CS 565

Programming Languages (graduate)
Spring 2024

Week 4
Propositions and Inductive Evidence

Propositions

A **proposition** is a factual claim.

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

equalities: 0 + n = n

implications: P -> Q

universally quantified propositions: forall 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

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

Proposition

```
Theorem ProofExample
  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


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

Propositions

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

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

What is the type of the following expression?

```
pred (S O) = O
```

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

```
∀ n:nat, pred (S n) = n
```

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

```
∀ n:nat, pred (S n) = n
```

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

```
∀ n:nat, S (pred n) = n
```

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

```
∀ n:nat, S (pred n)
```

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

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

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Concept Check

What is the type of the following expression?

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

A. Prop
B. nat→Prop
C. ∀ n:nat, Prop
D. nat→nat
E. Not typeable

Proofs

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.
Qed.
```

proof script

What is a formal proof?

Judgement

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

The judgement $\boxed{\Gamma \vdash A}$ 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

Proof systems construct evidence of judgements via inference rules:

Axioms

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

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

Inference Rules

Example Proof

Want a proof of:

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \rightarrow (B \rightarrow C) \in \Gamma}{\Gamma \vdash A \rightarrow (B \rightarrow C)} \quad \dfrac{A \in \Gamma}{\Gamma \vdash A}}{\Gamma \vdash B \rightarrow C} \qquad \dfrac{\dfrac{A \rightarrow B \in \Gamma}{\Gamma \vdash A \rightarrow B} \quad \dfrac{A \in \Gamma}{\Gamma \vdash A}}{\Gamma \vdash B}}{\Gamma = A \rightarrow (B \rightarrow C), A \rightarrow B, A \vdash C}}{A \rightarrow (B \rightarrow C), A \rightarrow B \vdash A \rightarrow C}}{A \rightarrow (B \rightarrow C) \vdash (A \rightarrow B) \rightarrow (A \rightarrow C)}}{\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))}$$

Symbol Pushing

$\mathbf{E_L} \wedge$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$$

$\mathbf{I} \wedge$

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

$\mathbf{E_R} \wedge$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

Inference Rules for $\wedge$

Example

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

Introduction Rules for Or?

Inference Rules for $\vee$

Example

$\mathbf{I_L} \vee$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$$

$\mathbf{E} \vee$

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

$\mathbf{I_R} \vee$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

Inference Rules for $\vee$

Example

Can you derive:

$\vdash A \rightarrow B \rightarrow B \wedge A$

I $\wedge$

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

I $\rightarrow$

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

E $\rightarrow$

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

Proof

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 proof?

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

Implication

$$\rightarrow$$

Symbol (Math)

->

Syntax (Coq)

I: intro
E: apply*

tactics (Coq)

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

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

Inference Rules for $\rightarrow$

Less Than

$\leq$

Symbol (Math)

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

Definition of ≤

$$\frac{}{\Gamma \vdash n \leq n}\ \textbf{le}_{\textbf{n}}$$

$$\frac{\Gamma \vdash n \leq m}{\Gamma \vdash n \leq 1 + m}\ \textbf{le}_{\textbf{s}}$$

Inference Rules for ≤

Eveness

EvenR

Symbol (Math)

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

Definition of EvenR

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

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

Inference Rules for EvenR