Logik für Informatiker
Proofs in propositional logic

Till Mossakowski

WiSe 2009/10

Logical consequence

- Q is a logical consequence of $P_1, \ldots, P_n$, if all worlds that make $P_1, \ldots, P_n$ true also make Q true.
- Q is a tautological consequence of $P_1, \ldots, P_n$, if all valuations of atomic formulas with truth values that make $P_1, \ldots, P_n$ true also make Q true.
- Q is a TW-logical consequence of $P_1, \ldots, P_n$, if all worlds from Tarski's world that make $P_1, \ldots, P_n$ true also make Q true.

Proofs

- With proofs, we try to show (tauto)logical consequence
- Truth-table method can lead to very large tables, proofs are often shorter
- Proofs are also available for consequence in full first-order logic, not only for tautological consequence

Limits of the truth-table method

1. truth-table method leads to *exponentially growing* tables
   - 20 atomic sentences ⇒ 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

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

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

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

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*
- 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 $P \land Q$, infer P.
  - From P and Q, infer $P \land Q$.
  - From P, infer $P \lor Q$.

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 $P \vee Q$.

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 $P \vee Q$.

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 $P \vee Q$.

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 $P \vee Q$.

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

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 $c = \sqrt{2}$.

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

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \ldots \vee P_n$, prove S from each of $P_1, \ldots, P_n$.
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 $c = \sqrt{2}$.

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

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \ldots \vee P_n$, prove S from each of $P_1, \ldots, P_n$.
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 $c = \sqrt{2}$.
Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \ldots \vee P_n$, prove S from each of $P_1, \ldots, P_n$.
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 $c = \sqrt{2}$.
Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$.

Proof by cases (disjunction elimination)

To prove S from $P_1 \vee \ldots \vee P_n$, prove S from each of $P_1, \ldots, P_n$.
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 $c = \sqrt{2}$.
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 infered 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 $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction $\perp$.
($\perp$ may be infered 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 $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction $\perp$.
($\perp$ may be infered 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 $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction $\perp$.
($\perp$ may be infered 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 $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction $\perp$.
($\perp$ may be infered 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 $\neg(b = c)$.

Proof by contradiction

To prove $\neg S$, assume S and prove a contradiction $\perp$.
($\perp$ may be infered 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 $P_1, \ldots, P_n$ (without additional assumptions) shows that the premises are *inconsistent*. An argument with inconsistent premises is always *valid*, but more importantly, always *unsound*.

$$
\begin{array}{|l}
\text{Home(max)} \lor \text{Home(claire)} \\
\neg\text{Home(max)} \\
\neg\text{Home(claire)} \\
\hline
\text{Home(max)} \land \text{Happy(carl)}
\end{array}
$$

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 can be *mechanically checked*
- For each connective, there is
  - an *introduction rule*, e.g. "from P, infer $P \lor Q$".
  - an *elimination rule*, e.g. "from $P \land Q$, infer P".

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".

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".

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".

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 (∧ Elim)

$$\begin{array}{r|l} & P_1 \wedge \ldots \wedge P_i \wedge \ldots \wedge P_n \\ & \vdots \\ \triangleright & P_i \end{array}$$

Conjunction Introduction ($\wedge$ Intro)

$$
\begin{array}{c|l}
 & P_1 \\
 & \Downarrow \\
 & P_n \\
 & \vdots \\
\triangleright & P_1 \wedge \ldots \wedge P_n
\end{array}
$$

Disjunction Introduction ($\vee$ Intro)

$$
\begin{array}{l|l}
 & \mathsf{P}_i \\
 & \vdots \\
\triangleright & \mathsf{P}_1 \vee \ldots \vee \mathsf{P}_i \vee \ldots \vee \mathsf{P}_n
\end{array}
$$

Disjunction Elimination (∨ Elim)

$$
\begin{array}{l|l}
 & P_1 \vee \ldots \vee P_n \\
 & \vdots \\
 & \quad \begin{array}{|l} P_1 \\ \hline \vdots \\ S \end{array} \\
 & \quad \Downarrow \\
 & \quad \begin{array}{|l} P_n \\ \hline \vdots \\ S \end{array} \\
 & \vdots \\
\triangleright & S
\end{array}
$$

The proper use of subproofs

1. $(B \land A) \lor (A \land C)$	
2. $B \land A$	
3. B	$\land$ **Elim**: 2
4. A	$\land$ **Elim**: 2
5. $A \land C$	
6. A	$\land$ **Elim**: 5
7. A	$\lor$ **Elim**: 1, 2–4, 5–6
8. $A \land B$	$\land$ **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*.
- Fitch enforces this automatically by not permitting the citation of individual steps inside subproofs that have 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.

$\perp$ Introduction ($\perp$ Intro)

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

Negation Introduction (¬ Intro)

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

Negation Elimination
(¬ Elim)

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

$\perp$ Elimination
($\perp$ Elim)

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