形式化方法导引-作业9

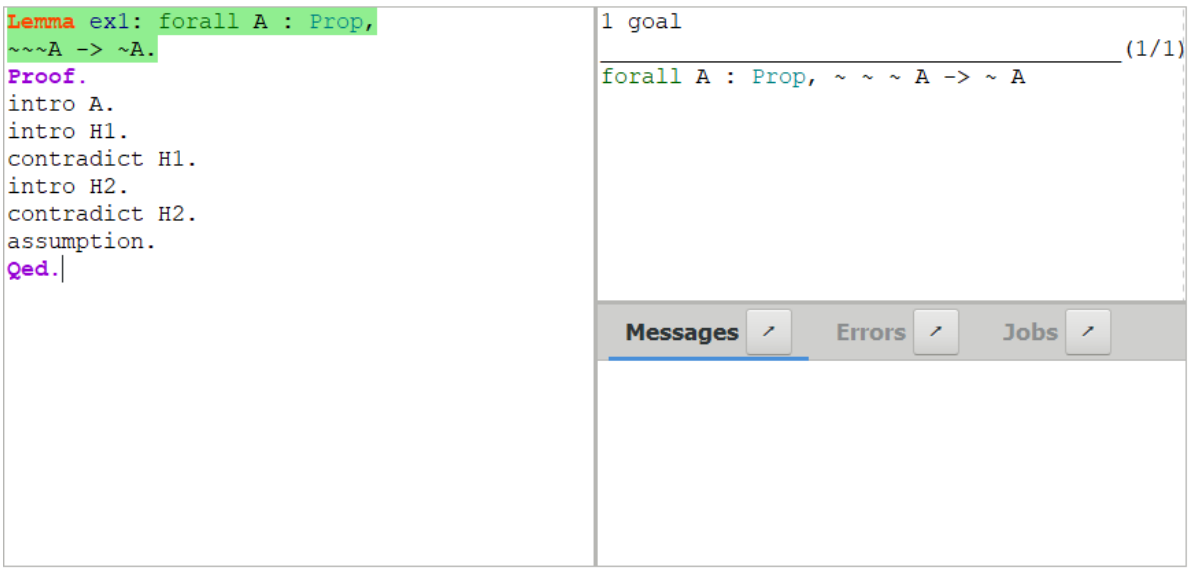
梁峻滔 PB19051175

EX1

代码

```
Lemma ex1: forall A : Prop,
~~~A -> ~A.
Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
```

证明过程



```
Lemma ex1: forall A : Prop,
~~~A -> ~A.
Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
```

```
1 goal
A : Prop
_____________________________________(1/1)
~ ~ ~ A -> ~ A
```

Messages ↗ Errors ↗ Jobs ↗

```
Lemma ex1: forall A : Prop,
~~~A -> ~A.
Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
```

```
1 goal
A : Prop
H1 : ~ ~ ~ A
_____________________________________(1/1)
~ A
```

Messages ↗ Errors ↗ Jobs ↗

> 根据官方文档的描述, 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.

```
Lemma ex1: forall A : Prop,
~~~A -> ~A.
Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
```

```
1 goal
A : Prop
H1 : A
_____________________________________(1/1)
~ ~ A
```

Messages ↗ Errors ↗ Jobs ↗

> 根据PPT 6.2.1-2 中18页处所给的tactics列表中的这一项

$\neg$	$\dfrac{\Gamma, h : A \vdash ? : \mathtt{False}}{\Gamma \vdash ? : \neg A}$	$\mathtt{intro}\ h$

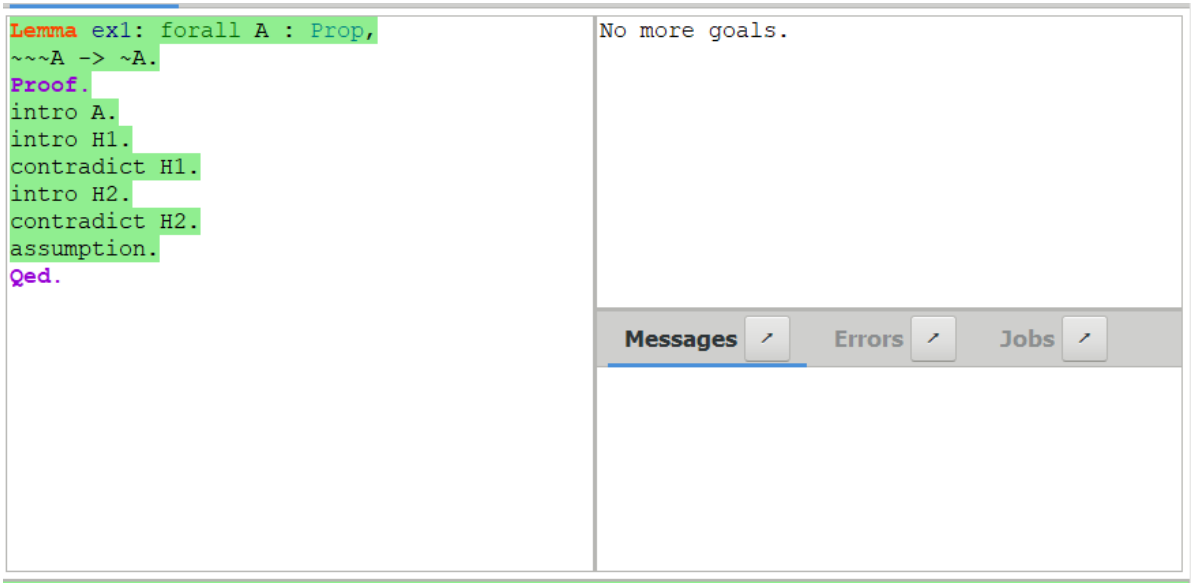
> 此处执行`intro H2`后会将原来的goal去掉一个否定词后作为新的hypothesis, 然后goal变成False.

```
Lemma ex1: forall A : Prop,
~~~A -> ~A.
Proof.
intro A.
intro H1.
contradict H1.
intro H2.
contradict H2.
assumption.
Qed.
```

```
1 goal
A : Prop
H1 : A
H2 : ~ A
_____________________________________(1/1)
False
```

Messages ↗ Errors ↗ Jobs ↗

> 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.



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,
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.
```

```
1 goal
                                                    (1/1)
forall A B : Prop,
A \/ B -> ~ (~ A /\ ~ B)
```

Messages ↗ Errors ↗ Jobs ↗

```
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.
```

```
1 goal
A, B : Prop
                                                    (1/1)
A \/ B -> ~ (~ A /\ ~ B)
```

Messages ↗ Errors ↗ Jobs ↗

```
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.
```

```
1 goal
A, B : Prop
H1 : A \/ B
                                                    (1/1)
~ (~ A /\ ~ B)
```

Messages ↗ Errors ↗ Jobs ↗

```
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.
```

```
1 goal
A, B : Prop
H1 : A \/ B
H2 : ~ A /\ ~ B
_____________________________________(1/1)
False
```

Messages ↗ Errors ↗ Jobs ↗

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,
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.
```

```
2 goals
A, B : Prop
H3 : A
H2 : ~ A /\ ~ B
_____________________________________(1/2)
False
_____________________________________(2/2)
False
```

Messages ↗ Errors ↗ Jobs ↗

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,
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.
```

```
2 goals
A, B : Prop
H3 : A
H5 : ~ A
H6 : ~ B
_____________________________________(1/2)
False
_____________________________________(2/2)
False
```

Messages ↗ Errors ↗ Jobs ↗

在A成立的假设分支中, 对 H5(¬A) 和 goal1(False) 应用`contradict`就能把 goal 变成 A.

而刚好 H3 就是A.

```
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.
```

```
2 goals
A, B : Prop
H3 : A
H6 : ~ B
_____________________________________(1/2)
A
_____________________________________(2/2)
False
```

Messages Errors Jobs

```
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.
```

```
1 goal
A, B : Prop
H4 : B
H2 : ~ A /\ ~ B
_____________________________________(1/1)
False
```

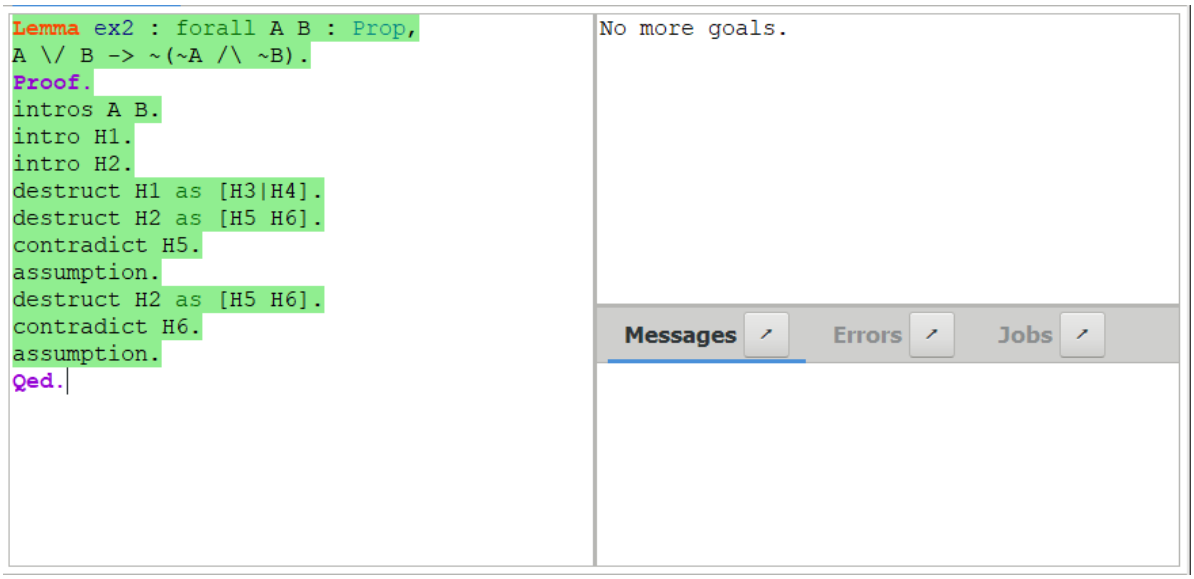
Messages Errors Jobs

下面重复类似的操作来证明第二个分支.

```
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.
```

```
1 goal
A, B : Prop
H4 : B
H5 : ~ A
H6 : ~ B
_____________________________________(1/1)
False
```

Messages Errors Jobs



EX3

Heurisitics

PPT 6.2.1-2 18页的表和以下这张表:

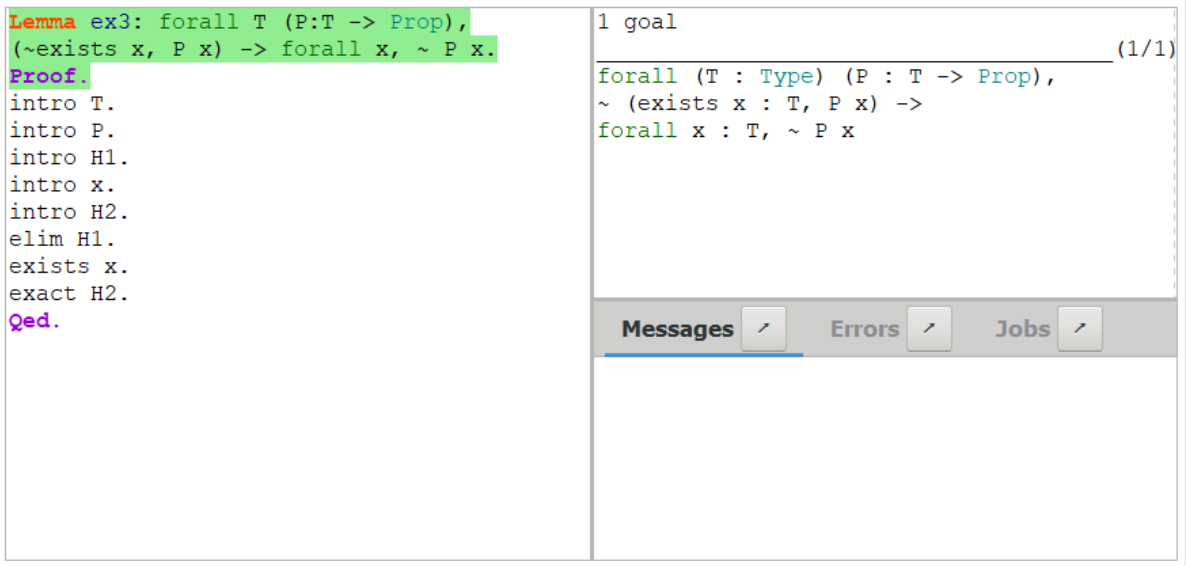
	$\Rightarrow$	$\forall$	$\wedge$
Hypothesis H	apply H	apply H	elim H case H destruct H as [H1 H2]
conclusion	intros H	intros H	split
	$\neg$	$\exists$	$\vee$
Hypothesis H	elim H case H	elim H case H destruct H as [x H1]	elim H case H destruct H as [H1 | H2]
conclusion	intros H	exists v	left or right
	$=$	False	
Hypothesis H	rewrite H rewrite <- H	elim H case H	
conclusion	reflexivity ring		

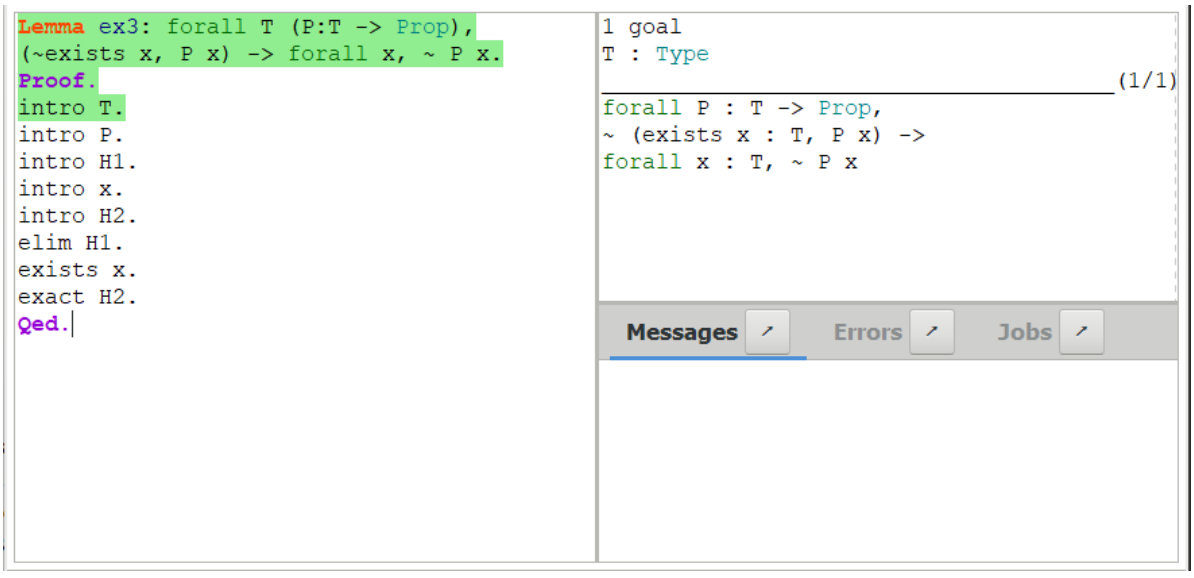
来源: Coq in a Hurry. 这两张表的参考方式是: 例如, 看到某个假设 H 中含有否定词, 则考虑对 H 使用 `elim`; 要证明的 goal 的命题中最前面是exists, 则考虑使用`exists`.

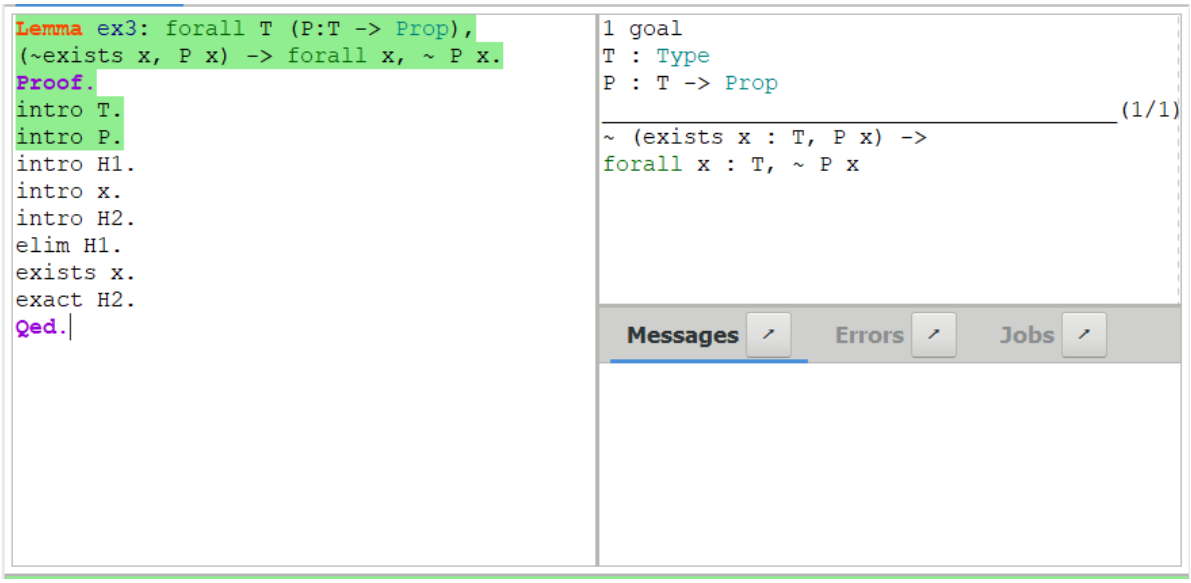
代码

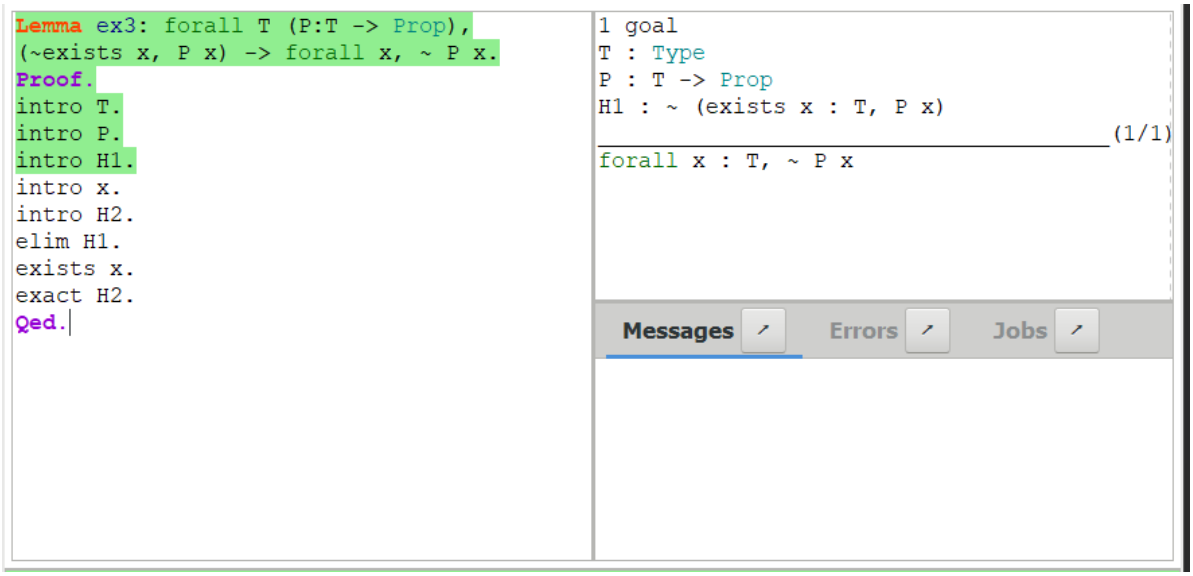
```
Lemma ex3: forall T (P:T -> Prop),
(~exists x, P x) -> forall x, ~ P x.
Proof.
intro T.
intro P.
intro H1.
intro x.
intro H2.
elim H1.
exists x.
exact H2.
Qed.
```

证明过程

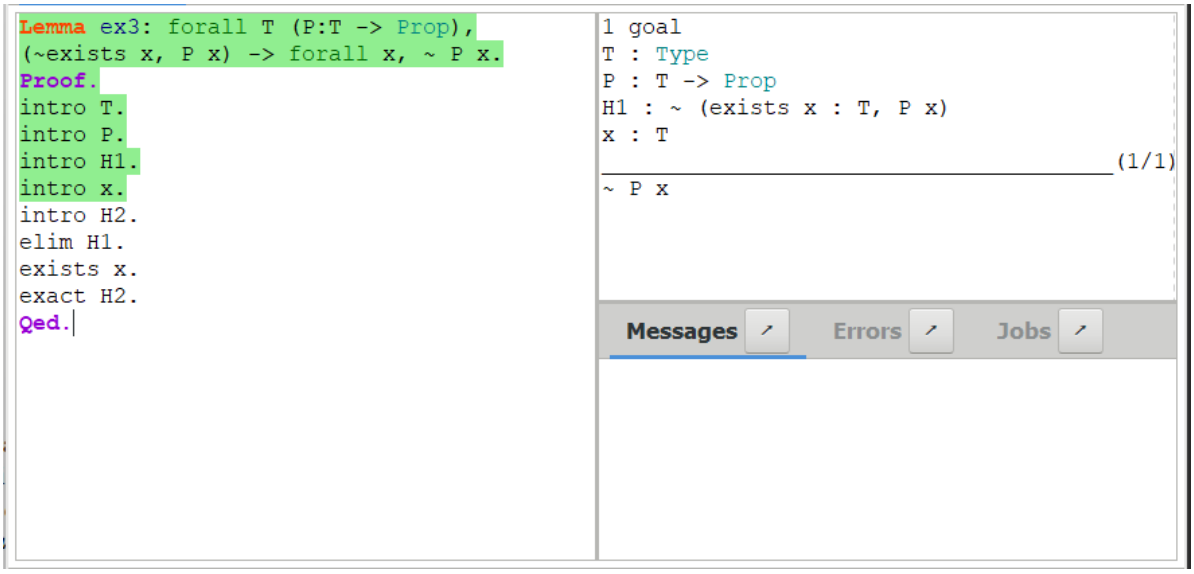


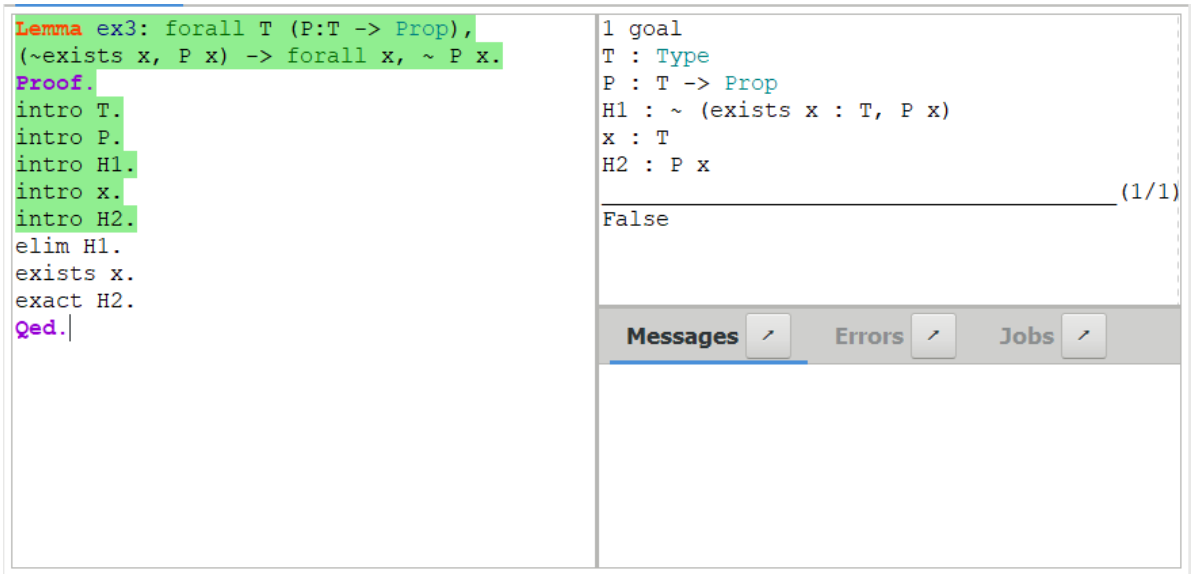




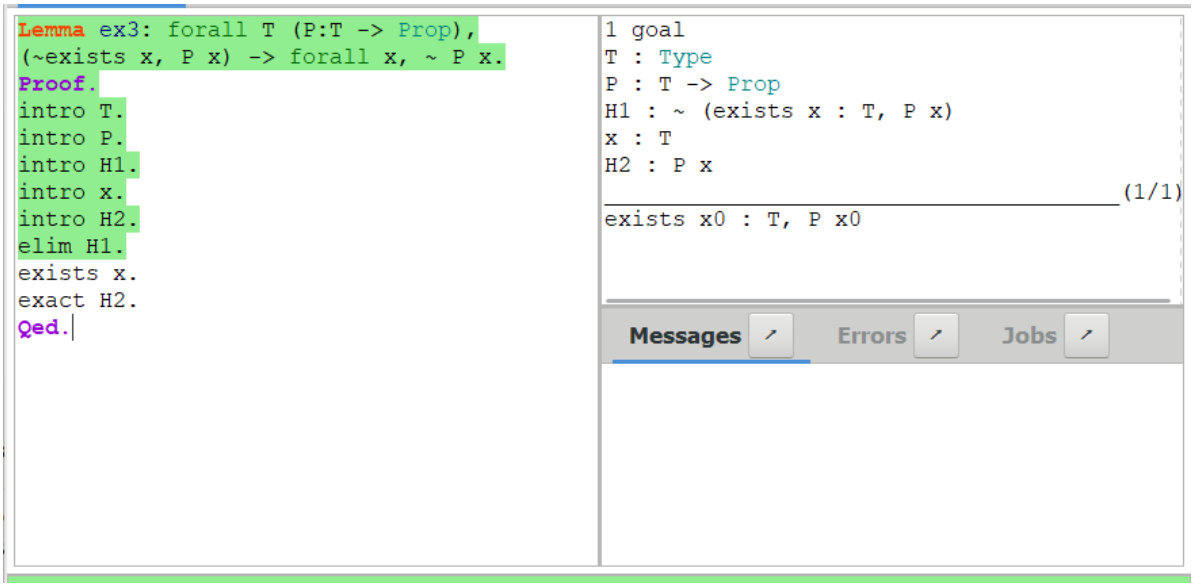


> goal中含forall, 考虑intro.





> 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`.



> 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),
(~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.
```

```
1 goal
T : Type
P : T -> Prop
H1 : ~ (exists x : T, P x)
x : T
H2 : P x
_____________________________________(1/1)
P x
```

Messages ↗ Errors ↗ Jobs ↗

```
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.
```

```
No more goals.
```

Messages ↗ Errors ↗ Jobs ↗