动态逻辑 (Dynamic logic)

王璐璐，白宗磊

北京大学信息科学与技术学院

2017/5/15

Outline

9.1 命题动态逻辑

背景

- 动态逻辑 (DL) 是一种对程序的正确性进行表达和推理的逻辑
- 动态逻辑是在霍尔逻辑 (Hoare logic) 的基础上发展出来的，是模态逻辑的一种扩充

霍尔逻辑 (Hoare logic)

语法

由霍尔三元组: $\{P\}C\{Q\}$ 构成, 其中 P 称为前置条件, C 为程序, Q 称为后置条件

语义

$\{P\}C\{Q\}$ 成立当且仅当, 对任意的程序状态 s, 若 s 满足前置条件 P, 且 s 经过程序 C 之行之后得到 s', 那么 s' 满足后置条件 Q

霍尔逻辑与动态逻辑

$\{P\}C\{Q\} \equiv P \rightarrow [C]Q$, eg: $(X=1) \rightarrow [X \leftarrow X+1](X=2)$

命题动态逻辑 (PDL) 的语言

命题动态逻辑的语言由两部分组成：程序与公式

程序集合 R

- R_0 为原子程序的集合且 $R_0 \in R$, $\theta \in R_0, \tau \in R_0$, 其中 θ 称为空程序, τ 称为幺程序。
- 若 $\alpha, \beta \in R$, 那么 $\alpha; \beta \in R$, 且 $\alpha; \beta$ 称为 α 和 β 的串联 (sequence)
- 若 $\alpha, \beta \in R$, 那么 $\alpha \cup \beta \in R$, 且 $\alpha; \beta$ 表示一个不确定程序，称为 α 和 β 的并联 (choice)
- 若 $\alpha \in R$, 那么 $\alpha^* \in R$, α^* 称为 α 的 kleene 闭包，或称之为 α 的循环

命题动态逻辑的语言

模态词

对任意的 $\alpha \in R$, $[\alpha]$ 与 $<\alpha>$ 均为模态词，其中 $[\alpha]$ 表示在 α 执行之后恒有..., $<\alpha>$ 表示在 α 执行之后将有...

由于 α 有无穷多个，因此 $[\alpha]$ 与 $<\alpha>$ 也有无穷多个，因此动态逻辑有无穷多个模态词，所以动态逻辑也称为多模态逻辑 (multimodal logic)

命题动态逻辑的语言

公式

动态逻辑的公式在命题演算 FSPC 的基础上进行如下扩充。

- *true* 与 *false* 为公式
- 如果 $\alpha \in R$, A 为一个公式，那么 $[\alpha]A$ 与 $<\alpha>A$ 也是公式

其中 $[\alpha]A$ 表示经 α 运行后的所有状态均使 A 成立，读作 α 后恒有 A；$<\alpha>A$ 表示经 α 运行后将有一个状态使 A 成立，读作 α 后将有 A

命题动态逻辑 (PDL) 的语义

PDL 的语义结构用 $< U, M, I >$ 表示，其中:

1.U 为状态集

非空集合 U 称为状态集，其中的成员称为状态，用 s, t 来表示。

2.M 为映射

$M : R_0 \to \rho(UxU)$，M 在原子程序和状态转换间建立了一个对应。特别的：$M(\theta) = \phi$(空关系)，即任何状态经 θ 执行后不能进入任何状态；$M(\tau) = \{< s, s > |s \in U\}$，即任何状态经 τ 执行后保持原来的状态。

命题动态逻辑 (PDL) 的语义

3.I 为映射

$I : Ux\{true, false, P1, P2, P3...\} \rightarrow \{0, 1\}$，即 I 对任一状态和任一原子命题指派该命题在该状态下的真值。

命题动态逻辑 (PDL) 的语义

将 M 拓展到整个 R 上 (定义 9.2)

$\bar{M} : R \to \rho(UxU)$, 对任意 $\alpha, \beta \in R$:

- $\bar{M}(\alpha) = M(\alpha)(\alpha \in R_0)$
- $\bar{M}(\alpha; \beta) = M(\alpha) \circ M(\beta) = \{< s, t > |\exists u(< s, u >\in \bar{M}(\alpha) \wedge < u, t >\in \bar{M}(\beta))\}$
- $\bar{M}(\alpha \cup \beta) = M(\alpha) \cup M(\beta) = \{< s, t > | < s, t >\in \bar{M}(\alpha) \vee < s, t >\in \bar{M}(\beta)\}$
- $\bar{M}(\alpha^*) = (M(\alpha))^* = \{< s, t > |s = t \vee < s, t >\in \bar{M}(\alpha) \vee < s, t >\in \bar{M}(\alpha^2) \vee ...\}$

下面将 $\bar{M}$ 简写为 M, 将 $< s, t >\in M(\alpha)$ 记为 $s\alpha t$

命题动态逻辑 (PDL) 的语义

公式真值的定义 (定义 9.3)

对任何结构 $\mathcal{K}$ 及其中任一状态 s, 对任意的公式 A, B:

- $\models^s_{\mathcal{K}}$ *true* (以下省略 $\mathcal{K}$ 与 s)
- $\not\models$ *false*
- $\models P_i$ 当且仅当 $I(s, P_i) = 1$
- $\models \neg A$ 当且仅当 $\not\models A$
- $\models A \vee B$ 当且仅当 $\models A$ 或者 $\models B$
- $\models A \wedge B$ 当且仅当 $\models A$ 并且 $\models B$
- $\models A \rightarrow B$ 当且仅当 $\not\models A$ 或者 $\models A \wedge B$
- $\models A \leftrightarrow B$ 当且仅当 $\models A \rightarrow B$ 并且 $\models B \rightarrow A$
- $[\alpha]A$ 当且仅当对所有 t, 若 $s\alpha t$ 则 $\models^t A$
- $< \alpha > A$ 当且仅当存在 t, 使 $s\alpha t$ 且 $\models^t A$

命题动态逻辑 (PDL) 的语义

永真式 1

根据上面的定义我们可以得到以下永真式:

- $[\theta]A \rightarrow A$
- $[\tau]A \leftrightarrow A, < \tau > A \leftrightarrow A$
- $[\alpha]A \leftrightarrow \neg < \alpha > \neg A$
- $< \alpha > A \leftrightarrow \neg[\alpha]\neg A$
- $[\alpha](A \rightarrow B) \rightarrow ([\alpha]A \rightarrow [\alpha]B)$
- $[\alpha](A \wedge B) \leftrightarrow ([\alpha]A \wedge [\alpha]B)$
- $[\alpha](A \vee B) \leftarrow ([\alpha]A \vee [\alpha]B)$
- $< \alpha > (A \vee B) \leftrightarrow (< \alpha > A \vee < \alpha > B)$
- $< \alpha > (A \wedge B) \rightarrow (< \alpha > A \wedge < \alpha > B)$

证明略。

命题动态逻辑 (PDL) 的语义

永真式 2

- $[\alpha;\beta]A \leftrightarrow [\alpha][\beta]A$
- $[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
- $< \alpha;\beta > A \leftrightarrow < \alpha >< \beta > A$
- $< \alpha \cup \beta > A \leftrightarrow < \alpha > A \vee < \beta > A$
- $[\alpha^*]A = A \wedge [\alpha][\alpha^*]A$
- $< \alpha^* > A = A \vee < \alpha >< \alpha^* > A$

证明略。

9.2 一阶动态逻辑

一种简单的程序语言 PL

PL 在一阶语言 $\mathcal{L}$ 上进行了扩充

PL 的基本表达式

- 一阶语言中所有变元和常元均为 PL 的基本表达式
- 若 $f^{(n)}e_1, e_2, , , e_n$ 为一阶语言中的 n 元函词， $e_1, e_2, , , e_n$ 为基本表达式， 那么 $f^{(n)}e_1, e_2, , , e_n$ 也是基本表达式

PL 的语句

- $x \leftarrow e$ 为赋值语句， 这里 x 为变元, e 为基本表达式
- θ, τ 为语句， 分别为空语句和幺语句
- $B?$ 为语句， 称为判断语句， 这里 B 为布尔表达式
- 同 PDL， 如果 α, β 为语句， 那么 $(\alpha; \beta), (\alpha \cup \beta), (\alpha^*)$ 也是语句

用 RG 表示 PL 中全体语句的集合。

一阶动态逻辑 (FDL) 的语言

一阶动态逻辑 (FDL) 的语言在一阶语言的基础上进行了扩充，与 PDL 的语法构成基本相同

语法

- 扩充一阶语言，定义程序集合 RG，RG 中的成员是不同于项和公式的，是另一类表达式
- 同 PDL, $[\alpha], < \alpha >$ 为模态词，但这里的 $\alpha \in RG$
- 同 PDL, 如果 A 是公式，那么 $[\alpha]A, < \alpha > A$ 也是公式

一阶动态逻辑 (FDL) 的语义

FDL 的语义结构为四元组 $< U, D, I, M >$，其中

U

U 为非空集合，称为状态集，其中的成员称为状态，用 s, t 来表示。

D

D 为非空集合，称为个体域，其中的成员称为个体，用 $d, d_0, d_1, \ldots$ 来表示。状态是变元集合到 D 的映射，即：$U = \{s | s : variable \to D\}$。一个状态就是某一时刻变元取值的情况。

一阶动态逻辑 (FDL) 的语义

I

I 为一解释，在解释 I 下，状态 s 可以扩充到任意项和基本表达式上，用 $\bar{s}$ 表示对 s 的扩充，则：

- $\bar{s}(x) = s(x)$，对一切变元 x
- $\bar{x}(f^{(n)}(e_1, .., e_n)) = \overline{f}^{(n)}\bar{s}(e_1), .., \bar{s}(e_n))$

一阶动态逻辑 (FDL) 的语义

M

$M: RG \to \rho(UxU)$，与 PDL 类似 M 为每个语句定义了状态转换规则:

- $M(\theta) = \phi$
- $M(\tau) = \{< s, s > | s \in U\}$
- $M(x \leftarrow e) = \{< s, s(x|e') > | s \in U\}$ 这里 $e' = \bar{s}(e)$,$s(x|e')$ 表示将 s 中的 x 替换为 e'
- $M(B?) = \{< s, s > | \models_{(D,I)} B[s]\}$, 显然 $M(true?) = M(\tau)$, $M(false?) = M(\theta)$
- $M(\alpha; \beta)$, $M(\alpha \cup \beta)$, $M(\alpha^*)$ 的定义与 PDL 中的相同

一阶动态逻辑 (FDL) 的语义

公式真值的定义

FDL 公式真值定义与 PDL 类似，在 PDL 的基础上增加了下面几条: (以下省略 $\mathcal{K}$ 与 s)

- $\models t_1 = t_2$ 当且仅当 $\bar{s}(t_1) = \bar{s}(t_2)$
- $\models P^{(n)} t_1, t_2, .., t_n$ 当且仅当 $< \bar{t_1}, .., \bar{t_n} > \in \bar{P}^{(n)}$, 其中 $P^{(n)}$ 为任一 n 元谓词。
- $\models \forall x A$ 当且仅当对所有 $s \in D, \models^{s(x|d)} A$
- $\models \exists x A$ 当且仅当存在 $s \in D, \models^{s(x|d)} A$
- 其他情况同 PDL

一些定理

根据上面的定义我们可以得到以下定理:

- $\models [x \leftarrow e]A \leftrightarrow A_e^x$
- $\models [B?]A \leftrightarrow (B \rightarrow A)$

证明略。

一阶动态逻辑 (FDL) 的公理系统

FDL 的公理系统由一些公理模式和推理规则模式构成：

公理模式

- 所有重言式均为 FDL 中的公理
- $\models [x \leftarrow e]A \leftrightarrow A_e^x$
- $\models [B?]A \leftrightarrow (B \rightarrow A)$
- $[\tau]A \leftrightarrow A$, $[\theta]A \leftrightarrow true$
- $[\alpha;\beta]A \leftrightarrow [\alpha][\beta]A$
- $[\alpha \cup \beta]A \leftrightarrow [\alpha]A \wedge [\beta]A$
- $\neg < \alpha > \neg A \leftrightarrow [\alpha]A$
- $\neg \exists x \neg A \leftrightarrow \forall x A$
- 在 N 结构中，全体自然数集上的真命题均为 FDL 的公理

一阶动态逻辑 (FDL) 的公理系统

推理规则模式

$$\frac{A \to B, A}{B}$$

$$\frac{A \to B}{[\alpha]A \to [\alpha]B}$$

$$\frac{A \to B}{\forall x A \to \forall x B}$$

$$\frac{A \to [\alpha]A}{A\alpha[\alpha^*]A}$$

在 N 结构中:

$$\frac{A(n+1) \to < \alpha > A(n)}{A(n) \to < \alpha^* > A(0)}$$

一阶动态逻辑 (FDL) 的合理性 (可靠性)

FDL 的合理性

对 FDL 中的任意公理 A 都有，$\models_N A$, 并且，对每一条规则 $\frac{\Gamma}{B}$，若 $\models_N \Gamma$ 成立，则 $\models_N B$ 成立。

一阶动态逻辑 (FDL) 的一些性质

引理 9.1

对任意公式 A, B，若 $\models_N A, \models_N A \to B$, 则 $\models_N B$ 证明略。

引理 9.2

对任意公式 A, B，以及任意程序 α, 若 $\models_N A \to B$, 则 $\models_N [\alpha]A \to [\alpha]B, \models_N \forall xA \to \forall xB$。证明略。

引理 9.3

对任意公式 A，以及任意程序 α, 若 $\models_N A \to [\alpha]A$, 那么 $\models_N A \to [\alpha^*]A$。证明略。

引理 9.4

对任意一阶公式 A，以及任意程序 α, 若 A 中的自由变元 n 不在赋值语句的左边出现，并且 $\models_N A(n+1) \to < \alpha > A(n)$, 那么 $\models_N, A(n) \to < \alpha^* > A(0)$ 证明略。

一阶动态逻辑 (FDL) 的导出规则

定理 9.5, 9.6, 9.7:

$$\frac{\vdash [\alpha^*](A \to [\alpha]A)}{\vdash A \to [\alpha^*]A}$$

$$\frac{A \to B}{< \alpha > A \to < \alpha > B}$$

$$\frac{A \to B}{\exists x A \to \exists x B}$$

$$\frac{C \to A, A \to [\alpha]A, A \to B}{C \to [\alpha^*]B}$$

证明略。

谢谢大家！