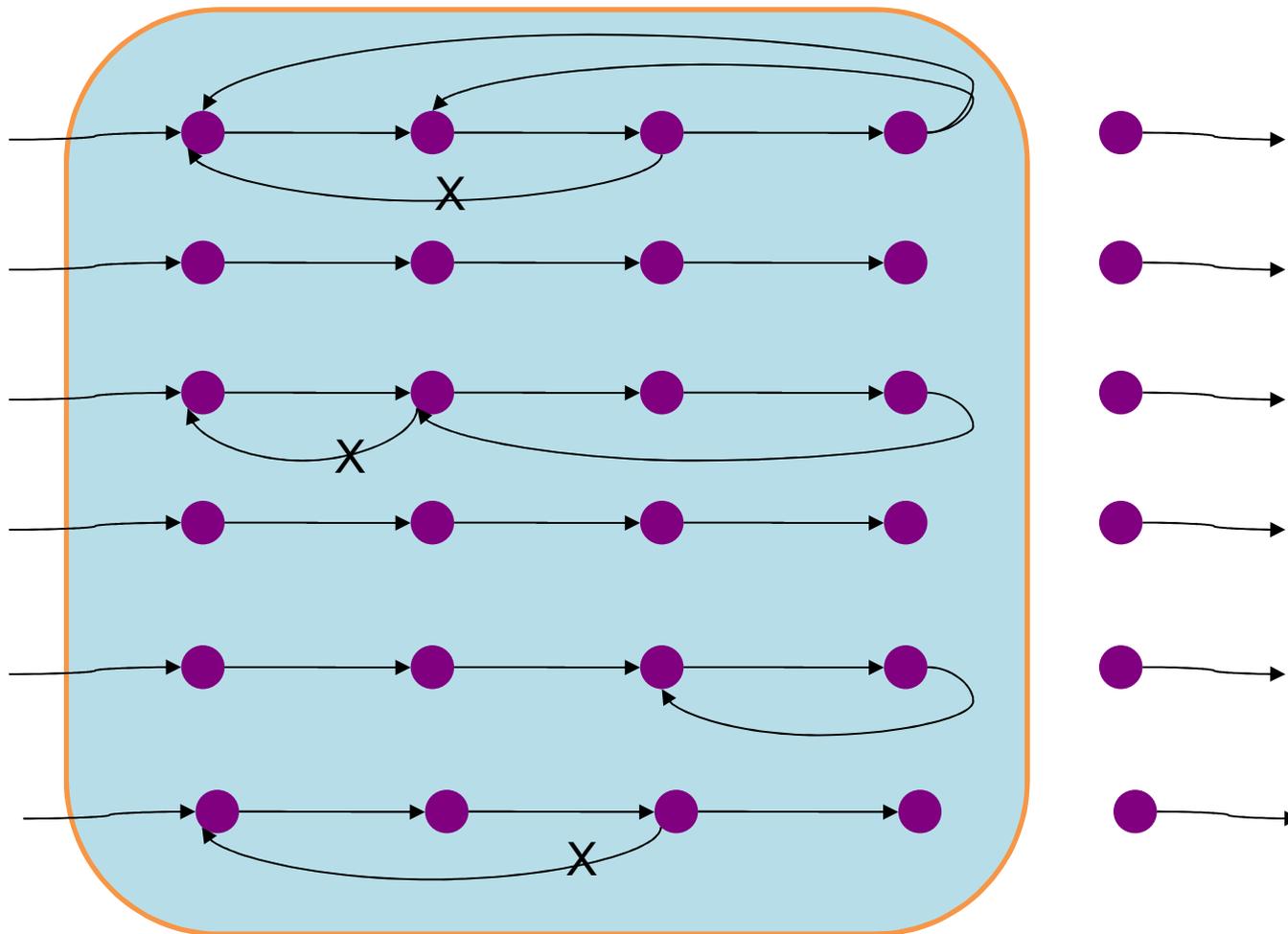
有穷路径



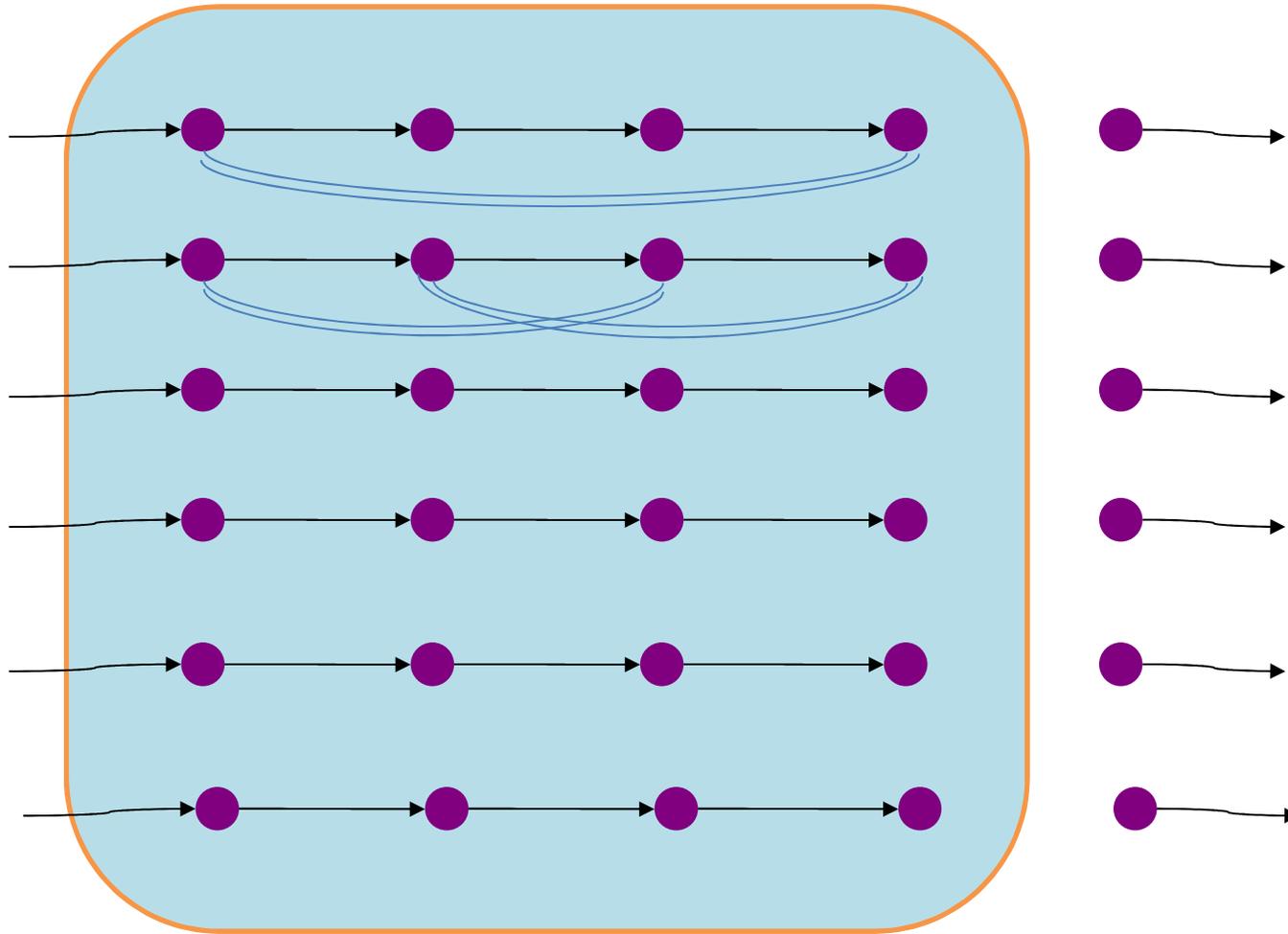
有穷路径(LTL限界语义)



有穷路径(LTL限界语义)



有穷路径



CTL

考虑NNF公式:

$$\begin{aligned} \Phi ::= & p \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg p \mid \\ & AX \Phi \mid A(\Phi R \Phi) \mid A(\Phi U \Phi) \mid \\ & EX \Phi \mid E(\Phi R \Phi) \mid E(\Phi U \Phi) \end{aligned}$$

语义: $M, u \models \phi$

$M, u \models p,$	if $p \in AP$ and $p \in L(u)$
$M, u \models \neg\phi,$	if $M, u \not\models \phi$
$M, u \models \phi \vee \psi,$	if $M, u \models \phi$ or $M, u \models \psi$
$M, u \models \phi \wedge \psi,$	if $M, u \models \phi$ and $M, u \models \psi$
$M, u \models A \psi,$	if for every path π of u , $(M, \pi \models \psi)$
$M, u \models E \psi,$	if there is a path π of u , $(M, \pi \models \psi)$
$M, \pi \models X \phi,$	if $M, \pi_1 \models \phi$
$M, \pi \models \phi U \psi,$	if $\exists i \geq 0, M, \pi_i \models \psi$ and $\forall j < i, M, \pi_j \models \phi$
$M, \pi \models \phi R \psi,$	if $\forall i \geq 0, (\forall j < i, M, \pi_j \not\models \phi) \rightarrow M, \pi_i \models \psi$

语义: F,G

$M, \pi \models F\psi,$ if $\exists i \geq 0, M, \pi_i \models \psi$

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

限界模型

k-path: 长度为k+1的路径

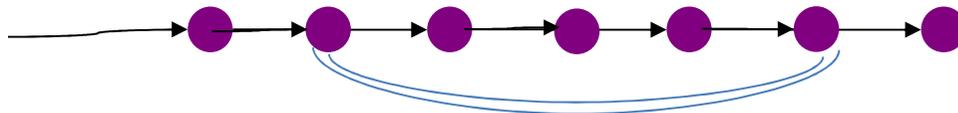
$$M = (S, R, I, L)$$

$$M_k = (S, Ph_k, I, L)$$

设 π 为k路径。

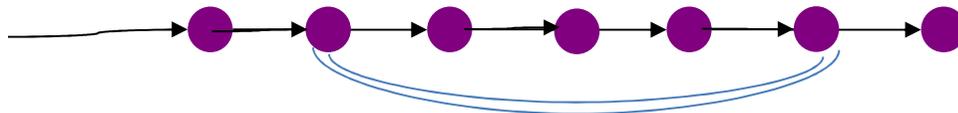
$rs(\pi)$:

路径 π 中有相同状态



限界语义: $M, u \models_k \phi$

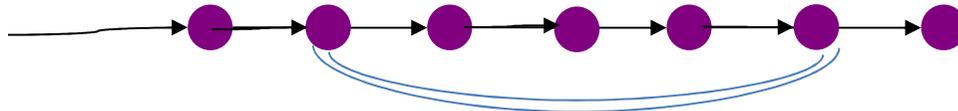
$M, u \models_k p,$	if $p \in AP$ and $p \in L(u)$
$M, u \models_k \neg p,$	if $p \in AP$ and $p \notin L(u)$
$M, u \models_k \phi \vee \psi,$	if $M, u \models_k \phi$ or $M, u \models_k \psi$
$M, u \models_k \phi \wedge \psi,$	if $M, u \models_k \phi$ and $M, u \models_k \psi$
$M, u \models_k A \psi,$	if for every k -path π of u , $(M, \pi \models_k \psi)$
$M, u \models_k E \psi,$	if there is a k -path π of u , $(M, \pi \models_k \psi)$
$M, \pi \models_k X \phi,$	if $k \geq 1$ and $M, \pi_1 \models_k \phi$
$M, \pi \models_k \phi U \psi,$	if $\exists i \leq k, M, \pi_i \models_k \psi$ and $\forall j < i, M, \pi_j \models_k \phi$
$M, \pi \models_k \phi R \psi,$	if $\forall i \leq k, (\forall j < i, M, \pi_j \not\models_k \phi) \rightarrow M, \pi_i \models_k \psi$ and $(\forall i \leq k. (M, \pi_i \not\models_k \phi)) \rightarrow rs(\pi)$



限界语义: F,G

$M, \pi \models_k F\psi,$ if $\exists i \leq k, M, \pi_i \models_k \psi$

$M, \pi \models_k G\psi,$ if $\forall i \leq k, (M, \pi_i \models_k \psi)$ and $rs(\pi)$



限界语义: $M \models_k \phi$

Definition

$M \models_k \phi$ if $M, u \models_k \phi$ for every initial state u .

Soundness

For every $i \geq 0$, if $M \models_i \phi$, then $M \models \phi$.

Completeness

If $M \models \phi$, then there is an $i \geq 0$ such that $M \models_i \phi$.

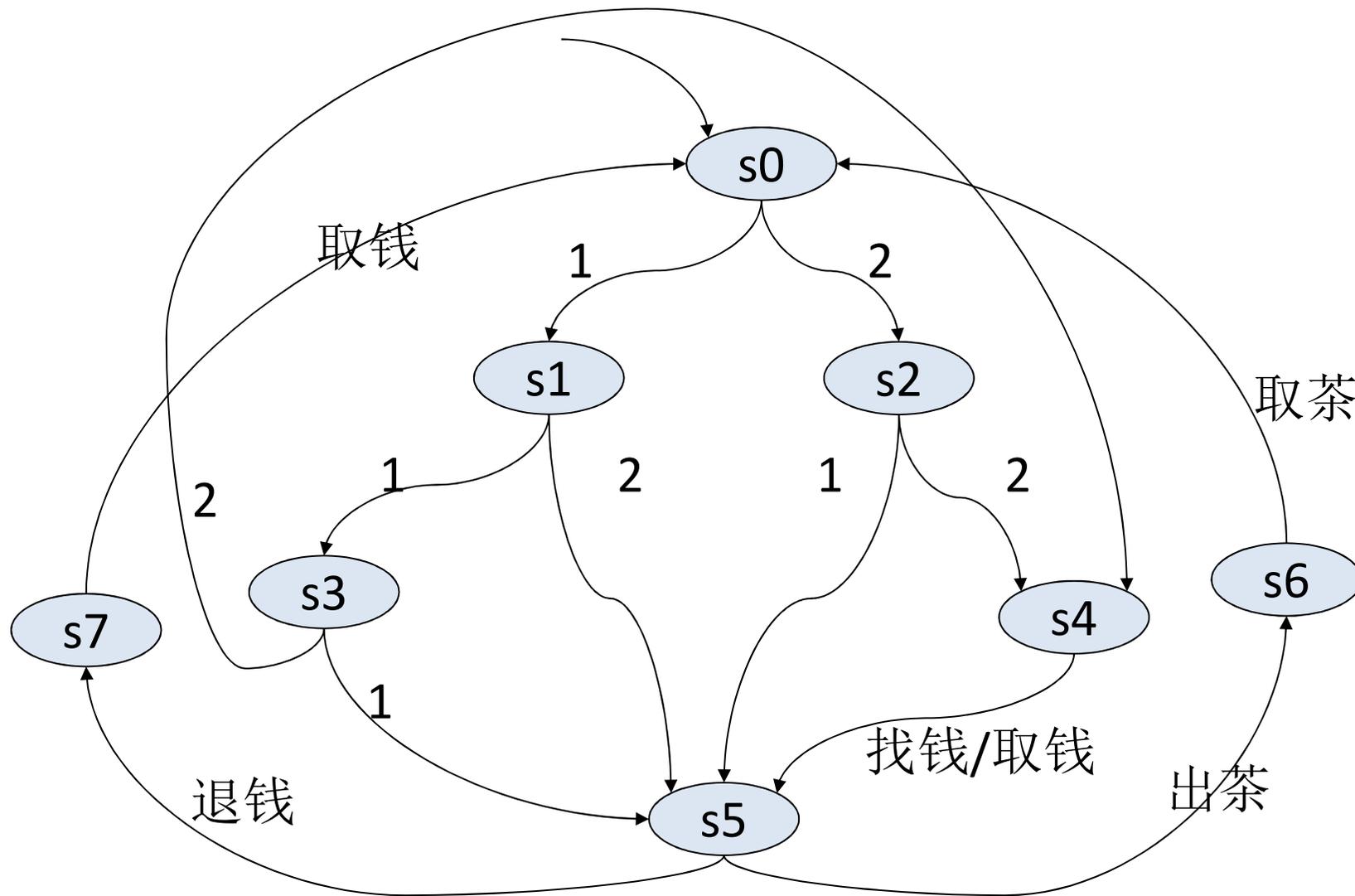
限界正确性检查

(Bounded Correctness Checking)

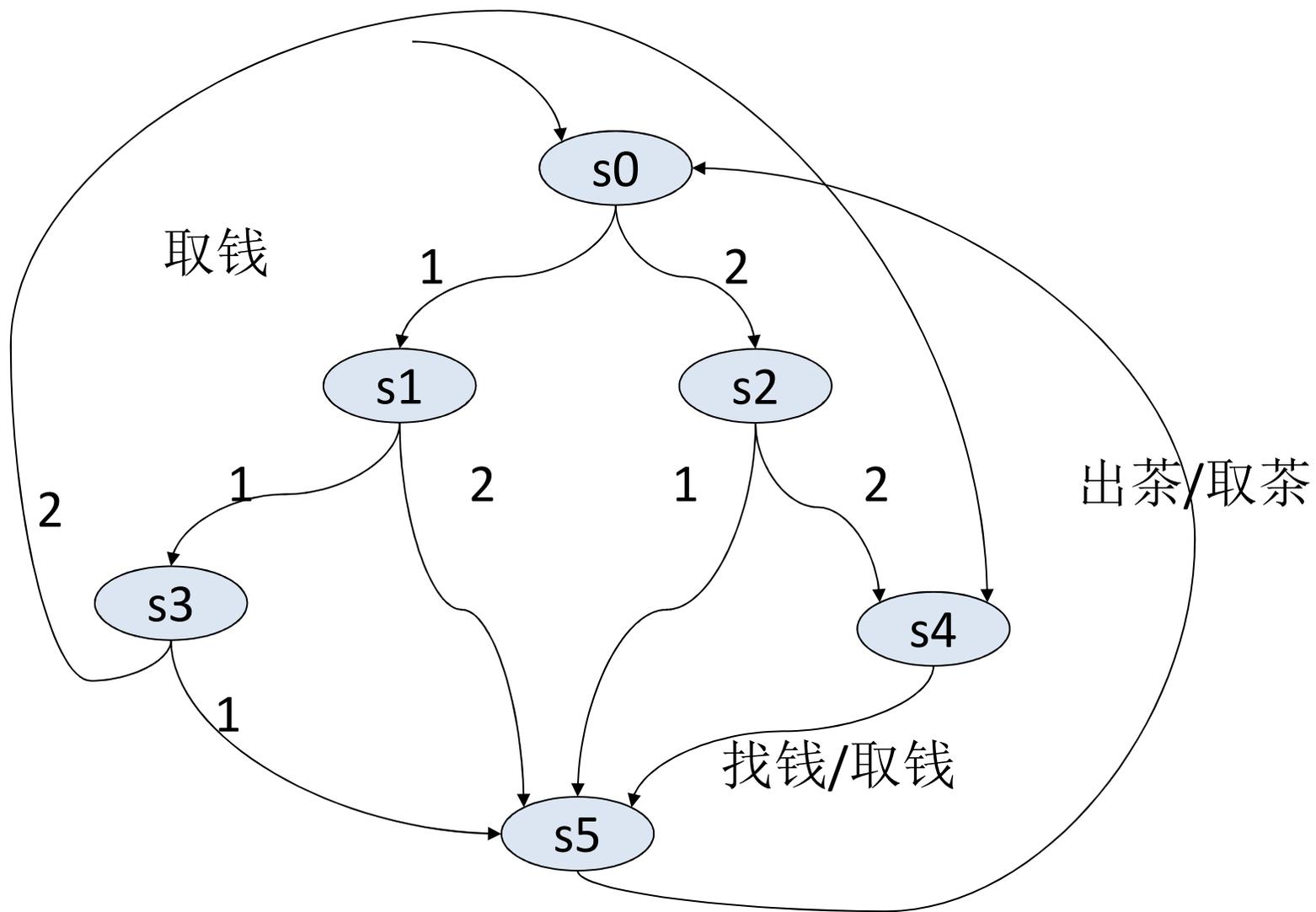
1. $k=0$;
2. if $M \models_k \varphi$, then report $M \models \varphi$;
3. if $M, s \models_k \neg \varphi$ for some $s \in I$, then report $M \not\models \varphi$;
4. $k=k+1$; goto step 2;

例子 

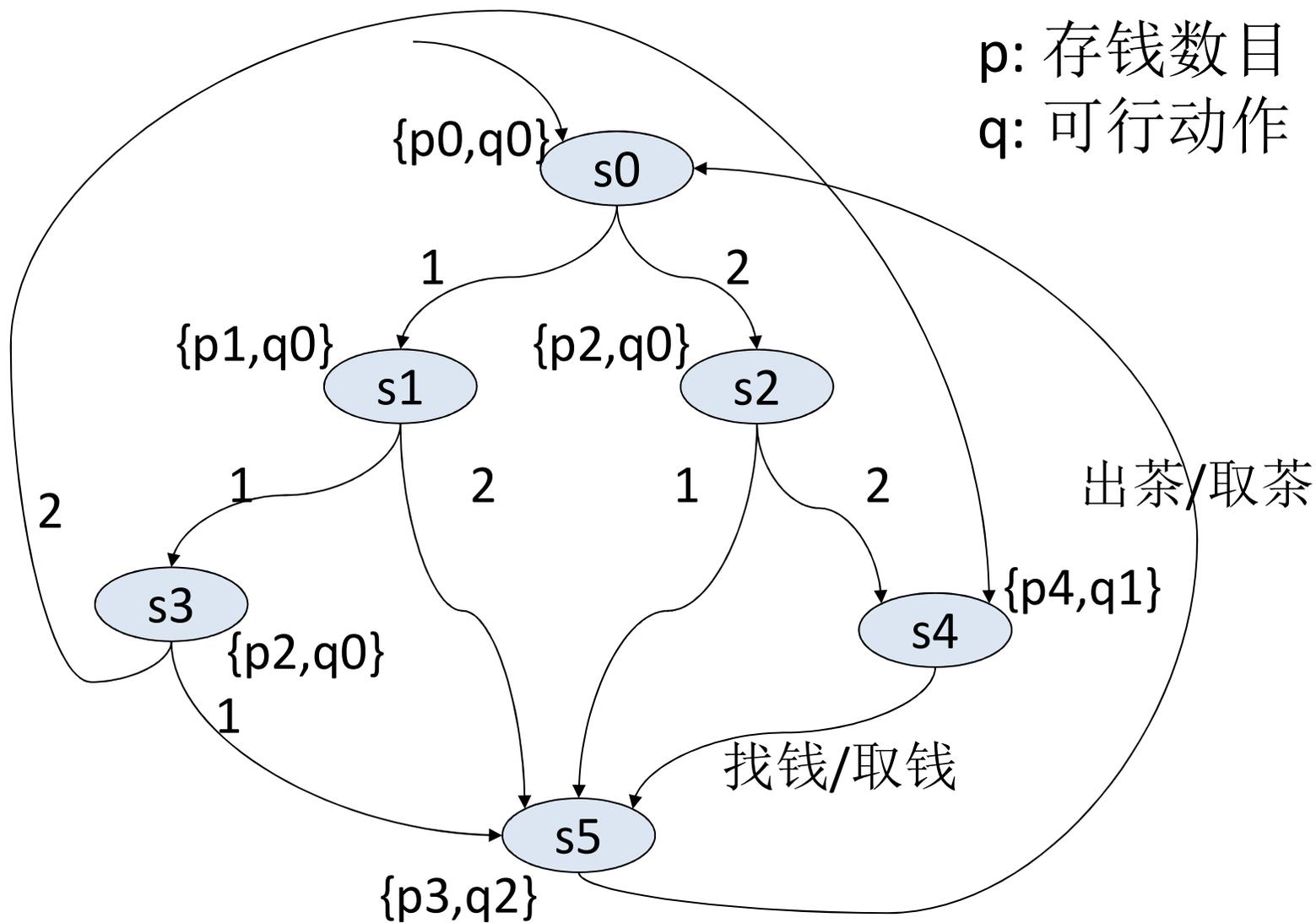
例子：自动售茶机模型



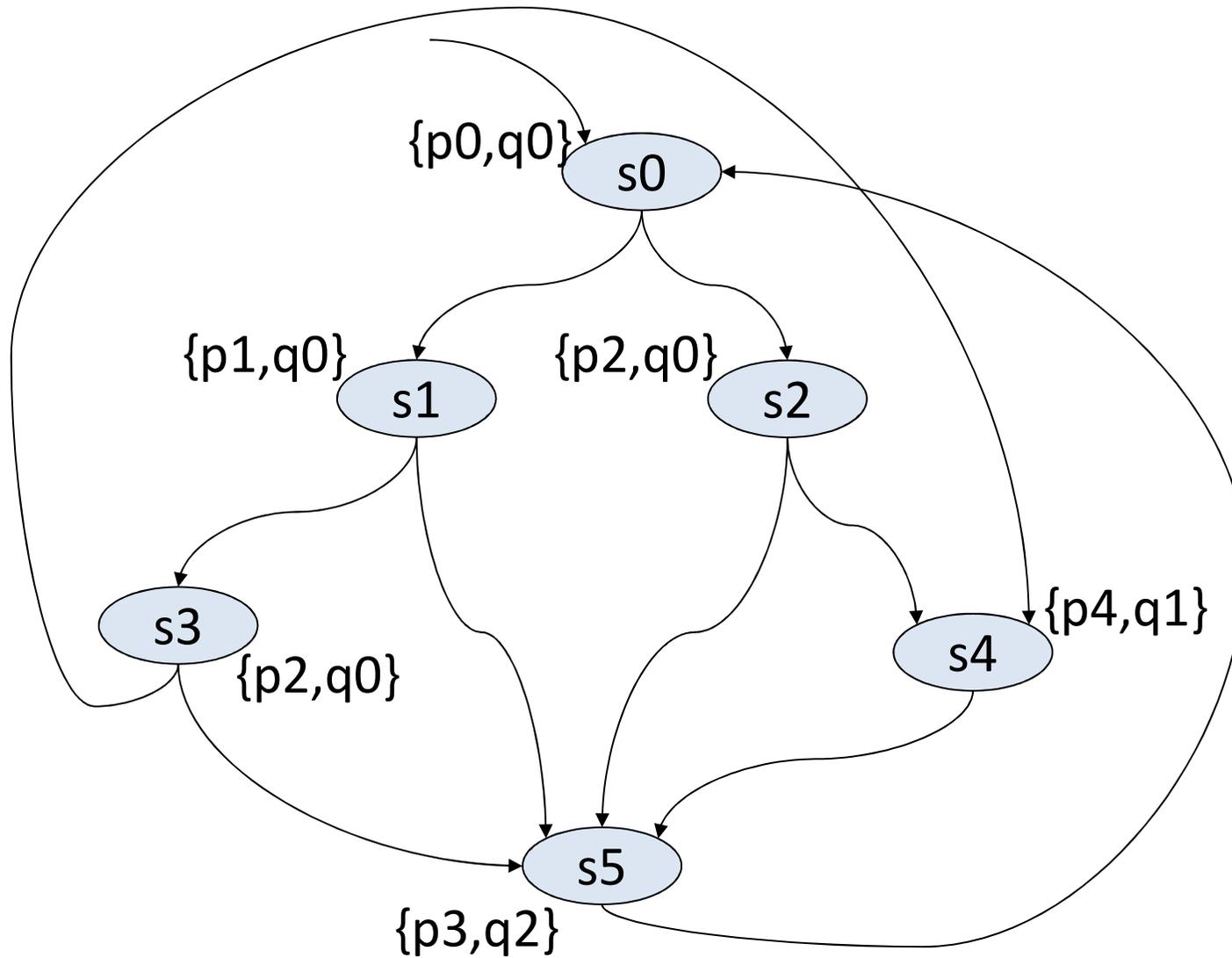
简化自动售茶机模型



简化自动售茶机模型



自动售茶机模型(标号Kripke结构)



例子

设M为简化自动售茶机模型。

用限界语义验证M是否满足 $E(q_0 \cup q_2)$ 和 $AG(q_0 \vee q_2)$ 。

分别给出最小可以确定以上公式是否满足的界。

$E(q_0 \cup q_2)$ vs $A(\neg q_0 \wedge \neg q_2)$

- Ph_0 : 我们有
- s_0 $M, s_0 \ s_1 \ s_5 \models_2 (q_0 \cup q_2)$
- $s_1/s_2/s_3/...$
- Ph_1 : 因此
- $s_0 \ s_1$; M_2 满足 $E(q_0 \cup q_2)$
- $s_0 \ s_2$; ... M 满足 $E(q_0 \cup q_2)$
- Ph_2 :
- $s_0 \ s_1 \ s_3$; 由于 M_0 不满足 $E(q_0 \cup q_2)$
- $s_0 \ s_1 \ s_5$; M_1 不满足 $E(q_0 \cup q_2)$
- $s_0 \ s_2 \ s_4$;
- $s_0 \ s_2 \ s_5$; ... $k=2$ 是最小可确定 $E(q_0 \cup q_2)$ 是否满足的界

$AG(q_0 \vee q_2)$ vs $EF(\neg q_0 \wedge \neg q_2)$

- Ph_0 : 我们有
- s_0 $M, s_0 \ s_2 \ s_4 \models_2 F(\neg q_0 \wedge \neg q_2)$
- $s_1/s_2/s_3/\dots$ 因此
- Ph_1 : M_2, s_0 满足 $EF(\neg q_0 \wedge \neg q_2)$
- $s_0 \ s_1$; M, s_0 满足 $EF(\neg q_0 \wedge \neg q_2)$
- $s_0 \ s_2$; ... M 不满足 $AG(q_0 \vee q_2)$
- Ph_2 :
- $s_0 \ s_1 \ s_3$; 由于 M_0 不满足 $EF(\neg q_0 \wedge \neg q_2)$
- $s_0 \ s_1 \ s_5$; M_1 不满足 $EF(\neg q_0 \wedge \neg q_2)$
- $s_0 \ s_2 \ s_4$;
- $s_0 \ s_2 \ s_5$; ... $k=2$ 是最小可确定 $AG(q_0 \vee q_2)$ 是否满足的界

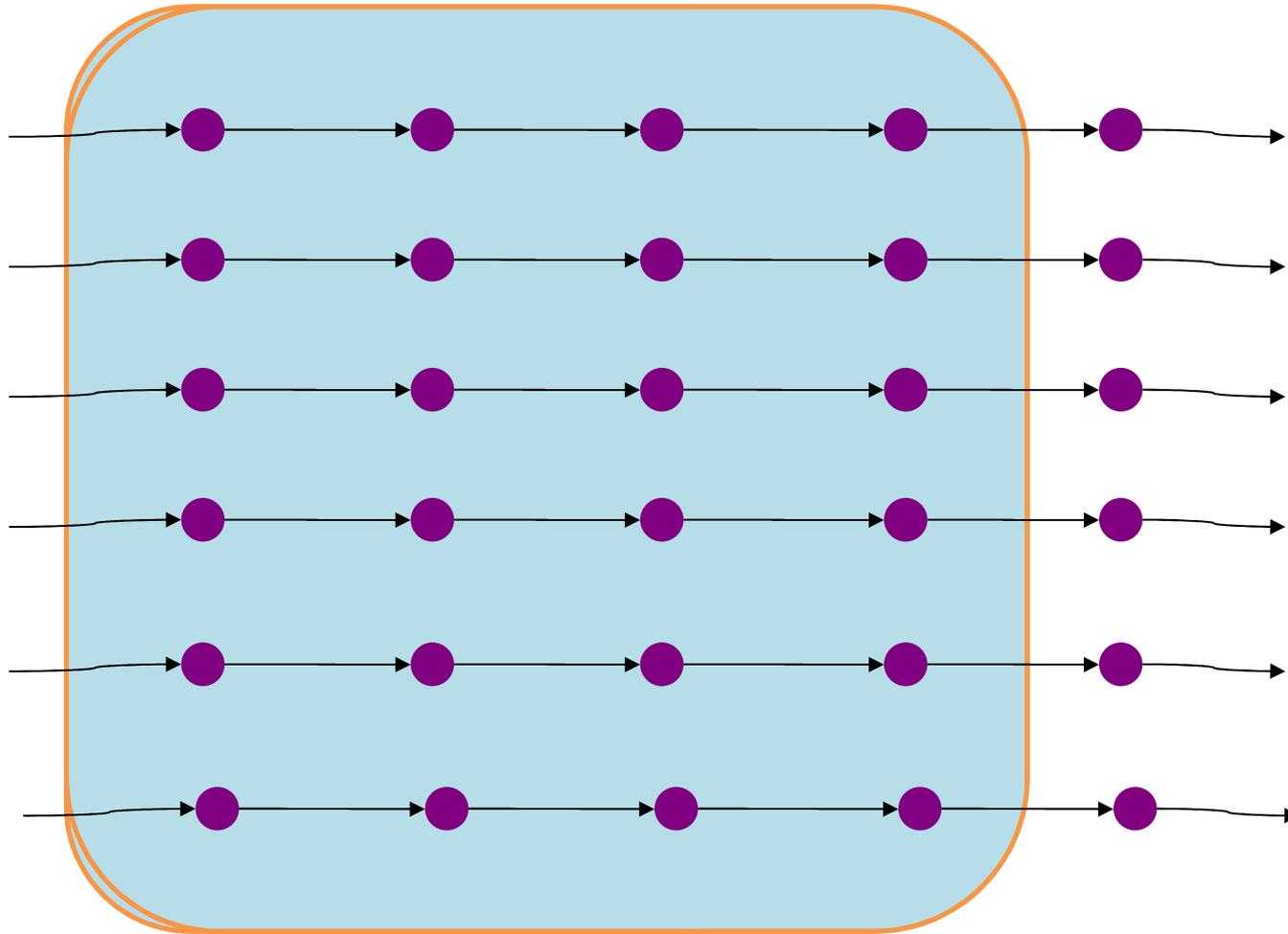
限界模型(s0...)

- Ph_0 :
- $s_0 ; \dots$
- Ph_1 :
- $s_0 s_1$;
- $s_0 s_2$; ...
- Ph_2 :
- $s_0 s_1 s_3$;
- $s_0 s_1 s_5$;
- $s_0 s_2 s_4$;
- $s_0 s_2 s_5$; ...
- Ph_3 :
- $s_0 s_1 s_3 s_4$;
- $s_0 s_1 s_3 s_5$;
- $s_0 s_1 s_5 s_0$;
- $s_0 s_2 s_4 s_5$;
- $s_0 s_2 s_5 s_0$;
- ...
- Ph_4 :
- $s_0 s_1 s_3 s_4 s_5$;
- $s_0 s_1 s_3 s_5 s_0$;
- $s_0 s_1 s_5 s_0 s_1$;
- $s_0 s_1 s_5 s_0 s_2$;
- $s_0 s_2 s_4 s_5 s_0$;
- $s_0 s_2 s_5 s_0 s_1$;
- $s_0 s_2 s_5 s_0 s_2$;
- ...

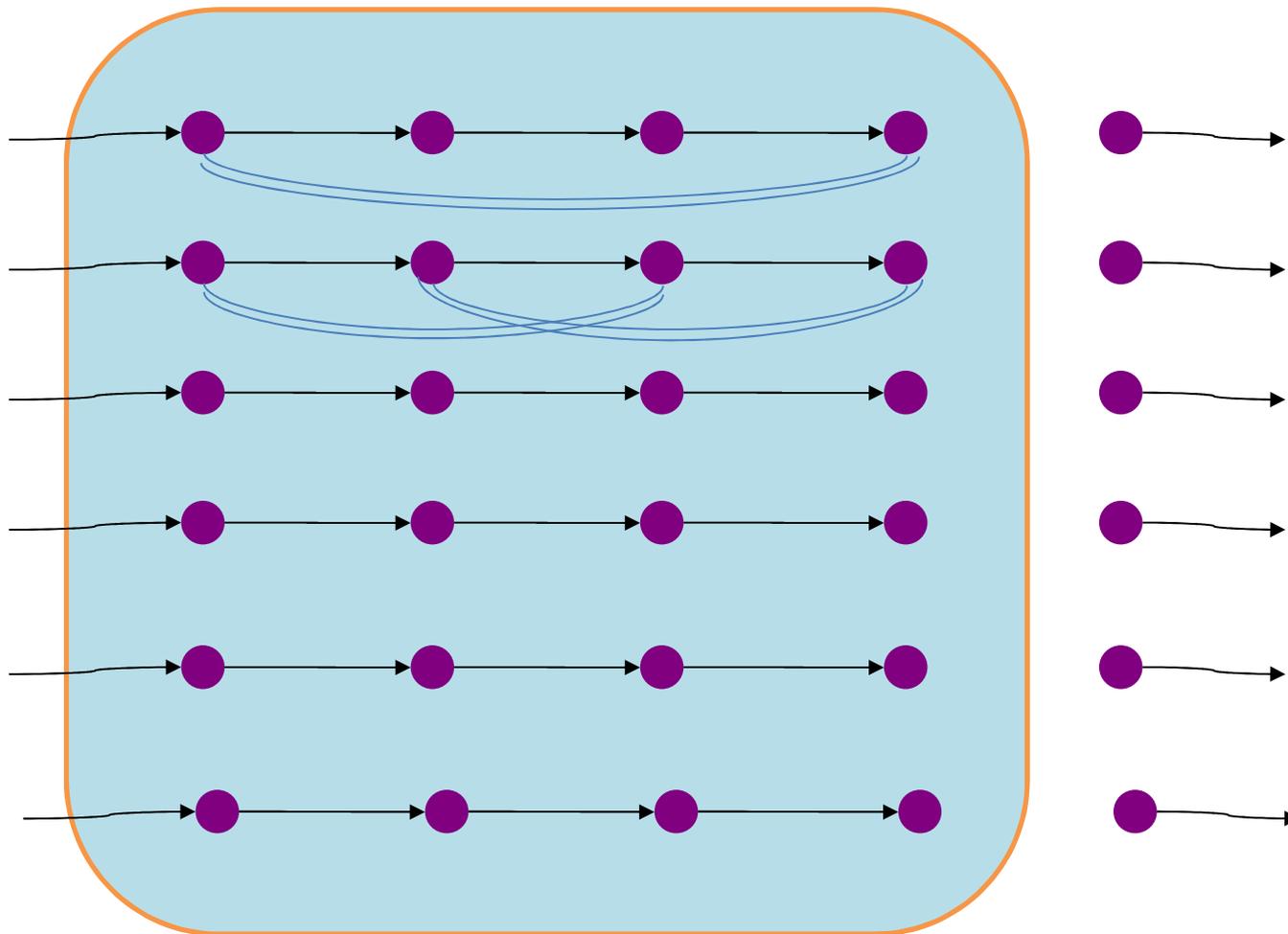
限界正确性检查 – 小结

- 从模型的局部考察一个性质是否满足
- 对一些不满足的性质可能很快知道问题
- 对一些满足的性质也可能很快知道结论

限界正确性检查



限界正确性检查



限界正确性检查

- $M, s \models \varphi$, 限界模型 M_0, M_1, \dots
问题: 是否存在 k , $M, s \models_k \varphi$?

- 存在 k , $M, s \models_k \varphi$, 则 $M, s \models \varphi$

可靠性

\implies

K 较小时,
较快验证系统性质

限界正确性检查

- $M, s \models \varphi$, 限界模型 M_0, M_1, \dots
问题: 是否存在 k , $M, s \models_k \neg\varphi$?

- 存在 k , $M, s \models_k \neg\varphi$, 则 $M, s \models \neg\varphi$

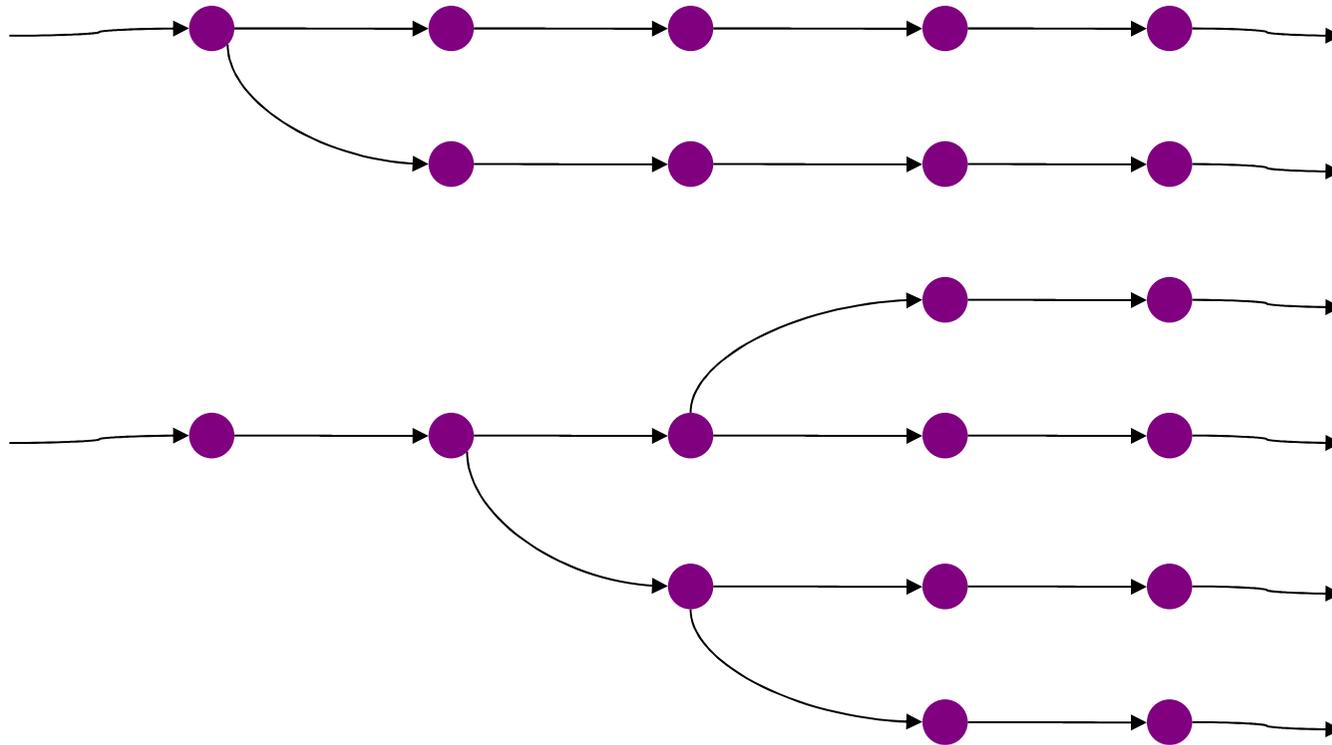
可靠性

则 $M, s \not\models \varphi$

K 较小时,
较快查出系统问题

(III) CTL的不动点表示

Computation Tree Logic



Specification

$$M \models \varphi$$

$$I \subseteq [[\varphi]]$$

Formulas

$$[[p]] = \{ s \mid p \in L(s) \}$$

$$[[\varphi \wedge \psi]] = [[\varphi]] \cap [[\psi]]$$

$$[[\varphi \vee \psi]] = [[\varphi]] \cup [[\psi]]$$

$$[[\neg \varphi]] = S \setminus [[\varphi]]$$

Minimal Complete Set

EX, EF, EG, ER, EU,
AX, AF, AG, AR, AU

EF is expressible by EU

ER is expressible by EU and EG

Then $\{EX, EG, EU\}$ is a complete set.

Formulas

$$[[EX \varphi]] = \{ s \mid s \rightarrow s', s' \in [[\varphi]] \}$$

$$[[E(\varphi \cup \psi)]] = ?$$

$$[[EG(\psi)]] = ?$$

Recursive Equations

$$E(\phi \cup \psi) \equiv \psi \vee (\phi \wedge EX(E(\phi \cup \psi)))$$

$$E(\phi \cap \psi) \equiv \psi \wedge (\phi \vee EX(E(\phi \cap \psi)))$$

$$[[E(\phi \cup \psi)]] \equiv [[\psi]] \cup ([[\phi]] \cap EX([[E(\phi \cup \psi)]]))$$

$$[[EG(\psi)]] \equiv [[\psi]] \cap EX([[EG(\psi)]])$$

Recursive Equations

$$E(\phi \cup \psi) \equiv \psi \vee (\phi \wedge EX(E(\phi \cup \psi)))$$

$$f(Z) = \psi \vee (\phi \wedge EX(Z))$$

Then $E(\phi \cup \psi)$ is a fixpoint of f .

$$f: \text{pow}(S) \rightarrow \text{pow}(S)$$

Fixpoint

$$f(Z) = \psi \vee (\phi \wedge EX(Z))$$

f is monotonic; f is continuous

pow(S) is a complete lattice.

f has a least and a greatest fixpoint

$$\mu Z.f(Z), \mu f$$

$$\nu Z.f(Z), \nu f$$

Fixpoint

$$\mu f = \cup \{ f^k(\perp) \mid k \in \mathbb{N} \}$$

We prove: $[[E(\phi \cup \psi)]] = \mu f$

Then we have:

$$E(\phi \cup \psi) = \mu Z. f(Z) = \mu Z. (\psi \vee (\phi \wedge EX(Z)))$$

Recursive Equations

$$EG(\psi) \equiv \psi \wedge EX(EG(\psi))$$

$$f(Z) = \psi \wedge EX(Z)$$

Then $EG(\psi)$ is a fixpoint of f .

$$f: \text{pow}(S) \rightarrow \text{pow}(S)$$

Fixpoint

$$f(Z) = \psi \wedge EX(Z)$$

f is monotonic; f is continuous

pow(S) is a complete lattice.

f has a least and a greatest fixpoint

$$\mu Z.f(Z), \mu f$$

$$\nu Z.f(Z), \nu f$$

Fixpoint

$$\nu f = \bigcap \{ f^k(S) \mid k \in \mathbb{N} \}$$

We prove: $[[EG(\psi)]] = \nu f$

Then we have:

$$EG(\psi) = \nu Z.f(Z) = \nu Z.(\psi \wedge EX(Z))$$

EG 和 EU

$\tau_1(Z) = (p \wedge EXZ)$ 是单调的

$\tau_2(Z) = (q \vee (p \wedge EXZ))$ 是单调的

EGp 是 τ_1 的一个不动点

$E(pUq)$ 是 τ_2 的一个不动点

EG 和 EU

需要证明

EGp 是 τ_1 的最大不动点

$E(pUq)$ 是 τ_2 的最小不动点

即

$$s \in \nu Z(p \wedge EXZ) \Rightarrow s \in EGp$$

$$s \in E(pUq) \Rightarrow s \in \mu Z(q \vee (p \wedge EXZ))$$

$$s \in E(pUq) \Rightarrow s \in \mu Z.(q \vee (p \wedge EX Z))$$

$$\mu Z(q \vee (p \wedge EX Z)) = \cup \tau_2^i(false)。$$

若 $s \in E(pUq)$,

则存在 $\pi_0 = s, n \geq 0, \pi = \pi_0 \pi_1 \cdots$

使得 $\pi_n \models q$ 且对所有 $j < n$, $\pi_j \models p$ 。

若 $n = 0$ 则 $\pi_0 \in \tau_2(false)$ 。

$$s \in E(pUq) \Rightarrow s \in \mu Z.(q \vee (p \wedge EX Z))$$

假设对所有 π 和给定 k ,

$\pi_k \models q$ 且对所有 $j < k$, $\pi_j \models p$ 则 $\pi_0 \in \tau_2^{k+1}(false)$ 。

设 $n = k + 1$ 时有

$\pi_n \models q$ 且对所有 $j < n$, $\pi_j \models p$ 。

根据假设, 我们有 $\pi_1 \in \tau_2^{k+1}(false)$ 。

由于 $(\pi_0, \pi_1) \in \Delta$, $\pi_0 \models p$,

根据 τ_2 的定义, $\pi_0 \in \tau_2(\pi_1)$ 。

因此 $\pi_0 \in \tau_2(\tau_2^{k+1}(false)) = \tau_2^{n+1}(false)$ 。

根据归纳原理, $s \in E(pUq) \Rightarrow s \in \mu Z(q \vee (p \wedge EX Z))$

$$s \in \nu Z.(p \wedge EX Z) \Rightarrow s \in EG p$$

$$\nu Z(p \wedge EX Z) = \bigcap \tau_1^i(true)$$

则存在 n , $\tau_1^n(true) = \tau_1^{n+1}(true)$ 。

设 $s_0 = s \in \nu Z(p \wedge EX Z)$ 。

则 $s_0 \in \bigcap \tau_1^n(true)$ 且 $p \in L(s_0)$ 。

同时 $s_0 \in \tau_1^{n+1}(true)$ 。

$$s \in \nu Z.(p \wedge EX Z) \Rightarrow s \in EG p$$

由 τ_1 的定义知

存在状态 s_1 和状态转换 $(s_0, s_1) \in \Delta$

使得 $s_1 \in \cap \tau_1^n(true)$ 且 $p \in L(s_1)$ 。

由此类推知对所有 $i \geq 0$,

存在状态 s_{i+1} 和状态转换 $(s_i, s_{i+1}) \in \Delta$

使得 $s_{i+1} \in \cap \tau_1^n(true)$ 且 $p \in L(s_{i+1})$ 。

根据 EGp 的语义, $s \in EGp$ 。

因此 $s \in \nu Z(p \wedge EX Z) \Rightarrow s \in EGp$ 。

Fixpoint Formulation of CTL

$$[[p]] = \{ s \mid p \in L(s) \}$$

$$[[EX \varphi]] = \{ s \mid s \rightarrow s', s' \in [[\varphi]] \}$$

$$E(\phi U \psi) = \mu Z.(\psi \vee (\phi \wedge EX(Z)))$$

$$E(\phi R \psi) = \nu Z.(\psi \wedge (\phi \vee EX(Z)))$$

$$EF\psi = \mu Z.(\psi \vee EX(Z))$$

$$EG\psi = \nu Z.(\psi \wedge EX(Z))$$

Fixpoint Formulation of CTL

$$[[AX \varphi]] = \{ s \mid (s \rightarrow s') \Rightarrow s' \in [[\varphi]] \}$$

$$A(\phi U \psi) = \mu Z.(\psi \vee (\phi \wedge AX(Z)))$$

$$A(\phi R \psi) = \nu Z.(\psi \wedge (\phi \vee AX(Z)))$$

$$AF\psi = \mu Z.(\psi \vee AX(Z))$$

$$AG\psi = \nu Z.(\psi \wedge AX(Z))$$

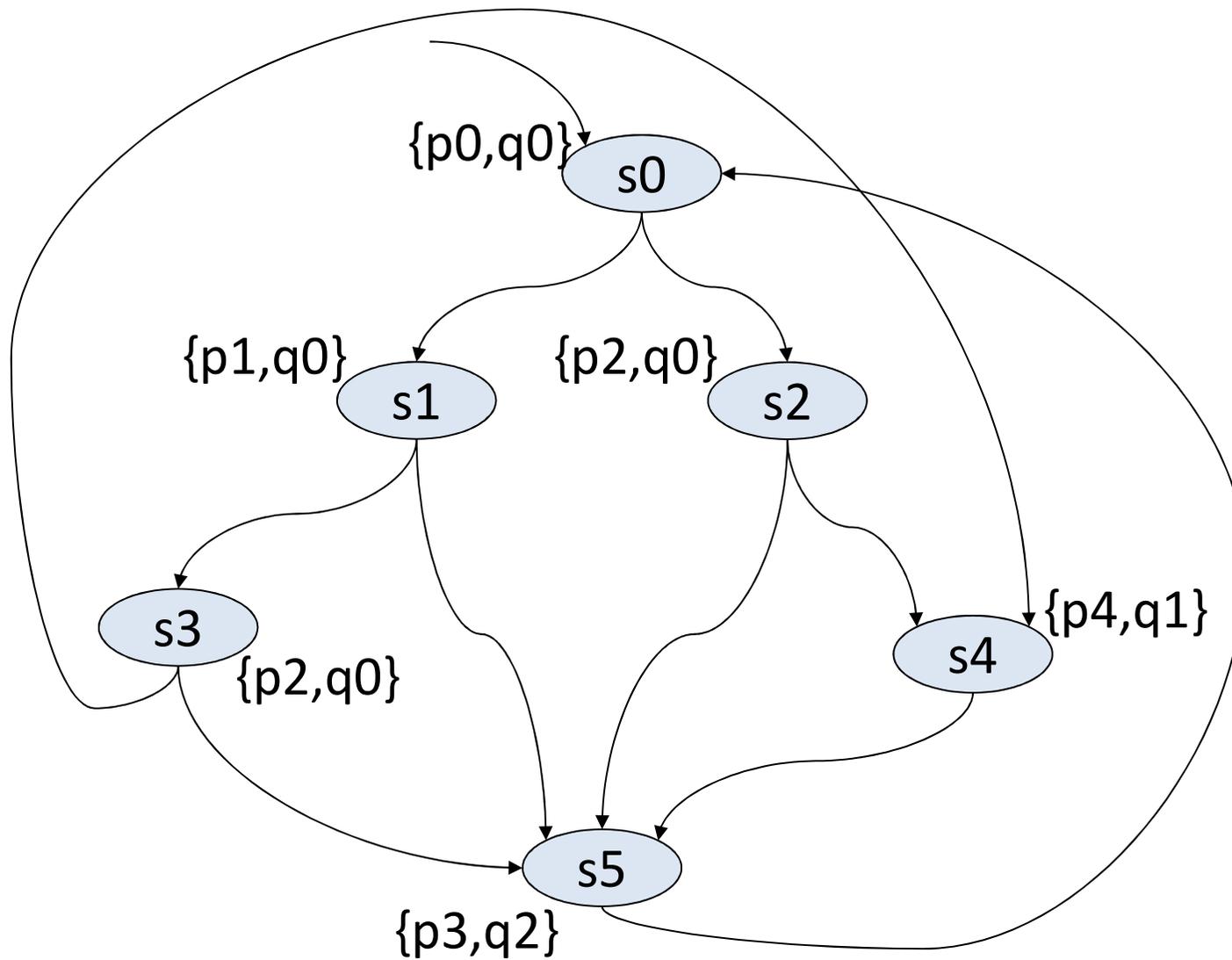
Model Checking

$$M \models \phi$$

$$I \subseteq [[\phi]]$$

例子 

例子：简化自动售茶机模型



自动售茶机: $E(q_0 \cup q_2)$

- $E(q_0 \cup q_2) = \mu_Z.(q_2 \vee (q_0 \wedge EX Z))$
- $S_0 = \text{false}$
- $S_1 = q_2 = \{s_5\}$
- $S_2 = \{s_5\} \cup (\{s_0, \dots, s_3\} \cap \{s_1, \dots, s_4\}) = \{s_1, s_2, s_3, s_5\}$
- $S_3 = \{s_5\} \cup (\{s_0, \dots, s_3\} \cap \{s_0, \dots, s_4\}) = \{s_0, s_1, s_2, s_3, s_5\}$
- $S_4 = \{s_5\} \cup (\{s_0, \dots, s_3\} \cap \{s_0, \dots, s_5\}) = \{s_0, s_1, s_2, s_3, s_5\}$
- 该模型满足 $E(q_0 \cup q_2)$

自动售茶机: $AG(q_0 \vee q_2)$

- $AG(q_0 \vee q_2) = \forall Z. ((q_0 \vee q_2) \wedge AX Z)$
- $S_0 = \text{true}$
- $S_1 = q_0 \vee q_2 = \{s_0, s_1, s_2, s_3, s_5\}$
- $S_2 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_0, s_1, s_4, s_5\} = \{s_0, s_1, s_5\}$
- $S_3 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4, s_5\} = \{s_5\}$
- $S_4 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4\} = \{\}$
- $S_5 = \{\}$
- 该模型不满足 $AG(q_0 \vee q_2)$

(IV) μ -Calculus

Syntax of μ -Calculus

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of μ -calculus formulas is as follows.

$$\Phi ::= p \mid Z \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg \Phi \mid \\ \langle . \rangle \Phi \mid [.] \Phi \mid \mu Z. \Phi \mid \nu Z. \Phi$$

Variables are in the scope of even number of neg.

Semantics

$e: \text{VAR} \rightarrow \text{pow}(S)$

$$[[p]]e = \{ s \mid p \in L(s) \}$$

$$[[Z]]e = e(Z)$$

$$[[<.\>\varphi]]e = \{ s \mid s \rightarrow s', s' \in [[\varphi]]e \}$$

$$[[[.\varphi]]e = \{ s \mid (s \rightarrow s') \Rightarrow (s' \in [[\varphi]]e) \}$$

$$[[\varphi \wedge \psi]]e = [[\varphi]]e \cap [[\psi]]e$$

$$[[\varphi \vee \psi]]e = [[\varphi]]e \cup [[\psi]]e$$

$$[[\neg\varphi]]e = S \setminus [[\varphi]]e$$

$$[[\mu Z.\varphi]]e = \bigcap \{ Y \subseteq S \mid [[\varphi]]e(Z/Y) \subseteq Y \}$$

$$[[\nu Z.\varphi]]e = \bigcup \{ Y \subseteq S \mid Y \subseteq [[\varphi]]e(Z/Y) \}$$

Closed Formulas

Formulas without free variables.

The semantics of such a formula does not depend on the initial assignment e .

$$[[\varphi]] = [[\varphi]]e \quad \text{for any } e$$

Example

$\forall Z.(p \wedge [.] [.] Z)$

p is true at all even places along all paths

Satisfiability

The complexity is EXPTIME-complete.

Applications of μ -Calculus

μ -Calculus as a Specification Language

System Models:

Kripke Structures (K)

System Specifications:

Closed Formulas (φ)

$K \models \varphi$

$I \subseteq [[\varphi]]$

Model Checking

Definition

Given a model K and a formula ϕ .

The model checking problem is the problem of checking whether $K \models \phi$ holds.

Model Checking

The complexity of model checking is in $NP \cap coNP$.



μ -Calculus with Actions

Syntax of μ -Calculus

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of μ -calculus formulas is as follows.

$$\Phi ::= p \mid Z \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg \Phi \mid \\ \langle a \rangle \Phi \mid [a] \Phi \mid \mu Z. \Phi \mid \nu Z. \Phi$$

Variables are in the scope of even number of neg.

Semantics

Interpreted on
Doubly Labeled Transition Systems

Labeled Transition Systems

Definition

A LTS is a quadruple $\langle \Sigma, S, \Delta, I \rangle$

- Σ : A finite set of symbols
- S : A finite set of states
- $\Delta \subseteq S \times \Sigma \times S$: A transition relation
- $I \subseteq S$: A set of initial states

Double-Labeled Transition Systems

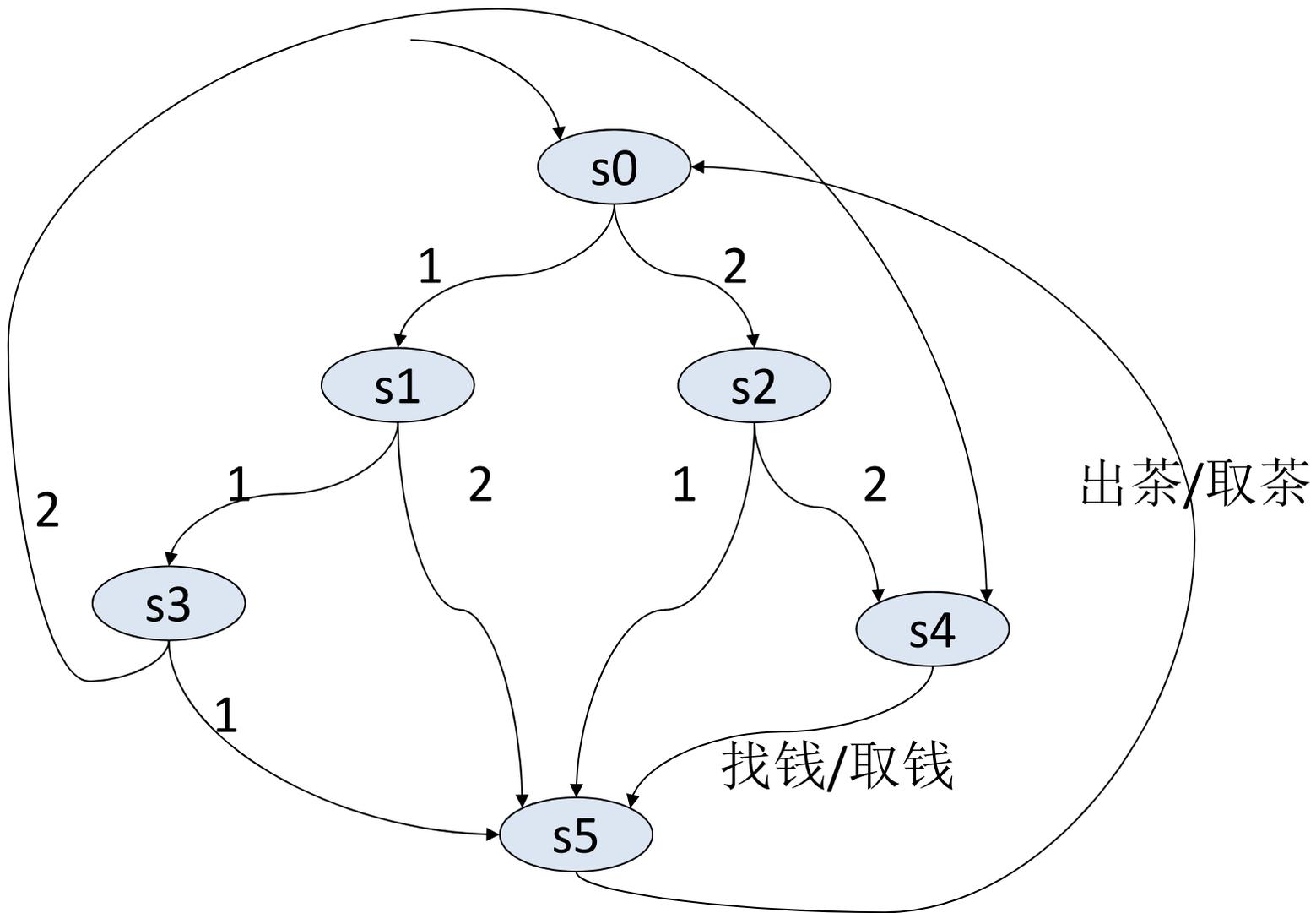
AP: A set of propositions.

Definition

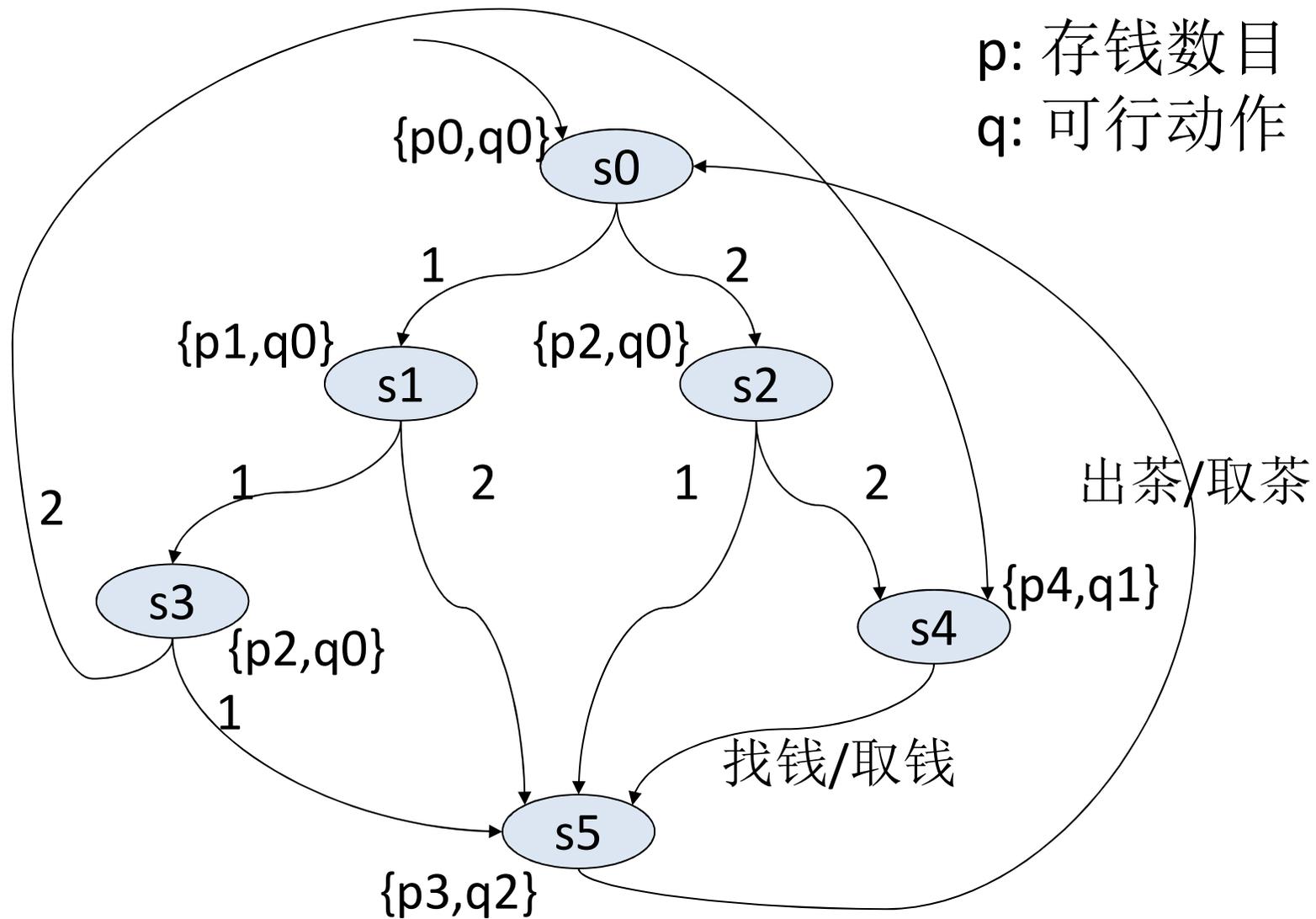
A DLTS is a quintuple $M = \langle \Sigma, S, \Delta, I, L \rangle$

- Σ : A set of action symbols
- S : A finite set of states
- $\Delta \subseteq S \times \Sigma \times S$: A total transition relation
- $I \subseteq S$: A set of initial states
- $L: S \rightarrow 2^{AP}$ is a labeling function

例子：简化自动售茶机模型



例子：双标号自动售茶机模型



Semantics

Let $e: \text{VAR} \rightarrow \text{pow}(S)$

$$[[p]]e = \{ s \mid p \in L(s) \}$$

$$[[Z]]e = e(Z)$$

$$[[\langle a \rangle \varphi]]e = \{ s \mid s \xrightarrow{a} s', s' \in [[\varphi]]e \}$$

$$[[[a]\varphi]]e = \{ s \mid (s \xrightarrow{a} s') \Rightarrow (s' \in [[\varphi]]e) \}$$

$$[[\varphi \wedge \psi]]e = [[\varphi]]e \cap [[\psi]]e$$

$$[[\varphi \vee \psi]]e = [[\varphi]]e \cup [[\psi]]e$$

$$[[\neg \varphi]]e = S \setminus [[\varphi]]e$$

$$[[\mu Z. \varphi]]e = \bigcap \{ Y \subseteq S \mid [[\varphi]]e(Z/Y) \subseteq Y \}$$

$$[[\nu Z. \varphi]]e = \bigcup \{ Y \subseteq S \mid Y \subseteq [[\varphi]]e(Z/Y) \}$$

Applications of μ -Calculus

μ -Calculus as a Specification Language

System Models:

DLTS (M)

System Specifications:

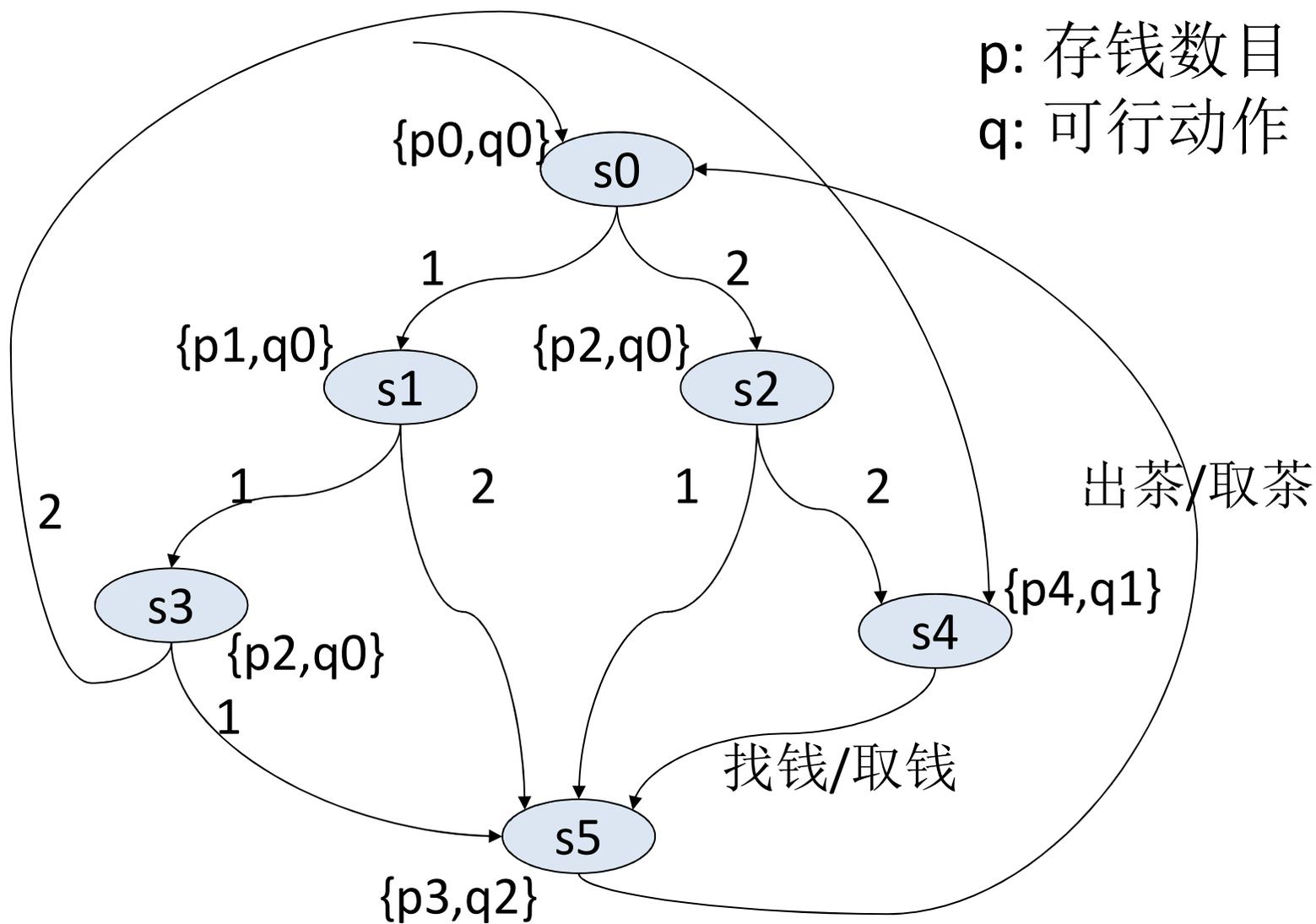
Closed Formulas (φ)

$M \models \varphi$

$I \subseteq [[\varphi]]$

例子 

例子：双标号自动售茶机模型



自动售茶机: $\mu X.(q2 \vee \langle 1 \rangle X)$

- $S_0 = \text{false}$
- $S_1 = q2 \vee \langle 1 \rangle \{\}$ = $\{s_5\}$
- $S_2 = \{s_5\} \cup \{s_2, s_3\}$ = $\{s_2, s_3, s_5\}$
- $S_3 = \{s_5\} \cup \{s_1, s_2, s_3\}$ = $\{s_1, s_2, s_3, s_5\}$
- $S_4 = \{s_5\} \cup \{s_0, s_1, s_2, s_3\}$ = $\{s_0, s_1, s_2, s_3, s_5\}$
- $S_5 = \{s_5\} \cup \{s_0, s_1, s_2, s_3\}$ = $\{s_0, s_1, s_2, s_3, s_5\}$

自动售茶机: $\forall X.(\neg q_2 \wedge [1]X)$

Negation of $\mu X.(q_2 \vee \langle 1 \rangle X)$

- $S_0 = \text{true}$
- $S_1 = \neg q_2 = \{s_0, s_1, s_2, s_3, s_4\}$
- $S_2 = \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_1, s_4, s_5\} = \{s_0, s_1, s_4\}$
- $S_3 = \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_4, s_5\} = \{s_0, s_4\}$
- $S_4 = \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} = \{s_4\}$
- $S_5 = \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} = \{s_4\}$

自动售茶机: $\mu X.(q2 \vee [1]X)$

- $S_0 = \text{false}$
- $S_1 = q2 \vee [1]\{\} = \{s_5\} \cup \{s_4, s_5\} = \{s_4, s_5\}$
- $S_2 = \{s_5\} \cup \{s_2, s_3, s_4, s_5\} = \{s_2, s_3, s_4, s_5\}$
- $S_3 = \{s_5\} \cup \{s_1, s_2, s_3, s_4, s_5\} = \{s_1, s_2, s_3, s_4, s_5\}$
- $S_4 = \{s_5\} \cup \{s_0, s_1, s_2, s_3, s_4, s_5\} = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
- $S_5 = \{s_0, s_1, s_2, s_3, s_4, s_5\}$

双标号与单标号

- $\mu X.(q2_{v<1}>X)$
- $\mu X.(<取茶>TRUE_{v<1}>X)$

Formulation of CTL in μ -Calculus (1)

$$\text{TR}(p) = p$$

$$\text{TR}(\phi \wedge \psi) = \text{TR}(\phi) \wedge \text{TR}(\psi)$$

$$\text{TR}(\phi \vee \psi) = \text{TR}(\phi) \vee \text{TR}(\psi)$$

$$\text{TR}(\neg \phi) = \neg \text{TR}(\phi)$$

$$\text{TR}(\text{EX } \phi) = \langle . \rangle \text{TR}(\phi)$$

$$\text{TR}(\text{E}(\phi \text{U} \psi)) = \mu Z. (\text{TR}(\psi) \vee (\text{TR}(\phi) \wedge \langle . \rangle (Z)))$$

$$\text{TR}(\text{E}(\phi \text{R} \psi)) = \nu Z. (\text{TR}(\psi) \wedge (\text{TR}(\phi) \vee \langle . \rangle (Z)))$$

$$\text{TR}(\text{EF} \psi) = \mu Z. (\text{TR}(\psi) \vee \langle . \rangle (Z))$$

$$\text{TR}(\text{EG} \psi) = \nu Z. (\text{TR}(\psi) \wedge \langle . \rangle (Z))$$

Formulation of CTL in μ -Calculus (2)

$$\begin{aligned} \text{TR}(AX \varphi) &= [.] \text{TR}(\varphi) \\ \text{TR}(A(\phi U \psi)) &= \mu Z. (\text{TR}(\psi) \vee (\text{TR}(\phi) \wedge [.](Z))) \\ \text{TR}(A(\phi R \psi)) &= \nu Z. (\text{TR}(\psi) \wedge (\text{TR}(\phi) \vee [.](Z))) \\ \text{TR}(AF \psi) &= \mu Z. (\text{TR}(\psi) \vee [.](Z)) \\ \text{TR}(AG \psi) &= \nu Z. (\text{TR}(\psi) \wedge [.](Z)) \end{aligned}$$

(V) Summary

- Computation Tree Logic (CTL)
- Bounded Semantics of CTL
- Fixpoint Representation of CTL Formulas
- μ -Calculus

练习1

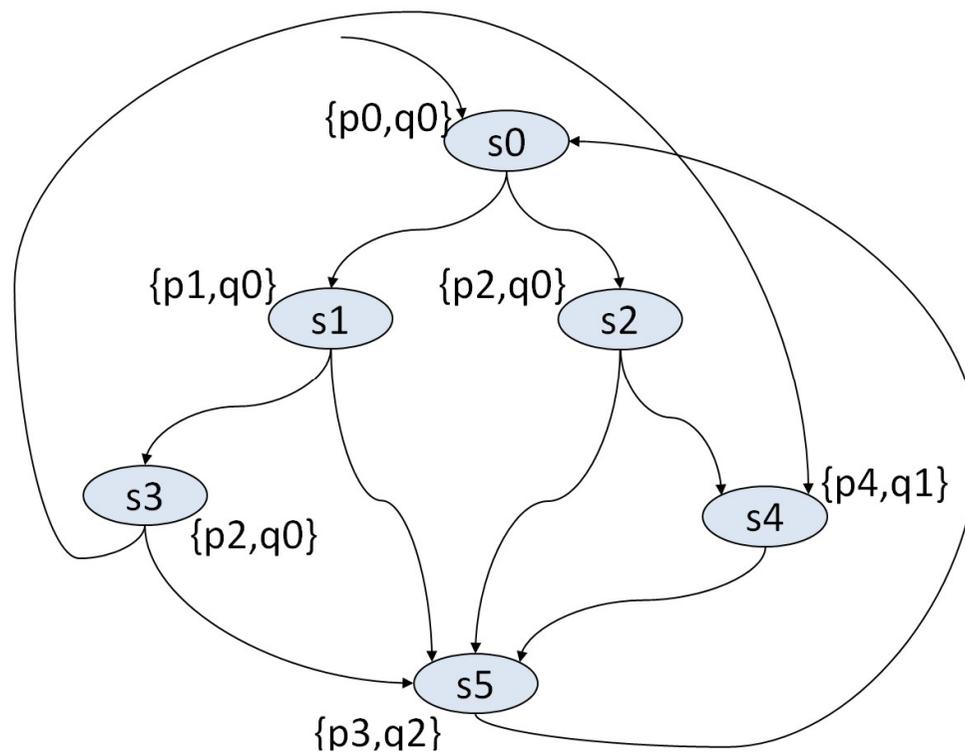
设M为简化自动售茶机模型。

用限界语义验证M是否满足

$A(q_0 \cup q_2)$ 和

$EG(q_0 \vee q_2)$,

分别给出最小的
可以确定以上公式
是否满足的界。



练习2

设M为简化自动售茶机模型。

用简化自动机模型M计算

$[[A(q_0 \cup q_2)]]$ 和

$[[EG(q_0 \vee q_2)]]$,

并讨论该模型

是否满足

$A(q_0 \cup q_2)$ 和

$EG(q_0 \vee q_2)$ 。

