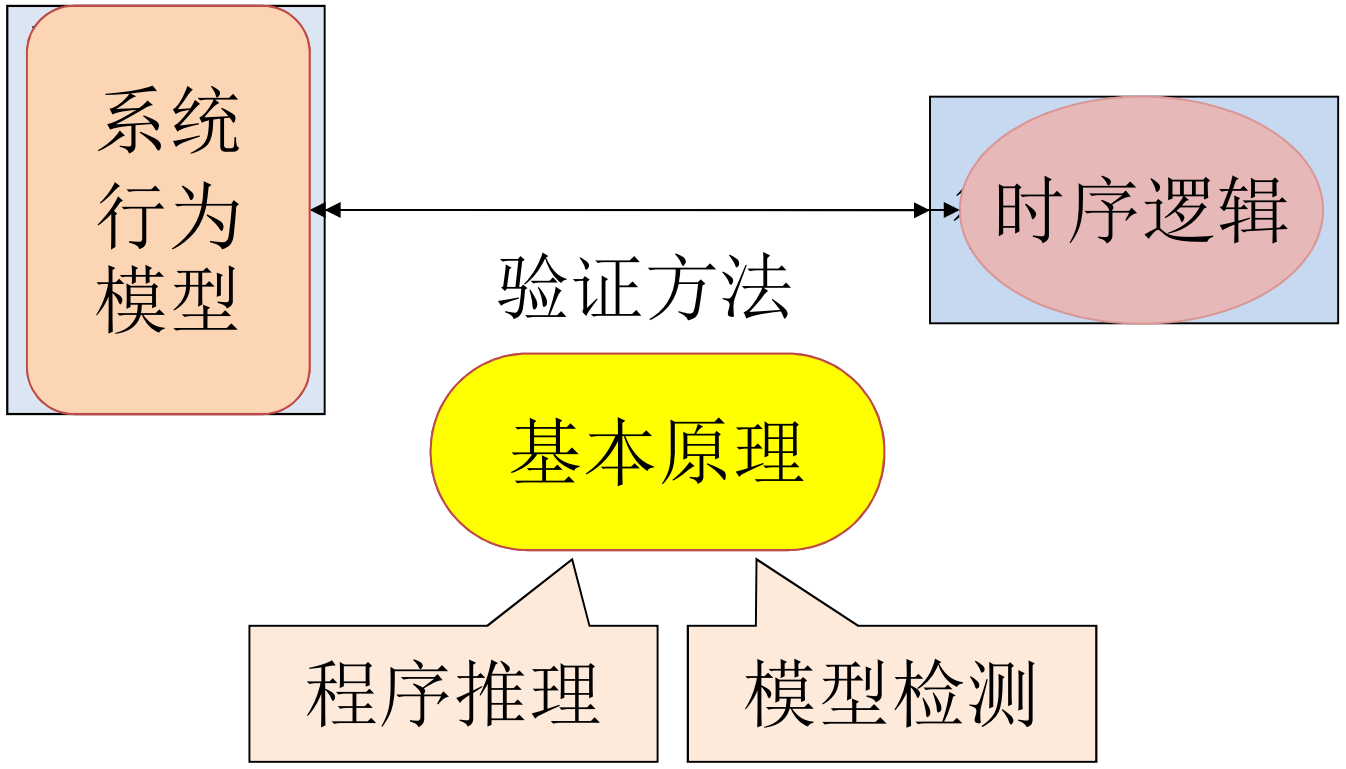
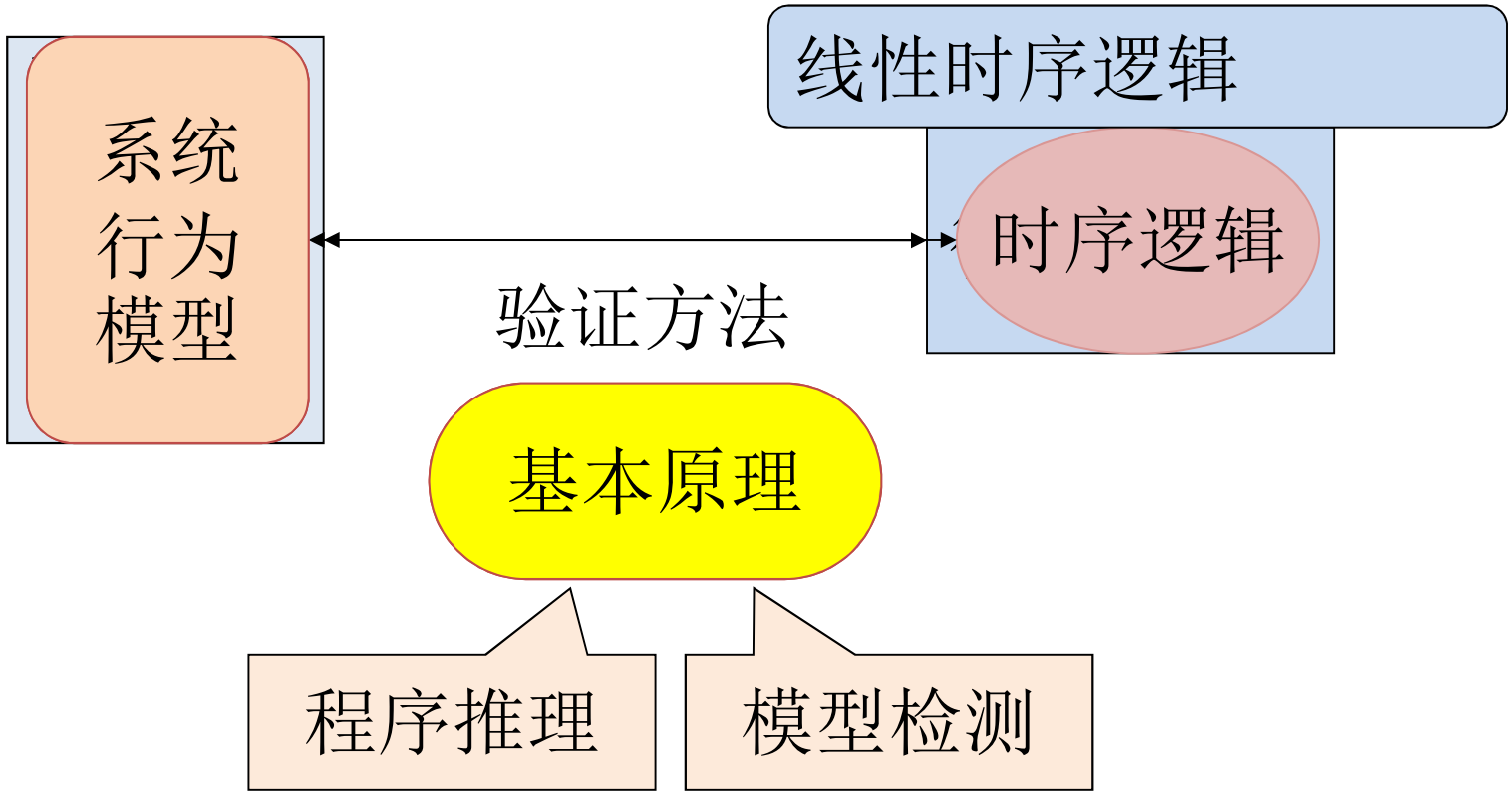
Linear Temporal Logic

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/

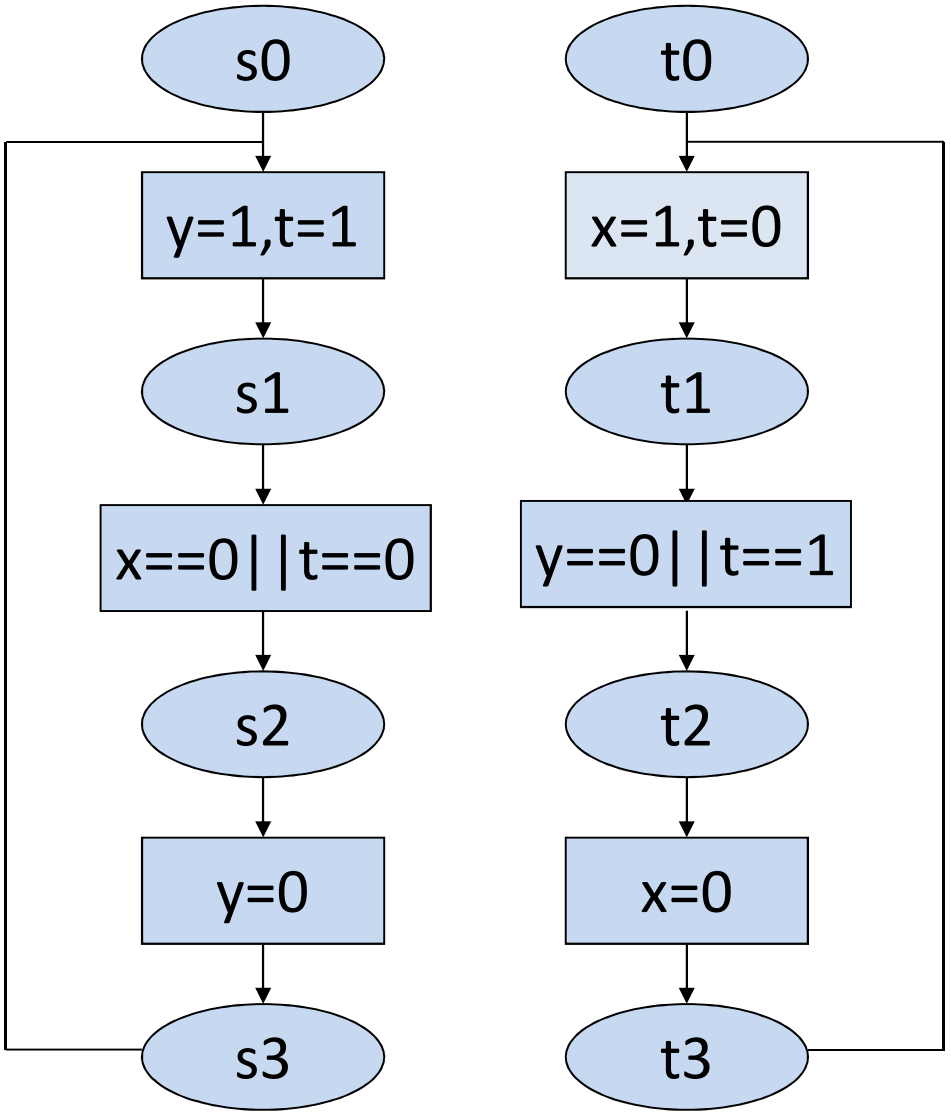
课程内容



课程内容

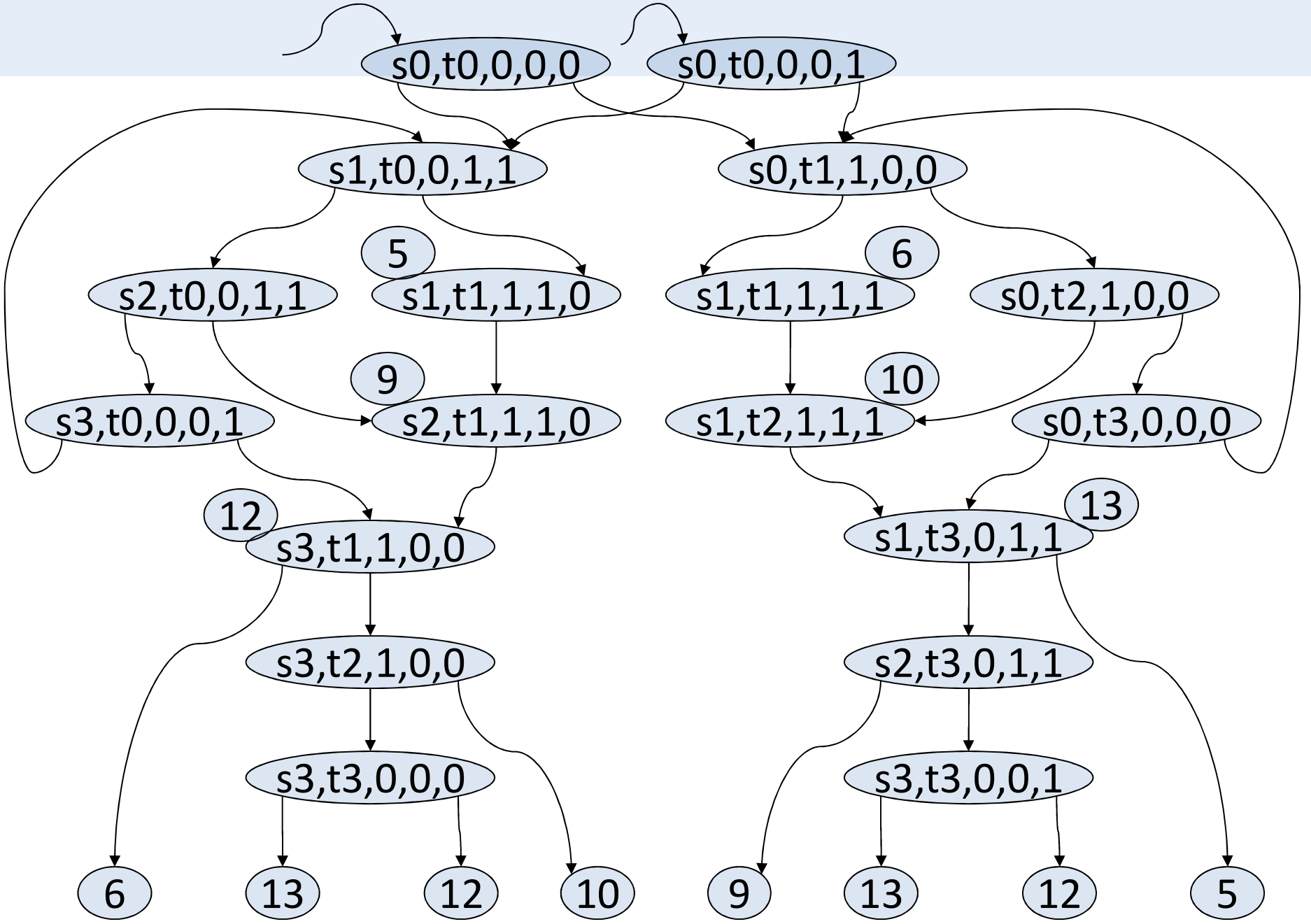


Example

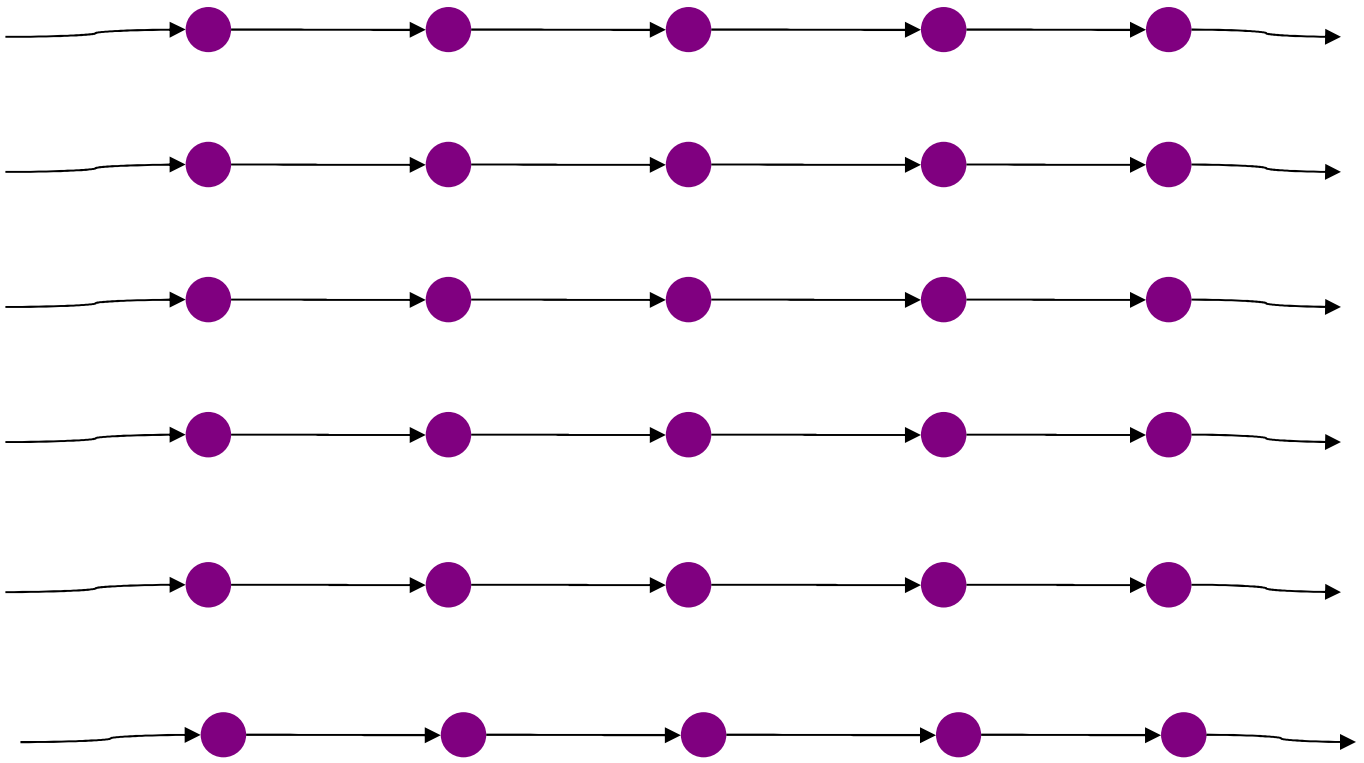


Initial States

s0
t0
x=0
y=0


s0,t0,0,0,0
s0,t0,0,0,1
s1,t0,0,1,1
s0,t1,1,0,0
5
6
s2,t0,0,1,1
s1,t1,1,1,0
s1,t1,1,1,1
s0,t2,1,0,0
9
10
s3,t0,0,0,1
s2,t1,1,1,0
s1,t2,1,1,1
s0,t3,0,0,0
12
13
s3,t1,1,0,0
s1,t3,0,1,1
s3,t2,1,0,0
s2,t3,0,1,1
s3,t3,0,0,0
s3,t3,0,0,1
6
13
12
10
9
13
12
5

Computations



Examples of Properties

- Safety
- Inevitability

- Response
- Immediate Response
- Priority
- First Come – First Served

Contents

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

(I) Propositional Linear Temporal Logic

- Examples of Properties
- Syntax and Semantics
- Satisfiability and Validity
- Equivalences
- Expressivity
- Complete Set of Operators
- Normal Form
- Proof System
- Applications

Examples of Properties

- Safety: G (!(a=s2∧b=t2))
- Inevitability F (a=s2∨b=t2)

- Response G (a=s1 → F (a=s2))
- Imm. Response G (a=s1 → X (a=s2))
- Priority G (a=s1∧b!=t1∧b!=t2 → (a=s2 R b!=t2))
- FCFS G (a=s1∧b!=t1∧b!=t2 → (b!=t2 U a=s2))

Syntax of PLTL

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of PLTL formulas is defined as follows.

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

Sometimes, X,G,F are written as O, □, ◊.

Examples of Properties

- Safety: G (!(a=s2∧b=t2))
- Inevitability F (a=s2∨b=t2)

- Response G (a=s1 → F (a=s2))
- Imm. Response G (a=s1 → X (a=s2))
- Priority G (a=s1∧b!=t1∧b!=t2 → (a=s2 R b!=t2))
- FCFS G (a=s1∧b!=t1∧b!=t2 → (b!=t2 U a=s2))

Proposition Symbols

Let AP be the set of proposition symbols {p0,p1,…,p13} 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: $G\ (\neg(p8 \wedge p12))$
- Inevitability $F\ (p8 \vee p12)$

- Response $G\ (p7 \rightarrow F\ p8)$
- Imm. Response $G\ (p7 \rightarrow X\ p8)$
- Priority $G\ (p7 \wedge \neg p11 \wedge \neg p12 \rightarrow (p8\ R\ \neg p12))$
- FCFS $G\ (p7 \wedge \neg p11 \wedge \neg p12 \rightarrow (\neg p12\ U\ p8))$

Semantics

Linear Structures

A linear structure is a triple $M=\langle S,\zeta,L\rangle$

- S : A finite set of states
- $\zeta \in S^{\omega}$: A sequence of states
- $L: S \rightarrow 2^{AP}$ is a labeling function

Definition: $M \models \phi$ or $\zeta \models \phi$

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

$\zeta \models p$, if $p \in AP$ and $p \in L(\zeta_0)$

$\zeta \models \neg\phi$, 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 and Validity

Satisfiability and Validity

Definition

A formula ϕ is satisfiable,

if there is a linear structure M such that $M \models \phi$.

Definition

A formula ϕ is valid,

if for every linear structure M, we have $M \models \phi$.

Satisfiability and Validity Checking

The complexities of PLTL satisfiability and validity checking are PSPACE-complete.

Equivalences

Definition

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

Dual Operators

$$X\,\phi \equiv \neg X \neg\, \phi$$

$$G\,\phi \equiv \neg F \neg\, \phi$$

$$\phi\ R\ \psi \equiv \neg(\neg\phi\ U\ \neg\psi)$$

Recursion

$$G\,\phi \equiv \phi \wedge X\,G\,\phi$$

$$F\,\phi \equiv \phi \vee X\,F\,\phi$$

$$\phi\,R\,\psi \equiv \psi \wedge (\phi \vee X\ (\phi R\,\psi))$$

$$\phi\,U\,\psi \equiv \psi \vee (\phi \wedge X\,(\phi U\,\psi))$$

Definable Operators

Let $p_0 \in$ AP be given.

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

$F\ \phi \equiv \neg\bot\ U\ \phi$

$G\ \phi \equiv \bot\ R\ \phi$

$\phi\ R\ \psi \equiv \psi\ U\ (\phi \wedge \psi) \vee G\ \psi$

Example: Proofs of Some Equivalences

$$X\,\phi \equiv \neg X \neg\, \phi$$

$$\phi\ R\ \psi \equiv \psi\ U\ (\phi \wedge \psi) \vee G\ \psi$$

These equivalences can be proved by applying the semantics.

Example 1： $X\phi \equiv \neg X \neg \phi$

- $\zeta \models X\phi$
- $\zeta^1 \models \phi$
- $\zeta^1 \not\models \neg\phi$
- $\zeta \not\models X\neg\phi$
- $\zeta \models \neg X \neg \phi$

Example 2： $\phi\ R\ \psi \equiv (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

- $\zeta \models (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或
  存在$i \geq 0$, $\zeta^i \models \phi \wedge \psi$ 且对任意$j < i$, $\zeta^j \models \psi$

- $\zeta \models \phi\ R\ \psi$

  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

Example 2： $\phi\ R\ \psi \equiv (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

- $\zeta \models (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或
  存在$i \geq 0$, $\zeta^i \models \phi$ 且对任意$j \leq i$, $\zeta^j \models \psi$

$\leftrightarrow$

- $\zeta \models \phi\ R\ \psi$

  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

Example 2： $\phi R \psi \equiv (\psi U(\phi \wedge \psi)) \vee G\, \psi$

- $\zeta \models (\psi U(\phi \wedge \psi)) \vee G\, \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或
  存在$i \geq 0$, $\zeta^i \models \phi$ 且对任意$j \leq i$, $\zeta^j \models \psi$

➔

- $\zeta \models \phi R \psi$

  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

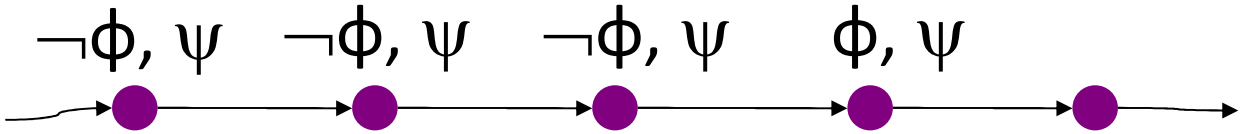
Example 2： $\phi\ R\ \psi \equiv (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

- $\zeta \models (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或

  存在$i \geq 0$, $\zeta^i \models \phi$ 且对任意$j \leq i$, $\zeta^j \models \psi$

- $\zeta \models \phi\ R\ \psi$



  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

Example 2： $\phi R \psi \equiv (\psi U(\phi \wedge \psi)) \vee G\, \psi$

- $\zeta \models (\psi U(\phi \wedge \psi)) \vee G\, \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或
  存在$i \geq 0$, $\zeta^i \models \phi$ 且对任意$j \leq i$, $\zeta^j \models \psi$

  ⇐

- $\zeta \models \phi R \psi$

  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

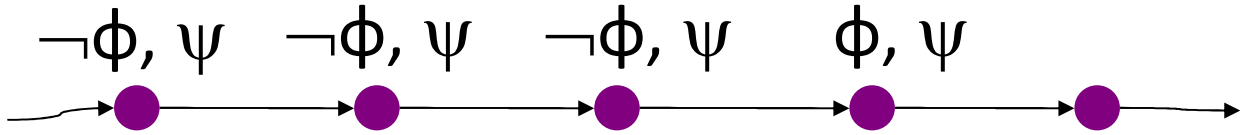
Example 2： $\phi\ R\ \psi \equiv (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

- $\zeta \models (\psi\ U(\phi \wedge \psi)) \vee G\ \psi$

  对任意$i \geq 0$, $\zeta^i \models \psi$ 或

  存在$i \geq 0$, $\zeta^i \models \phi$ 且对任意$j \leq i$, $\zeta^j \models \psi$

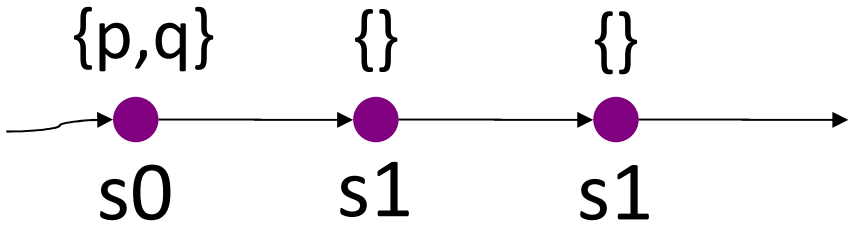
- $\zeta \models \phi\ R\ \psi$



  对任意$i \geq 0$, 若对所有$j < i$, $\zeta^j \not\models \phi$, 则$\zeta^i \models \psi$

Example 3： 证明(p R q → G q)不成立

- 构造AP={p,q}上的模型M=(S,ζ,L)
- S={s0,s1}
- ζ =s0(s1)$^{\omega}$
- L(s0)={p,q}, L(s1)={}



- M |= p R q 且 M ⊭ G q
- 因而存在不满足 (p R q → G q)的模型 。

Minimal Complete Set of Temporal Operators

Minimal Complete Set

X,F,G,R,U

F is expressible by U

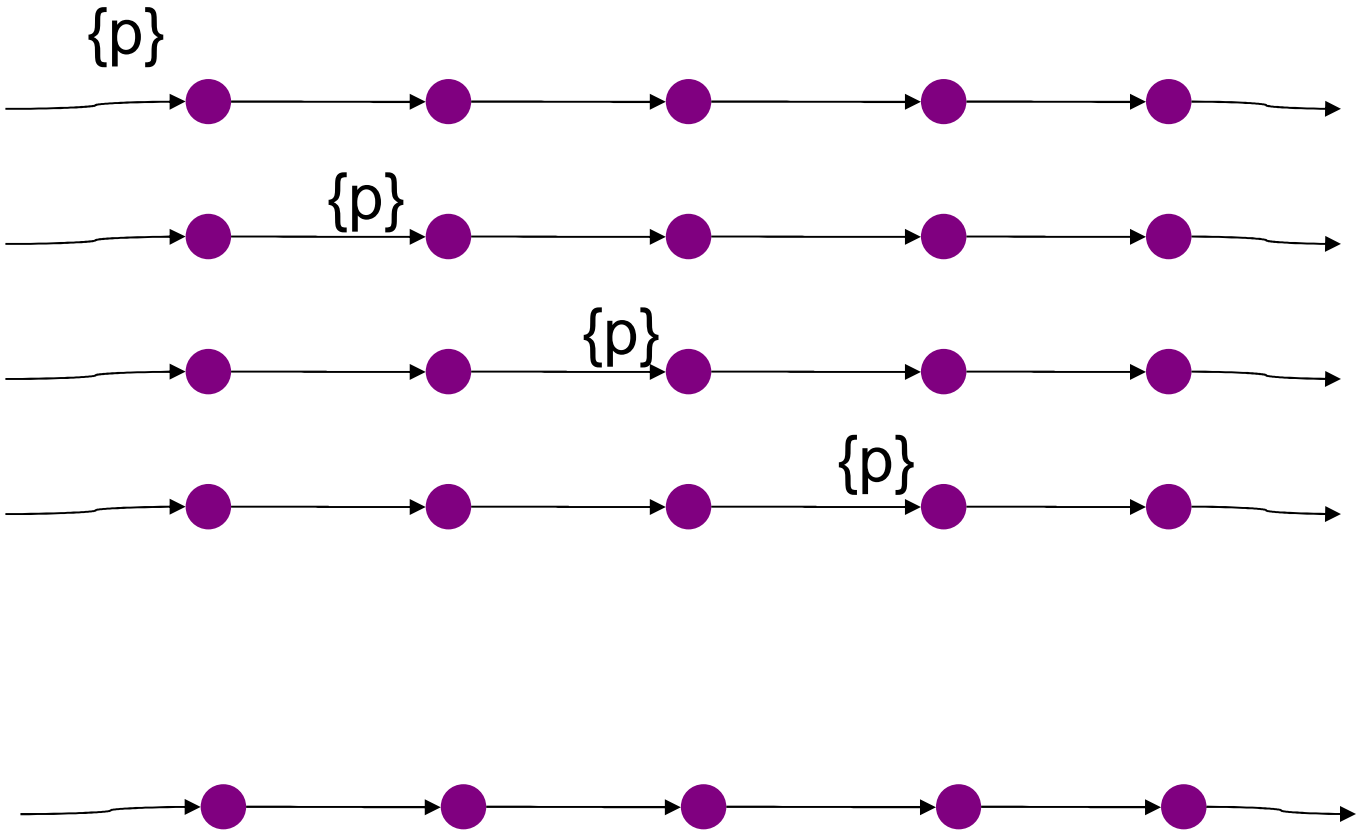
G is expressible by R

R is expressible by U

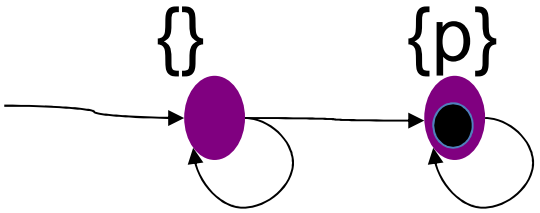
Then {X,U} is a complete set.

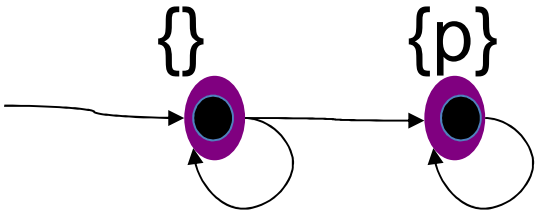
{X,U} is also a minimal complete set.

Examples for Orthogonality of X and U



Orthogonality of X and U



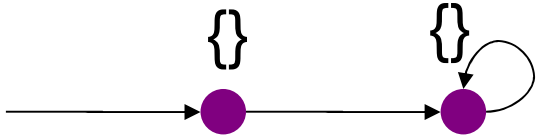


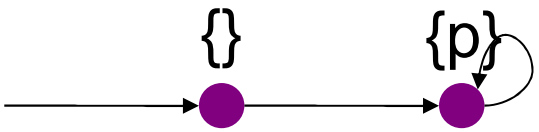
s0 |= (¬p U p)

not (s0' |= (¬p U p))

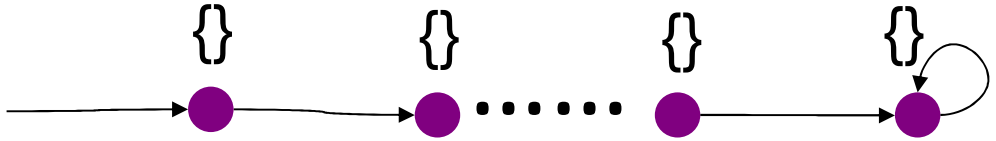
Proof by induction on length of formulas.

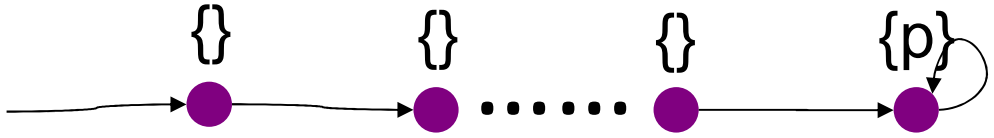
Propositional formulas, ¬, ∧, ∨, X





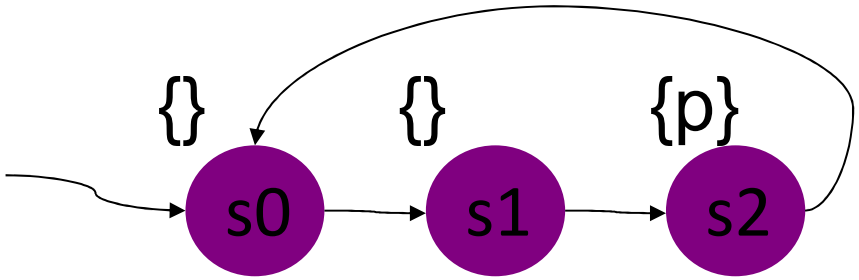
1

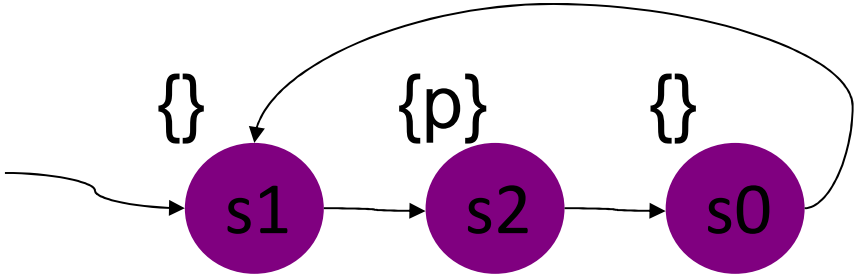




k+1 k

Orthogonality of X and U





M |= X¬p

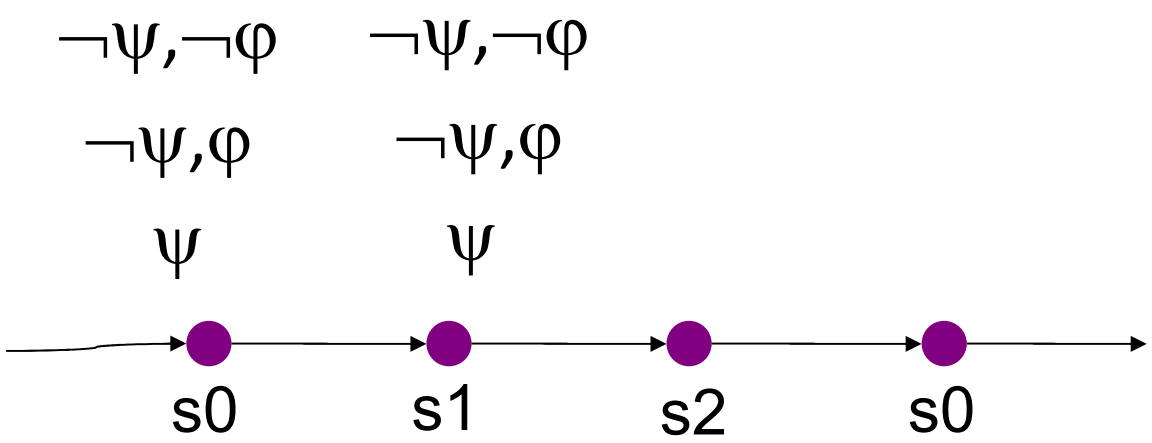
not (M' |= X¬p)

U:

Prop. formulas

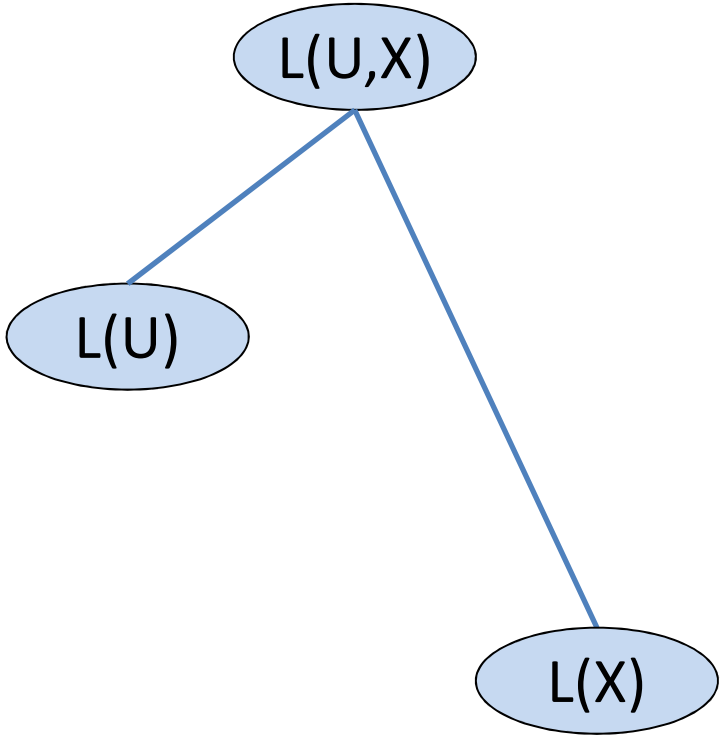
¬, ∧, ∨

φ U ψ

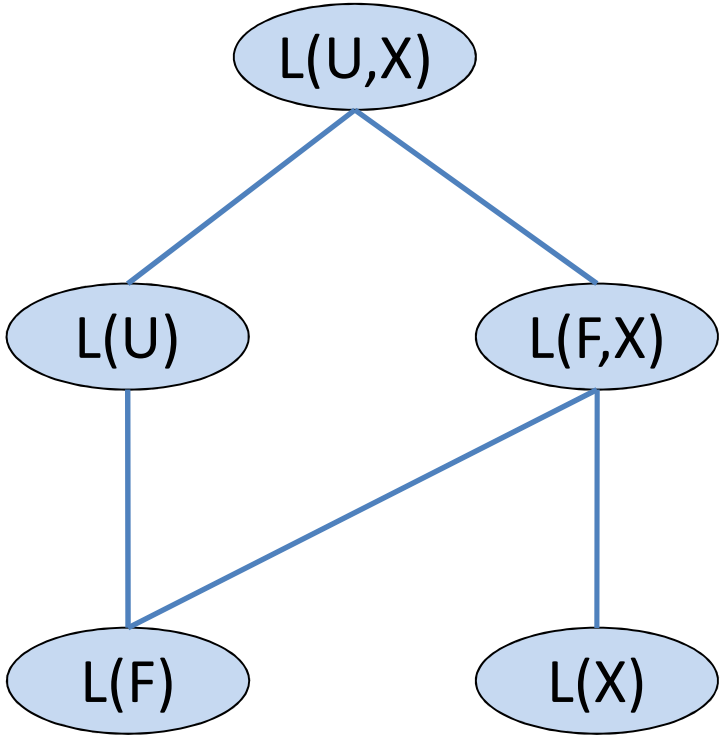


Expressivity

Expressivity of Subsets of PLTL



Expressivity of Subsets of PLTL



Expressivity

PLTL = star free regular ω-languages

Dual Operators and the Negation Normal Form (NNF)

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.

PLTL Proof System

Proof System for L(U,F,G,X)

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

Axioms for Temporal Logics Formulas

1. $G\neg p \leftrightarrow \neg Fp$
2. $G(p\rightarrow q)\rightarrow(Gp\rightarrow Gq)$
3. $Gp\rightarrow p$
4. $Gp\rightarrow Xp$
5. $Gp\rightarrow XGp$
6. $G(p\rightarrow Xp)\rightarrow(p\rightarrow Gp)$
7. $X\neg p\leftrightarrow \neg Xp$
8. $X(p\rightarrow q)\rightarrow(Xp\rightarrow Xq)$
9. $pUq\leftrightarrow(q\vee(p\wedge X(pUq))$
10. $pUq\rightarrow Fq$

Proof Rule (Generalization, G)

$$\frac{\vdash p}{\vdash Gp}$$

Propositional proof system

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

$$\frac{\vdash p \rightarrow q \qquad \vdash p}{\vdash q}$$

Proof System

The proof system is sound and complete.

例子x1(2)

Examples of Using Proof Rules

Example 1： $(p \wedge GXp) \rightarrow Gp$

1. p	AS1
2. GXP	AS2
3. $Xp \rightarrow (p \rightarrow Xp)$	AX
4. $G(Xp \rightarrow (p \rightarrow Xp))$	3+G
5. $GXp \rightarrow G(p \rightarrow Xp)$	4+A2+MP
6. $G(p \rightarrow Xp)$	5+AS2+MP
7. $p \rightarrow Gp$	6+A6+MP
8. Gp	7+AS1+MP

Example 2：(Xp → Xq) → X(p → q)

1. $\neg p \rightarrow (p \rightarrow q)$ AX
2. $G(\neg p \rightarrow (p \rightarrow q))$ G
3. $X(\neg p \rightarrow (p \rightarrow q))$ A4 + MP
4. $X\neg p \rightarrow X(p \rightarrow q)$ A8 + MP
5. $(\neg Xp \leftrightarrow X\neg p) \rightarrow((X\neg p \rightarrow X(p \rightarrow q)) \rightarrow (\neg Xp \rightarrow X(p \rightarrow q)))$ AX
6. $\neg Xp \rightarrow X(p \rightarrow q))$ A7+4+5+MP

Example 2: $(Xp \rightarrow Xq) \rightarrow X(p \rightarrow q)$

1. $q \rightarrow (p \rightarrow q)$ AX
2. $G(q \rightarrow (p \rightarrow q))$ G
3. $X(q \rightarrow (p \rightarrow q))$ A4 + MP
4. $Xq \rightarrow X(p \rightarrow q)$ A8 + MP

5. $(\neg Xp \rightarrow X(p \rightarrow q)) \rightarrow ((Xq \rightarrow X(p \rightarrow q)) \rightarrow ((Xp \rightarrow Xq) \rightarrow X(p \rightarrow q)))$ AX
6. $((Xp \rightarrow Xq) \rightarrow X(p \rightarrow q))$ q6+4+5+MP

Applications of PLTL

PLTL as a Specification Language

System Models: Labled Kripke Structures (K)

System Specifications: Formulas of PLTL (φ)

PLTL as a Specification Language

$K=\langle S,R,I,L\rangle$.

$K,\pi \models \phi$, if $\langle S,\pi,L\rangle \models \phi$.

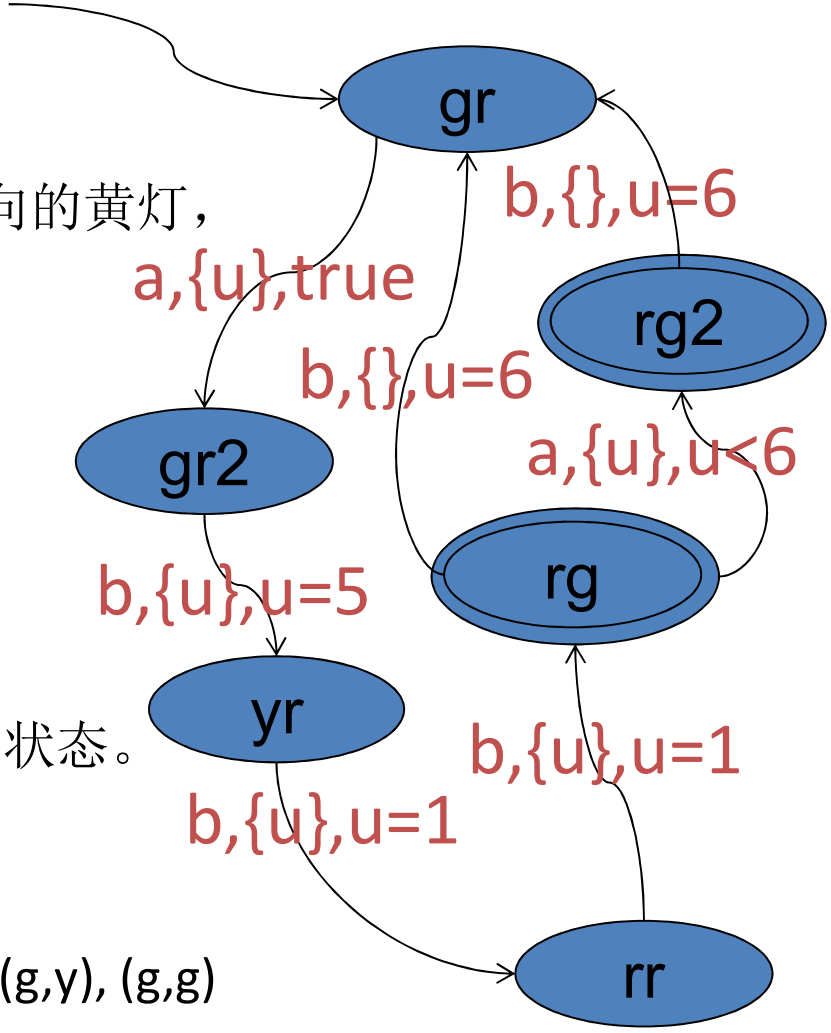
$K \models \phi$, if $K,\pi \models \phi$ for every computation π.

例子x1(3)

例子（时间自动机）

假设在一条街上，有行人过街用的红绿灯。
正常的时候是汽车绿灯和行人红灯。
行人按了绿色按钮之后5个时间单位有汽车方向的黄灯，
然后在1个时间单位后变成红灯，
又1个时间单位后有行人方向的绿灯。
汽车方向的红灯持续6个时间单位后恢复原状。

若在这6个时间单位中有行人按绿灯，
则红灯保持至行人按路灯之后6个时间单位。
系统的有效运行须包括无限次的行人方向绿灯状态。



状态(car,p): (r,r), (r,y), (r,g), (y,r), (y,y), (y,g), (g,r), (g,y), (g,g)
动作: a(按按钮), b(内部动作)

例子

只考虑行人方向的状态(r/g, a/¬a)：

r ∧ ¬a:　　gr

r ∧ a:　　gr2,yr,rr

g ∧ ¬a:　　rg

g ∧ a:　　rg2

G(r ∧ ¬a → ((r ∧ ¬a) U (r ∧ a))) ∧

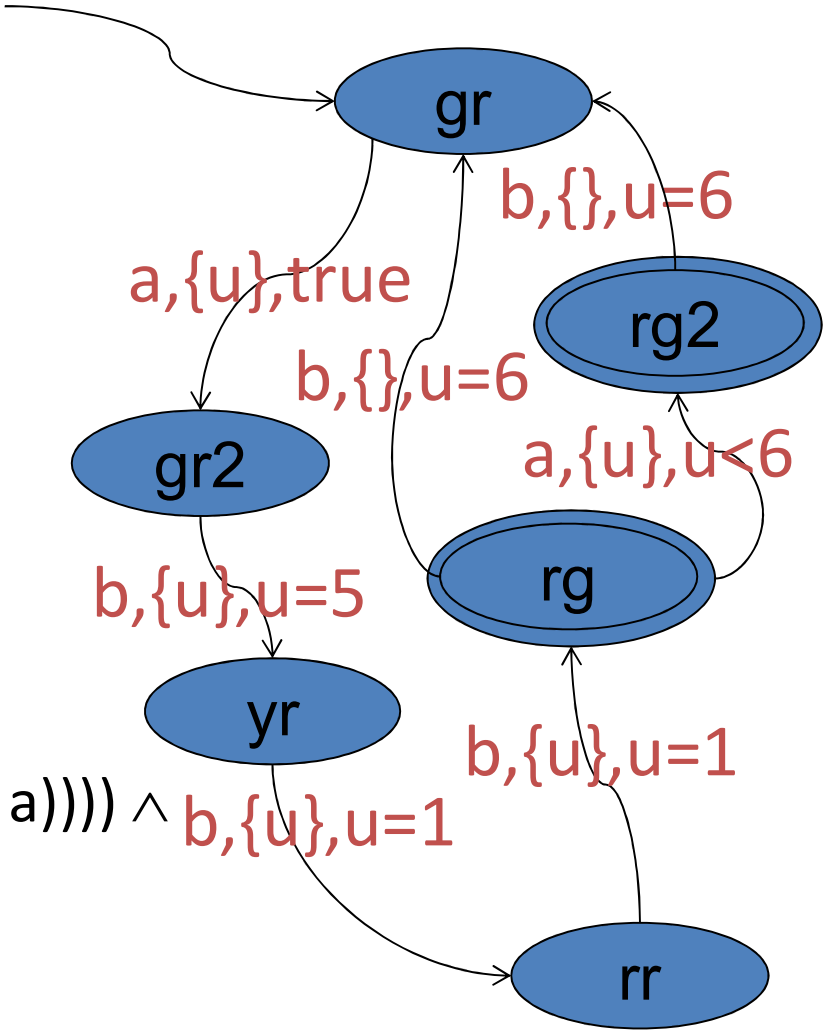
G(r ∧ a → ((r ∧ a) U (g ∧ ¬a))) ∧

G(g ∧ ¬a → ((g ∧ ¬a) U ((r ∧ ¬a) ∨ (g ∧ a)))) ∧

G(g ∧ a → ((g ∧ a) U (r ∧ ¬a))) ∧

G(¬(r ∧ g)) ∧

r ∧ ¬a



例子

只考虑行人方向的状态(r/g, a/¬a)：

r ∧ ¬a:　　gr

r ∧ a:　　gr2,yr,rr

g ∧ ¬a:　　rg

g ∧ a:　　rg2

G(r ∧ ¬a → ((r ∧ ¬a) U (r ∧ a))) ∧

G(r ∧ a → ((r ∧ a) U (g ∧ ¬a))) ∧

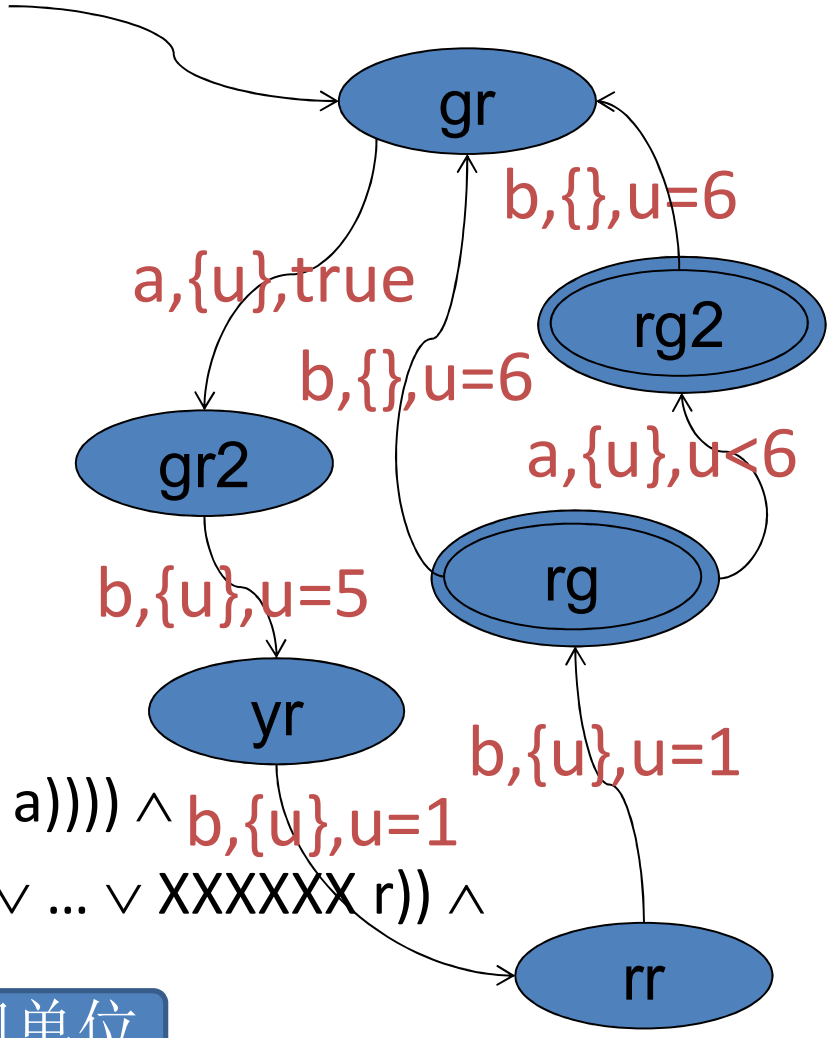
G(g ∧ ¬a → ((g ∧ ¬a) U ((r ∧ ¬a) ∨ (g ∧ a)))) ∧

G(g ∧ a → ((g ∧ a)U(r ∧¬a))∧(X r ∨ XX r ∨ … ∨ XXXXXX r)) ∧

G(¬(r ∧ g)) ∧

r ∧ ¬a

离散时间单位



PLTL as a Specification Language

System Models: Labeled Kripke Structures (K)

System Specifications: Formulas of PLTL (φ)

Verification of correctness:

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

PLTL as a Specification Language

Let φ be a propositional formula.

$K \models G\varphi$ -- φ is a safety property

$K \models F\varphi$ -- φ is an inevitability property

$K \not\models G\neg\varphi$ -- φ is a reachability property

$K \not\models F\varphi$ -- φ is an aviodability property

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.

The complexity of model checking is PSPACE-complete.

(II) Fixpoint Representation of PLTL

Given S, L.

Given $\zeta \in S^{\omega}$

$<S,\zeta,L> \models \varphi$

$[[\varphi]] = \{ \zeta \mid <S,\zeta,L> \models \varphi \}$

Fixpoint Representation of PLTL

Given M=<S,R,I,L>

$M \models \varphi$

$[[M]] \subseteq [[\varphi]]$

Fixpoint Representation of PLTL

- Preliminaries
- Representation of PLTL Formulas

Preliminaries

- Preliminaries
- Representation of PLTL Formulas

Sets

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)

函数

函数

单调(递增)函数

连续函数

a1,a2,… 是链

$f(a1 \cup a2 \cup \dots) = f(a1) \cup f(a2) \cup \dots$

不动点：$f(x)=x$

不动点

$f^0(a) = a, \quad f^{k+1}(a) = f(f^k(a))$

(完全偏序+最小元)上的连续函数f有最小不动点：

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

证明:

(1) μf 是不动点

(2) μf 是最小不动点

不动点

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

不动点:

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

$= \cup \{ f^{k+1}(\bot) \mid k \in N \}$

$= \cup \{ f^k(\bot) \mid k \in N \}$

$= \mu f$

最小不动点:

$B = f(B)$

$\bot \subseteq B$

$f(\bot) \subseteq B$

$ff(\bot) \subseteq B$

$\cup\{f^k(\bot)\} \subseteq B$

不动点

Knaster–Tarski 定理

完全格上的单调函数f有最小和最大不动点：

$$\mu f = \cap \{ a \mid f(a) \subseteq a \}$$
$$\nu f = \cup \{ a \mid a \subseteq f(a) \}$$

$$\nu Z.f(Z) = \neg \mu Z.\neg f(\neg Z)$$

不动点

$\mu f = \cap \{ a \mid f(a) \subseteq a \}$

不动点:

$A = \cap \{ a \mid f(a) \subseteq a \}$

$A \subseteq a$ for every a such that $f(a) \subseteq a$

$f(A) \subseteq f(a)$ 单调递增

$f(A) \subseteq a$

$f(A) \subseteq A$

$ff(A) \subseteq f(A)$ 则f(A)是某个a

$A \subseteq f(A)$ 则 $A = f(A)$

最小不动点:

$f(B) = B$

$A \subseteq B$

$\nu Z.f(Z)=\neg\mu Z.\neg f(\neg Z)$

- $\mu Z.f(Z) = \cap\{Z \mid f(Z)\subseteq Z\}$
- $\mu Z.\neg f(\neg Z) = \cap\{Z \mid \neg f(\neg Z)\subseteq Z\}$
- $\mu Z.\neg f(\neg Z) = \cap\{Z \mid f(\neg Z)\supseteq \neg Z\}$
- $\neg\mu Z.\neg f(\neg Z) = S\setminus \cap\{Z \mid f(\neg Z)\supseteq \neg Z\}$
- $\neg\mu Z.\neg f(\neg Z) = \cup\{S\setminus Z \mid f(\neg Z)\supseteq \neg Z\}$
- $\neg\mu Z.\neg f(\neg Z) = \cup\{\neg Z \mid f(\neg Z)\supseteq \neg Z\}$
- $\neg\mu Z.\neg f(\neg Z) = \cup\{Z \mid f(Z)\supseteq Z\} = \nu Z.f(Z)$

Representation of PLTL Formulas

$$[[p]] = \{ \pi \mid \pi \in S^{\omega}, p \in L(\pi_0) \}$$

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

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

$$[[\neg\varphi]] = S^{\omega} \setminus [[\varphi]]$$

Minimal Complete Set

X,F,G,R,U

R is expressible by U

G is expressible by R

F is expressible by U

Then {X,U} is a complete set.

Formulas

$[[X\ \varphi]] = \{ \pi \mid \pi \in S^{\omega}, \pi^{1} \in [[\varphi]] \}$

$[[\varphi\ U\ \psi]] = ?$

Recursive Equations

$\phi \, U \, \psi \equiv \psi \vee (\phi \wedge X(\phi \, U \, \psi))$

$\phi \, R \, \psi \equiv \psi \wedge (\phi \vee X(\phi \, R \, \psi))$

Let next(Y) denote $\{ \pi \mid \pi \in S^{\omega} , \pi^{1} \in Y \}$

Then $[[X(\phi \, U \, \psi)]] = next([[\phi \, U \, \psi]])$

$[[\phi \, U \, \psi]] \equiv [[\psi]] \cup ([[\phi \,]] \cap next([[\phi \, U \, \psi]]))$

Recursive Equations

$\phi \, U \, \psi \equiv \psi \vee (\phi \wedge X(\phi \, U \, \psi))$

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

$f: pow(S^{\omega}) \rightarrow pow(S^{\omega})$

Then $\phi \, U \, \psi$ is a fixpoint of f.

Fixpoint

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

f is monotonic;

$pow(S^{\omega})$ is a complete lattice.

f has a least and a greatest fixpoint

$\mu Z.f(Z)$, μf

$\nu Z.f(Z)$, νf

Fixpoint

f is continuous

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

We prove: $[[\phi \; U \; \psi]] = \mu f$

Then we have:

$\phi U \psi = \mu Z.f(Z) = \mu Z.(\psi \vee (\phi \wedge X(Z))$

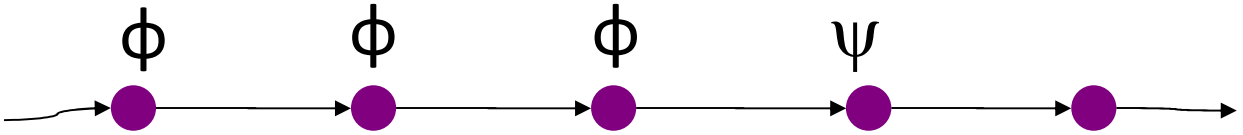
证明

证明 $\phi U \psi = \mu Z.f(Z) = \mu Z.(\psi \vee (\phi \wedge X(Z))$

证明

若 $\pi_0 \pi_1 \pi_2 \ldots \in \phi U \psi$

则 $\pi_0 \pi_1 \pi_2 \ldots \in \mu Z.(\psi \vee (\phi \wedge X(Z)) = \cup_{n \in N} f^n(\text{false})$



归纳法:

若 $\pi_0 \pi_1 \pi_2 \ldots \in \phi U \psi$

则 存在 $\pi_k \ldots \in \psi$ 且$\pi_i \ldots \in \phi$ for i=0,…,k-1

(k对应n-1)

k=0:

$\pi_0 \pi_1 \pi_2 \ldots \in \psi \in f^1(\text{false})$

假设k=m时:

若 $\pi_0 \pi_1 \pi_2 \ldots \in \phi U \psi$

且 $\pi_m \ldots \in \psi$ 且$\pi_i \ldots \in \phi$ for i=0,…,m-1

则 $\pi_0 \pi_1 \pi_2 \ldots \in f^{m+1}(\text{false})$

证明k=m+1时:

若 $\pi_0 \pi_1 \pi_2 \ldots \in \phi U \psi$

且 $\pi_{m+1} \ldots \in \psi$ 且$\pi_i \ldots \in \phi$ for i=0,…,m

则 $\pi_0 \pi_1 \pi_2 \ldots \in f^{m+2}(\text{false})$

k=m+1

要证明:

若 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi U \psi$

且 $\pi_{m+1}\,\ldots\ldots \in \psi$ 且$\pi_i\,\ldots\ldots \in \phi$ for i=0,…,m

则 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in f^{m+2}(\text{false})$

有 $f(Z)=(\psi \vee (\phi \wedge X(Z))$

已知 $\pi_1\,\pi_2\,\ldots\ldots \in f^{m+1}(\text{false})$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in X(\pi_1\,\pi_2\,\ldots\ldots)$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in X(f^{m+1}(\text{false}))$

又 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi \wedge X(f^{m+1}(\text{false}) \subseteq f^{m+2}(\text{false})$

k=m+1

要证明:

若 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi U \psi$

且 $\pi_{m+1}\,\ldots\ldots \in \psi$ 且$\pi_i\,\ldots\ldots \in \phi$ for i=0,…,m

则 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in f^{m+2}(\text{false})$

有 $f(Z)=(\psi \vee (\phi \wedge X(Z))$

已知 $\pi_1\,\pi_2\,\ldots\ldots \in f^{m+1}(\text{false})$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in X(\pi_1\,\pi_2\,\ldots\ldots)$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in X(f^{m+1}(\text{false}))$

又 $\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi$

$\pi_0\,\pi_1\,\pi_2\,\ldots\ldots \in \phi \wedge X(f^{m+1}(\text{false}) \subseteq f^{m+2}(\text{false})$

根据归纳法:

若 $\pi \in \phi U \psi$

则 $\pi \in \mu Z.(\psi \vee (\phi \wedge X(Z))$

Representation of PLTL Formulas

$$[[p]] = \{ \pi \mid \pi \in S^{\omega}, p \in L(\pi_0) \}$$

$$[[X\,\varphi]] = \{ \pi \mid \pi \in S^{\omega}, \pi^1 \in [[\varphi]] \}$$

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

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

$$F\psi = \mu Z.(\psi \vee X(Z))$$

$$G\psi = \nu Z.(\psi \wedge X(Z))$$

(III) νTL

Syntax of νTL

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of νTL formulas is defined as follows.

$$\Phi == p \mid Z \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \neg \Phi \mid X\, \Phi \mid \mu Z.\Phi \mid \nu Z.\Phi$$

Variables are in the scope of even number of neg.

Semantics

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

$[[p]]e = \{ \pi \mid \pi \in S^{\omega}, p \in L(\pi_0) \}$

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

$[[X \varphi]]e = \{ \pi \mid \pi \in S^{\omega}, \pi^1 \in [[\varphi]]e \}$

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

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

$[[\neg\varphi]]e = S^{\omega} \setminus [[\varphi]]e$

$[[\mu Z.\phi]]e = \cap\{ Y \subseteq S^{\omega} \mid [[\phi]]e(Z/Y) \subseteq Y \}$

$[[\nu Z.\phi]]e = \cup\{ Y \subseteq S^{\omega} \mid Y \subseteq [[\phi]]e(Z/Y) \}$

Closed Formulas

Formulas without free variables.

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

$[[\varphi]] = [[\varphi]]e$ for any e

Example

s0s1s2s3s4s5….

$\nu Z.(p \wedge XXZ)$

p is true at all even places

Satisfiability

The complexity is PSPACE-complete.

Applications of νTL

νTL as a Specification Language

System Models: Kripke Structures (K)

System Specifications: Closed Formulas of νTL (φ)

$K \models \varphi$

$[[K]] \subseteq [[\varphi]]$

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.

The complexity is PSPACE-complete.

(IV) Summary

PLTL

递推形式的公式 → 不动点表示 → νTL

PLTL: 基本、直观

νTL: 扩展、表达能力强

练习：

(1)

a. 应用语义证明$G(p \rightarrow Xp) \rightarrow (p \rightarrow Gp)$ 成立，
解释为什么这个蕴涵关系反过来是不成立的。

b. 应用推理系统证明以下等价关系:

$X(p \vee q) \leftrightarrow (Xp \vee Xq)$

(2)

用PLTL写下信号灯变化的规范：

信号灯依次序绿黄红变化，每个状态有且只有一个信号，初始信号为绿色，黄色只停留一个状态，红绿色可以连续在多个状态上成立。