《软件分析与验证》

霍尔证明系统

贺飞
清华大学软件学院

2024 年 4 月 7 日

上节课：IMP 程序设计语言及其语义

IMP 语法：

- 算术表达式、布尔表达式
- 程序语句

IMP 语义：

- 算术表达式和布尔表达式的语义
- 程序语句的语义

如何刻画对程序的正确性需求?

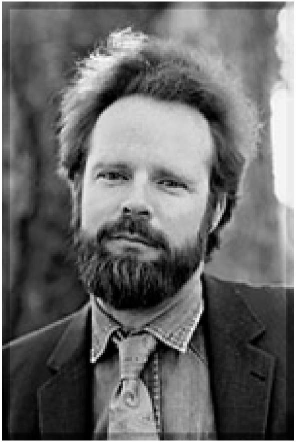
——**程序规约**

如何证明对程序的正确性需求?

——**霍尔证明系统**

罗伯特 · 佛洛伊德（Robert Floyd）

- 1936 年 6 月 8 日 - 2001 年 9 月 25 日
- 美国计算机科学家，图灵奖得主
- 重要贡献：
  - 图论算法（Floyd-Warshall 算法，Floyd's cycle-finding 算法）
  - 开创性地在程序验证中引入逻辑断言 (Assigning Meanings to Programs)



From: https://en.wikipedia.org/wiki/Robert_W._Floyd

托尼 · 霍尔（Tony Hoare）

- 生于 1934 年 1 月 11 日
- 英国计算机科学家，图灵奖得主
- 重要贡献：
  - 快速排序算法（Quicksort），快速选择算法（Quickselect）
  - 通信顺序进程（Communicating sequential process, CSP）
  - 霍尔三元组，霍尔逻辑

From: https://en.wikipedia.org/wiki/Tony_Hoare

程序规约

```c
int binarySearch(int* a,int key,int n){
    int low = 0, high = n;

    while (low <= high) {
        int mid = (low + high) / 2;

        if (a[mid] < key)
            low = mid + 1;
        else if (a[mid] > key)
            high = mid;
        else
            return mid; // key found
    }
    return -1; // key not found.
}
```

- 左边程序实现了二分查找算法
- 期望用这个程序在数组 a 中进行查找，如果找到 key，就返回 key 在 a 中的位置，否则返回 -1
- 如何精确地刻画该规约?

后置条件：

$$(-1 \leq retval < n) \land (0 \leq retval < n \to a[retval] = key) \\ \land (retval = -1 \to (\forall j.0 \leq j < n \to a[j] \neq key))$$

前置条件：$(n > 0) \land sorted(a)$

定义（霍尔三元组）

霍尔三元组（Hoare Triple）是形如

$$\{\varphi\}\ st\ \{\psi\}$$

的式子，其中 st 是程序，φ 和 ψ 是逻辑公式；φ 和 ψ 分别称为 st 的前置条件和后置条件。

霍尔三元组的含义：从任何满足 φ 的前状态出发执行 st，如果 st 终止，那么后状态必定满足 ψ。

注意： 霍尔三元组所约束的程序行为中，不包括

- 不终止的程序行为
- 从不满足 φ 的状态出发的程序行为

前置和后置条件的 φ 和 ψ 都是某个一阶理论（如整数算术理论 $\mathcal{T}_{PA}$）的 Σ_T 公式。

在前置和后置条件中允许出现三类变元：程序变元、通过量词引入的约束变元、其他逻辑变元。记 $LVar$ 为前后置条件中出现的其他逻辑变元的集合。

在前置和后置条件中可以出现常元符号、函数符号和谓词符号，这些非逻辑符号的解释 $\mathcal{M}$ 由对应的一阶理论（如整数算术理论）确定。

注意： 相比于条件表达式，前置和后置条件的逻辑公式中允许出现更多的语法元素。

例：霍尔三元组的含义

请写出下列霍尔三元组的含义：

1. $\{\top\}\ st\ \{\psi\}$：

2. $\{0 < x\}\ \textbf{while}\ (0 < x)\ \{x := x + 1\}\ \{\bot\}$：

3. $\{\top\}\ st\ \{\bot\}$：

请将下列规约写成霍尔三元组的形式：

- 语句 $t := x; x := y; y := t$ 交换变量 x 和 y 的值。

例：程序 P_{xy}

```
while (!(y == 0)) {
    if (y >= 0) {
        y = y - 1;
    } else {
        y = y + 1;
    }
    x = x + 1;
}
```

- 以 P_{xy} 代表左边的程序
- 考虑下面的规约
  - 前置条件：$x \times y \geq 0$
  - 后置条件：$x \geq 0$
- 写成霍尔三元组的形式：
  $\{\{x \times y \geq 0\}\}\ P_{xy}\ \{\{x \geq 0\}\}$

状态集合

设 φ 是一个逻辑公式，以 $\{\varphi\}$ 表示满足 φ 的所有状态的集合，即：

$$\{\varphi\} ::= \{s \mid [\![\varphi]\!]_{\mathcal{M},s} = \mathit{true}\}$$

其中，$[\![\varphi]\!]_{\mathcal{M},s}$ 中的 $\mathcal{M}$ 由对应的一阶理论确定；在不引起歧义的情况下，常简记为 $[\![\varphi]\!]_s$。

例 (程序 P_{xy} 的变元集是 $\{x, y\}$)

- $x = 5 \wedge y = 7$ 对应的状态集合为 $\{\langle 5, 7\rangle\}$
- $x = 5$ 对应的状态集合为 $\{\ldots, \langle 5, -1\rangle, \langle 5, 0\rangle, \langle 5, 1\rangle, \ldots\}$
- $\exists k.(x = 2 * k \wedge y = 2 * k + 1)$ 对应的状态集合为 $\{\ldots, \langle -2, -1\rangle, \langle 0, 1\rangle, \langle 2, 3\rangle, \ldots\}$

定义 (后像)

设 R 是定义在集合 X 上的一个二元关系，$Y \subseteq X$ 是 X 的一个子集，Y 关于 R 的后像（post-image）定义为：

$$post(Y, R) ::= \{x \in X \mid \text{存在 } y \in Y \text{ 使得 } (y, x) \in R\}$$

例

令 $Y = \{1, 2, \cdots, 10\}$，
考虑整数集上的加一关系 R，即 $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b = a + 1\}$，则

$$post(Y, R) = \{2, 3, ..., 11\}$$

考虑整数集上的小于关系 R'，即 $R' = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a < b\}$，则

$$post(Y, R') = ?$$

定义 (有效的霍尔三元组)

给定程序 st 及其前置条件 φ 和后置条件 ψ，如果

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

成立，称程序 st 满足规约 (φ, ψ)，记作 $st \models (\varphi, \psi)$；也称霍尔三元组 $\{\varphi\}\ st\ \{\psi\}$ 是有效式，记作 $\models \{\varphi\}\ st\ \{\psi\}$。

例

$\{x = 0 \wedge y = 1\}\ x := x + 1\ \{x = 1 \wedge y = 1\}$ 是否有效的霍尔三元组?

解

因为 $post(\{x = 0 \wedge y = 1\}, [\![x := x + 1]\!]) = \{x = 1 \wedge y = 1\}$，所以原式是有效的霍尔三元组。

例：有效的霍尔三元组

下面的霍尔三元组是有效式吗?

1. $\{x = 0 \wedge y = 1\}\ x := x + 1\ \{x = 1 \wedge y = 2\}$
2. $\{x = 2\}\ \textbf{while}\ (0 < x)\ \{x := x - 1\}\ \{x = 0\}$
3. $\{\top\}\ \textbf{while}\ (0 < x)\ \{x := x - 1\}\ \{x \leq 0\}$
4. $\{0 < x\}\ \textbf{while}\ (0 < x)\ \{x := x + 1\}\ \{x > 0\}$

霍尔证明系统

与其他证明系统的对比

$\mathcal{S}_{PL}$	$\mathcal{S}_{FOL}$	霍尔证明系统
推导有效命题逻辑公式 $\vdash F$	推导有效一阶逻辑公式 $\vdash \varphi$	推导有效霍尔三元组 $\vdash \{\varphi\}\ st\ \{\psi\}$

$$\text{（空语句）}\ \frac{}{\{\varphi\}\ \ \textbf{skip}\ \ \{\varphi\}}$$

$$\text{（赋值）}\ \frac{}{\{\varphi[x \mapsto e]\}\ \ x := e\ \ \{\varphi\}}$$

$$\text{（前提加强）}\ \frac{\{\varphi'\}\ \ st\ \ \{\psi\}}{\{\varphi\}\ \ st\ \ \{\psi\}}\ \ \text{如果}\ \varphi \Rightarrow \varphi'$$

$$\text{（结论弱化）}\ \frac{\{\varphi\}\ \ st\ \ \{\psi'\}}{\{\varphi\}\ \ st\ \ \{\psi\}}\ \ \text{如果}\ \psi' \Rightarrow \psi$$

$$\text{（分支）}\ \frac{\{\varphi \wedge p\}\ \ st_1\ \ \{\psi\} \qquad \{\varphi \wedge \neg p\}\ \ st_2\ \ \{\psi\}}{\{\varphi\}\ \ \textbf{if}\ (p)\ \{st_1\}\ \textbf{else}\ \{st_2\}\ \ \{\psi\}}$$

$$\text{（顺序）}\ \frac{\{\varphi_1\}\ \ st_1\ \ \{\varphi_2\} \qquad \{\varphi_2\}\ \ st_2\ \ \{\varphi_3\}}{\{\varphi_1\}\ \ st_1; st_2\ \ \{\varphi_3\}}$$

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

定义 (推导树)

推导树（*derivation tree*）是一棵满足下列条件的树：

- 每一个中间节点对应一个霍尔三元组；
- 每一个叶子结点要么为空，要么也对应一个霍尔三元组；
- 每一个中间节点和其子节点构成的片段，形如：

$$\frac{\{\varphi_1\}\ st_1\ \{\psi_1\} \quad \ldots \quad \{\varphi_n\}\ st_n\ \{\psi_n\}}{\{\varphi\}\ st\ \{\psi\}},$$

  都对应霍尔证明系统中某条推理规则的实例。

定义 (证明树)

所有叶子结点都是空的推导树成为证明树（proof tree）。如果存在一棵以霍尔三元组 $\{\varphi\}\ st\ \{\psi\}$ 为根节点的证明树，就说该霍尔三元组可证明，记作 $\vdash \{\varphi\}\ st\ \{\psi\}$。

$$(\text{空语句})\ \frac{}{\{\varphi\}\ \textbf{skip}\ \{\varphi\}}$$

引理 (空语句规则的可靠性)

霍尔三元组 $\{\varphi\}$ **skip** $\{\varphi\}$ 是有效式。

证明.

根据空操作语句的语义，显然成立。 □

$$(\text{赋值})\ \frac{}{\{\varphi[x \mapsto e]\}\ x := e\ \{\varphi\}}$$

其中，$\varphi[x \mapsto e]$ 是指将 φ 中所有 x 的自由出现替换为 e 所得的公式。例如，$(x > 0)[x \mapsto x+1]$ 的结果是 $x+1 > 0$。

可能有读者会对上面的规则觉得比较疑惑，为何不是下面的形式？

$$(\text{赋值}\ \times)\ \frac{}{\{\varphi\}\ x := e\ \{\varphi[x \mapsto e]\}}$$

示例：给定语句 $x := x+1$，假设执行这条语句之前满足 $x = y$，根据（赋值 $\times$）规则，执行这条语句之后应该满足 $x+1 = y$。这显然不对，正确的结果应该是 $x = y+1$。

（赋值）规则可以理解为：如果公式 φ 在将 x 赋值为 e 后成立，那么公式 φ 在将 x 替换成 e 后也成立。

$$\text{（赋值）}\quad \overline{\{\varphi[x \mapsto e]\}\ x := e\ \{\varphi\}}$$

请应用赋值规则确定下列霍尔三元组的前置条件 φ：

1. $\{\varphi\}\ x := x+1\ \{x = n\}$ $\qquad x+1=n$
2. $\{\varphi\}\ x := 1\ \{x = y\}$ $\qquad 1=y$
3. $\{\varphi\}\ x := 1\ \{y = 3\}$ $\qquad y=3$
4. $\{\varphi\}\ x := x^2+1\ \{xy \geq x+y)\}$ $\qquad (x^2+1)y \geq (x^2+1)+y$

示例

例

请应用赋值规则确定下列霍尔三元组的前置条件 φ:

$$\{\varphi\}\ \ y := x + 1\ \ \{\forall x.\ (x < z \to x < y) \to x + 1 \le y)\}$$

解

根据赋值语句的推理规则，前置条件似乎为:

$$\begin{aligned}(\forall x.\ (x < z \to x < y) \to x + 1 \le y))[y \mapsto x + 1]\\ \Leftrightarrow (\forall x.\ (x < z \to x < x + 1) \to x + 1 \le x + 1))\end{aligned}$$

错误，因为替换时发生了变元捕获!
为避免变元捕获，需要对约束变元进行重命名，正确结果为:

$$\forall x'.\ (x' < z \to x' < x + 1) \to x + 1 \le x + 1$$

引理 (赋值语句推理规则的可靠性)

霍尔三元组 $\{\varphi[x \mapsto e]\}\ x := e\ \{\varphi\}$ 是有效式。

回顾赋值语句的语义

$$[\![x := e]\!] = \{(s, s') \mid s' = s[x \mapsto [\![e]\!]_s]\}$$

引理

设 x 为变元，e 为项，φ 为公式。给定两组赋值 ρ_1, ρ_2，如果 $\rho_2 = \rho_1[x \mapsto [\![e]\!]_{\rho_1}]$，则 $[\![\varphi[x \mapsto e]]\!]_{\rho_1} = [\![\varphi]\!]_{\rho_2}$。

证明.

任取 $s \in \{\varphi[x \mapsto e]\}$，设 $(s, s') \in [\![x := e]\!]$，即从 s 出发执行 $x := e$ 之后得到的后状态为 s'。
根据赋值语句的语义，$s' = s[x \mapsto [\![e]\!]_s]$。
根据上面的引理，$[\![\varphi]\!]_{s'} = true$，即 $s' \in \{\varphi\}$。 $\square$

我们无法证明：$\vdash \{y = 0\}\ x := 1\ \{x = 1\}$
但却可以证明：$\vdash \{1 = 1\}\ x := 1\ \{x = 1\}$

注意后者的前置条件 $1 = 1$ 是永真式，相当于我们在没有做任何假设的情况下证明了执行语句 $x := 1$ 后一定满足 $x = 1$，那么当有一些假设的时候，该结论显然也成立。

前提加强规则：

$$\text{（前提加强）}\ \frac{\{\varphi'\}\ st\ \{\psi\}}{\{\varphi\}\ st\ \{\psi\}}\ \text{如果}\ \varphi \Rightarrow \varphi'$$

例

霍尔三元组 $\{y=0\}\ x:=1\ \{x=1\}$ 是否可证明?

$$\dfrac{\text{赋值}\ \dfrac{}{\{1=1\}\ x:=1\ \{x=1\}}}{\{y=0\}\ x:=1\ \{x=1\}}\ \text{前提加强} \qquad \text{如果}\ y=0\Rightarrow 1=1$$

推理规则：结论弱化

类似于前提加强，还可以有结论弱化规则：

$$\text{（结论弱化）}\ \frac{\{\varphi\}\ \ st\ \ \{\psi'\}}{\{\varphi\}\ \ st\ \ \{\psi\}}\ \text{如果}\ \psi' \Rightarrow \psi$$

直观理解，如果能证明一个包含了许多事实的**更强陈述**，则必定也能证明一个包含更少事实的**更弱陈述**。

示例

例

霍尔三元组 $\{y=0\}\ x:=1\ \{x\leq 1\}$ 是否可证明?

$$\dfrac{\dfrac{\dfrac{}{\{1=1\}\ x:=1\ \{x=1\}}}{\{y=0\}\ x:=1\ \{x=1\}}\; y=0\Rightarrow 1=1}{\{y=0\}\ x:=1\ \{x\leq 1\}}\; x=1\Rightarrow x\leq 1$$

推理规则：分支语句

$$（分支）\ \frac{\{\varphi \wedge p\}\ \ st_1\ \ \{\psi\} \qquad \{\varphi \wedge \neg p\}\ \ st_2\ \ \{\psi\}}{\{\varphi\}\ \ \textbf{if}\,(p)\,\{st_1\}\,\textbf{else}\,\{st_2\}\ \ \{\psi\}}$$

- 如果分支条件 p 成立，执行 st_1 分支，执行结束后要求满足后置条件 ψ。
- 如果分支条件 p 不成立，执行 st_2 分支，执行结束后也要满足后置条件 ψ。

例

证明 $\{x = y\}$ **if** $(y \geq 0)\{\texttt{y:=y-1}\}$ **else** $\{\texttt{y:=y+1}\}$ $\{\psi\}$

解

记

$$\psi = (x \geq 0 \rightarrow y = x - 1) \wedge (x < 0 \rightarrow y = x + 1)$$
$$\psi_1 = (x \geq 0 \rightarrow y - 1 = x - 1) \wedge (x < 0 \rightarrow y - 1 = x + 1)$$
$$\psi_2 = (x \geq 0 \rightarrow y + 1 = x - 1) \wedge (x < 0 \rightarrow y + 1 = x + 1)$$

$$\dfrac{\dfrac{\dfrac{}{\{\psi_1\}\ \textit{y=y-1}\ \{\psi\}}}{\{x = y \wedge y \geq 0\}\ \textit{y:=y-1}\ \{\psi\}} \qquad \dfrac{\dfrac{}{\{\psi_2\}\ \textit{y:=y+1}\ \{\psi\}}}{\{x = y \wedge y < 0\}\ \textit{y:=y+1}\ \{\psi\}}}{\{x = y\}\ \textbf{if}\ (y \geq 0)\{\textit{y:=y-1}\}\ \textbf{else}\ \{\textit{y:=y+1}\}\ \{\psi\}}$$

注意：在应用前提加强和结论弱化到上述证明的过程中，需要判断：

$$x = y \wedge y \geq 0 \Rightarrow \psi_1$$
$$x = y \wedge y < 0 \Rightarrow \psi_2$$

引理

如果霍尔三元组 $\{\varphi \wedge p\}\ st_1\ \{\psi\}$ 和 $\{\varphi \wedge \neg p\}\ st_2\ \{\psi\}$ 都是有效式，则霍尔三元组 $\{\varphi\}$ **if** (p) $\{st_1\}$ **else** $\{st_2\}$ $\{\psi\}$ 是有效式。

回顾分支语句的语义

$$[\![\textbf{if } (p)\{st_1\} \textbf{ else } \{st_2\}]\!] = \left\{ (s, s') \;\middle|\; \begin{array}{r} [\![p]\!]_s = \mathit{true} \text{ 且 } (s, s') \in [\![st_1]\!] \\ \text{或 } [\![p]\!]_s = \mathit{false} \text{ 且 } (s, s') \in [\![st_2]\!] \end{array} \right\}$$

证明.

任取 $s \in \{\varphi\}$，设 $(s, s') \in [\![\textbf{if } (p)\ \{st_1\} \textbf{ else } \{st_2\}]\!]$，需要证明 $s' \in \{\psi\}$。分两种情况讨论：（1）如果 $[\![p]\!]_s = \mathit{true}$ 且 $(s, s') \in [\![st_1]\!]$，根据 $\{\varphi \wedge p\}\ st_1\ \{\psi\}$ 是有效式知 $s' \in \{\psi\}$；（2）如果 $[\![p]\!]_s = \mathit{false}$ 且 $(s, s'') \in [\![st_2]\!]$，根据 $\{\varphi \wedge \neg p\}\ st_2\ \{\psi\}$ 是有效式知 $s'' \in \{\psi\}$。因此无论哪种情况，分支语句执行结束的后状态都满足 ψ。 $\square$

推理规则：顺序组合语句

$$\text{（顺序）}\ \frac{\{\varphi_1\}\ st_1\ \{\varphi_2\} \qquad \{\varphi_2\}\ st_2\ \{\varphi_3\}}{\{\varphi_1\}\ st_1; st_2\ \{\varphi_3\}}$$

- 注意：需要找到合适的逻辑公式 φ_2 使两个前提都成立。
- 在这个过程中，很可能需要用到前提加强和结论弱化规则。

例

证明 $\{x = x' \wedge y = y'\}\ t := x; x := y; y := t\ \{y = x' \wedge x = y'\}$。

解

$$
\dfrac{
\dfrac{
\left\{\begin{matrix} x = x' \\ \wedge y = y' \end{matrix}\right\} t := x \left\{\begin{matrix} t = x' \\ \wedge y = y' \end{matrix}\right\}
\quad
\left\{\begin{matrix} t = x' \\ \wedge y = y' \end{matrix}\right\} x := y \left\{\begin{matrix} t = x' \\ \wedge x = y' \end{matrix}\right\}
}{
\left\{\begin{matrix} x = x' \\ \wedge y = y' \end{matrix}\right\} t := x; x := y \left\{\begin{matrix} t = x' \\ \wedge x = y' \end{matrix}\right\}
}
\quad
\left\{\begin{matrix} t = x' \\ \wedge x = y' \end{matrix}\right\} y := t \left\{\begin{matrix} y = x' \\ \wedge x = y' \end{matrix}\right\}
}{
\left\{\begin{matrix} x = x' \\ \wedge y = y' \end{matrix}\right\} t := x; x := y; y := t \left\{\begin{matrix} y = x' \\ \wedge x = y' \end{matrix}\right\}
}
$$

注意：由于公式太大，省略了赋值语句推导规则的应用过程。

引理 (顺序组合语句推理规则的可靠性)

如果霍尔三元组 $\{\varphi_1\}\ st_1\ \{\varphi_2\}$ 和 $\{\varphi_2\}\ st_2\ \{\varphi_3\}$ 都是有效式，则霍尔三元组 $\{\varphi_1\}\ st_1; st_2\ \{\varphi_3\}$ 是有效式。

回顾顺序组合语句的语义

$$[\![st_1; st_2]\!] = \{(s, s') \mid \text{存在 } s'' \text{ 使得 } (s, s'') \in [\![st_1]\!], (s'', s') \in [\![st_2]\!]\}$$

证明.

任取 $s \in \{\varphi_1\}$，设 $(s, s') \in [\![st_1; st_2]\!]$，需要证明 $s' \in \{\varphi_3\}$。
根据顺序组合语句的语义，存在 s'' 使得 $(s, s'') \in [\![st_1]\!]$ 及 $(s'', s') \in [\![st_2]\!]$。
根据 $\{\varphi_1\}\ st_1\ \{\varphi_2\}$ 和 $\{\varphi_2\}\ st_2\ \{\varphi_3\}$ 都是有效式，有 $s'' \in \{\varphi_2\}$，$s' \in \{\varphi_3\}$。 $\square$

到此为止，我们已经分别针对空语句、赋值语句、分支语句和顺序组合语句引入了推理规则。应用这些推理规则会让待证霍尔三元组中的程序**至少减少一个构造子**，从而起到简化的作用。

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** 是语义等价的。

继而可得下面的推理规则：

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

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。

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

- φ 是一个循环不变式：
  - 首次到达循环头位置，φ 成立；
  - 从满足 φ 的状态出发，进入循环并迭代一次之后，φ 仍然成立。
- 该规则刻画了循环不变式的第二个条件，第一个条件（即程序执行到循环语句时，φ 成立）需要与其他规则配合来检查。

示例：P_{xy} 程序

例

证明 $\{x \geq 42 \wedge y \leq -23\}\ P_{xy}\ \{x \geq 53\}$ 是有效霍尔三元组。

解

以 $\texttt{if-st}$ 代表：$\textbf{if}\ (y \geq 0)\{y := y - 1\}\ \textbf{else}\ \{y := y + 1\}$

以 P_{xy} 代表：$\textbf{while}\ (y \neq 0)\{\texttt{if-st}; x := x + 1\}$

$$
\text{弱化}\ \dfrac{\text{加强}\ \dfrac{\text{循环}\ \dfrac{\text{顺序}\ \dfrac{\{\psi_1 \wedge (y \neq 0)\}\ \texttt{if-st}\ \{\psi_2\} \qquad \text{赋值}\ \dfrac{}{\{\psi_2\}\ x := x + 1\ \{\psi_1\}}}{\{\psi_1 \wedge (y \neq 0)\}\ \texttt{if-st}; x := x + 1\ \{\psi_1\}}}{\{\psi_1\}\ P_{xy}\ \{\psi_1 \wedge \neg(y \neq 0)\}}}{\{x \geq 42 \wedge y \leq -23\}\ P_{xy}\ \{\psi_1 \wedge \neg(y \neq 0)\}}}{\{x \geq 42 \wedge y \leq -23\}\ P_{xy}\ \{x \geq 53\}}
$$

其中：

$$
\begin{aligned}
\psi_1 &:= x - y \geq 53 \quad \text{(循环不变式)} \\
\psi_2 &:= x + 1 - y \geq 53
\end{aligned}
$$

$$
\text{分支}\ \dfrac{
\text{加强}\ \dfrac{\text{赋值}\ \dfrac{}{\{\psi_2'\}\ \texttt{y:=y-1}\ \{\psi_2\}}}{\left\{\begin{matrix}\psi_1\wedge y\neq 0\\ \wedge y\geq 0\end{matrix}\right\}\ \texttt{y:=y-1}\ \{\psi_2\}}
\qquad
\dfrac{\dfrac{}{\{\psi_2''\}\ \texttt{y:=y+1}\ \{\psi_2\}}}{\left\{\begin{matrix}\psi_1\wedge y\neq 0\\ \wedge\neg y\geq 0\end{matrix}\right\}\ \texttt{y:=y+1}\ \{\psi_2\}}
}{\{\psi_1\wedge y\neq 0\}\ \textbf{if}\ (y\geq 0)\{y:=y-1\}\ \textbf{else}\ \{y:=y+1\}\ \{\psi_2\}}
$$

其中:

$$
\begin{aligned}
\psi_1 &= x-y\geq 53 \quad (\text{循环不变式})\\
\psi_2 &= x+1-y\geq 53\\
\psi_2' &= x+1-(y-1)\geq 53\\
\psi_2'' &= x+1-(y+1)\geq 53
\end{aligned}
$$

引理 (循环规则的可靠性)

如果霍尔三元组 $\{\varphi \wedge p\}\ st\ \{\psi\}$ 是有效式，则霍尔三元组 $\{\varphi\}\ \mathbf{while}\ (p)\{st\}\ \{\psi\}$ 是有效式。

至此，我们证明了霍尔逻辑系统中每一条推理规则的可靠性。

定理 (霍尔证明系统的可靠性)

霍尔证明系统是可靠的（*sound*），即通过该证明系统推导出的所有霍尔三元组都是有效式。换句话说，如果存在一棵以 $\{\varphi\}\ st\ \{\psi\}$ 为根节点的证明树（记作 $\vdash \{\varphi\}\ st\ \{\psi\}$），则该霍尔三元组必是有效式（记作 $\models \{\varphi\}\ st\ \{\psi\}$），此时也称程序 st 满足规约 (φ, ψ)。

证明： 对证明树的高度 n 进行归纳以证明其根节点对应的霍尔三元组一定是有效式。

- 当 $n = 1$ 时，设根节点被标注 $\{\varphi\}\ st\ \{\psi\}$，其他节点都是叶子节点，且标注为空。根据证明树的定义，从根节点到叶子节点一定应用了前提为空的推理规则，只能是空语句规则或者赋值规则。根据这两条规则的可靠性可知结论成立。

- 假设结论在 $n \leq k$ 时成立，需要证明在 $n = k + 1$ 时也成立。设证明树的根节点被标注 $\{\varphi\}\ st\ \{\psi\}$，其子节点分别被标注 $\{\varphi_1\}\ st_1\ \{\psi_1\}$, ..., $\{\varphi_m\}\ st_m\ \{\psi_m\}$。显然，所有这些子节点对应的子树都是高度 $\leq k$ 的证明树。根据假设，在这些子节点上标注的霍尔三元组都是有效式。根据推导树的定义，

$$\frac{\{\varphi_1\}\ st_1\ \{\psi_1\} \qquad \ldots \qquad \{\varphi_m\}\ st_m\ \{\psi_m\}}{\{\varphi\}\ st\ \{\psi\}}$$

  必须是某条推理规则的实例。能够在此处应用的规则只能是前提加强、结论弱化、顺序、分支和循环规则中的一条。根据这些规则的可靠性，可证根节点的霍尔三元组 $\{\varphi\}\ st\ \{\psi\}$ 一定是有效式。

定理 (霍尔证明系统的完备性)

霍尔证明系统是相对完备的（*relatively complete*），即通过霍尔证明系统可以推导出 *IMP* 语言中所有有效的霍尔三元组。换句话说，如果 $\{\varphi\}\ st\ \{\psi\}$ 是有效式，即 $\models \{\varphi\}\ st\ \{\psi\}$，则必定存在一棵以该霍尔三元组为根节点的证明树。

- 注意在应用前提加强和结论弱化规则时，我们需要先证明形如 $p \to q$ 的一阶逻辑蕴涵式的有效性。
- 对于一个有效的霍尔三元组，能否找到对应的推导树依赖于一阶逻辑蕴涵式能否得到有效判定。
- 不幸的是，IMP 语言中允许乘法，对应的 $\mathcal{T}_{PA}$ 算术理论是不可判定的！
- 对于更复杂的语言，相对完备性可能也无法保证。

基本思路是减少证明过程的不确定性:

- 为每个循环选择一个“合适”的循环不变式
- 结论弱化规则仅用于等价变换（如公式的语法变形）
- 从后往前应用顺序组合规则
- 仅对循环之前的语句应用前提严格加强规则
- 如果选择的循环不变式不足以完成证明，则选择新的循环不变式，并重新开始推导。

应用的难点和关键是选择合适的循环不变式。
然而，生成合适的循环不变式的问题是不可判定问题（否则，程序验证将可判定!）。

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

下节课内容

- 进一步理解循环
- 包含数据结构的程序的验证

谢谢！