霍尔逻辑

1 霍尔三元组

对于任意程序状态 s_1 与 s_2，如果 s_1 满足性质 P 并且 $(s_1, s_2) \in [\![c]\!]$，那么 s_2 满足性质 Q。这一性质写作 $\{P\}c\{Q\}$，称为霍尔三元组，P 称为前条件，Q 称为后条件。

```
{ x == 0 }
y = 0;
while (y < 6) do {
  x = x + y;
  y = y + 1
}
{ x == 1 + 2 + 3 + 4 + 5 }
```

2 顺序执行规则、空语句规则与条件分支语句规则

下面是顺序执行规则：

如果 $\{P\}c_1\{Q\}$ 并且 $\{Q\}c_2\{R\}$，那么 $\{P\}c_1; c_2\{R\}$。

下面是一个顺序执行规则的例子。我们想要证明，下面程序确实交换了变量`x`与`y`的值。

```
{ x == m && y == n }
t = x;
x = y;
y = t
{ x == n && y == m }
```

首先，下面的霍尔三元组显然为真。

```
{ x == m && y == n }
t = x
{ t == m && y == n }
```

```
{ t == m && y == n }
x = y
{ t == m && x == n }
```

```
{ t == m && x == n }
y = t
{ x == n && y == m }
```

由其中的第二第三条可以得到：

```
{ t == m && y == n }
x = y;
y = t
{ x == n && y == m }
```

最后再用顺序执行规则和第一条霍尔三元组可知：

```
{ x == m && y == n }
t = x;
x = y;
y = t
{ x == n && y == m }
```

下面是空语句规则：

$\{P\}$ skip $\{P\}$

下面是条件分支语句规则：

如果 $\{P\&\&e\}c_1\{Q\}$ 并且 $\{P\&\&!e\}c_2\{Q\}$，那么

$$\{P\} \text{ if } (e) \text{ then } \{ c_1 \} \text{ else } \{ c_2 \} \{Q\}$$

3 While 语句规则与循环不变量

While 语句规则

如果 $\{ P \&\&e \}$ c $\{ P \}$，那么

$$\{ P \} \text{ while } (e) \text{ do } \{ c \} \{ P \&\& !e \}$$

其中，我们一般会称 P 为循环不变量。

例如，要证明下面霍尔三元组

```
{ x == 0 }
while (x < 10) do
{
  x = x + 1
}
{ x == 10 }
```

就只需证明：

```
{ x <= 10 }
while (x < 10) do
{
  x = x + 1
}
{ x <= 10 && ! (x < 10) }
```

这又可以被规约为：

```
{ x <= 10 && x < 10 }
  x = x + 1
{ x <= 10 }
```

习题 1. 如何证明：

```
{ x >= 0 }
while (0 < x) do {
  x = x - 1
}
{ x == 0 }
```

参考答案. 以`x >= 0`为循环不变量。下面霍尔三元组成立

```
{ x >= 0 && 0 < x }
x = x - 1
{ x >= 0 }
```

并且`x >= 0 && ! (0 < x)`等价于`x == 0`。

下面通过一个例子分析如何找循环不变量。

假如 m 与 n 是给定正整数，如何证明：

```
{ x == m && y == 0 }
while (! (x < n)) do {
  x = x - n;
  y = y + 1
}
{ n * y + x == m && 0 <= x < n }
```

考虑`n`的值为 3、`m`的值为 10 的具体情况。

```
{ x == 10 && y == 0 }
x = x - 3;
y = y + 1
{ x == 7 && y == 1 }
```

```
{ x == 7 && y == 1 }
x = x - 3;
y = y + 1
{ x == 4 && y == 2 }
```

```
{ x == 4 && y == 2 }
x = x - 3;
y = y + 1
{ x == 1 && y == 3 }
```

循环不变量 P 应当使得下面断言能推出 P：

```
x == 10 && y == 0 ||
x == 7 && y == 1 ||
x == 4 && y == 2 ||
x == 1 && y == 3
```

否则以下两个条件总有一个不成立：

- 循环的前条件能推出 P；
- { P &&循环条件 } 循环体 { P }。

另一方面，循环不变量 P 也不能太弱，否则

$$P \text{ \&\& !循环条件}$$

不足以推出循环整体的后条件。

结合这两点考虑，我们在刚才的例子中可以取循环不变量 P 为：

```
x == 10 && y == 0 ||
x == 7 && y == 1 ||
x == 4 && y == 2 ||
x == 1 && y == 3
```

不难检查，它满足下面三条性质：

- 循环前条件`x == 10 && y == 0`能推出 P
- 循环体能保持循环不变量

```
{ P && ! (x < 3) }
x = x - 3; y = y + 1
{ P }
```

- `P && ! ! (x < 3)`能推出循环后条件`3 * y + x == 10 && 0 <= x < 3`。

当然，循环不变量也可以是弱一些的断言，例如：`3 * y + x == 10 && 0 <= x`

构造循环不变量的一般思路如下：

- 循环的前条件要能推出循环不变量
- 循环不变量不能太强，至少要保证程序运行中每次循环体执行结束后的程序状态应当满足循环不变量，否则循环体不满足霍尔三元组：

$$\{\ P\ \&\&\ e\ \}c\{\ P\ \};$$

- 循环不变量不能太弱，否则 P && !e 不足以推出循环的后条件；
- 通常情况下，可以考虑选择一个循环不变量，使得满足这个循环不变量的程序状态恰好是所有循环体执行结束之后的程序状态。

习题 2. 假如 m 与 n 是给定正整数，如何证明：

```
{ x == m }
while (! (x < n)) do {
  x = x - n
}
{ exists y'. n * y' + x = m && 0 <= x < n }
```

参考答案. 选择`exists y', n * y + x == m && x >= 0`作为循环不变量。

习题 3. 假如 m 与 n 是给定正整数，如何证明：

```
{ x == m && y == n }
while (! (! (x < 0) && ! (0 < x))) do {
  y = y - 1;
  x = x - 1
}
{ y == n - m }
```

参考答案. 选择`y - x == n - m`作为循环不变量，或选择`exists k, y == n - k && x == m - k`作为循环不变量。

习题 4. 假如 m 是给定正整数，如何证明：

```
{ x == m && i == res == 0 }
while (i < x) do {
  res = res + x;
  i = i + 1
}
{ res == m * m }
```

参考答案. 选择`res == i * m && x == m && i <= m`作为循环不变量。

4 变量赋值语句规则（正向）与最强后条件

如何严格定义最佳后条件?

- $\{P\}c\{Q\}$ 成立;
- 如果 $\{P\}c\{Q'\}$ 成立，那么 Q 能推出 Q';

亦称为最强后条件：strongest postcondition。

习题 5. 对于前条件`0 <= y`与程序`x = y`，它们的最强后条件是什么？**参考答案.** `0 <= y && x == y`

习题 6. 对于前条件`n * y + x == m && 0 <= x && n <= x`与程序`x = x - n`，它们的最强后条件是什么？**参考答案.** `n * y + x + n == m && 0 <= x + n && 0 <= x`

习题 7. 对于前条件`n * y + x + n == m && 0 <= x`与程序`y = y + 1`，它们的最强后条件是什么？**参考答案.** `n * (y - 1) + x + n == m && 0 <= x`

习题 8. 对于前条件`x == n && y == m`与程序`x = x + y`，它们的最强后条件是什么？
参考答案. `x == n + m && y == m`

变量赋值规则（正向）:

$$\{P\}\ x = e\ \{\exists x'.\ e[x \mapsto x'] = x\ \&\&\ P[x \mapsto x']\}$$

这里，我们用 $P[x \mapsto x']$ 表示将断言 P 中出现的每一个 x 都替换成为 x'。例如:

- $(x \geqslant 0)[x \mapsto x']$ 表示 $x' \geqslant 0$,
- $(\exists k.\ x = a_k)[x \mapsto x']$ 表示 $\exists k.\ x' = a_k$,
- $(x + y)[x \mapsto x']$ 表示 $x' + y$。

  请注意，此处 $(x + y)$ 是一个 SimpleWhile 语言的表达式（变量加变量），将其中的 x 替换为 x' 之后得到的 $(x' + y)$ 还是一个程序表达式（常量加变量），它的求值结果是 $x' + y$，这里的加号是数学上的加号。
- $y[x \mapsto x']$ 表示 y。
- $(x + 1)[x \mapsto x']$ 表示 $x' + 1$。

例如

```
{ x == m && y == n }
x = x + y
{ exists x'. x' + y == x && x' == m && y == n }
```

```
{ x == m && y == n }
temp = x
{ exists temp'. x == temp && x == m && y == n }
```

习题 9. 对于前条件`x == temp == m && y == n`与程序`x = y`，它们的最强后条件是什么？
参考答案. `exists x'. y == x && x' == temp == m && y == n`

5 变量赋值语句规则（反向）与最弱前条件

后条件 Q 与程序 c 的最弱前条件 P 是指满足下面条件的断言 P。

- $\{P\}c\{Q\}$ 成立；
- 如果 $\{P'\}c\{Q\}$ 成立，那么 P' 能推出 P；

例如，后条件`temp == m && y == n`与程序`temp = x`的一个最弱前条件是：`x == m && y == n`。
下面我们写出变量赋值规则（反向）：

那么 $\{\ P[x \mapsto e]\ \}\ x = e\ \{\ P\ \}$

6 可靠性证明

7 Coq 中归纳定义命题

列表之间的置换关系在 Coq 中是一个归纳定义的命题。

```
Inductive Permutation {A: Type}: list A -> list A -> Prop :=
| perm_nil: Permutation nil nil
| perm_skip: forall x (l l': list A), Permutation l l' ->
    Permutation (x :: l) (x :: l')
| perm_swap: forall x y (l: list A),
    Permutation (x :: y :: l) (y :: x :: l)
| perm_trans: forall l1 l2 l3: list A,
    Permutation l1 l2 ->
    Permutation l2 l3 ->
    Permutation l1 l3.
```

在证明中，归纳定义命题的每个分支可以简单的用作引理或定义。下面这个例子演示了如何证明一个归纳定义的命题。

```
Example perm_fact1: Permutation [1 ; 3; 5] [3; 5; 1].
Proof.
  intros.
  apply (perm_trans _ [3; 1; 5]).
  + apply perm_swap.
  + apply perm_skip.
    apply perm_swap.
Qed.
```

利用类似的方法，可以证明上面定义的置换关系有自反性。

习题 10.

```
Lemma perm_refl: forall {A: Type} (l: list A),
  Permutation l l.
(* 请在此处填入你的证明，以_[Qed]_结束。 *)
```

参考答案.

```
Proof.
  intros.
  induction l.
  + apply perm_nil.
  + apply perm_skip; tauto.
Qed.
```

当归纳定义的命题在前提中时，可以对其做证明树归纳。

```
Lemma perm_symm: forall {A: Type} (l1 l2: list A),
  Permutation l1 l2 ->
  Permutation l2 l1.
Proof.
  intros.
  induction H.
  + apply perm_nil.
  + apply perm_skip; tauto.
  + apply perm_swap.
  + apply (perm_trans _ l2); tauto.
Qed.
```

8 导出规则

除了上述霍尔逻辑规则之外，其实也可以在保持逻辑可靠性的基础上增加一些其他的规则。例如，我们可以增加单侧的 Consequence 规则。

```
Lemma hoare_conseq_pre_sound:
  forall (P P' Q: assertion) (c: com),
    valid {{ P' }} c {{ Q }} ->
    P |-- P' ->
    valid {{ P }} c {{ Q }}.
(* 证明详见Coq源代码。 *)

Lemma hoare_conseq_post_sound:
  forall (P Q Q': assertion) (c: com),
    valid {{ P }} c {{ Q' }} ->
    Q' |-- Q ->
    valid {{ P }} c {{ Q }}.
(* 证明详见Coq源代码。 *)
```

然而，我们并不需要将其添加到霍尔逻辑的原始规则（primitive rules）集合中去。因为，这一规则可以由双侧的 Consequence 规则导出。

```
Lemma hoare_conseq_pre:
  forall (P P' Q: assertion) (c: com),
    provable {{ P' }} c {{ Q }} ->
    P |-- P' ->
    provable {{ P }} c {{ Q }}.
```

下面的证明即是导出证明。

```
Proof.
  intros.
  apply (hoare_conseq P P' Q Q).
  + tauto.
  + tauto.
  + unfold derives.
    intros; tauto.
Qed.
```

上面证明中用到了 `Q |-- Q` 这一性质。之后的证明中还会用到许多关于断言推导的命题逻辑性质。证明中可以使用 `assn_tauto` 指令用于证明。具体而言，`assn_tauto H1 H2 ... Hn` 表示在将 `H1` 等前提考虑在内的情况下使用命题逻辑证明。

```
Lemma hoare_conseq_post:
  forall (P Q Q': assertion) (c: com),
    provable {{ P }} c {{ Q' }} ->
    Q' |-- Q ->
    provable {{ P }} c {{ Q }}.
Proof.
  intros.
  apply (hoare_conseq P P Q Q').
  + tauto.
  + assn_tauto.
  + assn_tauto H0.
Qed.
```

类似的，可以用变量赋值规则（正向）与顺序执行规则导出下面规则。在 Coq 证明中，`eapply` 表示使用 `apply` 但是相关参数暂时空缺。

```
Lemma forward_symbolic_exe:
  forall P x e c Q,
    provable {{ exists x',
                  exprZ_subst [[ e ]] x [[ x' ]] == [[ x ]] &&
                  assn_subst P x [[ x' ]] }} c {{ Q }} ->
    provable {{ P }} x = e; c {{ Q }}.
Proof.
  intros.
  eapply hoare_seq.
  + apply hoare_asgn_fwd.
  + apply H.
Qed.
```

9 证明树归纳

```
Lemma hoare_seq_inv: forall P R c1 c2,
  provable {{ P }} c1 ; c2 {{ R }} ->
  exists Q: assertion,
    provable {{ P }} c1 {{ Q }} /\
    provable {{ Q }} c2 {{ R }}.
(* 证明详见Coq源代码。 *)

Lemma hoare_seq_assoc: forall P Q c1 c2 c3,
  provable {{ P }} c1 ; (c2; c3) {{ Q }} <->
  provable {{ P }} (c1 ; c2); c3 {{ Q }}.
(* 证明详见Coq源代码。 *)

Lemma hoare_asgn_fwd_inv: forall P Q x e,
  provable {{ P }} x = e {{ Q }} ->
  Assn (exists x',
          exprZ_subst [[ e ]] x [[ x' ]] == [[ x ]] &&
          assn_subst P x [[ x' ]]) |-- Q.
(* 证明详见Coq源代码。 *)
```

习题 11.

```
Lemma hoare_if_inv: forall P Q e c1 c2,
  provable {{ P }} if (e) then { c1 } else { c2 } {{ Q }} ->
  provable {{ P && [[ e ]] }} c1 {{ Q }} /\
  provable {{ P && [[ ! e ]] }} c2 {{ Q }}.
(* 请在此处填入你的证明，以_[Qed]_结束。 *)
```

参考答案.

```
Proof.
  intros.
  remember ( {{ P }} if (e) then { c1 } else { c2 } {{ Q }} ) as ht eqn:EQ.
  revert P Q EQ; induction H; intros.
  + discriminate EQ.
  + discriminate EQ.
  + clear IHprovable1 IHprovable2.
    injection EQ as ? ? ? ? ?.
    subst P0 e0 c0 c3 Q0.
    tauto.
  + discriminate EQ.
  + discriminate EQ.
  + injection EQ as ? ? ?.
    subst P0 c Q0.
    specialize (IHprovable _ _ eq_refl).
    destruct IHprovable.
    split.
    - eapply hoare_conseq; [eauto | | eauto].
      assn_tauto H0.
    - eapply hoare_conseq; [eauto | | eauto].
      assn_tauto H0.
Qed.
```

习题 12.

```
Lemma hoare_if_seq1: forall P Q e c1 c2 c3,
  provable {{ P }} if (e) then { c1 } else { c2 }; c3 {{ Q }} ->
  provable {{ P }} if (e) then { c1; c3 } else { c2; c3 } {{ Q }}.
(* 请在此处填入你的证明，以_[Qed]_结束。 *)
```

参考答案.

```
Proof.
  intros.
  apply hoare_seq_inv in H.
  destruct H as [M [? ?] ].
  apply hoare_if.
  + apply hoare_if_inv in H.
    destruct H.
    apply (hoare_seq _ M); tauto.
  + apply hoare_if_inv in H.
    destruct H.
    apply (hoare_seq _ M); tauto.
Qed.
```