软件理论基础：逻辑篇

为什么要学习逻辑？

数理逻辑是一门以**数学方法**为基础，用**符号系统**的形式来研究思维结构及规律的学科.

- 数理逻辑在计算机软件硬件设计中的应用
  - 开关电路---布尔代数
  - 搜索引擎---索引
  - 关系数据库 ---谓词逻辑
  - ……

为什么要学习逻辑？

数理逻辑是**规范语言、定理证明器、模型检测器**的基础

$$\mathcal{M} \models \phi$$

其中，$\mathcal{M}$-模型；ϕ--规范语言（用户需求），以逻辑的形式表示。

中心：设计好的算法计算$\models$

题外话—学得东西都是有用的

1. Google 2002年推出了自己的``新闻"服务。和传统媒体的做法不同，这些新闻不是记者写的，也不是人工编辑的，而是由计算机整理、分类和聚合各个新闻网站的内容，一切都是自动生成的。这里面关键的技术就是新闻的自动分类----**背后的数学（余弦定理）**

2. Google的网页排名技术。其``PageRank"网页排名算法是革命性的发明--公认的文献检索中最大的贡献之一，有人甚至认为整个公司的成功都是基于这个算法。创始人：拉里.佩奇、谢尔盖.布林. 佩奇也是因为这个算法在30岁时当选为美国工程院院士,是继乔布斯, 盖茨之后有一位当院士的辍学生. 其背后的数学---**线性代数**.

中国的大部分软件工程师在一个未知领域都是从直观感觉出发,用``凑"的方法来解决问题,说的不好听,就是山寨. Google招揽理论基础优异的工程师.-----吴军《数学之美》

时态逻辑系统

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。

时态逻辑系统

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。

时态逻辑系统分类

- 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-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

线性时态逻辑-LTL公式

定义　LTL的公式

公式ϕ定义为

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

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

线性时态逻辑-LTL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)。

线性时态逻辑-LTL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.

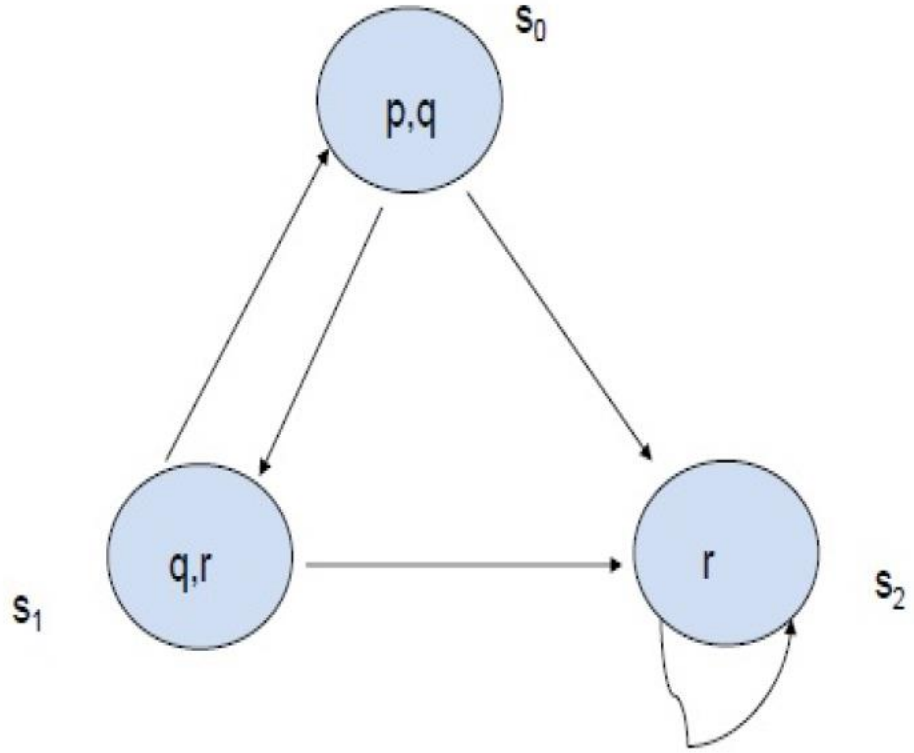
定义　迁移系统

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

- S是状态集
- $\rightarrow$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$s \rightarrow s'$, 即$\rightarrow$ 是S上的连续关系
- 标号函数$L : S \rightarrow \mathcal{P}(Atoms)$

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：

线性时态逻辑-LTL： 例子



线性时态逻辑-LTL语义

定义　路

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

通常将路写成：$s_1\rightarrow s_2\rightarrow\cdots$, 并用$\pi$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)。

线性时态逻辑-LTL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$\pi^i \models \phi$

线性时态逻辑-LTL语义

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$\pi^k \models \psi$.

例子：解释

- 原子命题a: $\bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \cdots$
  a 任意 任意 $\cdots$
- Xa: $\bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \cdots$
  任意 a 任意 任意 $\cdots$
- aUb: $\bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \cdots$
  $a, \neg b$ $a, \neg b$ b 任意 $\cdots$ ($\neg b$ 可以不标.)
- aRb: $\bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \cdots$
  b b a, b 任意 $\cdots$

  或者

  $\bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \bigcirc \to \cdots$
  b b b $\cdots$
- aWb: 请大家画出

线性时态逻辑-LTL语义

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.

例子：解释

- $s_0 \models (p \wedge q)$;
- $s_0 \models \neg r$;
- $s_0 \models \top$;
- $s_0 \models Xr$;
- $s_0 \not\models X(q \wedge r)$;
- $s_0 \models G\neg(p \wedge r)$;
- $s_2 \models Gr$;
- $s \models F(\neg q \wedge r) \rightarrow FGr$;
- $s_0 \not\models GFp$; 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$s_0 \not\models GFr \rightarrow GFp$.

线性时态逻辑-LTL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$s \models \psi$.

线性时态逻辑-LTL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: $F(\phi \wedge \psi) \equiv F\phi \wedge F\psi$ (?); $G(\phi \vee \psi) \equiv G\phi \vee G\psi$ (?)

线性时态逻辑-LTL： 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:

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

应用实例

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．

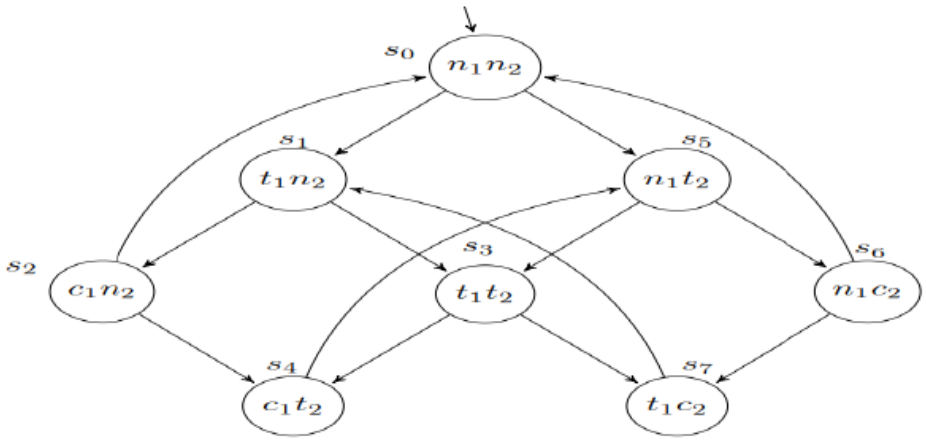
问题：如何设计协议以确定在任意时刻，哪个进程被允许进入临界区．

应用实例

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



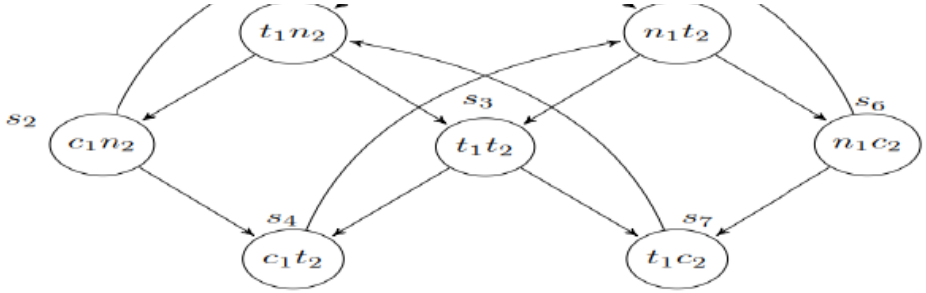
A model for mutual exclusion.

应用实例

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.



A model for mutual exclusion.

应用实例

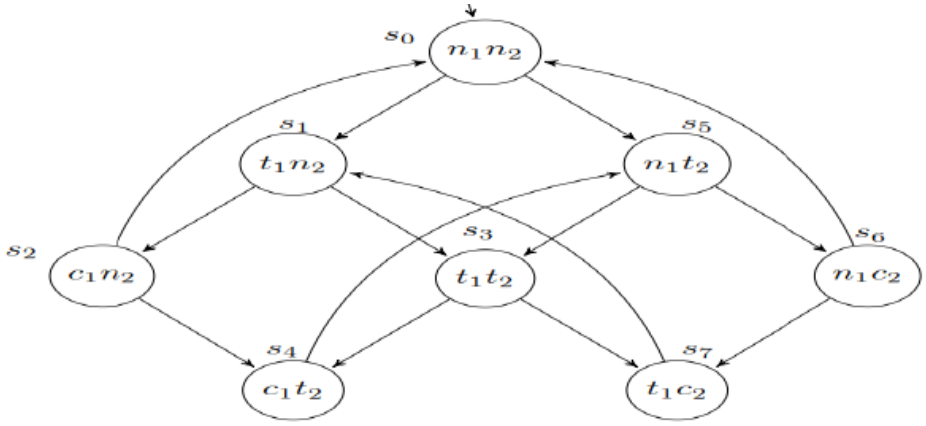
1. 安全性:

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

2.活性:

$$G(t_1 \rightarrow Fc_1)$$

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.



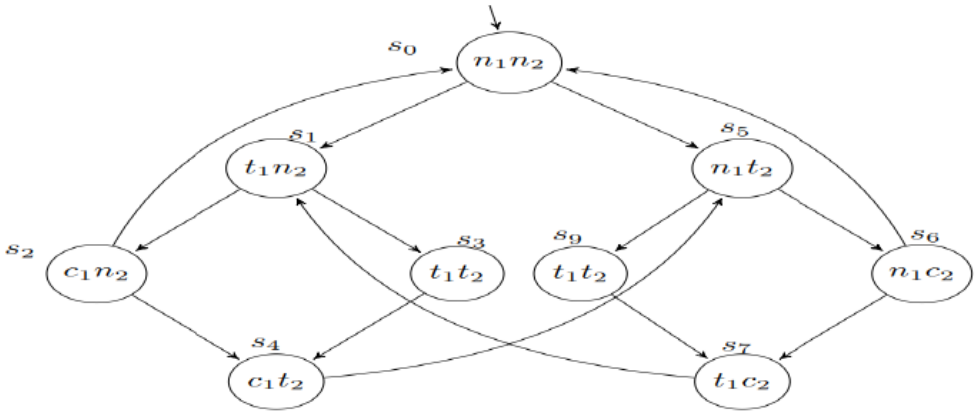
A model for mutual exclusion.

应用实例

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.