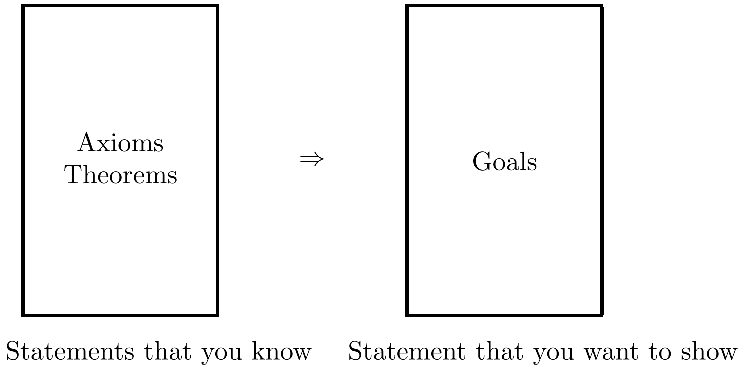
Problem Solving in Computer Science: Scribe Notes

October 29, 2008

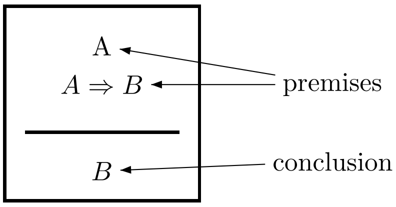
Writing a Proof

There are many different levels of detail you can write a proof at. You can switch between these, i.e. go up and down.

In a *proof* you have certain axioms and theorems you assume to be true.



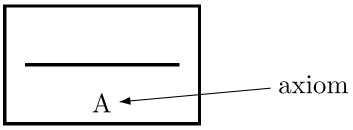
Expressing these facts in logical terms gives the finest granularity. To reason about these we use *proof rules*. One example of such a rule is *modus ponens*: “if you know A and you know that $A \Rightarrow B$, the you can conclude B”.



A proof is a sequence of statements:

$$\left.\begin{array}{l}A_0\\A_1\\\cdot\\\vdots\\A_n\end{array}\right\}\text{Proof of }A_n$$

Each A_i is the conclusion of a rule whose premises occur earlier in the sequence. The axioms and the theorems are the first in this sequence.



On lowest technical level one has to agree on what it is accepted, in terms of axioms and theorems, and the proof rules that can be used. One can build a software application that takes as input these sets of axioms and proof rules and the proof can check whether the proof is correct or not.

Normally, you do not want to write a proof like this, but you should be aware of it. The art is to write a proof detailed enough to convince yourself the proof is correct. If you are not sure about an argument, write it to a lower level.

Natural Deduction

In case of *modus ponens*, if you want to show B and you know $A \Rightarrow B$ then you have to prove A. This is a *goal oriented*, *top-down* approach.

There are two types of *proof rules*:

- break apart goals. In order to show G it suffices to show G', which is simpler.
- use assertions. Since we know A we also know A'.

The choice of the rule is directed by the syntax of A and G. It is completely determined.

Suppose we know the *universal assertion* $(\forall x\, A(x))$. Since we know that $A(x)$ holds for all x, we know that $A(e)$ holds, where e is any expression.

If we have an *universal goal*, we want to show $(\forall x\, G(x))$. To show this

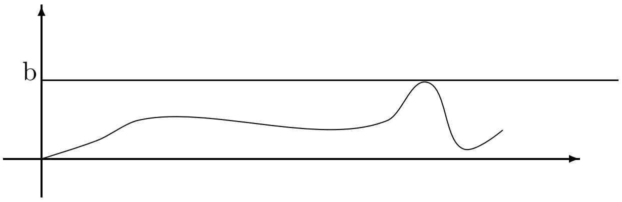
- choose an arbitrary fixed constant $\hat{x}$. You assume you do not know anything about $\hat{x}$.
- You show that $G(\hat{x})$ holds.

Suppose we know $(\exists x\, A(x))$. To use this knowledge you have to give x a name, create a new constant, e.g. let $\hat{x}$ be such that $A(\hat{x})$.

If you want to show $(\exists x\, G(x))$ then you have to construct e for which $G(e)$ is true. The expression e represents the creative step in a proof.

Example

Definition 1 *A function f: $\mathbb{N} \to \mathbb{N}$ is* bounded *if there exists a bound $b \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $f(n) \leq b$.*



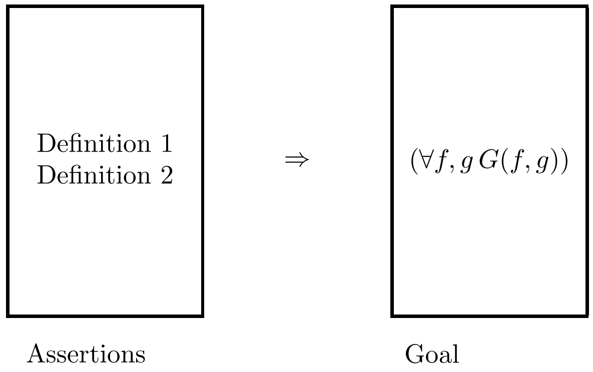
Theorem 1 *For all function f, g: $\mathbb{N} \to \mathbb{N}$ if f and g are bounded then $f + g$ is also bounded.*

Definition 2 *For all f, g: $\mathbb{N} \to \mathbb{N}$, f+g: $\mathbb{N} \to \mathbb{N}$ is the function such that for all $n \in \mathbb{N}$*

$$(f + g)(n) = f(n) + g(n).$$

Theorem 2 *For all $a, b, c, d \in \mathbb{N}$ if $a \leq b$ and $c \leq d$ then $a + c \leq b + d$.*

We want to prove Theorem 1. In order to do this, we start with the outermost operation. We replace Theorem 1 by $(\forall f, g\, G(f,g))$.



Proof of Theorem 1. We consider arbitrary fixed functions, $\hat{f}$, $\hat{g}\colon \mathbb{N} \to \mathbb{N}$. We show: if $\hat{f}$ and $\hat{g}$ are bounded then $\hat{f} + \hat{g}$ is bounded. Now, the goal is not universal anymore.

If you have a goal that is an implication, $A \Rightarrow B$, then you assume A and prove B. Assume $\hat{f}$, $\hat{g}$ are bounded and show that $\hat{f} + \hat{g}$ is bounded. This represents a level quite readable and might be necessary for the proof to be brought down to this level.

So, the new goal is to prove that $\hat{f} + \hat{g}$ is bounded. By Definition 1 we show that there exists b such that for all n, $(\hat{f} + \hat{g})(n) \leq b$. We replace f with $\hat{f} + \hat{g}$ in Definition 1. In this case b and n are the variables.

Now, the outermost operation is *there exists* b.

If you have A and $A \wedge B$ as assertions, then you can add B to the assertions also.

We plug-in Definition 1 and replace $\forall f$ with $\hat{f}$. Since $\hat{f}$ is bounded, by Definition 1 there exists b such that $\hat{f}(n) \leq b$ for all n. Let $\hat{b}$ be such that for all n, $\hat{f}(n) \leq \hat{b}$. We do the same for $\hat{g}$, since $\hat{g}$ is bounded, by Definition 1 there exists b such that for all n, $\hat{g}(n) \leq b$. Let $\hat{c}$ be such that for all n, $\hat{g}(n) \leq \hat{c}$.

We go back to our goal. We can build the expression we need. We show that for all n, $(\hat{f} + \hat{g})(n) \leq \hat{b} + \hat{c}$.

Consider an arbitrary fixed $\hat{n}$. We show $(\hat{f} + \hat{g})(\hat{n}) \leq \hat{b} + \hat{c}$ We plug-in Definition 2. By Definition 2 we need to show $\hat{f}(\hat{n}) + \hat{g}(\hat{n}) \leq \hat{b} + \hat{c}$.

This follows from $\hat{f}(\hat{n}) \leq \hat{b}$ and $\hat{g}(\hat{n}) \leq \hat{c}$ and Theorem 2.

The level of detail is more reduced when compared with the logical level, but also more detailed than necessary. One could write the proof as follows:

Proof: if b is a bound of f and c is a bound of g then $b + c$ is a bound of $f + g$. Q.e.d.

This expresses exactly the main ideas of the longer proof. You have to know how the lower-level proof looks like. After that you can abstract it. Someone who is reasonably experienced should be able to reconstruct the total proof.

It is an *art*.