# 形式化方法导引-作业9

梁峻滔 PB19051175

#### 形式化方法导引-作业9

```
EX1
代码
证明过程
EX2
代码
证明过程
EX3
Heurisitics
代码
证明过程
```

## EX1

## 代码

## 证明过程

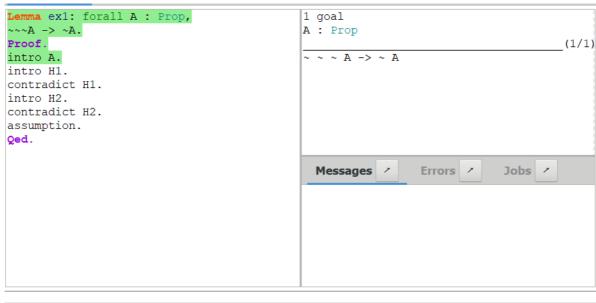
```
Lemma ex1: forall A: Prop,

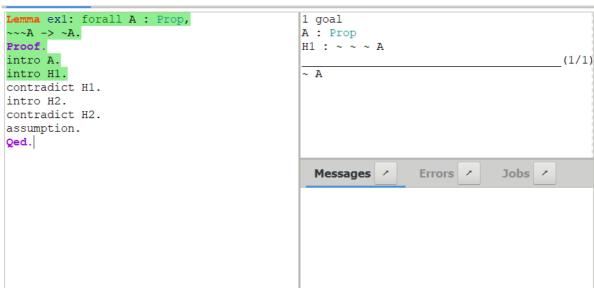
~~A -> ~A.

Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.

Qed.|

Messages / Errors / Jobs /
```





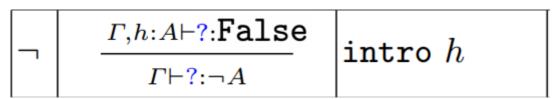
根据<u>官方文档的描述</u>, 当执行 contradict H后, "the current goal and context is transformed in the following way:"

- H:¬A ⊢ B becomes ⊢ A
- H:¬A ⊢ ¬B becomes H: B ⊢ A
- H: A ⊢ B becomes ⊢ ¬A
- H: A ⊢ ¬B becomes H: B ⊢ ¬A

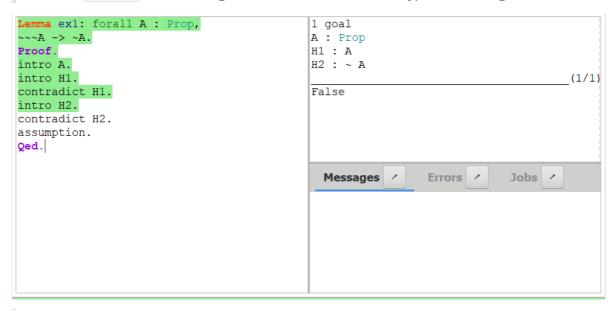
下面执行 contradict H1 后对应第二种情况.



根据PPT 6.2.1-2 中18页处所给的tactics列表中的这一项



此处执行 intro H2 后会将原来的goal去掉一个否定词后作为新的hypothesis, 然后goal变成False.



再应用一次 contradict 就可以把goal变成True -> A, 即A.

然后刚好我们的假设里有H1:A.

```
Lemma ex1: forall A : Prop,
                                           1 goal
~~~A -> ~A.
                                           A : Prop
Proof.
                                           H1 : A
                                                                                  (1/1)
intro A.
intro H1.
                                           A
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
                                             Messages /
                                                            Errors /
                                                                         Jobs /
```

```
Lemma ex1: forall A : Prop,

---A -> -A.

Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.

Messages / Errors / Jobs /
```

# EX2

## 代码

```
Lemma ex2 : forall A B : Prop,
A \/ B -> ~(~A /\ ~B).
Proof.
intros A B.
intro H1.
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
assumption.
Qed.
```

### 证明过程

```
Lemma ex2 : forall A B : Prop,
                                              1 goal
A \ \ B \rightarrow \ \ (\sim A /\ \sim B).
                                                                                        (1/1)
                                               forall A B : Prop,
Proof.
intros A B.
                                               A \setminus / B \rightarrow ( A / \ A B)
intro H1.
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                 Messages / Errors / Jobs /
assumption.
Qed.
Lemma ex2 : forall A B : Prop,
                                               1 goal
A \ \ B \rightarrow \ \ (\sim A /\ \sim B).
                                               A, B : Prop
Proof.
                                                                                       (1/1)
intros A B.
                                               A \/ B -> ~ (~ A /\ ~ B)
intro H1.
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                 Messages / Errors / Jobs /
assumption.
Qed.
Lemma ex2 : forall A B : Prop,
                                               1 goal
A \setminus / B \rightarrow ( A / \ A ).
                                               A, B : Prop
Proof.
                                               H1 : A \/ B
intros A B.
                                                                                        (1/1)
                                               ~ (~ A /\ ~ B)
intro H1.
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                 Messages / Errors / Jobs /
assumption.
Qed.
```

```
Lemma ex2 : forall A B : Prop,
A \setminus / B \rightarrow \sim (\sim A / \setminus \sim B).
                                                 A, B : Prop
                                                 H1 : A \/ B
Proof.
intros A B.
                                                 H2 : ~ A /\ ~ B
intro H1.
                                                                                             (1/1)
                                                 False
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                                     Errors /
                                                                                   Jobs /
                                                   Messages /
assumption.
Qed.
```

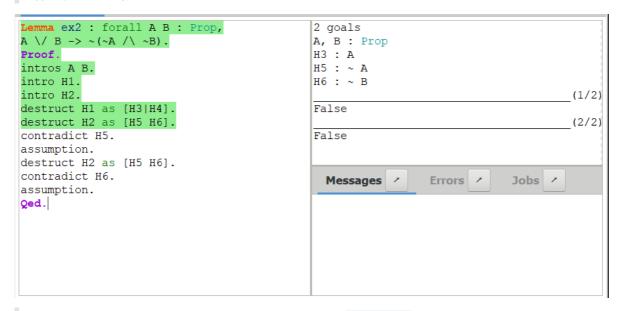
这里对是析取式的假设H1执行 destruct 就是分情况讨论: A成立或B成立.

H3对应A成立的分支,该分支需要证明goal1. 后面还需要在B成立的第二个分支证明goal2(这里goal1 和 goal2 都是False).

```
Lemma ex2 : forall A B : Prop,
                                                2 goals
A \setminus / B \rightarrow (A / A / B).
                                               A, B : Prop
Proof.
                                               H3 : A
intros A B.
                                                H2 : ~ A /\ ~ B
intro H1.
                                                                                          (1/2)
intro H2.
                                                False
destruct H1 as [H3|H4].
                                                                                          (2/2)
destruct H2 as [H5 H6].
                                                False
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                  Messages /
                                                                  Errors /
                                                                                Jobs /
assumption.
Qed.
```

看到假设中有合取式,我们可以考虑将其拆分成两个假设,也是使用 destruct.

将H2分成了H5和H6.



```
Lemma ex2 : forall A B : Prop,
                                               2 goals
A \setminus / B \rightarrow (A / A / B).
                                               A, B : Prop
Proof.
                                               H3 : A
intros A B.
                                               Н6 : ~ В
intro H1.
                                                                                         (1/2)
intro H2.
destruct H1 as [H3|H4].
                                                                                         (2/2)
destruct H2 as [H5 H6].
                                               False
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                                 Errors /
                                                 Messages /
                                                                               Jobs /
assumption.
Qed.
```

```
Lemma ex2 : forall A B : Prop,
                                                 1 goal
A \setminus / B \rightarrow \sim (\sim A / \setminus \sim B).
                                                 A, B : Prop
                                                 Н4 : В
Proof.
intros A B.
                                                 H2 : ~ A /\ ~ B
                                                                                             (1/1)
intro H1.
intro H2.
                                                 False
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                                     Errors /
                                                   Messages /
                                                                                   Jobs /
assumption.
Qed.
```

#### 下面重复类似的操作来证明第二个分支.

```
Lemma ex2 : forall A B : Prop,
                                                  1 goal
                                                 A, B : Prop
A \setminus / B \rightarrow \sim (\sim A / \setminus \sim B).
Proof.
                                                  H4 : B
intros A B.
                                                 H5 : ~ A
intro H1.
                                                 Н6 : ~ В
                                                                                              (1/1)
intro H2.
destruct H1 as [H3|H4].
                                                  False
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                    Messages /
                                                                     Errors /
                                                                                   Jobs /
assumption.
Qed.
```

```
Lemma ex2 : forall A B : Prop,
                                             1 goal
A \setminus B \rightarrow (\A / \A).
                                             A, B : Prop
Proof.
                                             Н4 : В
intros A B.
                                             H5 : ~ A
intro H1.
                                                                                     (1/1)
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                               Messages / Errors /
                                                                           Jobs /
assumption.
Qed.
```

```
Lemma ex2 : forall A B : Prop,
                                                    No more goals.
A \setminus / B \rightarrow \sim (\sim A / \setminus \sim B).
Proof.
intros A B.
intro H1.
intro H2.
destruct H1 as [H3|H4].
destruct H2 as [H5 H6].
contradict H5.
assumption.
destruct H2 as [H5 H6].
contradict H6.
                                                      Messages / Errors /
                                                                                        Jobs /
assumption.
Qed.
```

### EX3

### **Heurisitics**

PPT <u>6.2.1-2</u> 18页的表和以下这张表:

	$\Rightarrow$	A	٨
Hypothesis H	apply H	apply H	elim H
			case H
			destruct H as [H1 H2]
conclusion	intros H	intros H	split
	7	3	V
Hypothesis H	elim H	elim H	elim H
	case H	case H	case H
		destruct H as [x H1]	destruct H as [H1   H2]
conclusion	intros H	exists $v$	left or
			right
	=	False	
Hypothesis H	rewrite H	elim H	
	rewrite <- H	case H	
conclusion	reflexivity		
	ring		

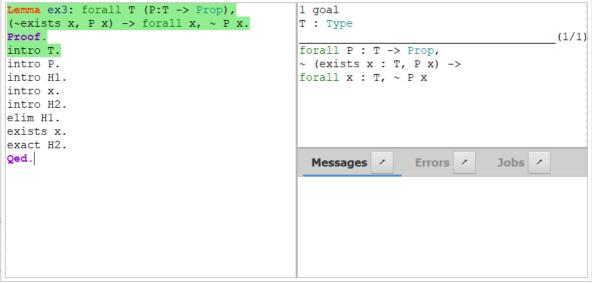
来源: Coq in a Hurry. 这两张表的参考方式是: 例如, 看到某个假设 H 中含有否定词, 则考虑对 H 使用elim; 要证明的 goal 的命题中最前面是exists, 则考虑使用 exists.

## 代码

```
Lemma ex3: forall T (P:T -> Prop),
  (~exists x, P x) -> forall x, ~ P x.
Proof.
intro T.
intro P.
intro H1.
intro x.
intro H2.
elim H1.
exists x.
exact H2.
Qed.
```

### 证明过程





```
Lemma ex3: forall T (P:T -> Prop),
                                               1 goal
                                               T : Type
(~exists x, P x) -> forall x, ~ P x.
Proof.
                                               P : T -> Prop
                                                                                       _(1/1)
intro T.
                                               ~ (exists x : T, P x) -> forall x : T, ~ P x
intro P.
intro H1.
intro x.
intro H2.
elim H1.
exists x.
exact H2.
Qed.
                                                 Messages / Errors /
                                                                              Jobs /
```

```
Lemma ex3: forall T (P:T -> Prop),
                                               1 goal
(~exists x, P x) -> forall x, \sim P x.
                                               T : Type
                                              P : T -> Prop
H1 : ~ (exists x : T, P x)
Proof.
intro T.
intro P.
                                                                                         (1/1)
intro H1.
                                               forall x : T, ~ P x
intro x.
intro H2.
elim H1.
exists x.
exact H2.
Qed.
                                                 Messages /
                                                                 Errors /
                                                                               Jobs /
```

```
Lemma ex3: forall T (P:T -> Prop),
                                            1 goal
(~exists x, P x) -> forall x, ~ P x.
                                            T : Type
Proof.
                                            P : T -> Prop
intro T.
                                            H1 : ~ (exists x : T, P x)
intro P.
                                                                                   (1/1)
intro H1.
                                            forall x : T, ~ P x
intro x.
intro H2.
elim H1.
exists x.
exact H2.
Qed.
                                              Messages /
                                                              Errors /
                                                                          Jobs /
```

goal中含forall, 考虑intro.

```
Lemma ex3: forall T (P:T -> Prop),
                                             1 goal
(~exists x, P x) -> forall x, ~ P x.
                                             T : Type
Proof.
                                             P : T -> Prop
intro T.
                                             H1 : \sim (exists x : T, P x)
intro P.
intro H1.
                                                                                    (1/1)
intro x.
                                             ~ P x
intro H2.
elim H1.
exists x.
exact H2.
Qed.
                                               Messages /
                                                              Errors /
                                                                           Jobs /
```

```
Lemma ex3: forall T (P:T -> Prop),
                                            1 goal
(~exists x, P x) -> forall x, ~ P x.
                                            T : Type
Proof.
                                            P : T -> Prop
intro T.
                                            H1 : ~ (exists x : T, P x)
                                            х : Т
intro P.
intro H1.
                                            H2 : P x
intro x.
                                                                                   (1/1)
intro H2.
                                            False
elim H1.
exists x.
exact H2.
Qed.
                                                              Errors /
                                              Messages /
                                                                          Jobs /
```

考察假设, 发现 H1 比较复杂, 然后最前面是否定词, 考虑使用 elim.

```
Lemma ex3: forall T (P:T -> Prop),
                                            1 goal
                                            T : Type
(~exists x, P x) -> forall x, ~ P x.
                                            P : T -> Prop
Proof.
intro T.
                                            H1 : ~ (exists x : T, P x)
intro P.
                                            х : Т
                                            H2 : P x
intro H1.
                                                                                   _(1/1)
intro x.
intro H2.
                                            exists x0 : T, P x0
elim H1.
exists x.
exact H2.
Qed.
                                                              Errors /
                                              Messages /
                                                                          Jobs /
```

goal是 exists 命题, 考虑使用 exists tactic.

Oops! 刚好目标就是H2.

```
Lemma ex3: forall T (P:T -> Prop),
                                            1 goal
(~exists x, P x) -> forall x, ~ P x.
                                            T : Type
                                            P : T -> Prop
Proof.
                                            H1 : ~ (exists x : T, P x)
x : T
intro T.
intro P.
intro H1.
                                            H2 : P x
                                                                                   (1/1)
intro x.
                                            P x
intro H2.
elim H1.
exists x.
exact H2.
Qed.
                                              Messages / Errors /
                                                                          Jobs /
```

