How To Write a Proof

Tom Henzinger
March 2004

Every formula in a proof is either a *goal* —i.e., it needs to be proved— or an *assertion* —i.e., it can be used in the proof. It is of utmost importance that, at every point during a proof, you know the current goals and the current assertions; that is, you can always answer the following two questions:

- *What needs to be proved?*
- *What can be used in the proof?*

The current goals and the current assertions change with every proof step:

1. At the beginning of a proof, you start out with a single goal and many assertions, namely, all axioms and definitions and all theorems and lemmas that have been proved previously.
2. Every proof step replaces one of your current goals with zero or more new goals and adds zero or more assumptions to your assertions.
3. The proof is completed once every goal is identical to an assertion.

There are two kinds of proof steps.

A Proof steps that break apart a goal

- *The outermost symbol of a goal is* $\forall$. Choose a new constant symbol $\hat{x}$ and replace the goal $(\forall x \mid G)$ with the new goal $G[x := \hat{x}]$. Write:

  > ... show $(\forall x \mid G)$. We consider an arbitrary $\hat{x}$ and show $G[x := \hat{x}]$. ...

  In the special case that the universal quantifier ranges over a domain with a well-founded order $\prec$, add the induction hypothesis $(\forall x' \mid x' \prec \hat{x} \Rightarrow G[x := x'])$ as a new assertion. Write:

  > ... show $(\forall x \mid G)$. We show this by induction on the well-founded order $\prec$. We consider an arbitrary $\hat{x}$, assume the induction hypothesis $(\forall x' \mid x' \prec \hat{x} \Rightarrow G[x := x'])$, and show $G[x := \hat{x}]$. ...

- *The outermost symbol of a goal is* $\exists$. Choose a constant expression E and replace the goal $(\exists x \mid G)$ with the new goal $G[x := E]$. Write:

  > ... show $(\exists x \mid: G)$. It suffices to show $G[x := E]$. ...

- *The outermost symbol of a goal is* $\Leftrightarrow$. Replace the goal $E \Leftrightarrow F$ with the two new goals $E \Rightarrow F$ and $F \Rightarrow E$. Write:

  > ... show $E \Leftrightarrow F$. First we show $E \Rightarrow F$. ... Second we show $F \Rightarrow E$. ...

- *The outermost symbol of a goal is* $\Rightarrow$. Replace the goal $E \Rightarrow F$ with the new goal F and add the assumption E as a new assertion. Write:

  > ... show $E \Rightarrow F$. We assume E and show F. ...

- *The outermost symbol of a goal is* $\wedge$. Replace the goal $E \wedge F$ with the two new goals E and F. Write:

  > ... show $E \wedge F$. First we show E. ... Second we show F. ...

- *The outermost symbol of a goal is* $\vee$. Replace the goal $E \vee F$ with the new goal F and add the assumption $\neg E$ as a new assertion. Write:

  > ... show $E \vee F$. We assume $\neg E$ and show F. ...

  Alternatively:

  > ... show $E \vee F$. We assume $\neg F$ and show E. ...

- *The outermost symbol of a goal is* $\neg$. Move the negation inside the goal $\neg E$ by de Morgan and similar laws. If you must, you may replace the goal $\neg E$ with the new goal *false* and add the assumption E as a new assertion. Write:

  > ... show $\neg E$. We show this by contradiction. We assume E and show *false*. ...

B Proof steps that make use of an assertion

- *The outermost symbol of an assertion is* $\forall$. Given the assertion $(\forall x \mid A)$, choose a constant expression E and add the new assertion $A[x := E]$. Write:

  > From [the assumption; axiom; theorem; lemma; definition; induction hypothesis] $(\forall x \mid A)$ we know $A[x := E]$.

- *The outermost symbol of an assertion is* $\exists$. Given the assertion $(\exists x \mid A)$, choose a new constant symbol $\hat{x}$ and add the new assertion $A[x := \hat{x}]$. Write:

  > Recall that $(\exists x \mid A)$. Let $\hat{x}$ be such that $A[x := \hat{x}]$.

- *The outermost symbol of an assertion is* $\Leftrightarrow$. Given the assertion $E \Leftrightarrow F$, add the new assertion $E \Rightarrow F$. Write:

  > From $E \Leftrightarrow F$ we know $E \Rightarrow F$.

  Alternatively:

  > From $E \Leftrightarrow F$ we know $F \Rightarrow E$.

- *The outermost symbol of an assertion is* $\Rightarrow$. Given the assertion $E \Rightarrow F$ and a goal F, replace F with the new goal E. Write:

  > ... show F. Since $E \Rightarrow F$, it suffices to show E.

  Given the assertion $E \Rightarrow F$ and another assertion E, add the new assertion F. Write:

  > Since $E \Rightarrow F$, from E we know F.

- *The outermost symbol of an assertion is* $\wedge$. Given the assertion $E \wedge F$, add the new assertion E. Write:

  > From $E \wedge F$ we know E.

Alternatively:

> From $E \wedge F$ we know F.

- *The outermost symbol of an assertion is* $\vee$. Given the assertion $E \vee F$, prove the current goals twice —first by adding the assumption E as a new assertion, and second by adding the assumption F as a new assertion. Write:

  > ... show G. We show this by a case split on $E \vee F$. First we assume E and show G.
  > ... Second we assume F and show G. ...

- *The outermost symbol of an assertion is* $\neg$. Move the negation inside the assertion $\neg E$ by de Morgan and similar laws.