

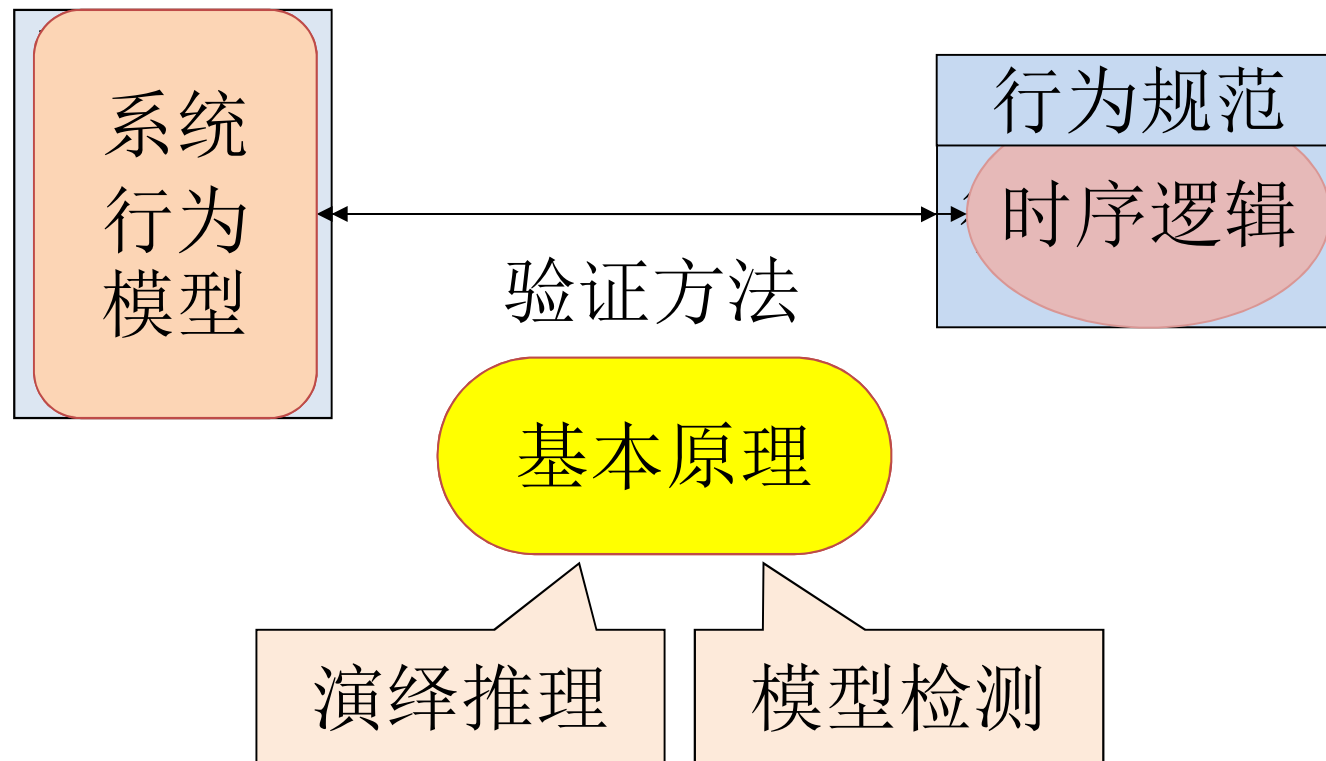
Linear Temporal Logic

中国科学院软件研究所
计算机科学国家重点实验室

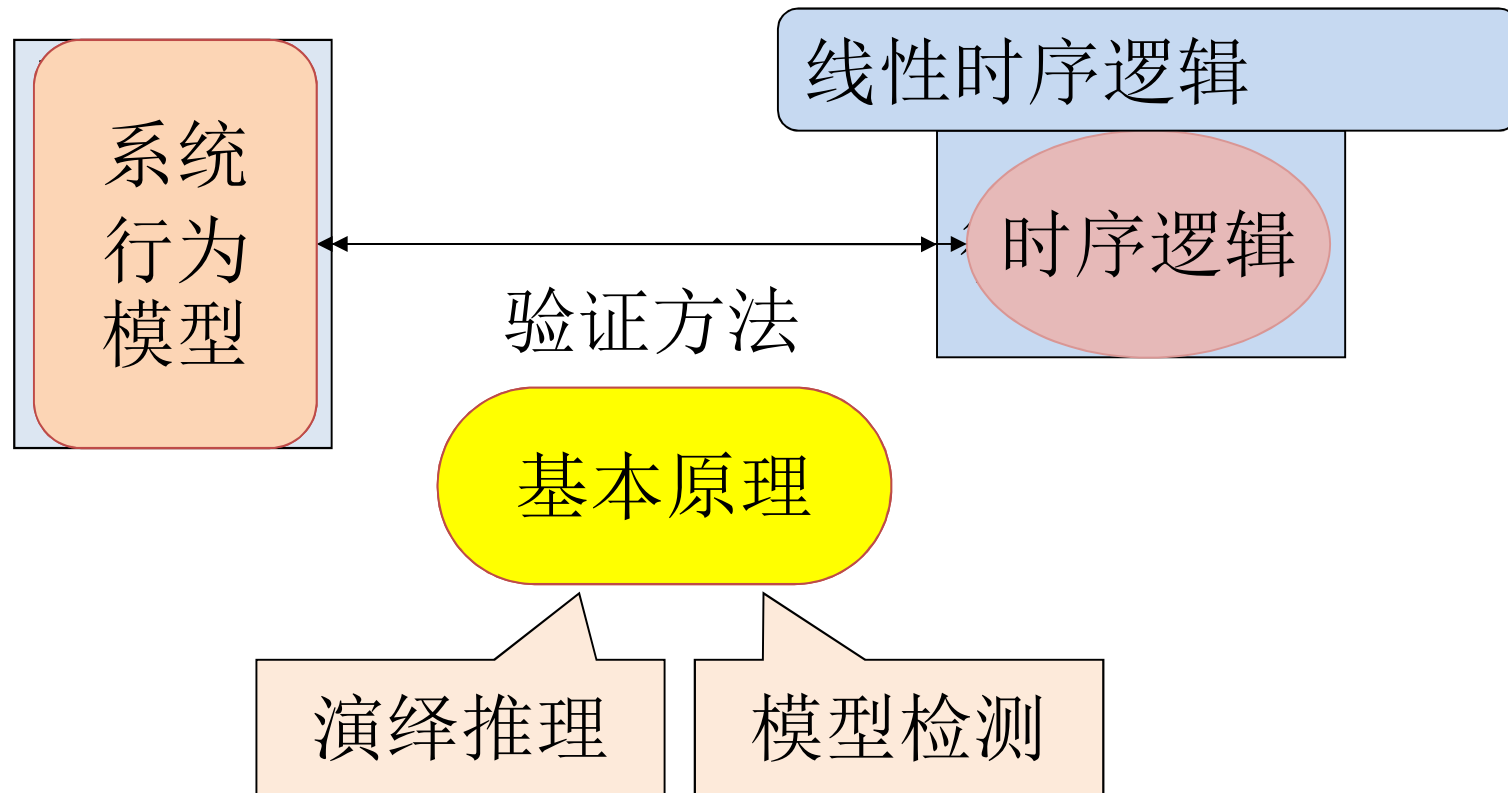
张文辉

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

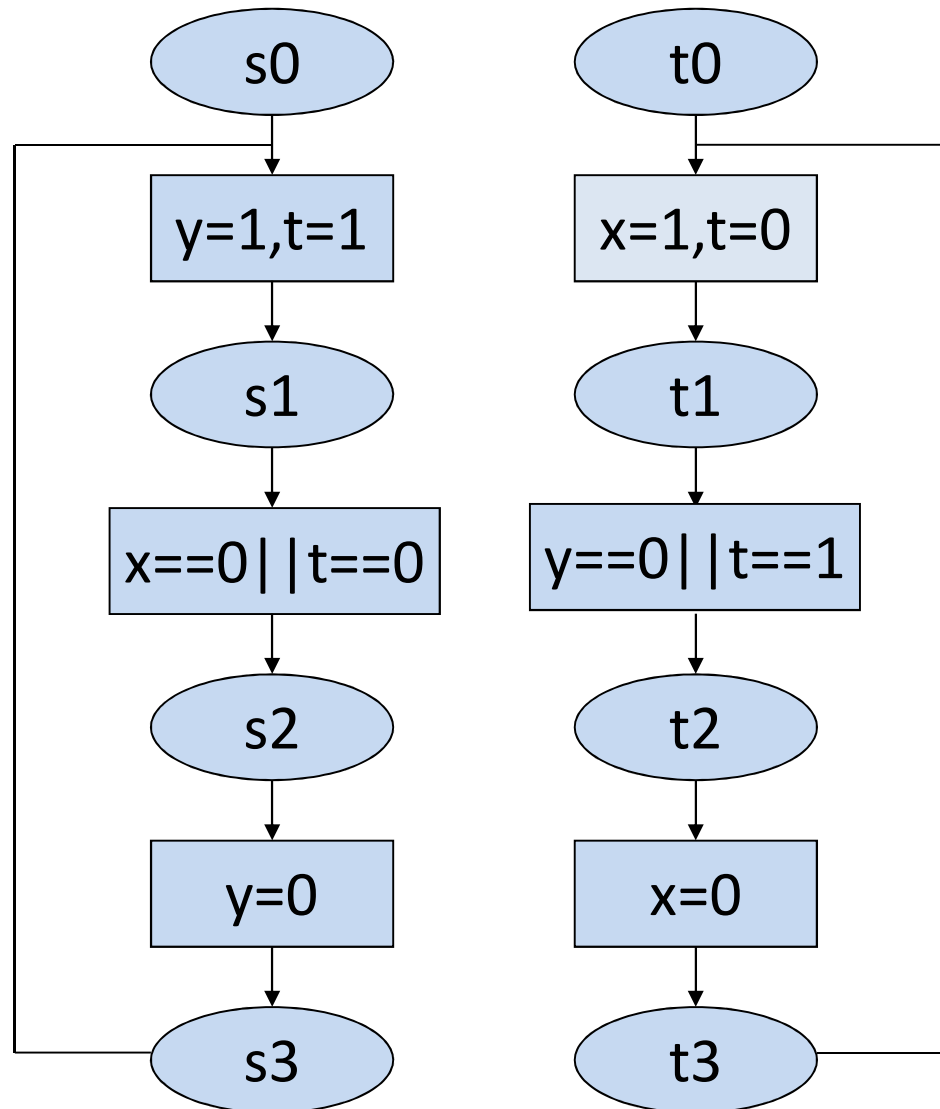
课程内容



课程内容



Example



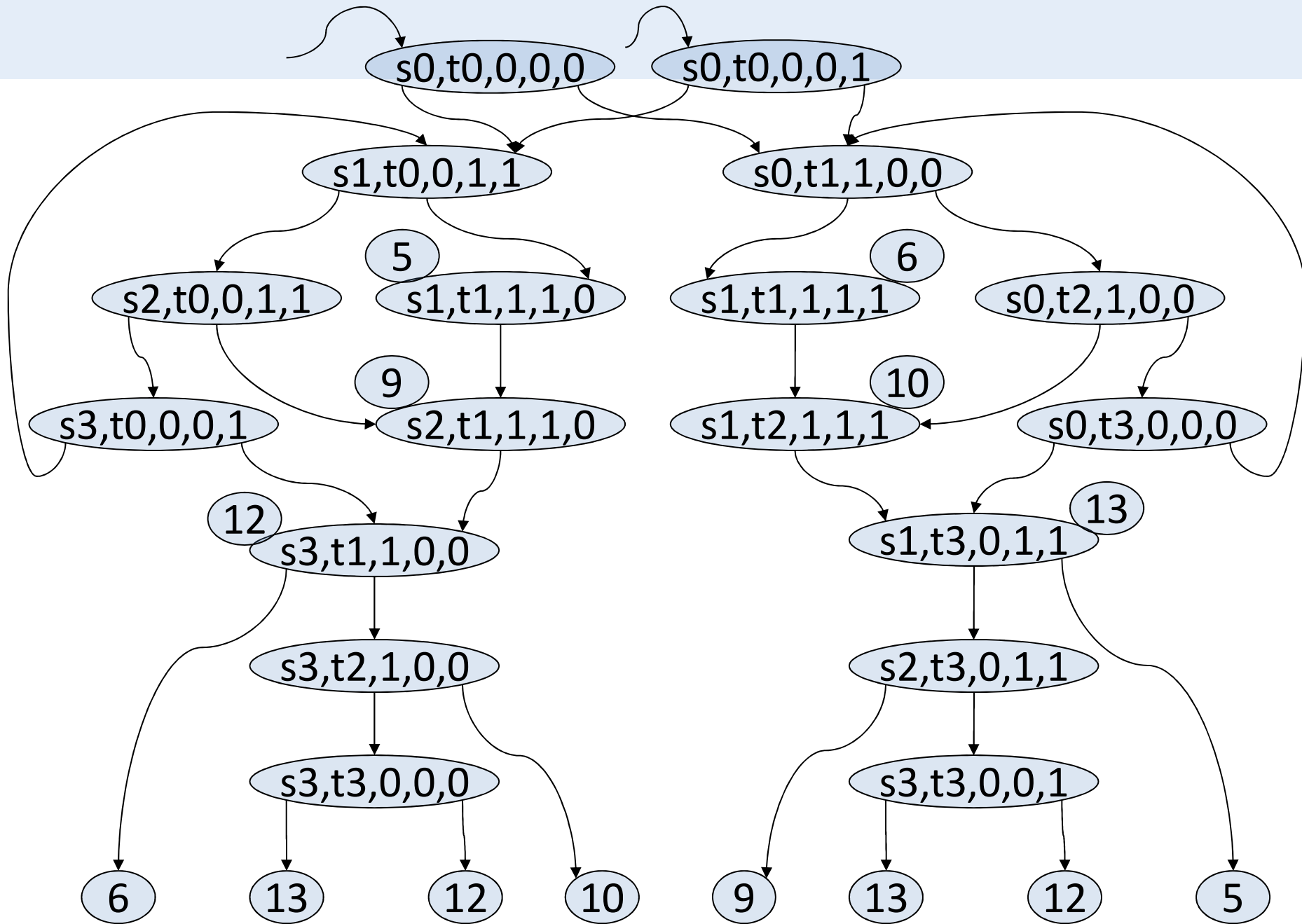
Initial States

s0

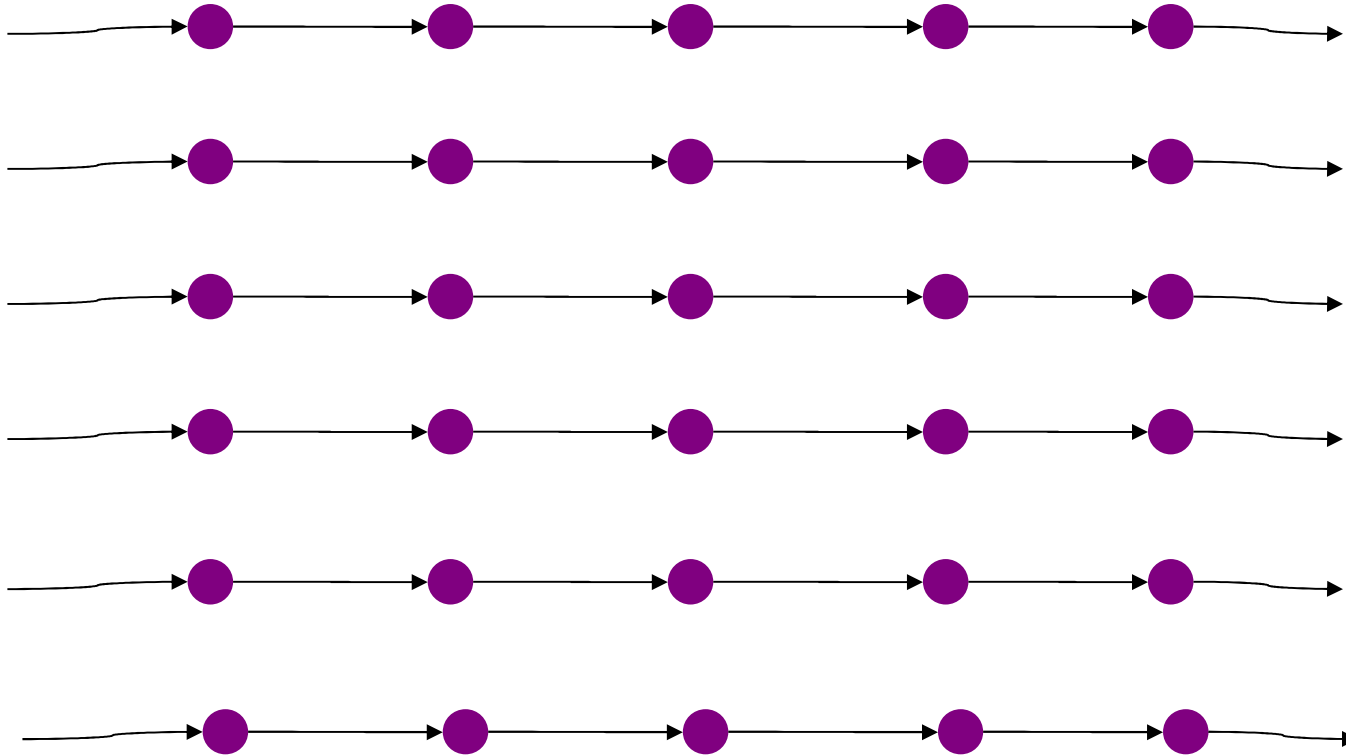
t0

x=0

y=0



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
- ν TL

(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: $G (\!(a=s2 \wedge b=t2)\!)$
- Inevitability $F (a=s2 \vee b=t2)$

- Response $G (a=s1 \rightarrow F (a=s2))$
- Imm. Response $G (a=s1 \rightarrow X (a=s2))$
- Priority $G (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow (a=s2 \text{ R } b \neq t2))$
- FCFS $G (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow (b \neq t2 \text{ U } a=s2))$

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.

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

Sometimes, X,G,F are written as O, \square , \diamond .

Examples of Properties

- Safety: $G (\!(a=s2 \wedge b=t2)\!)$
- Inevitability $F (a=s2 \vee b=t2)$

- Response $G (a=s1 \rightarrow F (a=s2))$
- Imm. Response $G (a=s1 \rightarrow X (a=s2))$
- Priority $G (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow (a=s2 R b \neq t2))$
- FCFS $G (a=s1 \wedge b \neq t1 \wedge b \neq t2 \rightarrow (b \neq t2 U a=s2))$

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: $G (\neg(p8 \wedge p12))$
- 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 , $(M \models \phi \text{ iff } M \models \psi)$.

Dual Operators

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

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

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

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

$$F \phi \equiv \neg \perp U \phi$$

$$G \phi \equiv \perp R \phi$$

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

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 $j \leq i$, $\zeta^j \models \psi$



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

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 $j \leq i$, $\zeta^j \models \psi$



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

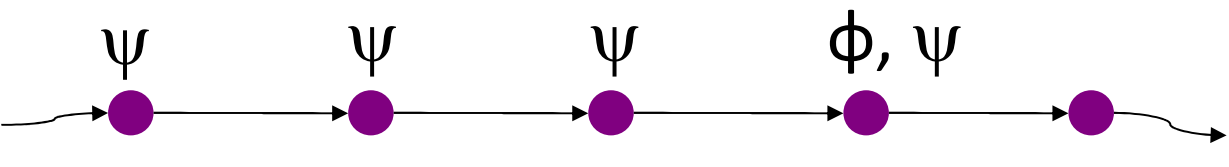
对任意 $i \geq 0$, 若对所有 $j < i$, $\zeta^j \not\models \phi$, 则 $\zeta^i \models \psi$

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 $j \leq i$, $\zeta^j \models \psi$



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

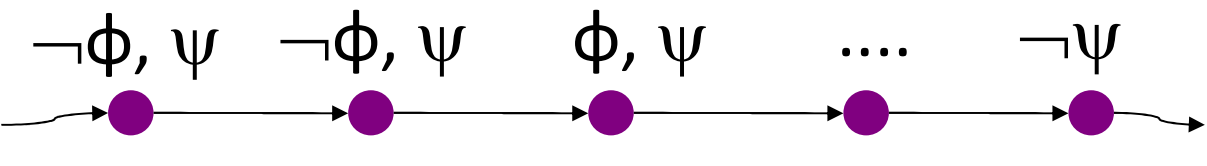
对任意 $i \geq 0$, 若对所有 $j < i$, $\zeta^j \not\models \phi$, 则 $\zeta^i \models \psi$

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

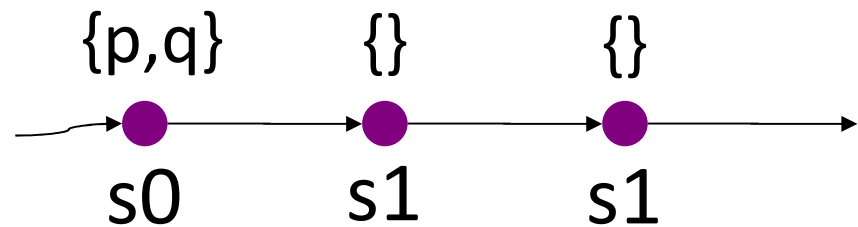
存在 $i \geq 0$, $\zeta^i \models \phi$ 且对任意 $j \leq i$, $\zeta^j \models \psi$

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

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 $(p R q \rightarrow G q)$ 不成立

- 构造 $AP = \{p, q\}$ 上的模型 $M = (S, \zeta, L)$
- $S = \{s_0, s_1\}$
- $\zeta = s_0(s_1)^\omega$
- $L(s_0) = \{p, q\}, L(s_1) = \{\}$



- $M \models p R q$ 且 $M \not\models G q$
- $M \not\models p R q \rightarrow G q$
- 存在不满足 $(p R q \rightarrow G q)$ 的模型

Minimal Complete Set of Temporal Operators

Minimal Complete Set

X, F, G, R, U

F is expressible by U

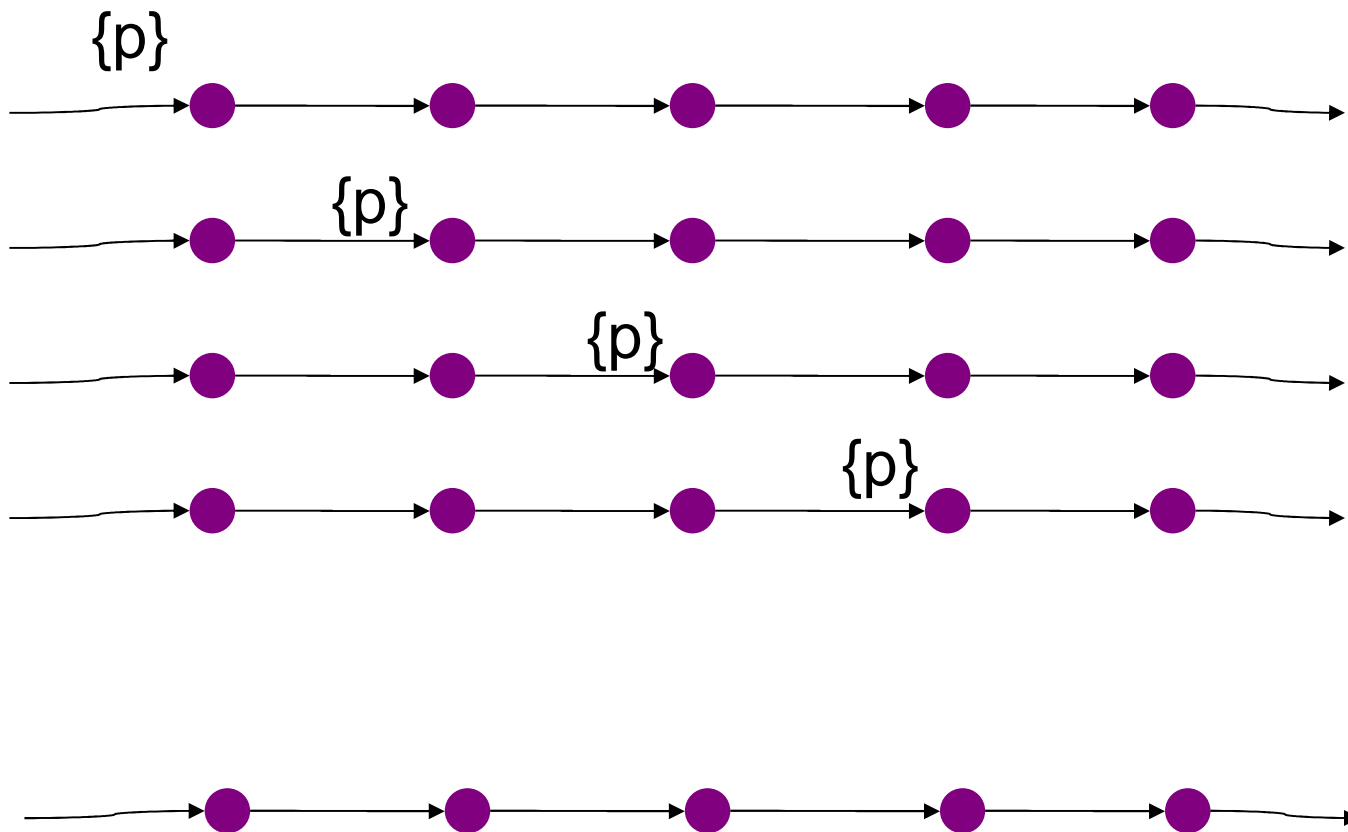
G is expressible by R

R is expressible by U

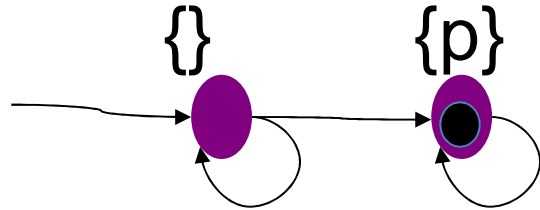
Then $\{X, U\}$ is a complete set.

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

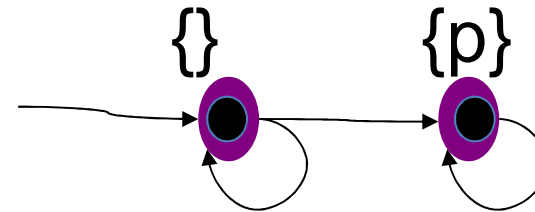
Examples for Orthogonality of X and U



Orthogonality of X and U



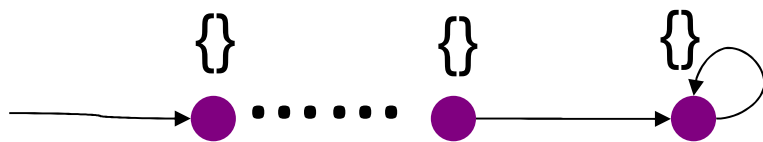
$M \models (\neg p \cup p)$



not $(M' \models (\neg p \cup p))$

Proof by induction on length of formulas.

Propositional formulas, \neg , \wedge , \vee , X



$n \geq 1$

0

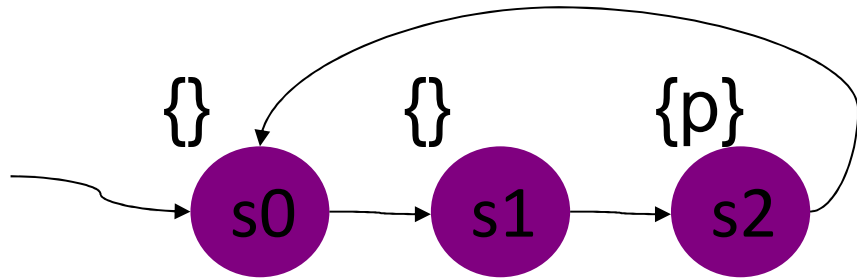


$n \geq k+1$

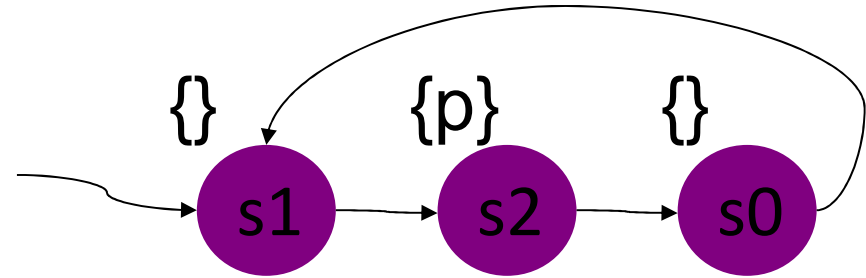
k

0

Orthogonality of X and U



$M \models X\neg p$



not $(M' \models X\neg p)$

U:

Prop. formulas

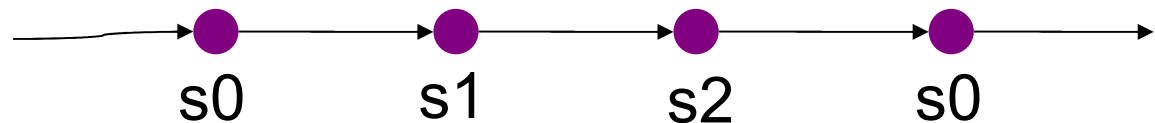
\neg, \wedge, \vee

$\varphi \cup \psi$

$\neg\neg\psi, \neg\neg\varphi$ $\neg\neg\psi, \neg\neg\varphi$

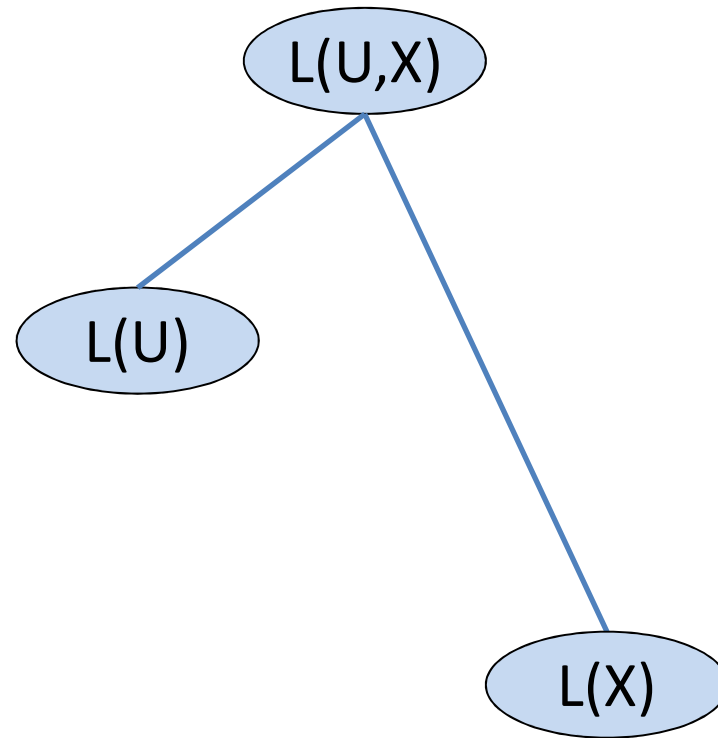
$\neg\neg\psi, \varphi$ $\neg\neg\psi, \varphi$

ψ ψ

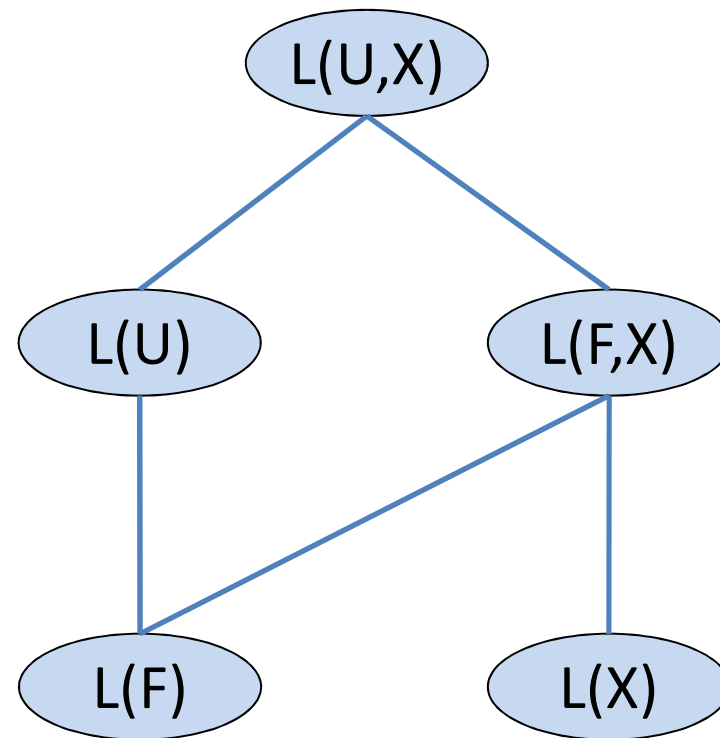


Expressivity

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):

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

Proof System

The proof system is sound and complete.



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

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. $((Xp \rightarrow Xq) \rightarrow X(p \rightarrow q))$ p6+4+5+MP

Applications of PLTL

PLTL as a Specification Language

System Models:

Labeled 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 .



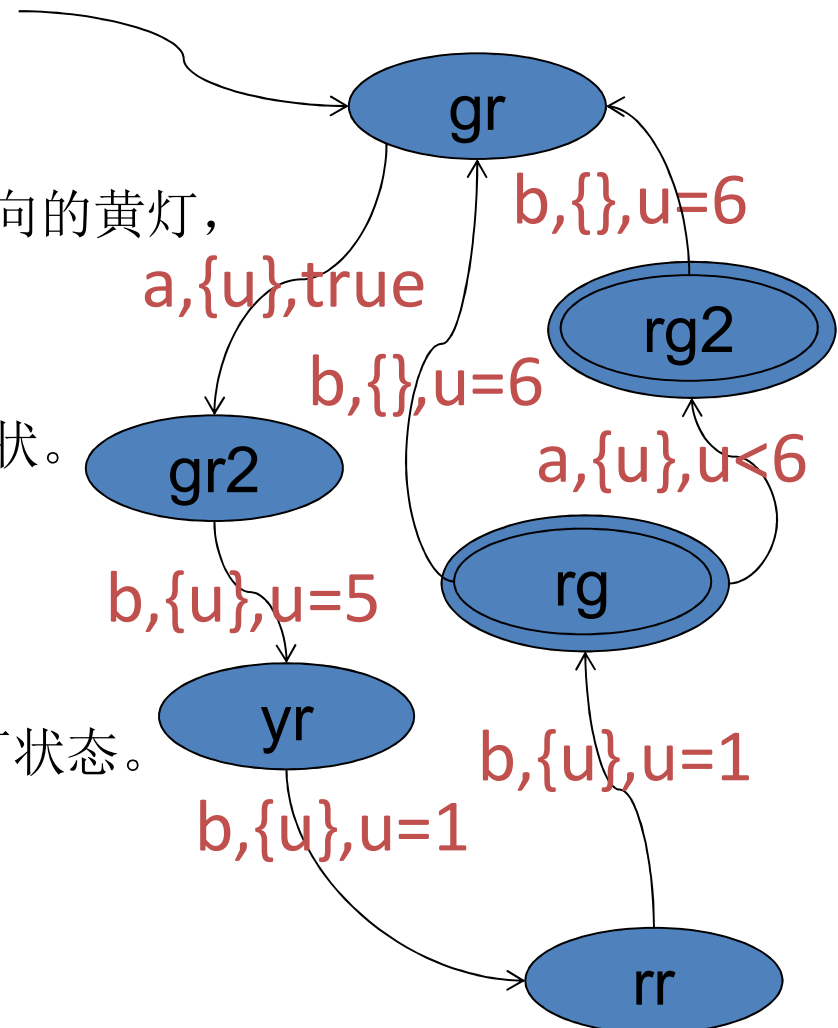
例子（时间自动机）

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。
汽车方向的红灯又持续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按钮，
则红灯保持至行人按按钮之后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,g), (y,r), (y,g), (g,r), (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):

$r \wedge \neg a$: gr

$r \wedge a$: gr2,yr,rr

$g \wedge \neg a$: rg

$g \wedge a$: rg2

$G(r \wedge \neg a \rightarrow ((r \wedge \neg a) \cup (r \wedge a))) \wedge$

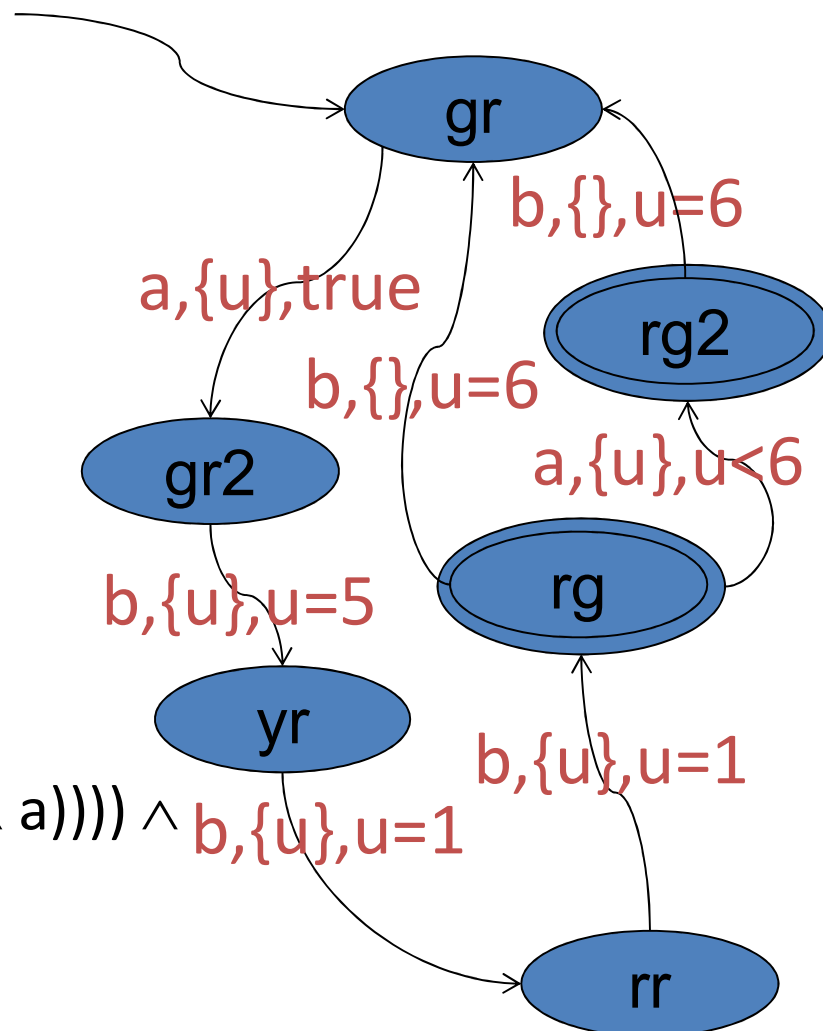
$G(r \wedge a \rightarrow ((r \wedge a) \cup (g \wedge \neg a))) \wedge$

$G(g \wedge \neg a \rightarrow ((g \wedge \neg a) \cup ((r \wedge \neg a) \vee (g \wedge a)))) \wedge$

$G(g \wedge a \rightarrow ((g \wedge a) \cup (r \wedge \neg a))) \wedge$

$G(\neg(r \wedge g)) \wedge$

$r \wedge \neg a$



例子

只考虑行人方向的状态(r/g, a/¬a):

$r \wedge \neg a$: gr

$r \wedge a$: gr2,yr,rr

$g \wedge \neg a$: rg

$g \wedge a$: rg2

$G(r \wedge \neg a \rightarrow ((r \wedge \neg a) \cup (r \wedge a))) \wedge$

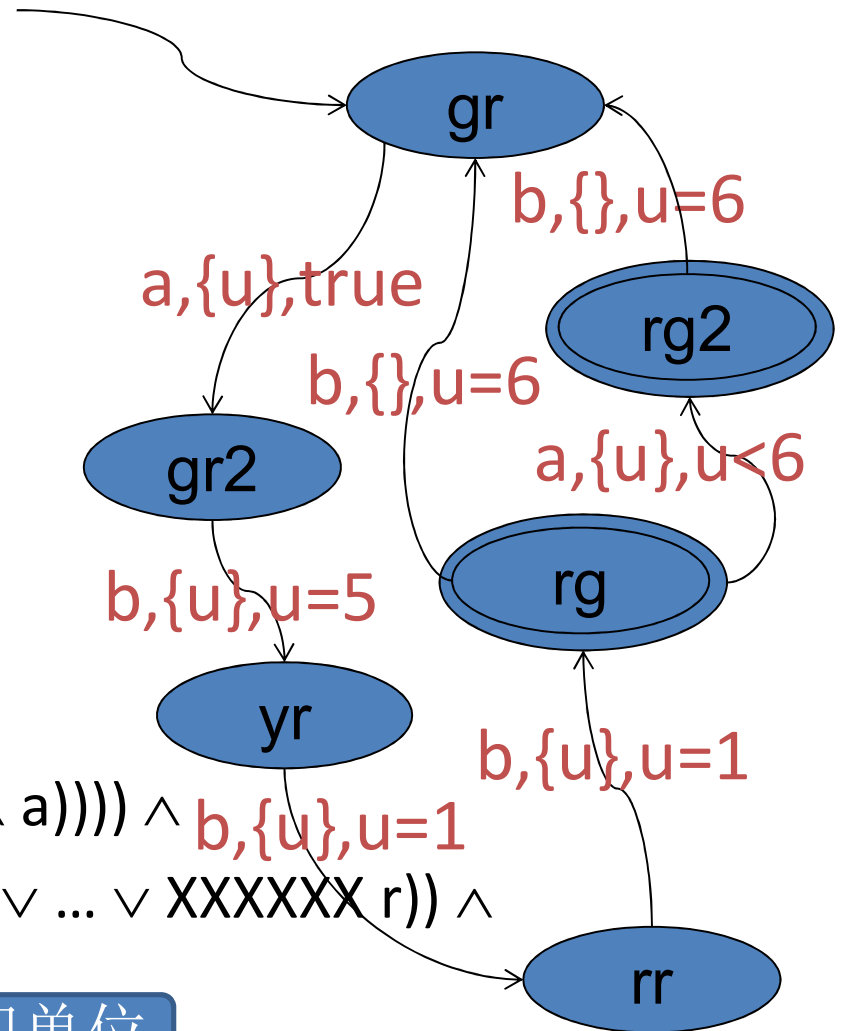
$G(r \wedge a \rightarrow ((r \wedge a) \cup (g \wedge \neg a))) \wedge$

$G(g \wedge \neg a \rightarrow ((g \wedge \neg a) \cup ((r \wedge \neg a) \vee (g \wedge a)))) \wedge$

$G(g \wedge a \rightarrow ((g \wedge a) \cup (r \wedge \neg a))) \wedge (X r \vee XX r \vee \dots \vee XXXXXX r)$

$G(\neg(r \wedge g)) \wedge$

$r \wedge \neg a$



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 $\zeta \in S^\omega$

$\langle S, \zeta, L \rangle \models \varphi$

$[[\varphi]] = \{ \zeta \mid \langle S, \zeta, L \rangle \models \varphi \}$

Fixpoint Representation of PLTL

Given $M = \langle S, R, I, L \rangle$

$M \models \varphi$

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

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

a_1, a_2, \dots 是链

$$f(a_1 \cup a_2 \cup \dots) = f(a_1) \cup f(a_2) \cup \dots$$

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:

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

证明:

- (1) μf 是不动点
- (2) μf 是最小不动点

不动点

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

不动点:

$$\begin{aligned} f(\mu f) &= f(\cup \{ f^k(\perp) \mid k \in \mathbb{N} \}) \\ &= \cup \{ f^{k+1}(\perp) \mid k \in \mathbb{N} \} \\ &= \cup \{ f^k(\perp) \mid k \in \mathbb{N} \} \\ &= \mu f \end{aligned}$$

最小不动点:

$$B = f(B)$$

$$\perp \subseteq B$$

$$f(\perp) \subseteq B$$

$$ff(\perp) \subseteq B$$

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

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:

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

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

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

不动点

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

不动点:

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

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

$f(A) \subseteq f(a)$ 单调递增

$$f(A) \subseteq a$$

$$f(A) \subseteq A$$

$$ff(A) \subseteq f(A)$$

$$A \subseteq f(A)$$

则 $f(A)$ 是某个 a

$$\text{则 } A = f(A)$$

最小不动点:

$$f(B) = B$$

$$A \subseteq B$$

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

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

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

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

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

Recursive Equations

$$\phi \text{ U } \psi \equiv \psi \vee (\phi \wedge X(\phi \text{ U } \psi))$$

$$\phi \text{ R } \psi \equiv \psi \wedge (\phi \vee X(\phi \text{ R } \psi))$$

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

Then $[[X(\phi \text{ U } \psi)]] = \text{next}([[\phi \text{ U } \psi]])$

$$[[\phi \text{ U } \psi]] \equiv [[\psi]] \cup ([[\phi]] \cap \text{next}([[\phi \text{ U } \psi]]))$$

Recursive Equations

$$\phi \cup \psi \equiv \psi \vee (\phi \wedge X(\phi \cup \psi))$$

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

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

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

Fixpoint

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

f is monotonic;

$\text{pow}(S^\omega)$ 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

f is continuous

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

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

Then we have:

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

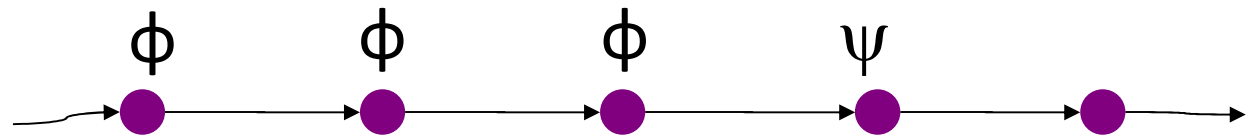
证明 

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

证明

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

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



归纳法:

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

则存在 $\pi_k \dots \in \psi$ 且 $\pi_i \dots \in \phi$ for $i=0, \dots, k-1$

(k对应n-1)

k=0:

$\pi_0 \pi_1 \pi_2 \dots \in \psi$, i.e., $f^1(\text{false})$

假设k=m时:

若 $\pi_0 \pi_1 \pi_2 \dots \in \phi \cup \psi$

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

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

证明k=m+1时:

若 $\pi_0 \pi_1 \pi_2 \dots \in \phi \cup \psi$

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

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

$k=m+1$

要证明:

若 $\pi_0 \pi_1 \pi_2 \dots \in \phi \cup \psi$

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

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

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

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

$\pi_0 \pi_1 \pi_2 \dots \in X(\{\pi_1 \pi_2 \dots\})$

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

又 $\pi_0 \pi_1 \pi_2 \dots \in \phi$

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

$k=m+1$

要证明:

若 $\pi_0 \pi_1 \pi_2 \dots \in \phi \cup \psi$

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

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

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

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

$\pi_0 \pi_1 \pi_2 \dots \in X(\{\pi_1 \pi_2 \dots\})$

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

又 $\pi_0 \pi_1 \pi_2 \dots \in \phi$

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

根据归纳法:

若 $\pi \in \phi \cup \psi$

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) vTL

Syntax of ν TL

Let AP be a set of proposition symbols.

Definition

Let p range over AP.

The set Φ of ν TL 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

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

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

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

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

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

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

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

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

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

Closed Formulas

Formulas without free variables.

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

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

Example

$s_0s_1s_2s_3s_4s_5\dots$

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

p is true at all even places

Satisfiability

The complexity is PSPACE-complete.

Applications of vTL

vTL as a Specification Language

System Models:

Kripke Structures (K)

System Specifications:

Closed Formulas of vTL (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 \rightarrow 不动点表示 \rightarrow vTL

PLTL: 基本、直观

vTL: 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。