Problem Solving in Computer Science · Summer 2007 Tom Henzinger

6 How to write a proof (continued)

Scribe: Vaibhav Rajan March 30, 2007

The following table summarizes the rules that can be used to build up a proof. The rules in the second column are applied for proof steps that break apart a goal and those in the third column for steps that make use of an assertion. The choice of rule depends on the outermost symbol of the assertion or the goal involved.

Outermost Symbol	of goal	of assertion
$\forall$	To show: $(\forall x)A(x)$. Consider an arbitrary $\hat{x}$. Show: $A(\hat{x})$.	We know $(\forall x)A(x)$. We thus know $A(e)$ for some constant e.
$\exists$	To show: $(\exists x)A(x)$. Show $A(e)$ for some constant e.	We know $(\exists x)A(x)$. Let $\hat{x}$ be such that $A(\hat{x})$.
$\Leftrightarrow$	To show: $A \Leftrightarrow B$. Show: $A \Rightarrow B$, and show: $B \Rightarrow A$.	We know $A \Leftrightarrow B$. We thus know: $A \Rightarrow B$, and symmetrically, we know $B \Rightarrow A$.
$\Rightarrow$	To show: $A \Rightarrow B$. Assume A, and show B.	We know $A \Rightarrow B$. If we know A then we know B. Thus, to show B, it suffices to show A.
$\wedge$	To show: $A \wedge B$. (1) Show A, and (2) show B.	We know $A \wedge B$. We thus know A, and we know B.
$\vee$	To show: $A \vee B$. Assume $\neg A$ and show B. Or, assume $\neg B$ and show A.	We know $A \vee B$. To show C, (1) assume A, show C, and (2) assume B, show C.

Negation: If $\neg$ is the outermost symbol, it can be pushed inside goals or assertions.

As seen from the table, once the outermost symbol is recognized, all the proof steps can be automated except when the goal is to show $(\exists x)A(x)$. Finding the constant e requires creativity and often, some domain knowledge.

The following example shows the application of the above rules in a proof.

Definition (D1). A function $f : \mathbb{N} \to \mathbb{N}$ is *bounded* if there exists a bound $b \in \mathbb{N}$ such that $f(n) \leq b$ for all $n \in \mathbb{N}$.

Definition (D2). Given two functions $f, g : \mathbb{N} \to \mathbb{N}$, the sum $f + g$ is a function from $\mathbb{N}$ to $\mathbb{N}$ such that $(f + g)(n) = f(n) + g(n)$ for all $n \in \mathbb{N}$.

Theorem. For all functions $f, g : \mathbb{N} \to \mathbb{N}$, if f and g are bounded, then $f + g$ is bounded.

Proof. At each step, we identify the outermost symbol and apply the corresponding rule from the table.

(Outermost symbol: $\forall$) Consider arbitrary functions: $\hat{f}, \hat{g} : \mathbb{N} \to \mathbb{N}$. To show: If $\hat{f}$ and $\hat{g}$ are bounded, then $\hat{f} + \hat{g}$ is bounded.

(Outermost symbol: $\Rightarrow$) Assume:

(A1) $\hat{f}$ and $\hat{g}$ are bounded.

To show: $\hat{f} + \hat{g}$ is bounded.

The definition of "bounded" can now be plugged into the current goal. Note that the current assertions are (D1), (D2), and (A1).

By (D1), we know that $\hat{f} + \hat{g}$ is bounded iff there exists $b \in \mathbb{N}$ such that $(\hat{f} + \hat{g})(n) \leq b$ for all $n \in \mathbb{N}$. Using only one direction of the double implication, we know that $\hat{f} + \hat{g}$ is bounded, if there exists $b \in \mathbb{N}$ such that $(\hat{f} + \hat{g})(n) \leq b$ for all $n \in \mathbb{N}$. Thus, it suffices to show:

(G1) There exists $b \in \mathbb{N}$ such that $(\hat{f} + \hat{g})(n) \leq b$ for all $n \in \mathbb{N}$.

By (A1), we know:

(A2) The function $\hat{f}$ is bounded.

By (D1), we know that $\hat{f}$ is bounded iff there exists $b \in \mathbb{N}$ such that $\hat{f}(n) \leq b$ for all $n \in \mathbb{N}$. Thus we know that,

(A3) If $\hat{f}$ is bounded, there exists $b \in \mathbb{N}$ such that $\hat{f}(n) \leq b$ for all $n \in \mathbb{N}$.

¿From (A2) and (A3), we know:

(A4) There exists $b \in \mathbb{N}$ such that $\hat{f}(n) \leq b$ for all $n \in \mathbb{N}$.

Let $\hat{b}_f$ be such that $\hat{f}(n) \leq \hat{b}_f$ for all $n \in \mathbb{N}$.

By (A1), we know that $\hat{g}$ is bounded. By arguments similar to those for $\hat{f}$, we know:

(A5) There exists $b \in \mathbb{N}$ such that $\hat{g}(n) \leq b$ for all $n \in \mathbb{N}$.

Let $\hat{b}_g$ be such that, $\hat{g}(n) \leq \hat{b}_g$ for all $n \in \mathbb{N}$.

Thus, to show (G1), it suffices to show:

(G2) For all $n \in \mathbb{N}$, $(\hat{f} + \hat{g})(n) \leq \hat{b}_f + \hat{b}_g$.

(Outermost symbol: $\forall$) Consider an arbitrary $\hat{n}$. Show: $(\hat{f} + \hat{g})(\hat{n}) \leq \hat{b}_f + \hat{b}_g$.

By (D2), we know that for all $n \in \mathbb{N}$, $(\hat{f} + \hat{g})(n) = \hat{f}(n) + \hat{g}(n)$. Thus, $(\hat{f} + \hat{g})(\hat{n}) = \hat{f}(\hat{n}) + \hat{g}(\hat{n})$. Using this in (G2), it suffices to show that: $\hat{f}(\hat{n}) + \hat{g}(\hat{n}) \leq \hat{b}_f + \hat{b}_g$.

Now, we need to use the assertion

(A6) $(\forall x, y, \hat{x}, \hat{y})\ \big((x \leq \hat{x}) \wedge (y \leq \hat{y})\big) \Rightarrow \big((x + y) \leq (\hat{x} + \hat{y})\big)$.

By (A4), $\hat{f}(\hat{n}) \leq \hat{b}_f$. By (A5), $\hat{g}(\hat{n}) \leq \hat{b}_g$. By (A6),

$$(\hat{f}(\hat{n}) \leq \hat{b}_f \wedge \hat{g}(\hat{n}) \leq \hat{b}_g) \Rightarrow (\hat{f}(\hat{n}) + \hat{g}(\hat{n}) \leq \hat{b}_f + \hat{b}_g).$$

(Q.E.D.)

This proof shows how the rules stated in the table can be applied mechanically (except for elimination of the existential quantifier) to prove a statement from previously known assertions. In practice, however, proofs are not written in such a detailed manner. For example, the proof for the theorem above can be written simply as follows:

> Let $\hat{b}_f$ be a bound for f. Let $\hat{b}_g$ be a bound for g. Then, $\hat{b}_f + \hat{b}_g$ is a bound for $f + g$. (Q.E.D.)

The rules given in the table suffice for writing most of the proofs that we come across in Computer Science. Proofs by contradiction is usually not needed. They can be rewritten using the rules stated above.

Proofs by induction

Most often one has to prove a statement of the form $(\forall x)A(x)$. Proofs by induction are common in Computer Science. They are based on the principle of well-founded induction which can be inferred using the rules stated above.

A binary relation, $\prec$ is *well-founded*, if there exists no infinite decreasing chain $x_0 \succ x_1 \succ x_2 \succ x_3 \succ \ldots$

Examples:

(i) the natural ordering $<$ is well founded on $\mathbb{N}$ but not on $\mathbb{Z}$;

(ii) on finite binary trees, the following relations $<$ are well-founded:

- proper subtree: $t_1 < t_2$ if t_1 is a proper subtree of t_2;
- fewer nodes: $t_1 < t_2$ if t_1 has fewer nodes than t_2;
- lesser height: $t_1 < t_2$ if t_1 is of lesser height than t_2.

If $\prec$ is well founded, then the following is valid:

$$(\forall x)\big(((\forall y)(y \prec x \Rightarrow A(y))) \Rightarrow A(x)\big) \Rightarrow (\forall x)A(x).$$

Since $\prec$ is well founded, it suffices to show:

$$(\forall x)\big(((\forall y)(y \prec x \Rightarrow A(y)) \Rightarrow A(x)) \Rightarrow A(x)\big).$$

Since the outermost symbol is $\forall$, consider an arbitrary $\hat{x}$ and show:

$$(\forall y)(y < \hat{x} \Rightarrow A(y)) \Rightarrow A(\hat{x}).$$

Since the outermost symbol is $\Rightarrow$, assume: $(\forall y)(y < \hat{x} \Rightarrow A(y))$. Show: $A(\hat{x})$.

The assumption here is the induction hypothesis. The effect of the basis step in induction can be illustrated with an example. Consider $x, y \in \mathbb{N}$. If $\hat{x} = 0$, then the induction hypothesis does not help because there is no $y < x$. So, we prove $A(0)$ first. Then, we assume the induction hypothesis and prove $A(\hat{x})$ for an arbitrary $\hat{x} > 0$.

Homework

Consider the relation $x \prec y$ meaning that x is a parent of y. Assume that $\prec$ is well-founded. The following axioms characterize the properties *ancestor*, *human*, *monkey*.

(A1) $(\forall x, y)\big(\mathrm{anc}(x, y) \Leftrightarrow (x \prec y \vee (\exists z)(\mathrm{anc}(x, z) \wedge z \prec y))\big)$;
(A2) $(\forall x)\neg(\mathrm{human}(x) \Leftrightarrow \mathrm{monkey}(x))$.

Prove the following theorem:

If there is a human with an ancestor that is a monkey, then there is a human with a parent that is a monkey.