

Proving

Proving

Wolfgang Schreiner
Engineering for Computer-based Learning
University of Applied Sciences at Hagenberg

Wolfgang.Schreiner@fh-hagenberg.at
<http://cbl.fh-hagenberg.at/~schreine>

Overview

- Preliminaries
- General Strategies
- Decomposing the Goal
- Deriving New Knowledge

Proving

Preliminaries

Motivation

A **proof** is a structured argument that a proposition is true.

- You claim that a formula is a true proposition (a **theorem**).
 - You **believe** that it is true.
- You want to convince yourself about this.
 - You want to **make sure** that it is true.
- You want to convince someone else about this.
 - You want to make a skeptic opponent **admit** that it is true.

Proving is the art of (scientifically) arguing.

Proof Rules

- Collection of proof rules.
 - Based on the **syntactic structure** of formulas.
 - Can decide whether application is correct by looking at **syntax**.
- Inventing a proof.
 - **Creative** (non-algorithmic) activity.
 - Proof rules provide a mental skeleton and give some guidelines.
 - Ultimately, some **insight** is required.
- Checking a proof.
 - **Mechanical** (algorithmic) activity.
 - Proof rules determine the framework.
 - Everyone is able to read and check a proof.

Every scientist and engineer should understand these rules.

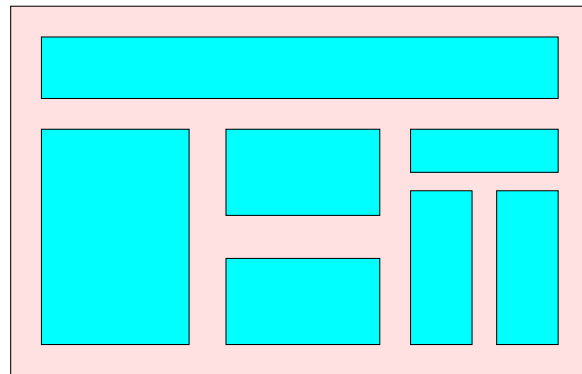
Proof Levels

A proof can be given on various levels of detail.

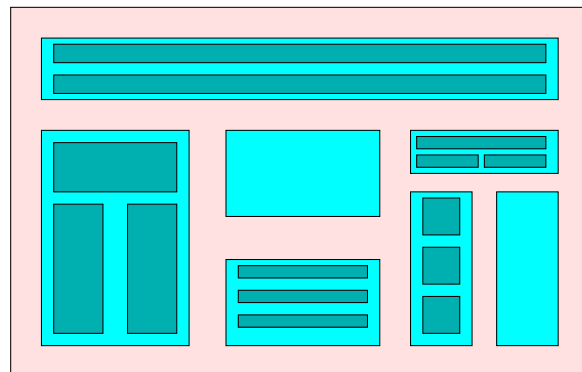
- Lowest level (most details).
 - Very small reasoning steps.
 - Correctness can be checked by **computer program**.
 - Proofs become very large.
- Higher level (fewer details).
 - Larger reasoning steps.
 - Proof becomes shorter and manageable by humans.
 - Each step can be decomposed into finer steps.

A high-level proof is a map of a (more detailed but larger) low-level proof; it can be refined on demand.

Refining a Proof



A proof in less detail



The same proof with some more details

Knowledge

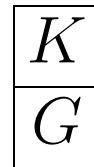
A proof is relative to given **knowledge**.

- Axioms (characterization of the considered domain),
- Definitions (a “harmless” extension of the domain),
- Tautologies (true propositions in every domain),
- Propositions (formulas that have been previously proved),
- Assumptions (knowledge gradually added in a proof).

The knowledge is usually implicit in a proof.

Proof Situations

A **proof situation** consists of available knowledge K (a set of formulas assumed true) and the goal G (a formula to be proved).



“We (have to) prove G with knowledge K .”

- The knowledge available in a particular situation is typically **not** explicitly written down.
- Knowledge at the beginning of the proof is extended by all definitions and assumptions in the proof branch that led to the situation.

Example

We want to prove $\forall A : A \subseteq A$.

- Our goal G is the formula

$$\forall A : A \subseteq A$$

- Our knowledge K consists of

- all the axioms of set theory and
- the theorem

$$\forall A, B : A \subseteq B \Leftrightarrow \forall x \in A : x \in B$$

which is a direct consequence of the definition of the predicate \subseteq .

Proof Rule

A **proof rule** reduces a proof situation to one or more other situations.

- We have to prove goal G_0 with knowledge K_0 .

$$\frac{K_0}{G_0} \rightsquigarrow \frac{K_1}{G_1} \frac{K_2}{G_2}$$

- We prove G_1 with knowledge K_1 and G_2 with knowledge K_2 .
- Proof text:
 - “In order to prove goal G_0 with knowledge K_0 it suffices to prove G_1 with knowledge K_1 and G_2 with knowledge K_2 ”.

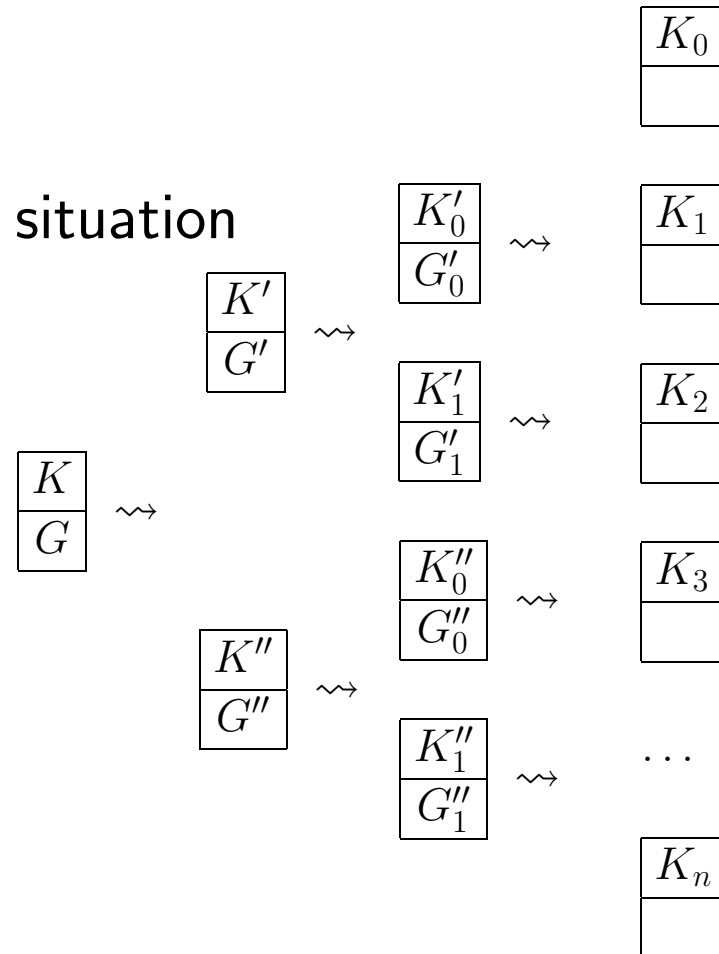
A **proof rule** reduces a proof situation to other proof situations.

Proof

What is a proof?

- A **proof** is the reduction of the start situation
 - to other situations that are again reduced
 - to other situations until we have only situations in which nothing is left to be proved.

A proof can be depicted as a tree of situations.



Proof Termination

Prove G with knowledge K and G .

$$\frac{K \cup \{G\}}{G} \rightsquigarrow \frac{K \cup \{G\}}{}$$

- We are done.
- Proof text.
 - “We prove G . But we know G , and are therefore done.”

The only rule to terminate a proof branch.

Proving

General Strategies

General Strategies

We may prove a goal in a direct way and in an indirect way.

- Direct proofs
 - Try to prove the goal.
 - Try to prove the negation of the goal.
- Indirect proofs.
 - Assume the goal does not hold and derive a contradiction.
 - Assume the goal does hold and derive a contradiction.

Two basic approaches in two variants.

Direct Proof

We do not know in advance whether G is true!

1. We try $\frac{K}{G}$. If we are successful, then G holds.
2. We try $\frac{K}{\neg G}$. If we are successful, then $\neg G$ holds.

If one approach does not succeed, try the other one.

Example

We are interested in the formula

$$(*) \forall A : \exists x : x \in A.$$

We have two possibilities.

1. We try to prove $\forall A : \exists x : x \in A$. If we succeed, $(*)$ holds.
2. We try to prove $\neg \forall A : \exists x : x \in A$, i.e.,

$$\exists A : \forall x : x \notin A.$$

If we succeed, $(*)$ does not hold.

If we do not succeed in both cases, we do not know whether $(*)$ holds.

Indirect Proof

Given some knowledge K and a goal G .

1. We try $\frac{K \cup \{\neg G\}}{F(\text{alse})}$. If we are successful, then G holds.

2. We try $\frac{K \cup \{G\}}{F(\text{alse})}$. If we are successful, then $\neg G$ holds.

Indirect proofs are proofs by contradiction.

Proof by Contradiction

Prove G with knowledge K .

$$\frac{K}{G} \rightsquigarrow \frac{K \cup \{\neg G\}}{F(\text{alse})}$$

- We assume $(\neg G)$ and derive $F(\text{alse})$.
 - Since $F(\text{alse})$ does not hold, this is a **contradiction**.
 - The assumption $\neg G$ is inconsistent with K .
 - If K holds, then also G must hold.
- Proof text:
 - “We prove G . We assume $\neg G$ and show a contradiction”.

Assume the negation of the goal and derive a contradiction.

Contradiction

A contradiction is usually derived by establishing a proof situation

$$\frac{K \cup \{G, \neg G\}}{F(\text{alse})}$$

because we then immediately have

$$\frac{K \cup \{G, \neg G\}}{F(\text{alse})} \rightsquigarrow \frac{K \cup \{F(\text{alse})\}}{F(\text{alse})} \rightsquigarrow \frac{K \cup \{F(\text{alse})\}}{\quad} .$$

We prove a formula that contradicts some formula in the knowledge.

Example

Theorem: There is no square root of 2 in \mathbb{Q} , i.e.,

$$\neg \exists x \in \mathbb{Q} : x^2 = 2.$$

Proof: We assume $\exists x \in \mathbb{Q} : x^2 = 2$ and show a contradiction.

Because of the assumption, we have some $x \in \mathbb{Q}$ with

$$(1) \quad x^2 = 2$$

We know

$$\mathbb{Q} := \{y : \exists a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} : y = a/b \wedge a \text{ and } b \text{ are relatively prime}\}.$$

Since $x \in \mathbb{Q}$, we thus know

$$\exists a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} : x = a/b \wedge a \text{ and } b \text{ are relatively prime.}$$

Thus we have some $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$ such that $x = \frac{a}{b}$ and a and b are relatively prime, i.e.,

$$(2) \quad \neg \exists d \in \mathbb{Z} \setminus \{\pm 1\} : d|a \wedge d|b.$$

...

Example (Continued)

We have $x^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2$ and thus

$$(3) \quad a^2 = 2b^2$$

From (3) and the definition of $|$, we know $2|a^2$ and thus also

$$(4) \quad 2|a.$$

(because, if a is odd, also a^2 is odd).

Then, by the definition of $|$, there exists some $c \in \mathbb{Z}$ such that

$$(5) \quad a = 2c.$$

From (3) and (5) we have $(2c)^2 = 2b^2$, i.e., $4c^2 = 2b^2$, thus $2c^2 = b^2$.

Thus, by definition of $|$, we have $2|b^2$ and therefore

$$(6) \quad 2|b$$

(because, if b is odd, also b^2 is odd).

(4) and (6) contradict (2).

Example

Theorem (second law of Peano):

$$\forall x, y : x' = y' \Rightarrow x = y.$$

Proof: Take arbitrary x and y . We have to prove

$$x' = y' \Rightarrow x = y.$$

We assume

$$(1) x' = y'$$

and show $x = y$.

We assume

$$(2) x \neq y$$

and show a contradiction.

From (1), we know by the definition of $'$

$$(3) x \cup \{x\} = y \cup \{y\}.$$

Example (Continued)

We know by the definition of \cup and set enumeration

$$(4) x \in x \cup \{x\},$$

$$(5) y \in y \cup \{y\}.$$

From (3), (4), and the definition of $=$, we have

$$(6) x \in y \cup \{y\}$$

which implies with (2)

$$(7) x \in y.$$

Likewise, we have from (3), (5), and the definition of $=$ that

$$(8) y \in x \cup \{x\}$$

which implies with (2)

$$(9) y \in x.$$

(7) and (9), i.e., $x \in y \wedge y \in x$, **contradicts** to the axiom of **regularity** that prohibits such “cycles”.

Example

Theorem: Every set is smaller than its powerset:

$$\forall S : S \text{ is smaller than } \mathbb{P}(S).$$

Proof: Take arbitrary S . We have to prove that S is smaller than $\mathbb{P}(S)$, i.e., by definition,

1. S is not larger than $\mathbb{P}(S)$.

By definition, we have to find some $f : S \xrightarrow{\text{injective}} \mathbb{P}(S)$.

Take $f(x) := \{x\}$.

2. S and $\mathbb{P}(S)$ are not of the same size.

Assume that S and $\mathbb{P}(S)$ are of the same size, i.e., there exists some $f : S \xrightarrow{\text{bijective}} \mathbb{P}(S)$.

We show a contradiction.

Take $A := \{x \in S : x \notin f(x)\}$. Since f is surjective and $A \subseteq S$, i.e., $A \in \mathbb{P}(S)$, we have some $a \in S$ with $f(a) = A$. But then we know

$$a \in A \Leftrightarrow a \notin f(a) \Leftrightarrow a \notin A.$$

Proof Directions

There are two basic directions in a proof.

1. **Top-Down:** decomposing the goal into simpler formulas.

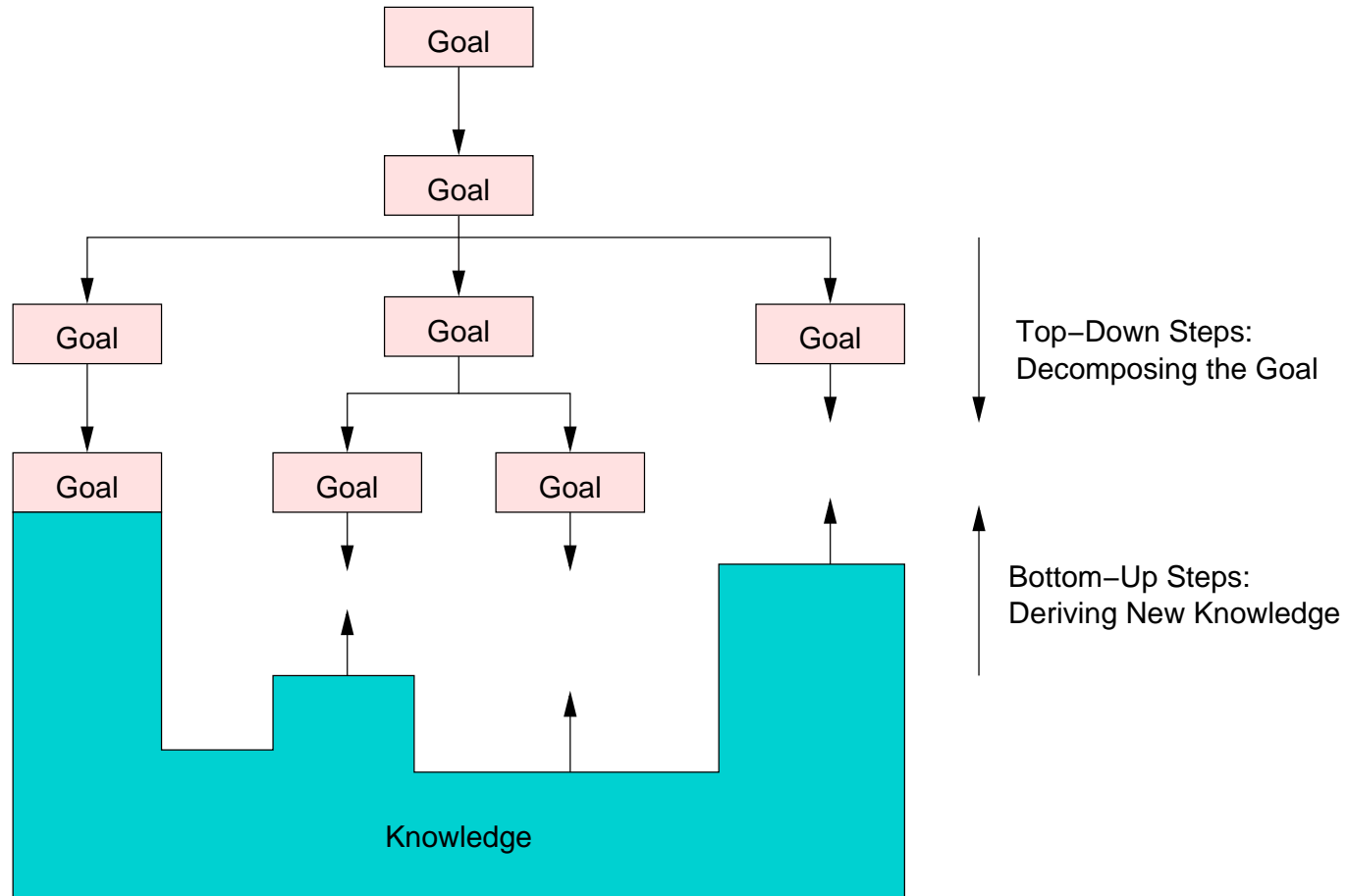
$$\frac{K}{G} \rightsquigarrow \frac{K_0}{G_0} \cdots \frac{K_{n-1}}{G_{n-1}}$$

2. **Bottom-Up:** deriving new knowledge from the given knowledge.

$$\frac{K}{G} \rightsquigarrow \frac{K \cup \{F\}}{G}$$

We usually begin with the top-down strategy.

Proof Directions



Example

Theorem (second law of Peano):

$$\forall x, y : x' = y' \Rightarrow x = y.$$

Proof: (We start in a proof situation where our goal G is above formula and the knowledge base K are the laws of set theory and the definition of $'$.)

Take arbitrary x and y . We have to prove

$$x' = y' \Rightarrow x = y.$$

(Here we have applied a top-down step where we have removed the outermost quantifier from G yielding a new goal G_0 . The knowledge K_0 for proving this new goal equals the original K .)

Example (Continued)

We assume

$$(1) \ x' = y'$$

and show $x = y$.

(Here we have applied another top-down step. The new proof situation has knowledge $K_1 := K_0 \cup \{x' = y'\}$ and $x = y$ as the new goal G_1 .)

We assume

$$(2) \ x \neq y$$

and show a contradiction.

(We start an indirect proof.)

Example (Continued)

From (1), we know by the definition of ' \prime

$$(3) x \cup \{x\} = y \cup \{y\}.$$

(This was a bottom-up step where we have added to our knowledge base K_1 a new formula (3) which is a consequence of two other formulas in the knowledge base, namely (1) and the definition of the successor function ' \prime .)

Then we know by the definition of \cup and set enumeration

$$(4) x \in x \cup \{x\},$$

$$(5) y \in y \cup \{y\}.$$

(Again a bottom-up step which adds two formulas to the knowledge base.)

Example (Continued)

From (3), (4), and the definition of $=$, we have

$$(6) x \in y \cup \{y\}$$

which implies with (2)

$$(7) x \in y.$$

(Two bottom-up steps which add two more formulas.)

Likewise, we have from (3), (5), and the definition of $=$ that

$$(8) y \in x \cup \{x\}$$

which implies with (2)

$$(9) y \in x.$$

(Two more bottom-up steps adding two formulas.)

(7) and (9), i.e., $x \in y \wedge y \in x$,

(This was the last bottom up step adding the conjunction to the knowledge base.)

contradicts the axiom of **regularity** that prohibits such “cycles”.

Proving

Decomposing the Goal

Decomposing the Goal

Decomposition is determined by outermost symbol of goal.

- Decomposition of quantifier formulas:
 - Universally quantified formulas,
 - Existentially quantified formulas.
- Decomposition of connective formulas:
 - Equivalences,
 - Implications,
 - Conjunctions,
 - Disjunctions.
- Inserting predicate and function definitions.

Decomposition of Universally Quantified Formulas

Prove $(\forall x : G)$ with knowledge K .

$$\frac{K}{\forall x : G} \rightsquigarrow \frac{K}{G[x \leftarrow a]} \quad (a \text{ not in } K \cup \{G\})$$

- Prove $G[x \leftarrow a]$.

– a is an object constant that does not appear in K and not in G .

- Proof text:

“We prove $(\forall x : G)$. We take an arbitrary (but fixed) constant a and show $G[x \leftarrow a]$.”

No knowledge is available about constant yet.

Typical Constant Names

Do not choose the constant name at random.

- Choose a constant name that reflects the name of the variable.

“We prove $(\forall x : G)$. We take an arbitrary constant x_0 and show $G[x \leftarrow x_0]$.”

- Choose the variable name itself as the constant name.

“We prove $(\forall x : G)$. We take an arbitrary constant x and show G .”

“We prove $(\forall x : G)$. Take arbitrary x . Then ... (proof of G).”

Constant name must not yet appear in knowledge or goal!

Indirect Method for Universal Formulas

Prove $(\forall x : G)$ with knowledge K .

$$\frac{K}{\forall x : G} \rightsquigarrow \frac{K \cup \{\exists x : \neg G\}}{F(\text{false})} \left(\rightsquigarrow \frac{K \cup \{\neg G[x \leftarrow a]\}}{F(\text{false})} \right)$$

- We assume $(\exists x : \neg G)$. and derive a contradiction:
 - Assumption is equivalent to $(\neg \forall x : G)$.
- Proof text:
 - “We prove $(\forall x : G)$. Assume $\neg G$ for some x . Then ... (derivation of a contradiction with additional knowledge $\neg G$).”

We will see later how to work with existential formulas in knowledge.

Decomposition of Existential Formulas

Prove $\exists x : G$ with knowledge K .

$$\frac{K}{\exists x : G} \rightsquigarrow \frac{K}{G[x \leftarrow T]}$$

- Prove $G[x \leftarrow T]$
 - *Witness* term T .
- Proof text:
 - “We have to prove $(\exists x : G)$. We prove $G[x \leftarrow T]$ ”.

We have to find a value for x that makes G true.

Typical Use

Give the witness value a name.

- Introduce a new constant name

“We have to prove $(\exists x : G)$. Take $a := T$. We prove $G[x \leftarrow a]$ ”.

- Use the variable name as the constant name

“We have to prove $(\exists x : G)$. Take $x := T$. We then have ... (proof of G with additional knowledge $x = T$).”

Constant name must not yet appear in knowledge or goal!

Indirect Method for Existential Formulas

Prove $(\exists x : G)$ with knowledge K .

$$\frac{K}{\exists x : G} \rightsquigarrow \frac{K \cup \{\forall x : \neg G\}}{F(\text{false})}$$

- Assume $(\neg \exists x : G)$ and derive a contradiction:
 - Assumption is equivalent to $(\forall x : \neg G)$.
- Proof text:
 - “We prove $(\exists x : G)$. Assume $(\forall x : \neg G)$. Then ... (derivation of a contradiction with additional knowledge $(\forall x : \neg G)$).”

We will see later how to work with universal formulas in knowledge.

Decomposition of Equivalences

Prove $(G_0 \Leftrightarrow G_1)$ with knowledge K .

$$\boxed{\begin{array}{c} K \\ \hline G_0 \Leftrightarrow G_1 \end{array}} \rightsquigarrow \boxed{\begin{array}{c} K \\ \hline G_0 \Rightarrow G_1 \end{array}} \quad \boxed{\begin{array}{c} K \\ \hline G_1 \Rightarrow G_0 \end{array}}$$

- Prove $G_0 \Rightarrow G_1$ and $G_1 \Rightarrow G_0$.
- Proof text:
 - “We prove $G_0 \Leftrightarrow G_1$:
 - * \Rightarrow : ... (proof of $G_0 \Rightarrow G_1$).
 - * \Leftarrow : ... (proof of $G_1 \Rightarrow G_0$).”

Prove the equivalence “from left to right” and “from right to left”

More General Rule

Sometimes multiple equivalences have to be shown.

- We have to prove $G_0 \Leftrightarrow G_1 \Leftrightarrow G_2$.
 - Actually: $(G_0 \Leftrightarrow G_1) \wedge (G_1 \Leftrightarrow G_2)$.
- It suffices to prove:
 - $G_0 \Rightarrow G_1$,
 - $G_1 \Rightarrow G_2$,
 - $G_2 \Rightarrow G_0$.

Traverse the “implication circle”!

Decomposition of Implications

Prove $(G_0 \Rightarrow G_1)$ with knowledge K .

$$\frac{K}{G_0 \Rightarrow G_1} \rightsquigarrow \frac{K \cup \{G_0\}}{G_1}$$

- Assume G_0 and prove G_1 .
 - Antecedent G_0 .
 - Consequent G_1 .
- Proof text:
 - “We show $G_0 \Rightarrow G_1$. Assume G_0 . Then ... (proof of G_1 with additional knowledge G_0).”

Add the antecedent to the knowledge and prove the consequent.

Alternative Rule for Implications

Prove $(G_0 \Rightarrow G_1)$ with knowledge K .

$$\frac{K}{G_0 \Rightarrow G_1} \rightsquigarrow \frac{K \cup \{\neg G_1\}}{\neg G_0}$$

- Assume $\neg G_1$ and prove $\neg G_0$.
 - $(G_0 \Rightarrow G_1)$ iff $(\neg G_1 \Rightarrow \neg G_0)$.
- Proof text:
 - “We show $G_0 \Rightarrow G_1$. Assume $\neg G_1$. Then ... (proof of $\neg G_0$ with knowledge $\neg G_1$).”

Reverse the direction of the implication.

Indirect Method for Implications

Prove $(G_0 \Rightarrow G_1)$ with knowledge K .

$$\frac{K}{G_0 \Rightarrow G_1} \rightsquigarrow \frac{K \cup \{G_0 \wedge \neg G_1\}}{\text{F(false)}}$$

- Assume $(G_0 \wedge \neg G_1)$ and show a contradiction.
 - $\neg(G_0 \Rightarrow G_1)$ iff $(G_0 \wedge \neg G_1)$.
- Proof text:
 - “We have to show $G_0 \Rightarrow G_1$. Assume $G_0 \wedge \neg G_1$. Then we have ... (derivation of a contradiction)”.

Assume antecedent and negated consequent and derive contradiction.

Decomposition of Conjunctions

Prove $(G_0 \wedge G_1)$ with knowledge K .

$$\frac{K}{G_0 \wedge G_1} \rightsquigarrow \frac{K}{G_0} \quad \frac{K}{G_1}$$

- Prove G_0 and G_1 .
 - **Conjuncts** G_0, G_1 .
- Proof text:
 - “We have to show $G_0 \wedge G_1$.
 1. ... (proof of G_0).
 2. ... (proof of G_1).”

A conjunction is shown by showing both conjuncts in turn.

Indirect Method for Conjunctions

Prove $(G_0 \wedge G_1)$ with knowledge K .

$$\begin{array}{|c|} \hline K \\ \hline G_0 \wedge G_1 \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|} \hline K \cup \{\neg G_0 \vee \neg G_1\} \\ \hline \text{F(false)} \\ \hline \end{array} \rightsquigarrow \begin{array}{|c|} \hline K \cup \{\neg G_0\} \\ \hline \text{F(false)} \\ \hline \end{array} \begin{array}{|c|} \hline K \cup \{\neg G_1\} \\ \hline \text{F(false)} \\ \hline \end{array}$$

- Assume $\neg G_0$ and derive contradiction; assume $\neg G_1$ and repeat.
 - $\neg(G_0 \wedge G_1)$ iff $\neg G_0 \vee \neg G_1$.
- Proof text:
 - “We have to prove $G_0 \wedge G_1$.
 - * Assume $\neg G_0$. Then ... (derivation of a contradiction.)
 - * Assume $\neg G_1$. Then ... (derivation of a contradiction.)”

We will see later this technique of “case distinction”.

Decomposition of Disjunctions

Prove $(G_0 \vee G_1)$ with knowledge K .

$$\frac{K}{G_0 \vee G_1} \rightsquigarrow \frac{K \cup \{\neg G_0\}}{G_1}$$

- Assume $\neg G_0$ and prove G_1 .
 - $(G_0 \vee G_1)$ iff $(\neg G_0 \Rightarrow G_1)$.
 - Roles of G_0 and G_1 can be inverted.
- Proof text:
 - “We have to show $G_0 \vee G_1$. Assume $\neg G_0$. Then ... (proof of G_1).”

Same technique as for decomposition of implications.

Explicitly Defined Predicates

Prove $p(a_0, \dots, a_{n-1})$ with knowledge K and definition of p .

$$\frac{K \cup \{\forall x_0, \dots, x_{n-1} : p(x_0, \dots, x_{n-1}) \Leftrightarrow G\}}{p(a_0, \dots, a_{n-1})} \rightsquigarrow$$

$$\frac{K \cup \{\forall x_0, \dots, x_{n-1} : p(x_0, \dots, x_{n-1}) \Leftrightarrow G\}}{G[x_0 \leftarrow a_0, \dots, x_{n-1} \leftarrow a_{n-1}]}$$

- Prove $G[x_0 \leftarrow a_0, \dots, x_{n-1} \leftarrow a_{n-1}]$.
 - Definition $p(x_0, \dots, x_{n-1}) \Leftrightarrow G$.
- Proof text:
 - “We prove $p(a_0, \dots, a_{n-1})$. By definition of p , we prove $G[x_0 \leftarrow a_0, \dots, x_{n-1} \leftarrow a_{n-1}]$.”

Insert the definition of the predicate!

Explicitly Defined Functions

Prove $G[x \leftarrow F(a_0, \dots, a_{n-1})]$ with knowledge K and def. of F .

$$\frac{K \cup \{\forall x_0, \dots, x_{n-1} : F(x_0, \dots, x_{n-1}) = T\}}{G[x \leftarrow F(a_0, \dots, a_{n-1})]} \rightsquigarrow$$

$$\frac{K \cup \{\forall x_0, \dots, x_{n-1} : F(x_0, \dots, x_{n-1}) = T\}}{G[x \leftarrow T[x_0 \leftarrow a_0, \dots, x_{n-1} \leftarrow a_{n-1}]]}$$

- Prove $G[x \leftarrow T[x_0 \leftarrow a_0, \dots, x_{n-1} \leftarrow a_{n-1}]]$.
 - Definition $F(x_0, \dots, x_{n-1}) := T$.
- Proof text:
 - “We prove $G[x \leftarrow F(a_0, \dots, a_{n-1})]$. By definition of F , we prove $G[x \leftarrow T[x_0 \leftarrow a_0, \dots]]$.”

Insert the definition of the function!

Proving

Deriving New Knowledge

Proof by Case Distinction

Prove G with knowledge K .

$$\frac{K}{G} \rightsquigarrow \frac{K \cup \{F\}}{G} \quad \frac{K \cup \{\neg F\}}{G}$$

- Assume F and prove G ; assume $\neg F$ and prove G .
 - Arbitrary formula F .
 - G iff $(F \Rightarrow G) \wedge (\neg F \Rightarrow G)$.
- Proof text:
 - “We prove G .
 - 1. Assume F . Then ... (proof of G with additional knowledge F).
 - 2. Assume $\neg F$. Then ... (proof of G with additional knowledge $\neg F$).”

Decompose the universe of situations by an assumption.

Typical Use

We know $(F_0 \vee \dots \vee F_{n-1})$.

$$\frac{K \cup \{F_0 \vee \dots \vee F_{n-1}\}}{G} \rightsquigarrow \frac{K \cup \{F_0\}}{G} \cdots \frac{K \cup \{F_{n-1}\}}{G}$$

- Proof text:

- “We prove G . Since we know $(F_0 \vee \dots \vee F_{n-1})$, it suffices to consider the following cases:
 - * Case F_0 : ... (proof of G with additional knowledge F_0).
 - * ...
 - * Case F_{n-1} : ... (proof of G with additional knowledge F_{n-1}).”

A disjunction in the knowledge leads to a proof by case distinction.

Universal Formula in Knowledge

Prove G with knowledge K and $(\forall x : F)$.

$$\frac{K \cup \{\forall x : F\}}{G} \rightsquigarrow \frac{K \cup \{\forall x : F, F[x \leftarrow T]\}}{G}$$

- Prove G with additional knowledge $F[x \leftarrow T]$.
 - Any term T .
- Proof text:
 - “We have to prove G . Since we know $(\forall x : F)$, we have $F[x \leftarrow T]$ and thus ... (proof of G with additional knowledge $F[x \leftarrow T]$).”

Universal formula in knowledge produces new knowledge on demand.

Existential Formula in Knowledge

Prove G with knowledge K and $(\exists x : F)$.

$$\frac{K \cup \{\exists x : F\}}{G} \rightsquigarrow \frac{K \cup \{\exists x : F, F[x \leftarrow a]\}}{G} \quad (a \text{ not in } K, G, F)$$

- Prove G with additional knowledge $F[x \leftarrow a]$.
 - Some object constant a that does not appear in K , G , or F .
- Proof text:
 - “We prove G . Since we know $(\exists x : F)$, we have some a with $F[x \leftarrow a]$. Thus ... (proof of G with new knowledge $F[x \leftarrow a]$).”

Existential formula in knowledge produces new knowledge once.

Additional Knowledge

Prove G with knowledge K .

$$\frac{K}{G} \rightsquigarrow \frac{K \cup \{F\}}{G} \quad (F \text{ holds in every domain in which } K \text{ holds})$$

- Prove G with additional knowledge F .
 - F holds in every domain in which (some of) the formulas in K hold.
- Proof text:
 - “We prove G . Since we know K , we know, by rule . . . , also F .”

Derive new knowledge F from (a subset of) K .

Inferring Additional Knowledge

This rule is a “placeholder” for a number of ways to prove $\frac{K}{F}$:

1. This is shown in a separate proof.
 - Previous proof or subproof of current proof.
2. F is a **propositional consequence** of K .
 - The conclusion holds independently of the truth values of the atomic formulas and of the quantified formulas contained in K and F .
3. This is an instance of a **quantifier consequence**.
 - Gives true conclusions in every domain.
4. This is derived by applying **substitution** rules.
 - Basis are known equalities and equivalences.

Propositional Consequences

The following conclusions are propositional consequences for every formula A and B :

Negation

$\neg\neg A$	A
A	$\neg\neg A$

And Introduction and Or Elimination

$A \wedge B$	A
A	$A \vee B$

Propositional Consequences (Continued)

De Morgan

$\neg(A \wedge B)$	$\neg(A \vee B)$	$\neg A \vee \neg B$	$\neg A \wedge \neg B$
$\neg A \vee \neg B$	$\neg A \wedge \neg B$	$\neg(A \wedge B)$	$\neg(A \vee B)$

Modus Ponens

$A, A \Rightarrow B$
B

Contraposition

$A \Rightarrow B$	$\neg A \Rightarrow \neg B$	$A \Leftrightarrow B$	$\neg A \Leftrightarrow \neg B$
$\neg B \Rightarrow \neg A$	$B \Rightarrow A$	$\neg A \Leftrightarrow \neg B$	$A \Leftrightarrow B$

Tautologies

How can we decide whether a propositional consequence is valid?

- (Propositional) tautology:

- A propositional formula with variables as subformulas that is true for every assignment of truth values to the variables.

- Example: $(A \vee \neg A)$ is a tautology.

- $(F \vee \neg F)$ iff T.

- $(T \vee \neg T)$ iff T.

- Show $(K \Rightarrow F)$ is a tautology.

- Then $\frac{K}{F}$ is a propositional consequence.

How can we show that a propositional formula is a tautology?

Truth Table

We show that

$$((A \vee B) \wedge (A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow C.$$

is a tautology by constructing a truth table:

A	B	C	$A \vee B$	$A \Rightarrow C$	$B \Rightarrow C$	Conjunction	Implication
F	F	F	F	T	T	F	T
F	F	T	F	T	T	F	T
F	T	F	T	T	F	F	T
F	T	T	T	T	T	T	T
T	F	F	T	F	T	F	T
T	F	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	T	T	T	T	T	T	T

Indirect Method

We show that the following is a tautology:

$$((A \vee B) \wedge (A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow C.$$

We assume that its truth value is false and then derive a contradiction:

$$\begin{array}{c}
 \text{false} \\
 \hline
 \text{true} \\
 \hline
 \begin{array}{ccc}
 \text{true} & \text{true} & \text{true} \\
 \hline
 \text{true} & \text{false} & \text{false} & \text{false} & \text{false} & \text{false} \\
 \hline
 ((\overline{A \vee B}) \wedge (\overline{A \Rightarrow C}) \wedge (\overline{B \Rightarrow C})) \Rightarrow \overline{C}
 \end{array}
 \end{array}$$

Because the implication is false, C is false and the conjuncts are true. Thus A and B must be false. Therefore $A \vee B$ is false, which contradicts above derivation.

Quantifier Consequences

For every formula A and B , the following conclusions hold:

Universal Quantification and Conjunction

$(\forall x : A \wedge B)$	$(\forall x : A) \wedge (\forall x : B)$
$(\forall x : A) \wedge (\forall x : B)$	$(\forall x : A \wedge B)$

Existential Quantification and Disjunction

$(\exists x : A \vee B)$	$(\exists x : A) \vee (\exists x : B)$
$(\exists x : A) \vee (\exists x : B)$	$(\exists x : A \vee B)$

Quantifier Consequences (Continued)

Universal and Disjunction, Existential and Conjunction

$(\forall x : A) \vee (\forall x : B)$	$(\exists x : A \wedge B)$
$(\forall x : A \vee B)$	$(\exists x : A) \wedge (\exists x : B)$

Universal and Existential Quantification

$\exists x : \forall y : A$
$\forall y : \exists x : A$

Quantifier Consequences (Continued)

De Morgan Laws

$\neg \forall x : A$	$\exists x : \neg A$	$\neg \exists x : A$	$\forall x : \neg A$
$\exists x : \neg A$	$\neg \forall x : A$	$\forall x : \neg A$	$\neg \exists x : A$

Such Quantifier

$\exists x : A$
$A[x \leftarrow \mathbf{such} \ x : A]$
$(\forall y_0, y_1 : (A[x \leftarrow y_0] \wedge A[x \leftarrow y_1]) \Rightarrow y_0 = y_1)$
$(\forall x : A \Rightarrow x = \mathbf{such} \ x : A)$

Example

We show for arbitrary formula A

$$(\neg \forall x : A) \Rightarrow (\exists x : \neg A)$$

by showing (contraposition)

$$(\neg \exists x : \neg A) \Rightarrow (\neg \neg \forall x : A)$$

i.e. (propositional consequence and substitution, see next subsection)

$$(\neg \exists x : \neg A) \Rightarrow (\forall x : A).$$

We assume (*) $\neg \exists x : \neg A$ and show $\forall x : A$. Take arbitrary x and assume $\neg A$. Then we have $(\exists x : \neg A)$ which contradicts (*).

Substitutions

For all terms S and T , formulas A and B , variables x and formula patterns C with variable F , the following holds:

Equality Substitutions

$$\frac{S = T \wedge A[x \leftarrow S]}{A[x \leftarrow T]}$$

Equivalence Substitutions

$$\frac{A \Leftrightarrow B \wedge C[F \leftarrow A]}{C[F \leftarrow B]}$$

Replace “equal things by equal things”, e.g., insert definitions.