# Basic Proof Techniques

## Proof Situations

Proving is stepwise arranging of "proof sitations". A proof situation is characterized by the current "knowledge base" (set of sentences that are assumed to be true or are already proven and, hence, can be "used") and a sentence that should be proven. The goal of proving is to arrive at a point where all proof situations considered are "trivial". A proof situation is trivial if the sentence to be proven occurs in the knowledge base.

In the following subsections we compile the basic proof techniques by which the possible proof situations can be handled. The description of these techniques is informal. The proof techniques as we present them here are meant to be guide-lines for proofs by humans. However, they are chosen in such a way that they could be formally extended to form a complete formal system of predicate logic ("system of natural deduction") and even a complete system for automated theorem proving.

There are only very few different proof situations possible. Each of them is characterized by the syntactical structure of the sentence to be proven and by the syntactical structure of the sentences in the knowledge base. For choosing a particular proof technique one has to determine the "outermost construct" (quantifier, propositional connective, predicate or function symbol) of the sentence considered. For this, one has to have a firm knowledge of logical syntax in various disguise. For each of the constructs basically two different proof techniques are available depending on whether the sentence considered is in the knowledge base or whether it is the sentence to be proven.

Each proof technique describes how a given proof situation may be transformed to another "simpler" proof situation. The new proof situations are simpler because either the sentence to be proven has a simpler structure or more sentences are added to the knowledge base.

In "human" proofs, as presented in papers or talks, there are many ways of announcing the application of a certain proof technique. We will train the appropriate use of these idioms in the course. In the following brief summary of the proof techniques we only mention the most typical idioms for some of the proof techniques.

In the sequel, $A$, $B$, $C$ are formulae, $s$ and $t$ are terms, $P$ is a predicate constant, $f$ is a function constant, and $x$ is a variable. $A[x]$ stands for a

formula $A$ in which $x$ occurs as free variable. Similarly, $A[C]$ is a formula in which $C$ occurs as subformula.

We assume that all free variables occurring in the sentences considered are universally bound before we apply any of the proof techniques. In particular, in all proof techniques for the "propositional connectives" ("not", "and", "or", "implies", "if and only if") we assume that the formulae involved do not contain any free variables.

## The Four Basic Approaches

If we are supposed to prove a sentence $A$ we actually do not know whether $A$ is really true. We suggest to proceed as follows:

- Try to prove $A$. If you are successful be happy. Otherwise:
- Assume "not $A$" and try to derive a contradiction. If you are successful be happy (you have proven $A$). Otherwise:
- Try to prove "not $A$". If you are successful be happy (you have shown that one never should trust the boss). Otherwise:
- Assume $A$ and try to derive a contradiction. If you are successful be happy (you have proven "not $A$"). Otherwise:
- Start again with the attempt to prove $A$. (Don't worry! You have gained a lot of new insight when you reach this stage. The second run will be much more successful.)

## Prove "for all $x$, $A[x]$"

For proving

$$\text{for all } x,\ A[x]$$

show

$$A[\bar{x}]$$

**where $\bar{x}$ is a constant that did not occur so far.**

One way of announcing the use of this proof technique is: "Let $\bar{x}$ be arbitrary but fixed. We show $A[\bar{x}]$." Sometimes one just assumes tacitly that, in the sequel, $x$ is a (new) constant and one shows $A[x]$.

## Use "for all $x$, $A[x]$"

**If**

$$\textbf{for all } x, A[x]$$

**is known then one may conclude**

$$A[t]$$

**where $t$ is an arbitrary term.**

One way of formulating this is: "Since we know that, for all $x$, $A[x]$ we also know that, in particular, $A[t]$."

## Prove "there exists $x$ such that $A[x]$"

**For proving**

$$\textbf{there exists } x \textbf{ such that } A[x]$$

**try to find a term $t$ for which**

$$A[t]$$

**can be shown.**

Finding a suitable term $t$, most times, is a non-trivial step in a proof, which needs creativity.

## Use "there exists $x$ such that $A[x]$"

**If it is known that**

$$\text{there exists } x \text{ such that } A[x]$$

**and one has to prove**

$$B$$

**assume**

$$A[\bar{x}]$$

**where $\bar{x}$ is a constant that did not occur so far and prove**

$$B.$$

One way of announcing the use of this proof technique is: "Let $\bar{x}$ be such that $A[\bar{x}]$. We have to prove $B$". Sometimes one just assumes tacitly that, in the sequel, $x$ is a (new) constant and one shows $B$.

## Prove "$A$ and $B$"

**For proving**

$$A \text{ and } B$$

**prove**

$$A$$

**and prove**

$$B.$$

## Use "$A$ and $B$"

**If one knows that**

$$A \text{ and } B$$

**one knows**

$$A$$

**and one knows**

$$B.$$

## Prove "$A$ or $B$"

**For proving**

$A$ or $B$

**assume**

**not** $A$

**and prove**

$B$

**(or assume**

**not** $B$

**and prove**

$A$.

## Use "$A$ or $B$"

**If**

$A$ or $B$

**is known and**

$C$

**should be proven assume**

$A$

**and prove**

$C$.

**Then assume**

$B$

**and prove**

$C$.

One way of formulating the use of this technique is as follows: "We know $A$ or $B$ and want to prove $C$. *Case* $A$: We prove $C$. *Case* $B$: We prove $C$."

## Prove "$A$ implies $B$"

For proving

$A$ implies $B$

assume

$A$

and prove

$B$.

## Use "$A$ implies $B$"

As a general strategy, if

$B$

has to be proven, always look for sentences of the kind

$A$ implies $B$

and prove

$A$.

## Prove "$A$ if and only if $B$"

For proving

$A$ if and only if $B$

assume

$A$

and prove

$B$.

Then assume

$B$

and prove

$A$.

## Use "$A$ if and only if $B$"

**In a situation where**

$$C[A]$$

**has to be proven it may be helpful to look for sentences of the kind**

$$A \text{ if and only if } B$$

**and to try to prove**

$$C[B].$$

This technique is often used in connection with "definitions" of predicate symbols, i.e. formulae of the form

$$P[x] \text{ if and only if } A[x]$$

## Prove "not $A$"

**For proving**

$$\text{not } A$$

**it is often helpful to assume**

$$A$$

**and to derive a contraction, i.e. to prove**

$$\text{not } C$$

**where**

$$C$$

**is in the knowledge base.**

## Prove "$P(t_1, \ldots, t_n)$"

For proving

$$P(t_1, \ldots, t_n)$$

look for an "explicit definition" of the form

$$P(x_1, \ldots, x_n) \text{ iff } A[x_1, \ldots, x_n]$$

and prove

$$A[t_1, \ldots, t_n].$$

## Use "$P(t_1, \ldots, t_n)$"

If one knows that

$$P(t_1, \ldots, t_n)$$

and an "explicit definition"

$$P(x_1, \ldots, x_n) \text{ if and only if } A[x_1, \ldots, x_n]$$

is in the knowledge base then

$$A[t_1, \ldots, t_n]$$

may be added to the knowledge base.

## Prove "$A[f(t_1, \ldots, t_n)]$"

For proving

$$A[f(t_1, \ldots, t_n)]$$

where, for $f$, an "explicit definition" of the form

$$f(x_1, \ldots, x_n) = s[x_1, \ldots, x_n]$$

is available prove

$$A[s[t_1, \ldots, t_n]].$$

For proving

$$A[f(t_1, \ldots, t_n)]$$

where, for $f$, an "implicit definition" of the form

$$f(x_1, \ldots, x_n) = \text{such a } y \text{ that } B[x_1, \ldots, x_n, y]$$

is available prove

$$\text{for all } y,\ B[t_1, \ldots, t_n, y] \text{ implies } A[y].$$

## Use "$A[f(t_1, \ldots, t_n)]$"

If one knows

$$A[f(t_1, \ldots, t_n)]$$

and an "explicit definition" of the form

$$f(x_1, \ldots, x_n) = s[x_1, \ldots, x_n]$$

is in the knowledge base then

$$A[s[t_1, \ldots, t_n]]$$

may be added to the knowledge base.

If one knows

$$A[f(t_1, \ldots, t_n)]$$

and an "implicit definition" of the form

$$f(x_1, \ldots, x_n) = \text{such a } y \text{ that } B[x_1, \ldots, x_n, y]$$

is in the knowledge base then the sentence

$$\text{there exists a } y \text{ such that } B[t_1, \ldots, t_n, y] \text{ and } A[y]$$

may be added to the knowledge base.