《软件分析与验证》

深入理解循环

贺飞
清华大学软件学院

2024 年 4 月 12 日

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

进一步理解循环和循环不变式

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

对于循环，容易得到下面的结论：

引理

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

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（即构建证明树的过程）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。

以下面的循环为例，

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

程序反复来到循环头位置，然后检查条件 p 是否成立；如果成立，进入循环体并执行 st；否则，退出循环。

很难用一个算法来确定任意给定的循环的迭代次数。

设 R 是定义在集合 X 上的一个二元关系。

定义（自反传递闭包）

R 的自反传递闭包（reflexive transitive closure）是满足下列条件的最小关系 R^*：

- $R \subseteq R^*$，
- R^* 是自反关系，
- R^* 是传递关系。

预备知识：关系的自反传递闭包

以 $id_X = \{(x, x) \mid x \in X\}$ 表示集合 X 上的恒等关系。
定义

$$R^i = \begin{cases} id_X, & \text{如果 } i = 0 \\ R \circ R^{i-1}, & \text{否则} \end{cases}$$

定理

$\bigcup_{i\in\mathbb{N}} R^i$ 是 R 的自反传递闭包。

证明.

- 由于 $R \subseteq \bigcup_{i\in\mathbb{N}} R^i$，所以是 R 的超集；
- 由于 $id_X \subseteq \bigcup_{i\in\mathbb{N}} R^i$，所以具有自反性；
- 由于$R^i \subseteq \bigcup_{i\in\mathbb{N}} R^i$，所以具有传递性；
- 从 $\bigcup_{i\in\mathbb{N}} R^i$ 中删去任何一个状态对，都会导致自反传递闭包的一个条件被违反，所以是最小集合。

□

以 st^i 表示重复 i 次执行 st 语句，即

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

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

$$[\![st^i]\!] = [\![\underbrace{st; st; \ldots st}_{i}]\!] = \underbrace{[\![st]\!] \circ [\![st]\!] \circ \ldots [\![st]\!]}_{i} = [\![st]\!]^i$$

特别地，$st^0 = skip$，$[\![st^0]\!] = id_{\mathcal{S}}$。

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

$$st^* = st^0 \mid st^1 \mid \cdots \mid st^i \mid \ldots$$

其关系语义为：

$$[\![st^*]\!] = [\![st^0]\!] \cup [\![st^1]\!] \cup ... = [\![st]\!]^0 \cup [\![st]\!]^1 \cup ... = \bigcup_{i \in \mathbb{N}} [\![st]\!]^i$$

即，$[\![st^*]\!]$ 就是 $[\![st]\!]$ 的自反传递闭包。

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

如果从满足 φ 的状态出发执行语句 st 后还满足 φ，则从该状态出发执行 st 任意多次后仍满足 φ。

如果 st 是循环体，则称 φ 为归纳不变式（inductive invariant）。

引理

如果霍尔三元组 $\{\varphi\}\ st\ \{\varphi\}$ 是有效式，则霍尔三元组 $\{\varphi\}\ st^i\ \{\varphi\}$ 也是有效式，其中 $i \in \mathbb{N}$ 是任意自然数。

证明.

1. **基本步：** $i = 0$ 时，$st^0 =$**skip**，$\models \{\varphi\}$ **skip** $\{\varphi\}$ 显然成立。
2. **归纳步：** 假设 $i = k$ 时，$\models \{\varphi\}\ st^i\ \{\varphi\}$ 成立。根据前提，$\models \{\varphi\}\ st\ \{\varphi\}$ 成立。当 $i = k+1$ 时，由于 $st^{k+1} = st^k; st$，根据顺序组合语句的推理规则

$$\frac{\{\varphi\}\ st^k\ \{\varphi\} \qquad \{\varphi\}\ st\ \{\varphi\}}{\{\varphi\}\ st^{k+1}\ \{\varphi\}}$$

即 $\{\varphi\}\ st^i\ \{\varphi\}$ 在 $i = k+1$ 时也成立。

$\square$

规则可靠性

引理 (重复语句推理规则的可靠性)

如果霍尔三元组 $\{\varphi\}\ st\ \{\varphi\}$ 是有效式，则霍尔三元组 $\{\varphi\}\ st^*\ \{\varphi\}$ 也是有效式。

证明.

根据 $st^* = st^0 \mid st \mid st^2 \mid \ldots$ 分情况讨论。根据前面的引理知道，$\{\varphi\}\ st^i\ \{\varphi\}$ 对任意 $i \in \mathbb{N}$ 都成立，即无论 st^* 取哪一种情况，$\{\varphi\}\ st^*\ \{\varphi\}$ 都成立。 $\square$

对比循环语句

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

与重复语句 st^*。循环语句在反复执行 st 的过程中，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 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。

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

推理规则：测试语句

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

引理 (测试语句推理规则的可靠性)

霍尔三元组 $\{\varphi\}\ ?p\ \{\varphi \wedge p\}$ 是有效式。

证明.

任取一个状态 $s \models \varphi$，如果 $s \not\models p$，程序终止执行且无后状态；否则，令 s' 为后状态，根据 $?p$ 的语义，$s' = s$ 且 $s' \models p$，所以 $s' \models \varphi \wedge p$。综合上述两种情况，从满足 φ 的状态出发执行 $?p$ 所能得到的后状态一定满足 $\varphi \wedge p$。 $\square$

定理

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

证明： 对任意状态 s, s'，

$\Rightarrow$ 如果 $(s, s') \in [\![\textbf{while}\ (p)\{st\}]\!]$，根据循环语句的语义，存在一个整数 n 和一组状态序列 $t_0, t_1, t_2, \ldots, t_n$，其中 $t_0 = s$，$t_n = s'$，使得：

- 对任意 $0 \le i < n$，$t_i \models p$，即 $(t_i, t_i) \in [\![?p]\!]$，且 $(t_i, t_{i+1}) \in [\![st]\!]$。根据关系组合的定义，$(t_i, t_{i+1}) \in [\![?p]\!] \circ [\![st]\!] = [\![?p;\ st]\!]$。所以

$$(t_0, t_n) \in \underbrace{[\![?p;\ st]\!] \circ \cdots \circ [\![?p;\ st]\!]}_{n} = [\![?p;\ st]\!]^n = [\![(?p;\ st)^n]\!]$$

- $t_n \not\models p$，即 $(t_n, t_n) \in [\![?\neg p]\!]$。联合上式，有

$$(t_0, t_n) \in [\![(?p;\ st)^n]\!] \circ [\![?\neg p]\!] \subseteq [\![(?p;\ st)^*]\!] \circ [\![?\neg p]\!] = [\![(?p;\ st)^*;\ ?\neg p]\!]$$

$\Leftarrow$ 如果 $(s, s') \in [\![(?p;\ st)^*;\ ?\neg p]\!]$,

- 根据顺序组合语句的语义，$(s, s') \in [\![(?p;\ st)^*]\!] \circ [\![?\neg p]\!]$。
- 根据关系组合的语义，存在状态 s''，使得 $(s, s'') \in [\![(?p;\ st)^*]\!]$, $(s'', s') \in [\![(?\neg p)]\!]$。
- 根据 $?\neg p$ 的语义，$s'' = s'$，于是 $(s, s') \in [\![(?p;\ st)^*]\!]$。
- 根据重复语句的语义，必定存在一个整数 n，使得

$$(s, s') \in [\![(?p;\ st)^n]\!]$$

  即存在状态序列 $t_0, t_1, \ldots, t_n$，其中 $t_0 = s, t_n = s'$，使得 (1) 对任意 $0 \leq i < n$，$t_i \models p$，且 $(t_i, t_{i+1}) \in [\![st]\!]$。
- 再根据 $(t_n, t_n) \in [\![?\neg p]\!]$，有 (2) $t_n \not\models p$。
- 联立 (1) 和 (2)，有 $(s, s') \in [\![\textbf{while}\ (p)\{st\}]\!]$。

于是，我们有：

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

即：

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

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!