

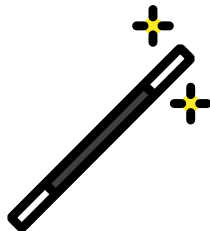
Formalizing and Proving Theorems in Coq — Lecture 2

Tobias Kappé

Today's lecture

You will learn how to...

- ▶ Define inductive datatypes.
- ▶ Define recursive functions.
- ▶ Reason about recursive functions.
- ▶ Define inductive propositions.
- ▶ Reason about inductive propositions.



Peano arithmetic

Peano's definition of natural numbers:

- ▶ 0 is a natural number
- ▶ If n is a natural number, then $S(n)$ is a natural number.

$$\overline{0 \in \mathbb{N}}$$

$$\frac{n \in \mathbb{N}}{S(n) \in \mathbb{N}}$$

Let's see how this works in Coq.

Peano arithmetic: addition

Addition can be defined recursively:

$$n + m = \begin{cases} n & m = 0 \\ S(n + m') & m = S(m') \end{cases}$$

Which properties of addition can we verify?

Peano arithmetic: multiplication

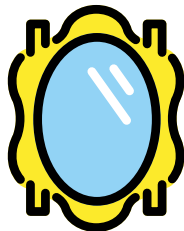
How would you define multiplication?

$$n \cdot m = \begin{cases} 0 & m = 0 \\ (n \cdot m') + n & m = S(m') \end{cases}$$

Which properties can we verify?

Peano arithmetic: brief reflection

- ▶ New tactic: `induction`.
- ▶ Also saw `f_equals` along the way.
- ▶ We developed concepts *from scratch*.
- ▶ Coq provides `Coq.Init.Nat`.



Sum of odd numbers

Lemma

The sum of the first n odd numbers is equal to n^2 .

How would you formalize this in Coq?

$$f(n) = \begin{cases} 0 & n = 0 \\ S(f(n') + 2 \cdot n') & n = S(n') \end{cases}$$

Sum of odd numbers: proof

Lemma

$$f(n) = n \cdot n$$

Proof.

By induction on n . In the base, $f(0) = 0 = 0 \cdot 0$. For the inductive step:

$$\begin{aligned} f(S(n)) &= S(f(n) + 2 \cdot n) && \text{(def. } f) \\ &= S(n \cdot n + 2 \cdot n) && \text{(IH)} \\ &= S(n \cdot n + n + n) && \text{(def. multiplication)} \\ &= S(n \cdot S(n) + n) && \text{(def. multiplication)} \\ &= S(S(n) \cdot n + n) && \text{(commutativity)} \\ &= S(n) \cdot n + S(n) && \text{(def. addition)} \\ &= S(n) \cdot S(n) && \text{(def. multiplication)} \quad \square \end{aligned}$$

Sum of odd numbers: reflection

- ▶ Think before you start.
- ▶ Mind the gap.
- ▶ Auxiliary lemmas are good.



Fibonacci numbers

The Fibonacci sequence is defined as follows:

$$F_0 = 0$$

$$F_1 = 1$$

$$F_{n+2} = F_n + F_{n+1}$$

Let's try and encode this in Coq.

Fibonacci numbers: a claim

Lemma (Honsberger's identity)

$$F_{n+m+1} = F_{n+1} \cdot F_{m+1} + F_n \cdot F_m$$

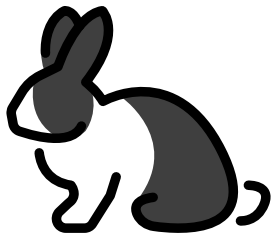
Proof.

By induction on m . The base is easy; for the inductive step:

$$\begin{aligned} F_{n+m+2} &= F_{(n+1)+m+1} && \text{(Shift 1 to the left)} \\ &= F_{n+2} \cdot F_{m+1} + F_{n+1} \cdot F_m && \text{(IH)} \\ &= (F_n + F_{n+1}) \cdot F_{m+1} + F_{n+1} \cdot F_m && \text{(def. } F) \\ &= F_n \cdot F_{m+1} + F_{n+1} \cdot F_{m+1} + F_{n+1} \cdot F_m && \text{(distributivity)} \\ &= F_n \cdot F_{m+1} + F_{n+1} \cdot (F_{m+1} + F_m) && \text{(distributivity)} \\ &= F_n \cdot F_{m+1} + F_{n+1} \cdot F_{m+2} && \text{(def. } F) \\ &= F_{n+1} \cdot F_{m+2} + F_n \cdot F_{m+1} && \text{(commutativity) } \square \end{aligned}$$

Fibonacci numbers: reflection

- ▶ High-level reasoning helps a lot.
- ▶ Be careful about your induction hypothesis.



Inductive predicates

How would you define $\leq$ on Peano numbers?

$$\frac{}{n \leq n}$$

$$\frac{n \leq m}{n \leq S(m)}$$

Inductive predicates: proving properties

Which properties could we prove?

Lemma

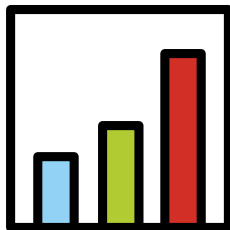
The relation $\leq$ is transitive.

Lemma

If $n \leq 0$, then $n = 0$.

Inductive predicates: reflection

- ▶ You can prove by induction.
- ▶ You can prove by case distinction.
- ▶ Sometimes Coq does some work for you.



Lucas numbers

The Lucas numbers are defined as follows:

$$L_0 = 2$$

$$L_1 = 1$$

$$L_{n+2} = L_n + L_{n+1}$$

Lucas numbers: properties

Lemma

$$L_{n+1} = F_n + F_{n+2}$$

Proof.

For $n = 0$, the claim holds; for the inductive step:

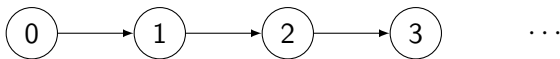
$$\begin{aligned} L_{n+2} &= L_n + L_{n+1} \\ &= F_{n-1} + F_{n+1} + F_n + F_{n+2} \\ &= F_{n-1} + F_n + F_{n+1} + F_{n+2} \\ &= F_{n+1} + F_{n+3} \end{aligned}$$



Detour: Induction flavors

Lemma (Induction)

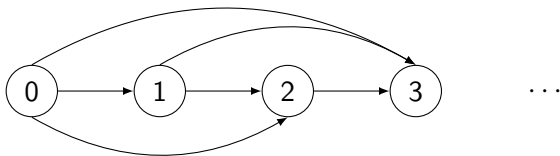
Let P be a predicate that holds for 0. Suppose furthermore that, if P holds for n , then P also holds for $n + 1$. Then P holds for all n .



Detour: Induction flavors

Lemma (Strong induction)

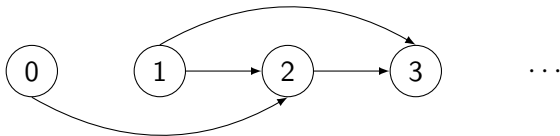
Let P be a predicate that holds for 0. Suppose furthermore that, given that P holds for all m below n , it follows that P holds for n . Then P holds for all n .



Detour: Induction flavors

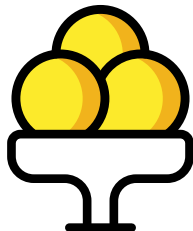
Lemma (Pair induction)

Let P be a predicate that holds for 0 and 1. Suppose furthermore that, if P holds for n and $n + 1$, then P also holds for $n + 2$. Then P holds for all n .



Lucas numbers: reflection

- ▶ There are different induction principles.
- ▶ You need a principle that works for you.
- ▶ Coq lets you add custom principles.



Next lecture

- ▶ Tactical proof combinators.
- ▶ Some nifty proof automation.
- ▶ Reasoning with existentials.

Homework:

- ▶ Complete the missing proofs in `lecture-2.v`.