华东师范大学
软硬件协同设计技术与应用教育部工程研究中心
URL—http://faculty.ecnu.edu.cn/chenyixiang
yxchen@sei.ecnu.edu.cn

时态逻辑系统

陈仪香,吴恒洋

MoE Engineering Center for Software/Hardware Co-Design Technology and Application
Software Engineering Institute
East China Normal University(ECNU)
Shanghai, China

2018级研究生软件工程理论课程，2018年4月

Back
Close

时态逻辑系统

- 表达/刻画逻辑中的时态性：一个公式不是静态地取真值，而是动态地取真值。
- 一个公式可能在某些状态是真的，而在其它状态是假的。
- 真值的静态性变成动态性。
- 公式随着系统的状态演化而改变真值。

模型检测

时态逻辑系统可用于模型检测。

- 模型通常是迁移系统/有限自动机,它描述了状态迁移过程，反映状态的演化, 而公式是时态逻辑公式ϕ。
- 模型检测的目的是表明模型$\mathcal{M}$满足公式ϕ, 即$\mathcal{M} \models \phi$。
- 通常实现模型检测，需要做下面三件事情:
  - 建立模型$\mathcal{M}$,
  - 编写公式ϕ,
  - 运行模型检测器，输入$\mathcal{M}$和ϕ,
- 模型检测器将输出Yes若$\mathcal{M} \models \phi$成立,否则输出No。

时态逻辑分类

- 线性时态逻辑系统LTL：时间是按照线性进行迁移的
- 计算树逻辑系统CTL：时间是按照树进行迁移的.

线性时态逻辑系统LTL

- 引入连接词表示时间：X, F, G, U, W, R
  - X—Next 下一个状态，
  - F—某个Future 状态，
  - G—所有将来的状态(Globally)，
  - U—Until 直到
  - W—Weak-Until,弱直到
  - R—Release, 解释,释放
- 引入原子公式Atoms：$p, q, e, \cdots, p_1, p_2, \cdots$

  如: 打印机Q_5是忙的, 进程3259在悬挂, 记录$R1$的内容是整数值6, 数据的长度是99,等
- 计算路,也叫状态序列，简称路

LTL的语法

定义 LTL的公式

公式ϕ定义为

$$
\begin{aligned}
\phi \ ::= \ & \top \mid \bot \mid p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \\
& (X\phi) \mid (F\phi) \mid (G\phi) \mid (\phi U \phi) \mid (\phi W \phi) \mid (\phi R \phi)
\end{aligned}
$$

例子: $(F(p \to Gr) \vee ((\neg q)Up))$,画出Parse tree; 非法公式: Ur, pGq.

LTL的语法

1. 在任何状态下，若有一个请求出现,那么这个请求将会被接受.
   G (请求出现$\longrightarrow$ F接受)
2. 某个进程往往在每个计算路上被无限次地激活.
   GF激活
3. 一部上升的电梯在第二层时不会改变上升方向直到第5层楼,若电梯内有人要到第5层楼.
   G (2层$\wedge$向上$\wedge$ 有人要到5层$\longrightarrow$(向上方向U5层楼))
4. 已经到达了开始状态，但准备工作还没有做好是不可能的.
   $G\neg$(开始了$\wedge\neg$ 准备)。

LTL的语义

迁移系统(Transition System)：通过状态(静态结构)和迁移(动态结构)来为系统提供模型.

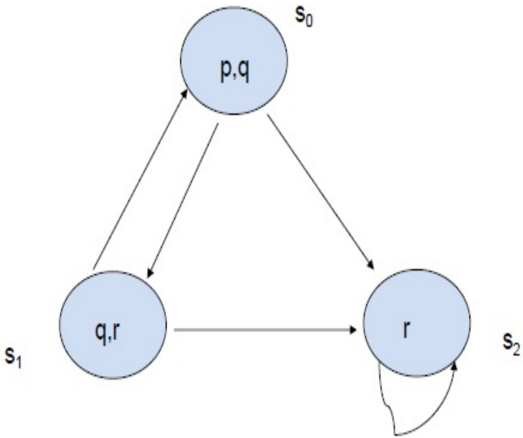
定义 迁移系统

迁移系统$\mathcal{M} = (S, \to, L)$是由下面三部分组成:

- S是状态集
- $\to$是S上的二元关系,称为迁移关系,使得$\forall s \in S$,都有$s' \in S$且$s \to s'$, 即$\to$ 是S上的连续关系
- 标号函数$L : S \to \mathcal{P}(Atoms)$

注：(1) 迁移系统是一种特殊的Kripke模型。
(2) 迁移系统可直接称为模型.
(3) 例子：

例子



LTL的语义

定义　路

模型$\mathcal{M} = (S, \to, L)$的路是指$S$中的无限状态序列$s_1, s_2, \cdots, s_n, \cdots$使得$\forall i \geq 1, s_i \to s_{i+1}$.

通常将路写成：$s_1 \to s_2 \to \cdots$, 并用π表示一条路.

注：(1) π^i表示从状态s_i开始的路. 请写出上例中的一些路.

(2)计算路的展开(unwinding)。

LTL的语义

定义　路满足公式

给定模型$\mathcal{M} = (S, \rightarrow, L)$以及路$\pi = s_1 \rightarrow s_2 \rightarrow \cdots$. 定义$\pi$满足公式$\phi$，记作$\pi \models \phi$, 归纳如下:

1. $\pi \models \top$
2. $\pi \not\models \bot$
3. $\pi \models p$ 当且仅当$p \in L(s_1)$
4. $\pi \models \neg\phi$ 若$\pi \not\models \phi$
5. $\pi \models \phi \wedge \psi$ 若$\pi \models \phi$且$\pi \models \psi$.
6. $\pi \models \phi \vee \psi$ 若$\pi \models \phi$或$\pi \models \psi$.
7. $\pi \models \phi \rightarrow \psi$ 若$\pi \models \phi$则$\pi \models \psi$
8. $\pi \models X\phi$ 若$\pi^2 \models \phi$
9. $\pi \models G\phi$ 若$\forall i \geq 1, \pi^i \models \phi$
10. $\pi \models F\phi$ 若$\exists i \geq 1$使得$\pi^i \models \phi$

11. $\pi \models \phi U \psi$ 若$\exists i \geq 1$使得$\pi^i \models \psi$且对于所有的$j = 1, 2, \cdots, i-1$都有$\pi^j \models \phi$.

12. $\pi \models \phi W \psi$ 若或者$\exists i \geq 1$使得$\pi^i \models \psi$且对于所有的$j = 1, 2, \cdots, i-1$都有$\pi^j \models \phi$或者对于所有的$k \geq 1$都有$\pi^k \models \phi$.

13. $\pi \models \phi R \psi$ 若或者$\exists i \geq 1$使得$\pi^i \models \phi$且对于所有的$j = 1, 2, \cdots, i$都有$\pi^j \models \psi$或者对于所有的$k \geq 1$都有$\pi^k \models \psi$.

图示: $\pi \models \phi$.

- 原子命题a: $$\begin{array}{ccccccccccc} \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \cdots \\ a & & \text{任意} & & \text{任意} & & \cdots & & & & \end{array}$$

- Xa: $$\begin{array}{ccccccccccc} \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \cdots \\ \text{任意} & & a & & \text{任意} & & \text{任意} & & \cdots & & \end{array}$$

- aUb: $$\begin{array}{ccccccccccc} \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \cdots \\ a, \neg b & & a, \neg b & & b & & \text{任意} & & \cdots & & \end{array}$$ $(\neg b$ 可以不标.)

- aRb: $$\begin{array}{ccccccccccc} \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \cdots \\ b & & b & & a, b & & \text{任意} & & \cdots & & \end{array}$$

  或者

  $$\begin{array}{ccccccccccc} \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \bigcirc & \to & \cdots \\ b & & b & & b & & \cdots & & & & \end{array}$$

- aWb: 请大家画出

定义　状态满足公式

设$\mathcal{M}=(S,\rightarrow,L)$是一个模型,$s\in S$, ϕ是一个LTL公式，若对$\mathcal{M}$的从s出发的每条路π都有$\pi\models\phi$，则称状态s满足ϕ，记作$\mathcal{M},s\models\phi$，或$s\models\phi$.

例子: 接前面的例子, 考察迁移系统中，状态满足哪些逻辑公式.

- $s_0 \models (p \wedge q)$;
- $s_0 \models \neg r$;
- $s_0 \models \top$;
- $s_0 \models Xr$;
- $s_0 \not\models X(q \wedge r)$;
- $s_0 \models G\neg(p \wedge r)$;
- $s_2 \models Gr$;
- $s \models F(\neg q \wedge r) \rightarrow FGr$;
- $s_0 \not\models GFp$; 路$s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_1 \rightarrow \cdots$满足该公式, 但路$s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow s_2 \rightarrow \cdots$不满足.
- $s_0 \models GFp \rightarrow GFr$, 但$s_0 \not\models GFr \rightarrow GFp$.

语义等价

定义　语义等价$\phi \equiv \psi$

设ϕ, ψ是LTL公式,若对于所有的模型$\mathcal{M}$以及$\mathcal{M}$中的所有的路π都有$\pi \models \phi$ 当且仅当$\pi \models \psi$, 则称ϕ 与ψ 是语义等价的,记作$\phi \equiv \psi$.

定理　语义等价等价刻画 设ϕ, ψ是LTL公式,它们是语义等价的, 当且仅当若对于所有的模型$\mathcal{M}$以及$\mathcal{M}$中的所有的状态s都有$s \models \phi$ 当且仅当$s \models \psi$.

语义等价

定理　下面各条成立

de Margan律	$\phi \wedge \psi \equiv \neg(\neg\phi \vee \neg\psi)$
	$\phi \vee \psi \equiv \neg(\neg\phi \wedge \neg\psi)$
幂等律	$\neg\neg\phi \equiv \phi$
对偶性	$G\phi \equiv \neg F\neg\phi$
	$F\phi \equiv \neg G\neg\phi$
	$\phi U\psi \equiv \neg(\neg\phi R\neg\psi)$
	$\phi R\psi \equiv \neg(\neg\phi U\neg\psi)$
自对偶性	$X\phi \equiv \neg X\neg\phi$
分配性	$F(\phi \vee \psi) \equiv F\phi \vee F\psi$
	$G(\phi \wedge \psi) \equiv G\phi \wedge G\psi$

思考: $F(\phi \wedge \psi) \equiv F\phi \wedge F\psi$ (?); $G(\phi \vee \psi) \equiv G\phi \vee G\psi$ (?)

连接词的充分性

定理 连接词相互定义

$$
\begin{aligned}
F\phi &\equiv \top U \phi \\
G\phi &\equiv \bot R \phi \\
\phi W \psi &\equiv \phi U \psi \vee G\phi \\
\phi W \psi &\equiv \psi R(\phi \vee \psi) \\
\phi R \psi &\equiv \psi W(\phi \wedge \psi) \\
\phi U \psi &\equiv \phi W \psi \wedge F\psi
\end{aligned}
$$

连接词的充分性：
$\{U, X\}, \{R, X\}, \{W, X\}$

综上, LTL可以简便的表示如下:

$$\phi ::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid X\phi \mid \phi U \phi$$

Back
Close

与$\Box$, $\diamond$的关系

定义:

$$\diamond\,\phi \stackrel{def}{=} \top U \phi \tag{1}$$

与

$$\Box\phi \stackrel{def}{=} \neg \diamond \neg\phi \tag{2}$$

进一步:

$$\diamond\phi = F\phi,\quad \Box\phi = G\phi.$$

$\diamond$:最终,将来; $\Box$: 总是, 从现在起永远.

模型检测:互斥

当并发进程共享资源(如磁盘上的某个文件, 或数据库登陆), 通常要求两个进程不能同时获取进入. 进程不能同时编辑相同的文件.

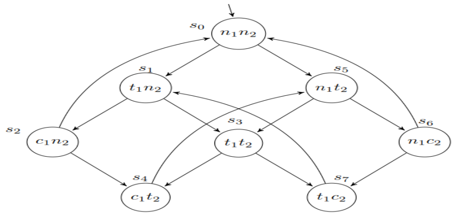
需要给定某个临界区, 在任意时刻只安排一个进程在临界区.

问题：如何设计协议以确定在任意时刻，哪个进程被允许进入临界区.

1. n:表示在非临界状态

2. t: 试图进入临界状态

3. c: 已在临界区的状态



A model for mutual exclusion.

exclusion.png

1.安全性: 任何时候最多一个进程在临界区

2.活性: 任何进程只要要求进入临界区,最终会进入.

3.非阻塞性: 任何进程总能要求进入临界区.

1. 安全性:

$$G\neg(c_1 \wedge c_2)$$

2.活性:

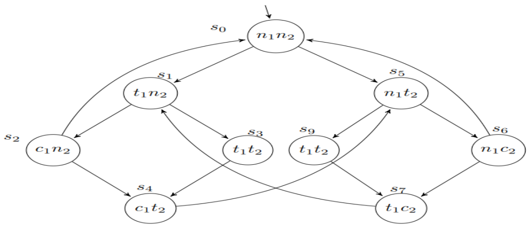
$$G(t_1 \to Fc_1)$$

3.非阻塞性: 不能被LTL表示. 这是因为需要表达:对于满足n_1的每个状态, 要有后继状态满足t_1,然而路径上的存在量词不能被LTL表示.

1.安全性:被初始状态满足(每个状态都满足).

2. 活性: 不被初始状态满足, 这是因为在路$s_0 \to s_1 \to s_3 \to s_7 \to s_1 \to s_3 \to s_7 \cdots$上$c_1$总是错的.

问题: 能否设计满足活性的互斥模型



Another model for mutual exclusion.

exclusion2.png

Back

Close

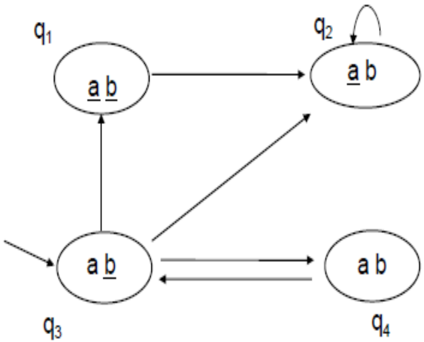
作业

1. 画出下面LTL公式的Parse 树
   - $Fp \wedge Gq \rightarrow pWr$
   - $F(p \rightarrow Gr) \vee \neg qUp$
   - $pW(qWr)$
   - $GFp \rightarrow F(q \vee s)$
2. 证明: $\phi U\psi \equiv \psi R(\phi \vee \psi) \wedge F\psi$
3. 依照下图的系统，考虑下面每个LTL公式ϕ
   - Ga
   - aUb
   - $aUX(a \wedge \neg b)$
   - $X\neg b \wedge G(\neg a \vee \neg b)$
   - $X(a \wedge b) \wedge F(\neg a \wedge \neg b)$

   (a) 找到一条从q_3出发的路，满足公式ϕ

(b) 确定是否有$\mathcal{M}, q_3 \models \phi$.

(c) 若将$\underline{a}$和$\underline{b}$解释为a与b的非，并表示通信协议中的发射信息，而a, b为接受信息，解释这些公式的具体含义.



Back
Close

计算树逻辑CTL

- 计算树逻辑，也叫分支时间逻辑，Computation Tree Logic，Branching-Time Logic。
- 它的时间模型向一棵树的结构，其未来是不确定的，未来会有不同的路，而且任何一条路都是一条实际的路。
- LTL的时态连接词U, F, G, X+量词A和E，其中A表示所有的路，而E表示存在一条路。

CTL的语法

CTL的公式定义为:

$$\begin{array}{rcl}\phi & ::= & \bot \mid \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \rightarrow \phi \mid \\ & & AX\phi \mid EX\phi \mid AF\phi \mid EF\phi \mid AG\phi \mid EG\phi \mid \\ & & A[\phi U \phi] \mid E[\phi U \phi].\end{array}$$

其中p是原子命题公式。

例子: $A(AX\neg pUE(EX(p\wedge q)U\neg p)$

Parse树：

例子

1. 存在一可到达满足q的状态

$$EFq$$

2. 从所有满足p的状态出发，有一直保持p直到满足q的状态出现

$$AG(p \rightarrow E[pUq])$$

3. 只要满足p的状态出现，就有系统可能永远保持q

$$AG(p \rightarrow EGq)$$

4. 有一可达的状态使得从此状态出发的所有可达状态都满足q

$$EFAGq$$

5. 进程总可以请求进入它的界区

$$AG(r \rightarrow EXt)$$

6. 对于任何状态，若一个请求出现则这个请求最终会被接受

$$AG(\underline{请求} \rightarrow AF\ \underline{接受})$$

7. 一部在2楼处于上升电梯，当有乘客在想到5楼时，电梯不会改变上升方向直到5楼

$$AG(\underline{2楼} \wedge \underline{上升} \wedge \underline{按下5楼按钮} \rightarrow A[\underline{上升}U\underline{5楼}])$$

8. 从任何状态出发总能到达Restart状态

$$AG(EF\underline{\mathrm{Restart}})$$

CTL的语义

定义

给定模型$\mathcal{M} = (S, \to, L)$, $s \in S$, ϕ是CTL公式。以ϕ的结构归纳定义$\mathcal{M}, s \models \phi$如下：

1. $\mathcal{M}, s \models \top$
2. $\mathcal{M}, s \not\models \bot$
3. $\mathcal{M}, s \models p$ 当且仅当$p \in L(s)$
4. $\mathcal{M}, s \models \neg\phi$ 若$\mathcal{M}, s \not\models \phi$
5. $\mathcal{M}, s \models \phi \wedge \psi$ 若$\mathcal{M}, s \models \phi$且$\mathcal{M}, s \models \psi$.
6. $\mathcal{M}, s \models \phi \vee \psi$ 若$\mathcal{M}, s \models \phi$或$\mathcal{M}, s \models \psi$.
7. $\mathcal{M}, s \models \phi \to \psi$ 若$\mathcal{M}, s \models \phi$则$\mathcal{M}, s \models \psi$
8. $\mathcal{M}, s \models AX\phi$ 若对于所有的s_1, 只要$s \to s_1$就有$\mathcal{M}, s_1 \models \phi$
9. $\mathcal{M}, s \models EX\phi$ 若存在某个s_1使得$s \to s_1$且$\mathcal{M}, s_1 \models \phi$
10. $\mathcal{M}, s \models AG\phi$ 若对于从s出发的所有路$s_1 \to s_2 \to \cdots$,其中s_1就是s，以及此路上的所有s_i 都有$\mathcal{M}, s_i \models \phi$

11. $\mathcal{M}, s \models EG\phi$ 存在一条从s出发的路$s_1 \to s_2 \to \cdots$,其中s_1就是s，以及此路上的所有s_i 都有$\mathcal{M}, s_i \models \phi$

12. $\mathcal{M}, s \models AF\phi$ 若对于从s出发的所有路$s_1 \to s_2 \to \cdots$,其中s_1就是s，以及路上有s_i使得$\mathcal{M}, s_i \models \phi$

13. $\mathcal{M}, s \models EF\phi$ 若存在一条从s出发的路$s_1 \to s_2 \to \cdots$,其中s_1就是s，以及此路上有s_i使得$\mathcal{M}, s_i \models \phi$

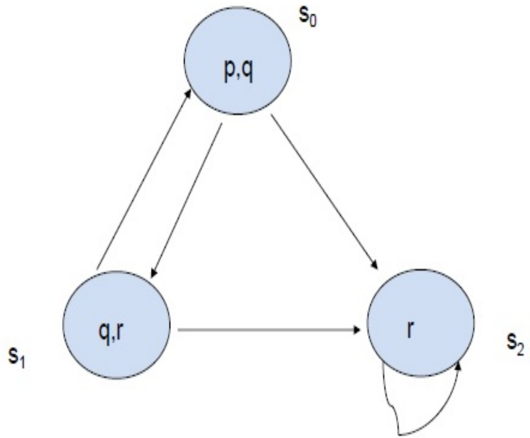
14. $\mathcal{M}, s \models A[\phi U \psi]$ 若对于从s出发的所有路$s_1 \to s_2 \to \cdots$,其中s_1就是s ,存在$i \geq 1$使得$\mathcal{M}, s_i \models \psi$且对于所有的$j = 1, 2, \cdots, i-1$都有$\mathcal{M}, s_i \models \phi$.

15. $\mathcal{M}, s \models E[\phi U \psi]$ 若存在从s出发的路$s_1 \to s_2 \to \cdots$,其中s_1就是s ,存在$i \geq 1$使得$\mathcal{M}, s_i \models \psi$且对于所有的$j = 1, 2, \cdots, i-1$都有$\mathcal{M}, s_i \models \phi$.

定义 **模型满足性**

设$\mathcal{M} = \{S, \to, L\}$是模型，$\phi$是CTL公式。若对于任一$s \in S$都有$\mathcal{M}, s \models \phi$，则称模型$\mathcal{M}$满足CTL公式$\phi$，记作$\mathcal{M} \models \phi$。

例子



语义等价

定义　语义等价

CTL公式ϕ,ψ称为语义等价，记作$\phi\equiv\psi$，若对于任何模型$\mathcal{M}$都有$\mathcal{M}\models\phi$当且仅当$\mathcal{M}\models\psi$。

定理　下面各条成立：

1. $AF\phi\equiv\neg EG\neg\phi$
2. $EF\phi\equiv\neg AG\neg\phi$
3. $AX\phi\equiv\neg EX\neg\phi$
4. $AF\phi\equiv A[\top U\phi]$
5. $EF\phi\equiv E[\top U\phi]$

CTL连接词充分性

定理

CTL时态连接词集是充分的当且仅当它包含EU以及$\{AX, EX\}$中一个元素以及$\{EG, AF, AU\}$中一个元素。

若选用$\{EX, EU, AF\}$为时态连接词充分集，则有下面各条成立：

1. $AX\phi \equiv \neg EX\neg\phi$
2. $EF\phi \equiv E[\top U\phi]$
3. $EG\phi \equiv \neg AF\neg\phi$
4. $AG\phi \equiv \neg EF\neg\phi$
5. $A[\phi_1 U\phi_2] \equiv \neg(E[\neg\phi_2 U(\neg\phi_1 \wedge \neg\phi_2)] \vee EG\neg\phi_2)$

可写成:

$$\phi ::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid EX\phi \mid EG\phi \mid E[\phi U\phi].$$

CTL和LTL表达能力

- 存在LTL公式, 在CTL中没有等价的形式, 例如: FGq;
- 存在CTL公式, 在LTL中没有等价的形式, 例如: $AFAGq$;

CTL*

状态公式:

$$\phi ::= \top \mid p \mid \neg\phi \mid \phi \wedge \phi \mid A[\alpha] \mid E[\alpha]$$

路径公式

$$\alpha ::= \phi \mid \neg\alpha \mid \alpha \wedge \alpha \mid \alpha U \alpha \mid G\alpha \mid F\alpha \mid X\alpha$$

注:LTL和CTL是CTL*子集.

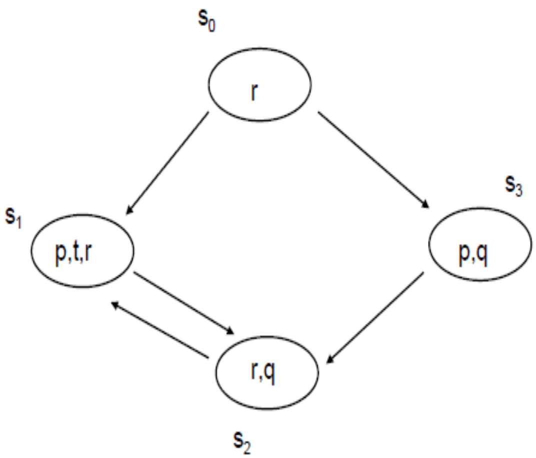
作业

1. 画出下面CTL公式的Parse树
   - $EFEGp \to AFr$
   - $A[pUA[qUr]]$
   - $E[A[pUq]Ur]$
   - $AG(p \to A[pU(\neg p \wedge A[\neg Uq])])$
2. 依照下图的系统，
   (a) 从s_0开始，将这个系统展开成一个无穷树，并画出所有长度为4的计算路.
   (b) 确定是否有$\mathcal{M}, s_0 \models \phi$以及$\mathcal{M}, s_2 \models \phi$成立，其中$\phi$是LTL或CTL公式:
      i. $\neg p \to r$
      ii. Ft
      iii. $\neg EGr$
      iv. $E(tUq)$

v. EFq

vi. EGr

vii. $G(r \vee q)$



3. 设$\mathcal{M} = (S, \rightarrow, L)$是任何CTL模型，用符号$[\![\phi]\!]$表示集合$\{s \mid s \in S, \mathcal{M}, s \models \phi\}$.证明：

   (a) $[\![\top]\!] = S$

(b) $[\![\bot]\!] = \emptyset$

(c) $[\![\neg\phi]\!] = S - [\![\phi]\!]$

(d) $[\![\phi \wedge \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$

(e) $[\![\phi \vee \psi]\!] = [\![\phi]\!] \cup [\![\psi]\!]$

(f) $[\![\phi \to \psi]\!] = (S - [\![\phi]\!]) \cup [\![\psi]\!]$

(g) $[\![AX\phi]\!] = S - [\![EX\neg\phi]\!]$

(h) $[\![A(\phi U \psi)]\!] = [\![\neg(E(\neg\phi U(\neg\phi \wedge \neg\psi)) \vee EG\neg\psi)]\!]$