课前阅读：Coq 中的归纳类型

1 关于等式的证明

在先前证明单调函数性质的过程中，我们经常会要通过参数之间的大小关系推导出函数值之间的大小关系。例如，当 f 是一个单调函数时，可以由 $x \leqslant y$ 推出 $f(x) \leqslant f(y)$。对于一般的函数，我们也可以由参数相等，推出函数值相等，即由 $x = y$ 推出 $f(x) = f(y)$。下面的证明中就要用到这一性质。

```
Definition is_fixpoint (f: Z -> Z) (x: Z): Prop :=
  f x = x.
```

```
Theorem fixpoint_self_comp: forall f x,
  is_fixpoint f x ->
  is_fixpoint (Zcomp f f) x.
Proof.
  unfold is_fixpoint, Zcomp.
  intros.
  rewrite H.
  rewrite H.
  reflexivity.
Qed.
```

在数学上，如果`f x = x`，那么我们就称`x`是函数`f`的一个不动点。上面的定理证明了，如果`x`是`f`的不动点，那么`x`也是`f`与自身复合结果的不动点。在这一证明中，前提`H`是命题`f x = x`。证明指令`rewrite H`的效果是将结论中的`f x`替换为`x`，因此，第一次使用该指令后，原先需要证明的`f (f x) = x`规约为了`f x = x`。这一步背后的证明实际就用到了“只要函数`f`的参数不变，那么函数值也不变”这条性质。

```
```

Coq 证明脚本 1. 利用等式做证明的 rewrite 指令. 如果`H`是具有形式`a = b`定理或证明前提，`rewrite H`可以将待证明结论中的`a`替换成`b`，`rewrite H in H0`也可以将前提`H0`中的`a`替换成`b`。有时，这个`a`可能出现了多次，但是我们只希望将其中的若干个`a`而不是全部的`a`都替换成`b`，此时可以在 rewrite 指令中增加`at`，即使用`rewrite H at ...`或`rewrite H at ... in ...`指明需要进行替换的位置。例如，当前提`H`为`x = f x`，待证明结论为`x = f (f x)`时，

`rewrite H` 与 `rewrite H at 1, 2`

都会将结论变为`f x = f (f (f x))`；

`rewrite H at 1`

会将结论变为`f x = f (f x)`；而

`rewrite H at 2`

会将结论变为`x = f (f (f x))`。

Coq 允许 rewrite 使用的定理或前提中有`forall`概称量词，用户可以手动地填入这些`forall`约束的变量或由 Coq 自动填入这些变量。例如，当前提`H1`与待证明结论分别为：

```
forall x y: Z, g x y = g y x
g 3 5 = 6
```

时，`rewrite H1`、`rewrite (H1 3)`或`rewrite (H1 3 5)`都会将待证明结论变换为`g 5 3 = 6`。Coq 还允许 rewrite 使用的定理或前提中带有附加条件，例如当前提 `H2`与待证明结论分别为：

```
forall x: Z, x <= 0 -> h x = 0
h (h (-5)) = 0
```

时，Coq 中的`rewrite H2`指令会将原证明目标规约为两个新的证明目标：第一个证明目标中结论变为`h 0 = 0`，第二个证明目标为需要补充证明的附加条件`-5 <= 0`。如果产生的附加条件可以用一条证明脚本完成证明，那么可以在 rewrite 指令中加入`by`。上面例子中，`rewrite H2 by lia`可以直接将结论变为`h 0 = 0`并不再额外产生附加的证明条件。

最后，Coq 中不仅允许将等式左侧的内容替换为等式右侧的内容，也允许使用`<-`进行反向操作。例如，当`H`具有形式`a = b`时，`rewrite <- H`会将结论中的`b`替换为`a`。同时，Coq 也允许在一条 rewrite 指令中，按指定顺序连续进行多次替换，例如`rewrite H1, H2`表示先`rewrite H1`再`rewrite H2`。

下面关于不动点简单性质的证明需要我们灵活使用 rewrite 指令。

```
Example fixpoint_self_comp23: forall f x,
  is_fixpoint (Zcomp f f) x ->
  is_fixpoint (Zcomp f (Zcomp f f)) x ->
  is_fixpoint f x.
Proof.
  unfold is_fixpoint, Zcomp.
  intros.
  rewrite H in H0.
  rewrite H0.
  reflexivity.
Qed.
```

2 用 Coq 归纳类型定义二叉树

```
Inductive tree: Type :=
| Leaf: tree
| Node (l: tree) (v: Z) (r: tree): tree.
```

这个定义说的是，一棵二叉树要么是一棵空树`Leaf`，要么有一棵左子树、有一棵右子树外加有一个根节点整数标号。我们可以在 Coq 中写出一些具体的二叉树的例子。

```
Definition tree_example0: tree :=
  Node Leaf 1 Leaf.
```

```
Definition tree_example1: tree :=
  Node (Node Leaf 0 Leaf) 2 Leaf.
```

```
Definition tree_example2a: tree :=
  Node (Node Leaf 8 Leaf) 100 (Node Leaf 9 Leaf).
```

```
Definition tree_example2b: tree :=
  Node (Node Leaf 9 Leaf) 100 (Node Leaf 8 Leaf).
```

```
Definition tree_example3a: tree :=
  Node (Node Leaf 3 Leaf) 5 tree_example2a.
```

```
Definition tree_example3b: tree :=
  Node tree_example2b 5 (Node Leaf 3 Leaf).
```

它们分别表示下面这些树结构

```
          2       100         100
    1    /       /   \       /   \
        0       8     9     9     8
```

```
        5                   5
       / \                 / \
      3  100             100  3
        / \               / \
       8   9             9   8
```

Coq 中，我们往往可以使用递归函数定义归纳类型元素的性质。Coq 中定义递归函数时使用的关键字是`Fixpoint`。下面两个定义通过递归定义了二叉树的高度和节点个数。

```
Fixpoint tree_height (t: tree): Z :=
  match t with
  | Leaf => 0
  | Node l v r => Z.max (tree_height l) (tree_height r) + 1
  end.
```

```
Fixpoint tree_size (t: tree): Z :=
  match t with
  | Leaf => 0
  | Node l v r => tree_size l + tree_size r + 1
  end.
```

Coq 系统“知道”每一棵特定树的高度和节点个数是多少。下面是一些 Coq 代码的例子。

```
Example Leaf_height:
  tree_height Leaf = 0.
Proof. reflexivity. Qed.
```

```
Example tree_example2a_height:
  tree_height tree_example2a = 2.
Proof. reflexivity. Qed.
```

```
Example treeexample3b_size:
  tree_size tree_example3b = 5.
Proof. reflexivity. Qed.
```

Coq 中也可以定义树到树的函数。下面的`tree_reverse`函数把二叉树进行了左右翻转。

```
Fixpoint tree_reverse (t: tree): tree :=
  match t with
  | Leaf => Leaf
  | Node l v r => Node (tree_reverse r) v (tree_reverse l)
  end.
```

下面是三个二叉树左右翻转的例子：

```
Example Leaf_tree_reverse:
  tree_reverse Leaf = Leaf.
Proof. reflexivity. Qed.
```

```
Example tree_example0_tree_reverse:
  tree_reverse tree_example0 = tree_example0.
Proof. reflexivity. Qed.
```

```
Example tree_example3_tree_reverse:
  tree_reverse tree_example3a = tree_example3b.
Proof. reflexivity. Qed.
```

归纳类型有几条基本性质。(1) 归纳定义规定了一种分类方法，以`tree`类型为例，一棵二叉树`t`要么是`Leaf`，要么具有形式`Node l v r`；(2) 以上的分类之间是互斥的，即无论`l`、`v`与`r`取什么值，`Leaf`与`Node l v r`都不会相等；(3) `Node`这样的构造子是函数也是单射。这三条性质对应了 Coq 中的三条证明指令：`destruct`、`discriminate`与`injection`。利用它们就可以证明几条最简单的性质：

```
Lemma Node_inj_left: forall l1 v1 r1 l2 v2 r2,
  Node l1 v1 r1 = Node l2 v2 r2 ->
  l1 = l2.
Proof.
  intros.
  injection H as H_l H_v H_r.
```

上面的`injection`指令使用了`Node`是单射这一性质。

```
  rewrite H_l.
  reflexivity.
Qed.
```

有时，手动为`injection`生成的命题进行命名显得很啰嗦，Coq 允许用户使用问号占位，从而让 Coq 进行自动命名。

```
Lemma Node_inj_right: forall l1 v1 r1 l2 v2 r2,
  Node l1 v1 r1 = Node l2 v2 r2 ->
  r1 = r2.
Proof.
  intros.
  injection H as ? ? ?.
```

这里，Coq 自动命名的结果是使用了`H`、`H0`与`H1`。下面也使用`apply`指令取代`rewrite`简化后续证明。

```
  apply H1.
Qed.
```

如果不需要用到`injection`生成的左右命题，可以将不需要用到的部分用下划线占位。

```
Lemma Node_inj_value: forall l1 v1 r1 l2 v2 r2,
  Node l1 v1 r1 = Node l2 v2 r2 ->
  v1 = v2.
Proof.
  intros.
  injection H as _ ? _.
  apply H.
Qed.
```

下面引理说：若`Leaf`与`Node l v r`相等，那么`1 = 2`。换言之，`Leaf`与`Node l v r`始终不相等，否则就形成了一个矛盾的前提。

```
Lemma Leaf_Node_conflict: forall l v r,
  Leaf = Node l v r -> 1 = 2.
Proof.
  intros.
  discriminate.
Qed.
```

下面这个简单性质与`tree_reverse`有关。

```
Lemma reverse_result_Leaf: forall t,
  tree_reverse t = Leaf ->
  t = Leaf.
Proof.
  intros.
```

下面的`destruct`指令根据`t`是否为空树进行分类讨论。

```
  destruct t.
```

执行这一条指令之后，Coq 中待证明的证明目标由一条变成了两条，对应两种情况。为了增加 Coq 证明的可读性，我们推荐大家使用 bullet 记号把各个子证明过程分割开来，就像一个一个抽屉或者一个一个文件夹一样。Coq 中可以使用的 bullet 标记有：`+ - * ++ -- **`等等

```
  + reflexivity.
```

第一种情况是`t`是空树的情况。这时，待证明的结论是显然的。

```
  + discriminate H.
```

第二种情况下，其实前提`H`就可以推出矛盾。可以看出，`discriminate`指令也会先根据定义化简，再试图推出矛盾。

```
Qed.
```

3 结构归纳法

我们接下去将证明一些关于`tree_height`，`tree_size`与`tree_reverse`的基本性质。我们在证明中将会使用的主要方法是归纳法。

相信大家都很熟悉自然数集上的数学归纳法。数学归纳法说的是：如果我们要证明某性质`P`对于任意自然数`n`都成立，那么我可以将证明分为如下两步：

- 奠基步骤：证明`P 0`成立；
- 归纳步骤：证明对于任意自然数`n`，如果`P n`成立，那么`P (n + 1)`也成立。

对二叉树的归纳证明与上面的数学归纳法稍有不同。具体而言，如果我们要证明某性质`P`对于一切二叉树`t`都成立，那么我们只需要证明以下两个结论：

- 奠基步骤：证明`P Leaf`成立；
- 归纳步骤:证明对于任意二叉树`l` `r`以及任意整数标签`n`,如果`P l`与`P r`都成立,那么`P (Node l n r)`也成立。

这样的证明方法就成为结构归纳法。在 Coq 中，`induction`指令表示：使用结构归纳法。下面是几个证明的例子。

第一个例子是证明`tree_size`与`tree_reverse`之间的关系。

```
Lemma reverse_size: forall t,
  tree_size (tree_reverse t) = tree_size t.
Proof.
  intros.
  induction t.
```

上面这个指令说的是：对`t`结构归纳。Coq 会自动将原命题规约为两个证明目标，即奠基步骤和归纳步骤。

```
  + simpl.
```

第一个分支是奠基步骤。这个`simpl`指令表示将结论中用到的递归函数根据定义化简。

```
    reflexivity.
  + simpl.
```

第二个分支是归纳步骤。我们看到证明目标中有两个前提`IHt1`以及`IHt2`。在英文中`IH`表示 induction hypothesis 的缩写，也就是归纳假设。在这个证明中`IHt1`与`IHt2`分别是左子树`t1`与右子树`t2`的归纳假设。

```
    rewrite IHt1.
    rewrite IHt2.
    lia.
Qed.
```

第二个例子很类似，是证明`tree_height`与`tree_reverse`之间的关系。

```
Lemma reverse_height: forall t,
  tree_height (tree_reverse t) = tree_height t.
Proof.
  intros.
  induction t.
  + simpl.
    reflexivity.
  + simpl.
    rewrite IHt1.
    rewrite IHt2.
    lia.
```

注意：`lia`指令也是能够处理`Z.max`与`Z.min`的。

```
Qed.
```

下面我们将通过重写上面这一段证明，介绍 Coq 证明语言的一些其他功能。

```
Lemma reverse_height_attempt2: forall t,
  tree_height (tree_reverse t) = tree_height t.
Proof.
  intros.
  induction t; simpl.
```

在 Coq 证明语言中可以用分号将小的证明指令连接起来形成大的证明指令，其中`tac1 ; tac2`这个证明指令表示先执行指令`tac1`，再对于`tac1`生成的每一个证明目标执行`tac2`。分号是右结合的。

```
  + reflexivity.
  + simpl.
    lia.
Qed.
```

习题 1.

```
Lemma reverse_involutive: forall t,
  tree_reverse (tree_reverse t) = t.
(* 请在此处填入你的证明，以_[Qed]_结束。 *)
```

4 加强归纳

下面证明`tree_reverse`是一个单射。

```
Lemma tree_reverse_inj: forall t1 t2,
  tree_reverse t1 = tree_reverse t2 ->
  t1 = t2.
Proof.
```

这个引理的 Coq 证明需要我们特别关注：真正需要归纳证明的结论是什么？如果选择对`t1`做结构归纳，那么究竟是归纳证明对于任意`t2`上述性质成立，还是归纳证明对于某“特定”的`t2`上述性质成立？如果我们按照之前的 Coq 证明习惯，用`intros`与`induction t1`两条指令开始证明，那就表示用归纳法证明一条关于“特定”`t2`的性质。

```
  intros.
  induction t1.
  + destruct t2.
```

奠基步骤的证明可以通过对`t2`的分类讨论完成。

```
    - reflexivity.
```

如果`t2`是空树，那么结论是显然的。

```
    - simpl in H.
      discriminate H.
```

如果`t2`是非空树，那么前提`H`就能导出矛盾。如上面指令展示的那样，`simpl`指令也可以对前提中的递归定义化简。当然，在这个证明中，由于之后的`discriminate`指令也会完成自动化简，这条`simpl`指令其实是可以省略的。

```
Abort.
```

进入归纳步骤的证明时，不难发现，证明已经无法继续进行。因为需要使用的归纳假设并非关于原`t2`值的性质。正确的证明方法是用归纳法证明一条对于一切`t2`的结论。

```
Lemma tree_reverse_inj: forall t1 t2,
  tree_reverse t1 = tree_reverse t2 ->
  t1 = t2.
Proof.
  intros t1.
```

上面这条`intros 1t`指令可以精确地将`t1`放到证明目标的前提中，同时却将`t2`保留在待证明目标的结论中。

```
  induction t1; simpl; intros.
  + destruct t2.
    - reflexivity.
    - discriminate H.
  + destruct t2.
    - discriminate H.
    - injection H as ? ? ?.
      rewrite (IHt1_1 _ H1).
      rewrite (IHt1_2 _ H).
      rewrite H0.
      reflexivity.
Qed.
```

当然，上面这条引理其实可以不用归纳法证明。下面的证明中使用了前面证明的结论：`reverse_involutive`。

```
Lemma tree_reverse_inj_again: forall t1 t2,
  tree_reverse t1 = tree_reverse t2 ->
  t1 = t2.
Proof.
  intros.
  rewrite <- (reverse_involutive t1), <- (reverse_involutive t2).
  rewrite H.
  reflexivity.
Qed.
```