

CS 565

Programming Languages (graduate) Spring 2024

Week 4

Propositions and Inductive Evidence

Propositions

2

A **proposition** is a factual claim.

Have seen a couple of propositions (in Coq) so far:

equalities: $0 + n = n$

implications: $P \rightarrow Q$

universally quantified propositions: for all x , P

A **proof** is some evidence for the truth of a proposition

A **proof system** is a formalization of particular kinds of evidence.

Propositions

3

- ★ We've already seen a number of propositions in Coq:

Theorem ProofExample

Proposition

```
forall n m : nat, n = 0 -> m = 0 -> n + m = 0.
```

Proof.

```
intros n m Hn Hm.  
rewrite Hn. rewrite Hm.  
reflexivity.
```

Qed.

Evidence

★

Propositions

4

```
Check (2 = 2).      (* : Prop *)  
Check (3 = 2).      (* : Prop *)  
Check (3 = 2 -> 2 = 3).  (* : Prop *)  
Check (forall n: nat, n = 2). (* : Prop *)
```

Propositions

5

Propositions are first-class entities in Coq. Can name them:

```
Definition plus_claim : Prop := 2 + 2 = 4.
```

```
Theorem ProofExample : plus_claim.
```

```
Proof.
```

```
... (* unfold plus_claim *)
```

We can also write parameterized propositions
(**predicates**)

```
Definition is_three (n : nat) : Prop := n = 3.
```

```
Theorem ProofExample2 : is_three 3.
```

```
Proof.
```

```
... (* unfold is_three *)
```

Propositions

6

Can have polymorphic predicates:

Definition `injective {A B} (f : A -> B) : Prop :=`

`forall x y : A, f x = f y -> x = y.`

Theorem `plus1_inj : injective (plus 1).`

Proof.

`... (* unfold injective *)`

Equality is a polymorphic binary predicate:

Check `@eq. (* : ∀ A : Type, A → A → Prop *)`

Concept Check

7

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

$\text{pred } (S \ 0) = 0$

Concept Check

8

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

$\forall n:\text{nat}, \text{pred } (\text{S } n) = n$

Concept Check

9

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

$\forall n:\text{nat}, \text{pred } (S n) = n$

Concept Check

10

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

$\forall n:\text{nat}, S(\text{pred } n) = n$

Concept Check

11

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

$\forall n:\text{nat}, S(\text{pred } n)$

Concept Check

12

What is the type of the following expression?

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

```
fun n:nat => S (pred n)
```

Concept Check

13

What is the type of the following expression?

```
fun n:nat => S (pred n) = n
```

- A. Prop
- B. $\text{nat} \rightarrow \text{Prop}$
- C. $\forall n:\text{nat}, \text{Prop}$
- D. $\text{nat} \rightarrow \text{nat}$
- E. Not typeable

Proofs

14

Haven't we already seen a bunch of proofs too?

Theorem ProofExample

: forall n m : nat, n = 0 -> m = 0 -> n + m = 0.

Proof.

```
intros n m Hn Hm.  
rewrite Hn. rewrite Hm.  
reflexivity.
```

proof script

Qed.

formal

What is a \wedge proof?

Judgement

15

A **judgement** is a claim of a proof system

The judgement $\Gamma \vdash A$ is read as:
“assuming the propositions in Γ are true, A is true”.

We’ll see other judgements over the course of the semester:

Inference Rules

16

Proof systems construct evidence of judgements via inference rules:

Axioms

$$\overline{\Gamma \vdash \top}$$

$$\frac{A \in \Gamma}{\Gamma \vdash A}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \text{I} \rightarrow$$

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \text{E} \rightarrow$$

Inference Rules

Example Proof

17

Want a proof of:

$$\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$\begin{array}{c} \frac{A \rightarrow (B \rightarrow C) \in \Gamma}{\Gamma \vdash A \rightarrow (B \rightarrow C)} \quad \frac{A \in \Gamma}{\Gamma \vdash A} \\ \hline \Gamma \vdash B \rightarrow C \\ \hline \Gamma = A \rightarrow (B \rightarrow C), A \rightarrow B, A \vdash C \\ \hline A \rightarrow (B \rightarrow C), A \rightarrow B \vdash A \rightarrow C \\ \hline A \rightarrow (B \rightarrow C) \vdash (A \rightarrow B) \rightarrow (A \rightarrow C) \\ \hline \vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) \end{array}$$

Symbol Pushing

18

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \quad \mathbf{I} \wedge$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \mathbf{E}_L \wedge$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad \mathbf{E}_R \wedge$$

Inference Rules for \wedge

Example

19

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} E \vee$$

Introduction
Rules for Or?

Inference Rules for \vee

Example

20

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad \mathbf{I}_L \vee$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \quad \mathbf{E} \vee$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \quad \mathbf{I}_R \vee$$

Inference Rules for \vee

Example

21

Can you derive:
 $\vdash A \rightarrow B \rightarrow B \wedge A$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \quad \mathbf{I} \wedge$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \quad \mathbf{I} \rightarrow$$

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad \mathbf{E} \rightarrow$$

Proof

22

Haven't we already seen a number of proofs?

Theorem ProofExample

: **forall** n m : nat, n = 0 -> m = 0 -> n + m = 0.

Proof.

```
intros n m Hn Hm.  
rewrite Hn. rewrite Hm.  
reflexivity.
```

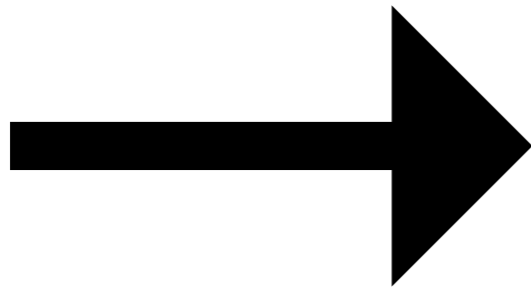
proofscript

What is a **formal** \wedge proof?

A proof tree in the Calculus of co-Inductive Constructions.

Implication

23



Symbol (Math)



Syntax (Coq)

I: intro

E: apply*

tactics (Coq)

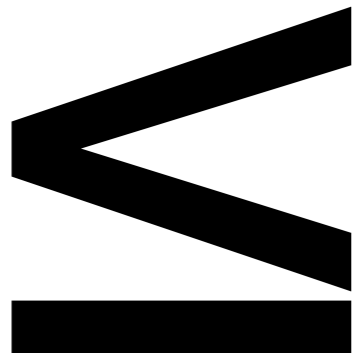
$$\frac{\Gamma, A \vdash B \quad \mathbf{I} \rightarrow}{\Gamma \vdash A \rightarrow B}$$

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A \quad \mathbf{E} \rightarrow}{\Gamma \vdash B}$$

Inference Rules for \rightarrow

Less Than

24



Symbol (Math)

$$n \leq m \equiv \exists k. n+k = m$$

Definition of \leq

$$\frac{}{\Gamma \vdash n \leq n} \text{le}_n$$

$$\frac{\Gamma \vdash n \leq m}{\Gamma \vdash n \leq l + m} \text{les}$$

Inference Rules for \leq

Evenness

25

EvenR

Symbol (Math)

$$\text{EvenR } n \equiv \exists k. n = k + k$$

Definition of EvenR

$$\frac{}{\Gamma \vdash \text{EvenR } 0} \quad \mathbf{ev}_0$$

$$\frac{\Gamma \vdash \text{EvenR } n}{\Gamma \vdash \text{EvenR } (2+n)} \quad \mathbf{ev}_2$$

Inference Rules for EvenR