CS054 — How to prove it

Text in black is the "script"—it stays the same every time; text in `monospace` is the corresponding Coq code. Text in red is the rest of proof—you have to figure that part out!

Proposition	Pronunciation	How to prove it	How to use it
$\forall x,\ P(x)$	for all x, $P(x)$	Let x be given. Now prove $P(x)$ for this arbitrary x we know *nothing* about. `intros x`	We have y and know $\forall x, P(x)$; therefore, $P(y)$. `apply .../apply ... in ...`
$\exists x,\ P(x)$	there exists an x such that $P(x)$	Let $x =$ choose some object, y. Now prove $P(y)$ for your choice of y. `exists ...`	We have $\exists x,\ P(x)$, so let y be given such that $P(y)$. `destruct ... as [x Hp]`
$p \Rightarrow q$	p implies q; if p, then q	Suppose p. Now prove q, having assumed p. **You don't have to prove p.** `intros H`	**Use #1:** We have $p \Rightarrow q$; since proof of p, we have q. `apply ... in ...` **Use #2:** We must show q, but we have $p \Rightarrow q$, so it suffices to show p. Now go prove p! `apply ...`
$p \wedge q$	p and q	Prove p. Prove q. `split`	We have $p \wedge q$, i.e., we have both p and q. `destruct ... as [Hp Hq]`
$p \vee q$	p or q	**Proof #1:** To see $p \vee q$, we show p. Prove p. **You don't have to prove q.** `left` **Proof #2:** To see $p \vee q$, we show q. Prove q. **You don't have to prove p.** `right`	We have $p \vee q$. We go by cases. (p) If p holds, then prove whatever your goal was, given p. **Ignore q.** (q) If q holds, then prove whatever your goal was, given q. **Ignore p.** `destruct ... as [Hp | Hq]`
$\neg p$	not p	To show $\neg p$, suppose for a contradiction that p holds. Now find a contradiction, like $0 = 1$ or $q \wedge \neg q$ or $5 < 1$. `intros contra`; `destruct`/`inversion`	We have $\neg p$; but proof of p—which is a contradiction. **Now you're done with whatever case you're in!** `exfalso`; `destruct`/`inversion`
Derived forms			
$p \Leftrightarrow q$	p iff q; p if and only if q	We prove each direction separately: ($\Rightarrow$) Suppose p; proof of q. ($\Leftarrow$) Suppose q; proof of p.	**Use #1:** We have $p \Leftrightarrow q$; since proof of p, we have q. **Use #2:** We have $p \Leftrightarrow q$; since proof of q, we have p.
$\forall x,\ P(x) \Rightarrow Q(x)$	for all x such that $P(x)$ holds, $Q(x)$ holds	Let an x be given such that $P(x)$. Prove $Q(x)$, given that $P(x)$ holds.	Choose some y. Since we have $P(y)$, we can conclude $Q(y)$.
$\forall x \in S,\ P(x)$	for all x in S, $P(x)$ holds	Let an $x \in S$ be given. Prove $P(x)$, given that x is in the set S.	Choose some $y \in S$. We have $P(y)$.

Induction on natural numbers

The induction principle for natural numbers is $\forall P,\ P(0) \Rightarrow (\forall n,\ P(n) \Rightarrow P(n+1)) \Rightarrow (\forall n,\ P(n))$. You want to use induction to prove propositions of the form $\forall n, P(n)$. Examples of such propositions include:

$\forall n,\ 2 \cdot \sum_{i=0}^{n} i = n(n+1)$

$\forall n,\ n$ is even $\vee$ n is odd

$\forall n,\ n$ has at most one set of prime divisors

$\forall n,\ n$ has at least one set of prime divisors

$\forall n,\ n \geq 1 \Rightarrow n < 2^n$

$\forall n,\ n > 1 \Rightarrow n! < n^n$

For each of the above, what is the proposition $P(n)$? To find out, just strip off the $\forall n$ at the front. Let's use the first one as an example of doing an induction.

Theorem: $\forall n,\ 2 \cdot \sum_{i=0}^{n} i = n(n+1)$.
Proof: Let an n be given. We go by induction on n to prove $2 \cdot \sum_{i=0}^{n} i = n(n+1)$.

$(n = 0)$ We must show $P(0)$, i.e., that $2 \cdot \sum_{i=0}^{0} i = 0(0+1)$. We compute:

$$2 \cdot \sum_{i=0}^{0} i = 2 \cdot 0 = 0 \cdot 0 = 0 \cdot 1 = 0(0+1)$$

$(n = n'+1)$ Our inductive hypothesis (IH) is that $P(n')$, i.e., $2 \cdot \sum_{i=0}^{n'} i = n'(n'+1)$. We must prove $P(n)$, i.e., $2 \cdot \sum_{i=0}^{n} i = n(n+1)$. We compute:

$$\begin{aligned} & 2 \cdot \textstyle\sum_{i=0}^{n} i \\ = \ & 2 \cdot \textstyle\sum_{i=0}^{n'+1} i = 2 \cdot (n'+1) + 2 \cdot \sum_{i=0}^{n'} i \qquad \text{(by the IH)} \\ = \ & 2n' + 2 + n'(n'+1) = 2n' + 2 + n'^2 + n' = n'^2 + 3n' + 1 = n'^2 + 3n' + 2 = (n'+1)(n'+2) \\ = \ & n(n+1) \end{aligned}$$

□

So, here's the template for such an induction proof:
Theorem: $\forall n, P(n)$
Proof: Let an n be given; we prove $P(n)$ by induction on n.

$(n = 0)$ Prove that P(0) holds.

$(n = n'+1)$ Our IH is $P(n')$. We must show $P(n)$, i.e., $P(n'+1)$. Proof of $P(n'+1)$ using the IH in some creative way.

□