《软件分析与验证》

深入理解循环

贺飞

清华大学软件学院

2022 年 4 月 4 日

上节课：霍尔证明系统

IMP 程序规约:

- 前置条件、后置条件、后像
- 霍尔三元组

IMP 霍尔证明系统:

- 推理规则
- 可靠、相对完备

本节课的内容

$$\textbf{while } (p)\{st\}$$

- 进一步理解循环、循环不变式

对于循环，容易得到下面的结论：

引理

语句 $\textbf{while }(p)\{st\}$ 和语句 $\textbf{if }(p)\{st; \textbf{while }(p)\{st\}\}\textbf{ else skip}$ 是语义等价的。

继而可得下面的推理规则：

$$\frac{\{\varphi\}\ \ \textbf{if }(p)\{st; \textbf{while }(p)\{st\}\}\textbf{ else skip}\ \ \{\psi\}}{\{\varphi\}\ \ \textbf{while }(p)\{st\}\ \ \{\psi\}}$$

该推理规则的本质是将循环展开，但展开后的程序仍然包含原来的 `while` 循环。包含这条规则的证明系统将无法保证整个证明过程（即构建推导树的过程）的终止性。

循环分析的主要难点是除非给定具体的初始状态，否则很难确定循环的迭代次数。

先考虑循环条件为 $true$ 的情况，此时循环就相当于反复执行 st。

$$\textbf{while } (true)\{st\}$$

引入新语法 st^*（称重复语句）表示执行 st 任意多次（从 0 到正无穷）。

$$\begin{aligned} st \in Stmt ::= \textbf{skip} \mid x := e \mid st_1; st_2 \\ \mid \textbf{if } (p)\ \{st_1\} \textbf{ else } \{st_2\} \\ \mid \textbf{while } (p)\ \{st\} \\ \mid st^* \end{aligned}$$

以 st^i 表示重复执行语句 i 次，即

$$st^i = \underbrace{st; \ldots st}_{i}$$

语句 st^* 表示不确定地执行语句 st 任意多次（从 0 到正无穷），即

$$st^* = \textbf{skip} \mid st^1 \mid st^2 \mid \ldots$$

定义 (重复语句的语义)

$$[\![st^*]\!] = \left\{ (s, s') \,\middle|\, \begin{array}{l} \text{存在一个整数 } n \text{ 和一组状态序列} \\ t_0 = s, t_1, t_2, \ldots, t_n = s', \text{使得} \\ (t_i, t_{i+1}) \in [\![st]\!] \text{ 对任意 } 0 \le i < n \text{ 成立} \end{array} \right\}$$

注意 st^* 和 st^i 的区别：

$$[\![st^i]\!] \subseteq [\![st^*]\!]$$

设 R 是一个定义在集合 X 上的二元关系，定义

$$R^i = \begin{cases} \{(x,x) \mid x \in X\}, & \text{如果 } i = 0 \\ R \circ R^{i-1}, & \text{否则} \end{cases}$$

定义 (自反传递闭包)

R 的自反传递闭包（reflexive transitive closure）R^* 是满足下列条件的最小关系：$R \subseteq R^*$，R^* 是自反关系，R^* 是传递关系。

定理 (自反传递闭包)

自反传递闭包 $R^* = \bigcup_{i \in \mathbb{N}} R^i$

注意 $\llbracket st \rrbracket$ 是一个二元关系，根据重复语句和顺序组合的语义，有：

$$\llbracket st^i \rrbracket = \llbracket \underbrace{st; st; \ldots st}_{i} \rrbracket = \underbrace{\llbracket st \rrbracket \circ \llbracket st \rrbracket \circ \ldots \llbracket st \rrbracket}_{i} = \llbracket st \rrbracket^i$$

$\llbracket st^* \rrbracket$ 是 $\llbracket st \rrbracket$ 的自反传递闭包，有

$$\llbracket st^* \rrbracket = \llbracket st^0 \rrbracket \cup \llbracket st^1 \rrbracket \cup ... = \bigcup_{i \in \mathbb{N}} \llbracket st \rrbracket^i$$

令

$$st^{(k)} = st^0 \mid st^1 \mid \cdots \mid st^k$$

则

$$st^{(k)}; st = st^1 \mid st^2 \mid \cdots \mid st^{k+1}$$

于是

$$\begin{aligned} st^{(k+1)} &= st^0 \mid st^1 \mid \cdots \mid st^{k+1} \\ &= st^0 \mid st^{(k)}; st \end{aligned}$$

下面以归纳法分析该如何证明 $\models \{\varphi\}\ st^*\ \{\psi\}$。

1. **基本步：** 证明 $\models \{\varphi\}\ st^{(0)}\ \{\psi\}$，即证明

$$post(\{\varphi\}, [\![st^0]\!]) \subseteq \{\psi\} \tag{1}$$

   注意 $[\![st^0]\!] = \{(s,s) \mid s \in \mathcal{S}\}$，这等价于证明 $\varphi \models \psi$。

2. **归纳步：** 假设 $\models \{\varphi\}\ st^{(k)}\ \{\psi\}$，即 $post(\{\varphi\}, [\![st^{(k)}]\!]) \subseteq \{\psi\}$ 成立，需要证明 $\models \{\varphi\}\ st^{(k+1)}\ \{\psi\}$ 成立；
   注意 $st^{(k+1)} = st^0 \mid st^{(k)}; st$，这等价于证明 $\models \{\varphi\}\ st^{(0)}\ \{\psi\}$ 和 $\models \{\varphi\}\ st^{(k)}; st\ \{\psi\}$。前者在基本步已经证明，后者等价于

$$post\left(post(\{\varphi\}, [\![st^{(k)}]\!]), [\![st]\!]\right) \subseteq \{\psi\} \tag{2}$$

   记 $\mathcal{S}_\varphi^{(k)} = post(\{\varphi\}, [\![st^{(k)}]\!])$，表示从满足 φ 的状态出发，执行 $st^{(k)}$ 后的可达状态集合。
   式 (2) 可理解为：从满足 $\mathcal{S}_\varphi^{(k)}$ 的状态出发，执行 st 的后状态必须满足 ψ。

根据假设，$\mathcal{S}_{\varphi}^{(k)} \subseteq \{\psi\}$，我们把式 (2) 的条件放宽为：从任意满足 ψ 的状态出发执行 st 的后状态需要满足 ψ，记作：

$$post(\psi, [\![st]\!]) \subseteq \{\psi\} \tag{3}$$

或者 $\models \{\psi\}\ st\ \{\psi\}$。

根据归纳原理，式 (1) 和式 (2) 可证明结论成立。式 (3) 是式 (2) 的充分条件。于是，我们有：

$$\text{（归纳）}\ \frac{\varphi \models \psi \qquad \{\psi\}\ st\ \{\psi\}}{\{\varphi\}\ st^*\ \{\psi\}}$$

并称 ψ 为归纳不变式（inductive invariant）。

如果 $\varphi = \psi$，归纳推理规则可以进一步简化为：

$$\text{（归纳-）}\ \frac{\{\psi\}\ st\ \{\psi\}}{\{\psi\}\ st^*\ \{\psi\}}$$

再考虑循环条件为 p 的情况

$$\textbf{while } (p)\{st\}$$

相较于 $\textbf{while } (\mathit{true})\{st\}$，这里相当于在反复执行 st 的时候，增加了一个先测试循环条件是否满足的环节。如果满足，继续执行 st；否则，退出循环。

引入新语法 $?p$（称测试语句）用于测试条件 p 是否成立。

$$\begin{aligned} st \in \mathit{Stmt} ::= \;& \textbf{skip} \mid x := e \mid st_1; st_2 \\ & \mid \textbf{if } (p)\ \{st_1\} \textbf{ else } \{st_2\} \\ & \mid \textbf{while } (p)\ \{st\} \\ & \mid\ st^* \mid ?p \end{aligned}$$

语句 $?p$ 测试布尔表达式 p 在当前状态下是否成立，只有在 p 成立时才继续执行（不改变状态），否则中止执行。这里“中止”执行的具体含义是没有后状态。

$$[\![?p]\!] = \{(s, s) \mid s \models p\}$$

根据其语义，有下面的推理规则

$$\text{（测试）}\ \frac{}{\{\varphi\}\ ?p\ \{\varphi \wedge p\}}$$

根据循环、重复和测试语句的语义，有：

$$\mathbf{while}\ (p)\ \{st\} \equiv (?p; st)^*;\ ?\neg p$$

于是，我们有：

$$\equiv\dfrac{;\dfrac{*\dfrac{;\dfrac{?\dfrac{}{\{\psi\}\ ?p\ \{\psi\wedge p\}}\qquad \{\psi\wedge p\}\ st\ \{\psi\}}{\{\psi\}\ ?p;st\ \{\psi\}}}{\{\psi\}\ (?p;st)^*\ \{\psi\}}\qquad ?\dfrac{}{\{\psi\}\ ?\neg p\ \{\psi\wedge\neg p\}}}{\{\psi\}\ (?p;st)^*;?\neg p\ \{\psi\wedge\neg p\}}}{\{\psi\}\ \mathbf{while}\ (p)\{st\}\ \{\psi\wedge\neg p\}}$$

即：

$$\text{（循环）}\ \dfrac{\{\varphi\wedge p\}\ st\ \{\varphi\}}{\{\varphi\}\ \mathbf{while}\ (p)\{st\}\ \{\varphi\wedge\neg p\}}$$

总结：进一步理解循环

- 重复语句、测试语句
- 关系的自反传递闭包
- 循环的另一种表示方式
- 相应的推理规则

下节课内容

- 在 IMP 语言中扩展数组

谢谢!