

# 霍尔逻辑

霍尔逻辑 (Hoare Logic) 是一套用来证明程序正确性的形式系统，用它可以定义程序语义。所定义的语义属于公理化语义 (Axiomatic Semantics)。

## 霍尔三元组

霍尔逻辑的中心特征是**霍尔三元组** (Hoare Triple)，其为如下的形式：

$$\{P\} c \{Q\}$$

其中  $P$  和  $Q$  是**断言** (Assertion)，是描述程序状态的命题。而  $c$  是程序指令 (Command)，其本质上是一棵语法树。 $P$  称为**前条件** (Pre-condition)， $Q$  称为**后条件** (Post-condition)。

这个三元组的直觉意义是：如果  $P$  在  $c$  执行之前成立，那么  $c$  执行终止后， $Q$  成立。如果  $Q$  为  $\perp$ ，那么意味着  $c$  不终止。

## 断言

断言本身是命题。什么是命题？对此在逻辑学中有语法角度 (Syntax) 和语义角度 (Semantics) 的两种理解。到这里，两种理解分别对应语法树与程序状态的集合两种表现形式。

断言之间存在推导关系。如果所有满足  $P$  的程序状态也满足  $Q$ ，就说  $P$  比  $Q$  强，记作  $P \vdash Q$ 。若同时  $Q \vdash P$ ，则称两者等价。

后面在讨论霍尔逻辑的可靠性和完备性时，会给出更加严格的定义。

## 推理规则

霍尔逻辑的推理规则数量很少，但是都十分符合直觉。

下面会用到一些简单的程序语句，简单到不用给出严格的声明就能知道它们说了什么。不过有一点需要说明：这类程序只包含三种要素，整数表达式 (简称 aexp)、布尔表达式 (简称 bexp) 和程序语句 (简称 com)。

## 跳过

$$\forall P, \frac{}{\{P\} \text{skip} \{P\}}$$

## 顺序执行

$$\forall P, Q, R, \frac{\{P\} c_1 \{Q\}, \{Q\} c_2 \{R\}}{\{P\} c_1; c_2 \{R\}}$$

## 分支

$$\forall b, P, Q, \frac{\{P \wedge b\} c_1 \{Q\}, \{P \wedge \neg b\} c_2 \{Q\}}{\{P\} \text{If } b \text{ Then } c_1 \text{ Else } c_2 \text{ EndIf } \{Q\}}$$

注意这里的  $b$  是布尔表达式，且必须不会产生除了求值外的其他影响 (即不会改变程序状态)。下同。

## 循环

$$\forall b, P, c, \frac{\{P \wedge b\} c \{P\}}{\{P\} \text{ While } b \text{ Do } c \text{ EndWhile } \{P \wedge \neg b\}}$$

在这里  $P$  就是算法分析中常见的循环不变量 (Loop Invariant)，即从进入循环、重复循环到结束循环为止都需要保持的性质。

## 赋值

赋值公理包含两种：前向规则和后向规则。选择其中一个即可。

这里选择其中一个即可的意思是：无论选择哪一个，都不会破坏霍尔逻辑的表达力。

前向规则：

$$\forall P, X, E, \frac{}{\{P\} X := E \{ \exists x, P[X \mapsto x] \wedge X = E[X \mapsto x] \}}$$

其中  $E[X \mapsto x]$  表示将  $E$  中所有  $X$  的出现全部替换为  $x$ 。其是通过在语法树层面的替换实现的。对于整数表达式、布尔表达式、断言均可做这样的替换。

后向规则：

$$\forall P, X, E, \frac{}{\{P[X \mapsto E]\} X := E \{P\}}$$

## 条件修改

前条件和后条件分别可以进行一定的加强和减弱。

$$\forall P, P', Q, Q', \frac{P \vdash P', Q' \vdash Q, \{P'\} c \{Q'\}}{\{P\} c \{Q\}}$$

## 小结

霍尔逻辑的推理规则都很符合直觉，同时很有意思的是，这样的规则表达力也足够强大。即在合理的框架下，只要一个会终止的程序具备某种性质，那么这个性质就可以用霍尔逻辑证明出来。

所谓合理的框架，即意味着断言推导所依赖的规则（或逻辑）应当足够好。这一点会在后面提及。

需要注意的是，这里强调了程序应当终止。在这里，唯一不会终止的程序就是死循环。对于死循环  $c$  而言，其满足下面的霍尔三元组

$$\{\top\} c \{\perp\}$$

其中  $\top$  表示命题“真”， $\perp$  表示命题“假”。