

Logik für Informatiker

Proofs in propositional logic

Till Mossakowski

WiSe 2007/08



Limits of the truth-table method

1. truth-table method leads to **exponentially growing** tables

Limits of the truth-table method

1. truth-table method leads to **exponentially growing** tables
 - 20 atomic sentences \Rightarrow more than 1.000.000 rows

Limits of the truth-table method

1. truth-table method leads to **exponentially growing** tables
 - 20 atomic sentences \Rightarrow more than 1.000.000 rows
2. truth-table method cannot be extended to **first-order logic**

Limits of the truth-table method

1. truth-table method leads to **exponentially growing** tables
 - 20 atomic sentences \Rightarrow more than 1.000.000 rows
 2. truth-table method cannot be extended to **first-order logic**
- **model checking** can overcome the first limitation (up to 1.000.000 atomic sentences)

Limits of the truth-table method

1. truth-table method leads to **exponentially growing** tables
 - 20 atomic sentences \Rightarrow more than 1.000.000 rows
2. truth-table method cannot be extended to **first-order logic**
 - **model checking** can overcome the first limitation (up to 1.000.000 atomic sentences)
 - **proofs** can overcome both limitations

Proofs

- A proof consists of a sequence of **proof steps**

Proofs

- A proof consists of a sequence of **proof steps**
- Each proof step is known to be valid and should

Proofs

- A proof consists of a sequence of **proof steps**
- Each proof step is known to be valid and should
 - be significant but easily understood, in **informal** proofs,

Proofs

- A proof consists of a sequence of **proof steps**
- Each proof step is known to be valid and should
 - be significant but easily understood, in **informal** proofs,
 - follow some **proof rule**, in **formal** proofs.

Proofs

- A proof consists of a sequence of **proof steps**
- Each proof step is known to be valid and should
 - be significant but easily understood, in **informal** proofs,
 - follow some **proof rule**, in **formal** proofs.
- Some valid patterns of inference that generally go unmentioned in informal (but not in formal) proofs:

Proofs

- A proof consists of a sequence of **proof steps**
- Each proof step is known to be valid and should
 - be significant but easily understood, in **informal** proofs,
 - follow some **proof rule**, in **formal** proofs.
- Some valid patterns of inference that generally go unmentioned in informal (but not in formal) proofs:
 - From $P \wedge Q$, infer P .
 - From P and Q , infer $P \wedge Q$.
 - From P , infer $P \vee Q$.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \dots \vee P_n$, prove S from each of P_1, \dots, P_n .

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \dots \vee P_n$, prove S from each of P_1, \dots, P_n .

Claim: there are irrational numbers b and c such that b^c is rational.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \dots \vee P_n$, prove S from each of P_1, \dots, P_n .

Claim: there are irrational numbers b and c such that b^c is rational.

Proof: $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \dots \vee P_n$, prove S from each of P_1, \dots, P_n .

Claim: there are irrational numbers b and c such that b^c is rational.

Proof: $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational: take $b = c = \sqrt{2}$.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \dots \vee P_n$, prove S from each of P_1, \dots, P_n .

Claim: there are irrational numbers b and c such that b^c is rational.

Proof: $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational: take $b = c = \sqrt{2}$.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational: take $b = \sqrt{2}^{\sqrt{2}}$ and $c = \sqrt{2}$.

$$\text{Then } b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2.$$

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .
(\perp may be inferred from P and $\neg P$.)

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .

(\perp may be inferred from P and $\neg P$.)

Assume $Cube(c) \vee Dodec(c)$ and $Tet(b)$.

Claim: $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .
(\perp may be inferred from P and $\neg P$.)

Assume $Cube(c) \vee Dodec(c)$ and $Tet(b)$.

Claim: $\neg(b = c)$.

Proof: Let us assume $b = c$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .
(\perp may be inferred from P and $\neg P$.)

Assume $Cube(c) \vee Dodec(c)$ and $Tet(b)$.

Claim: $\neg(b = c)$.

Proof: Let us assume $b = c$.

Case 1: If $Cube(c)$, then by $b = c$, also $Cube(b)$, which contradicts $Tet(b)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .
(\perp may be inferred from P and $\neg P$.)

Assume $Cube(c) \vee Dodec(c)$ and $Tet(b)$.

Claim: $\neg(b = c)$.

Proof: Let us assume $b = c$.

Case 1: If $Cube(c)$, then by $b = c$, also $Cube(b)$, which contradicts $Tet(b)$.

Case 2: $Dodec(c)$ similarly contradicts $Tet(b)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction \perp .
(\perp may be inferred from P and $\neg P$.)

Assume $Cube(c) \vee Dodec(c)$ and $Tet(b)$.

Claim: $\neg(b = c)$.

Proof: Let us assume $b = c$.

Case 1: If $Cube(c)$, then by $b = c$, also $Cube(b)$, which contradicts $Tet(b)$.

Case 2: $Dodec(c)$ similarly contradicts $Tet(b)$.

In both case, we arrive at a contradiction. Hence, our assumption $b = c$ cannot be true, thus $\neg(b = c)$.

Arguments with inconsistent premises

A proof of a contradiction \perp from premises P_1, \dots, P_n (without additional assumptions) shows that the premises are **inconsistent**. An argument with inconsistent premises is always **valid**, but more importantly, always **unsound**.

Home(max) \vee Home(claire)

\neg Home(max)

\neg Home(claire)

Home(max) \wedge Happy(carl)

Arguments without premises

A proof without any premises shows that its conclusion is a **logical truth**.

Example: $\neg(P \wedge \neg P)$.

Formal proofs in Fitch

- Well-defined set of formal proof rules

Formal proofs in Fitch

- Well-defined set of **formal proof rules**
- Formal proofs in Fitch can be **mechanically checked**

Formal proofs in Fitch

- Well-defined set of **formal proof rules**
- Formal proofs in Fitch can be **mechanically checked**
- For each connective, there is

Formal proofs in Fitch

- Well-defined set of **formal proof rules**
- Formal proofs in Fitch can be **mechanically checked**
- For each connective, there is
 - an **introduction rule**, e.g. “from P , infer $P \vee Q$ ”.

Formal proofs in Fitch

- Well-defined set of **formal proof rules**
- Formal proofs in Fitch can be **mechanically checked**
- For each connective, there is
 - an **introduction rule**, e.g. “from P , infer $P \vee Q$ ”.
 - an **elimination rule**, e.g. “from $P \wedge Q$, infer P ”.

Conjunction Elimination (\wedge Elim)

$$\begin{array}{l} \triangleright \left| \begin{array}{l} P_1 \wedge \dots \wedge P_i \wedge \dots \wedge P_n \\ \vdots \\ P_i \end{array} \right. \end{array}$$

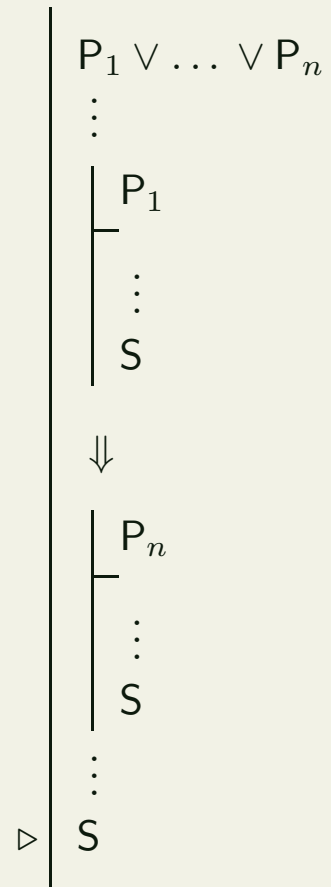
Conjunction Introduction (\wedge Intro)

$$\begin{array}{l} \vdots \\ P_1 \\ \Downarrow \\ P_n \\ \vdots \\ \triangleright P_1 \wedge \dots \wedge P_n \end{array}$$

Disjunction Introduction (\vee Intro)

$$\triangleright \left| \begin{array}{l} P_i \\ \vdots \\ P_1 \vee \dots \vee P_i \vee \dots \vee P_n \end{array} \right.$$

Disjunction Elimination (\vee Elim)



The proper use of subproofs

1. $(B \wedge A) \vee (A \wedge C)$	
2. $B \wedge A$	
3. B	\wedge Elim: 2
4. A	\wedge Elim: 2
5. $A \wedge C$	
6. A	\wedge Elim: 5
7. A	\vee Elim: 1, 2–4, 5–6
8. $A \wedge B$	\wedge Intro: 7, 3

The proper use of subproofs (cont'd)

- In justifying a step of a subproof, you may cite any **earlier step** contained in the main proof, or in any subproof whose assumption is **still in force**. You may **never** cite individual steps inside a subproof that has **already ended**.

The proper use of subproofs (cont'd)

- In justifying a step of a subproof, you may cite any **earlier step** contained in the main proof, or in any subproof whose assumption is **still in force**. You may **never** cite individual steps inside a subproof that has **already ended**.
- Fitch enforces this automatically by not permitting the citation of individual steps inside subproofs that have ended.

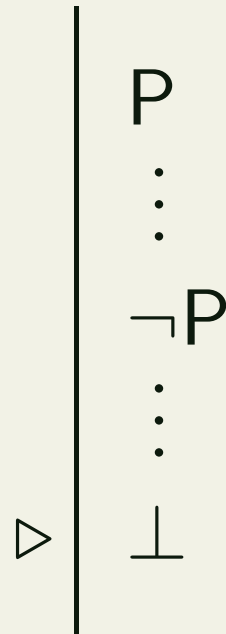
Negation Elimination

(\neg Elim)

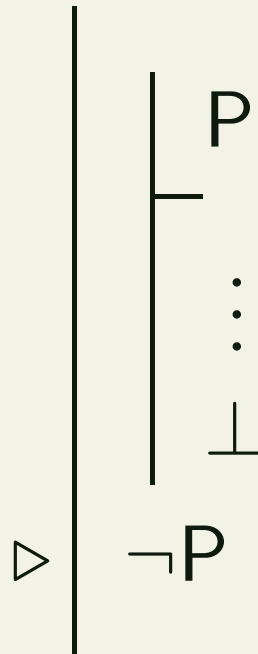
$$\begin{array}{l|l} & \neg\neg P \\ & \vdots \\ \triangleright & P \end{array}$$

\perp Introduction

(\perp Intro)



Negation Introduction (\neg Intro)



\perp Elimination

(\perp Elim)



Strategies and tactics

1. **Understand** what the sentences are saying.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.
3. If you think it does not follow, or are not sure, try to find a **counterexample**.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.
3. If you think it does not follow, or are not sure, try to find a **counterexample**.
4. If you think it does follow, try to give an **informal proof**.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.
3. If you think it does not follow, or are not sure, try to find a **counterexample**.
4. If you think it does follow, try to give an **informal proof**.
5. If a **formal proof** is called for, use the **informal proof to guide** you in finding one.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.
3. If you think it does not follow, or are not sure, try to find a **counterexample**.
4. If you think it does follow, try to give an **informal proof**.
5. If a **formal proof** is called for, use the **informal proof to guide** you in finding one.
6. In giving consequence proofs, both formal and informal, don't forget the tactic of **working backwards**.

Strategies and tactics

1. **Understand** what the sentences are saying.
2. **Decide** whether you think the conclusion follows from the premises.
3. If you think it does not follow, or are not sure, try to find a **counterexample**.
4. If you think it does follow, try to give an **informal proof**.
5. If a **formal proof** is called for, use the **informal proof to guide** you in finding one.
6. In giving consequence proofs, both formal and informal, don't forget the tactic of **working backwards**.
7. In working backwards, though, always check that your **intermediate goals are consequences** of the available information.

Conditionals

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Game rule: $P \rightarrow Q$ is replaced by $\neg P \vee Q$.

Formalisation of conditional sentences

- The following English constructions are all translated

$P \rightarrow Q$:

If P then Q ; Q if P ; P only if Q ; and Provided P , Q .

Formalisation of conditional sentences

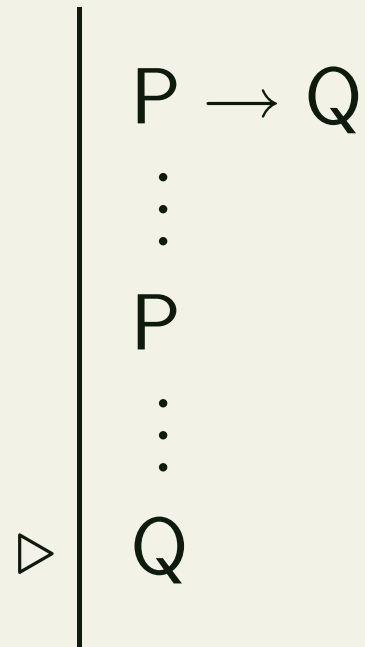
- The following English constructions are all translated $P \rightarrow Q$:
If P then Q ; Q if P ; P only if Q ; and Provided P , Q .
- Unless P , Q and Q unless P are translated: $\neg P \rightarrow Q$.

Formalisation of conditional sentences

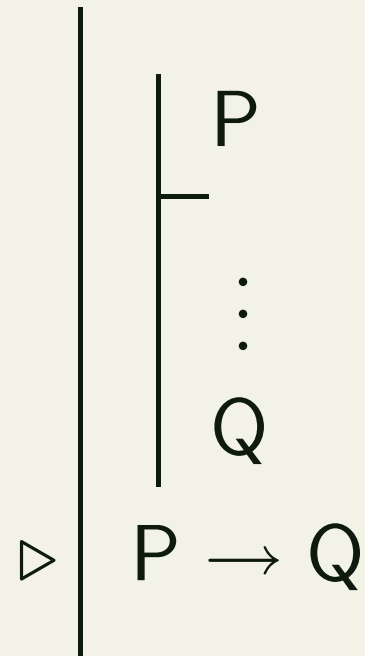
- The following English constructions are all translated $P \rightarrow Q$:
If P then Q ; Q if P ; P only if Q ; and Provided P , Q .
- Unless P , Q and Q unless P are translated: $\neg P \rightarrow Q$.
- Q is a logical consequence of P_1, \dots, P_n if and only if the sentence $(P_1 \wedge \dots \wedge P_n) \rightarrow Q$ is a logical truth.

Conditional Elimination

(\rightarrow Elim)



Conditional Introduction (\rightarrow Intro)



Biconditionals

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

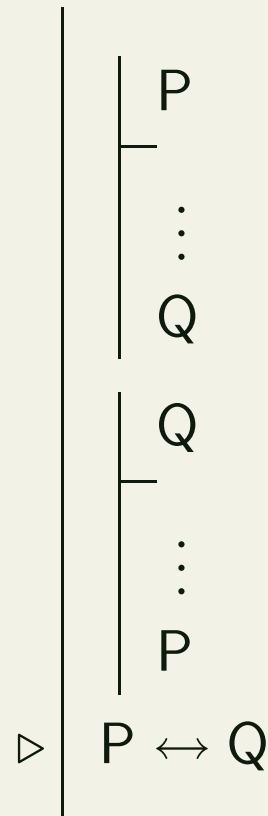
Game rule: $P \leftrightarrow Q$ is replaced by $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

Biconditional Elimination

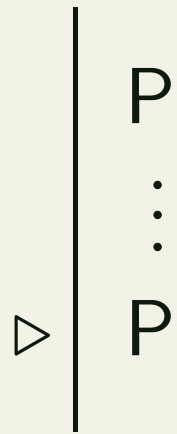
(\leftrightarrow Elim)

	$P \leftrightarrow Q$ (or $Q \leftrightarrow P$)
	\vdots
	P
	\vdots
\triangleright	Q

Biconditional Introduction (\leftrightarrow Intro)



Reiteration (Reit)



Object and meta theory

Object theory = reasoning **within** a formal proof system (e.g. Fitch)

Meta theory = reasoning **about** a formal proof system

Tautological consequence

A sentence S is a **tautological consequence** of a set of sentences \mathcal{T} , written

$$\mathcal{T} \models_T S,$$

if all valuations of atomic formulas with truth values that make all sentences in \mathcal{T} true also make S true.

\mathcal{T} is called **tt-satisfiable**, if there is a valuation making all sentences in \mathcal{T} true. (Note: \mathcal{T} may be infinite.)

Propositional proofs

S is \mathcal{F}_T -**provable** from \mathcal{T} , written

$$\mathcal{T} \vdash_T S,$$

if there is a formal proof of S with premises drawn from \mathcal{T} using the elimination and introduction rules for $\vee, \wedge, \neg, \rightarrow, \leftrightarrow$ and \perp .

Again note: \mathcal{T} may be infinite.

Consistency

A set of sentences \mathcal{T} is called **formally inconsistent**, if

$$\mathcal{T} \vdash_T \perp.$$

Example: $\{A \vee B, \neg A, \neg B\}$.

Otherwise, \mathcal{T} is called **formally consistent**.

Example: $\{A \vee B, A, \neg B\}$

Soundness

Theorem 1. The proof calculus \mathcal{F}_T is sound, i.e. if

$$\mathcal{T} \vdash_T S,$$

then

$$\mathcal{T} \models_T S.$$

Proof: Book: by contradiction, using the first invalid step.
Here: by induction on the length of the proof.

Completeness

Theorem 2 (Bernays, Post). The proof calculus \mathcal{F}_T is complete, i.e. if

$$\mathcal{T} \models_T S,$$

then

$$\mathcal{T} \vdash_T S.$$

Theorem 2 follows from:

Theorem 3. Every formally consistent set of sentences is tt-satisfiable.

Lemma 4. $\mathcal{T} \cup \{\neg S\} \vdash_T \perp$ if and only if $\mathcal{T} \vdash_T S$.

Proof of Theorem 3

A set \mathcal{T} is **formally complete**, if for any sentence S , either $\mathcal{T} \vdash_T S$ or $\mathcal{T} \vdash_T \neg S$.

Proposition 5. Every formally complete and formally consistent set of sentences is tt-satisfiable.

Proposition 6. Every formally consistent set of sentences can be expanded to a formally complete and formally consistent set of sentences.

Proof of Proposition 5

Lemma 7. Let \mathcal{T} be formally complete and formally consistent. Then

1. $\mathcal{T} \vdash_T (R \wedge S)$ iff $\mathcal{T} \vdash_T R$ and $\mathcal{T} \vdash_T S$
2. $\mathcal{T} \vdash_T (R \vee S)$ iff $\mathcal{T} \vdash_T R$ or $\mathcal{T} \vdash_T S$
3. $\mathcal{T} \vdash_T (\neg S)$ iff $\mathcal{T} \not\vdash_T S$
4. $\mathcal{T} \vdash_T (R \rightarrow S)$ iff $\mathcal{T} \not\vdash_T R$ or $\mathcal{T} \vdash_T S$
5. $\mathcal{T} \vdash_T (R \leftrightarrow S)$ iff $(\mathcal{T} \vdash_T R \text{ iff } \mathcal{T} \vdash_T S)$

Proof of Proposition 6

Lemma 8. A set of sentences \mathcal{T} is formally complete if and only if for any **atomic** sentence A ,

either $\mathcal{T} \vdash_T A$ or $\mathcal{T} \vdash_T \neg A$.

Compactness Theorem

Theorem 9. Let \mathcal{T} be any set of sentences. If every finite subset of \mathcal{T} is tt-satisfiable, then \mathcal{T} itself is satisfiable.