Logik für Informatiker
Formal proofs for propositional logic

Till Mossakowski, Lutz Schröder

WiSe 2011/12

The truth table method

- A sentence is a tautology if and only if it evaluates to TRUE in all rows of its complete truth table.
- Truth tables can be constructed with the program Boole.

Tautological equivalence and consequence

- Two sentences P and Q are tautologically equivalent, if they evaluate to the same truth value in all valuations (rows of the truth table).
- Q is a tautological consequence of $P_1, \ldots, P_n$ if and only if every row that assigns TRUE to each of $P1, \ldots P_n$ also assigns TRUE to Q.
- If Q is a tautological consequence of $P_1, \ldots P_n$, then Q is also a logical consequence of $P_1, \ldots, P_n$.
- Some logical consequences are not tautological ones.

Tautological equivalence and consequence

- Two sentences P and Q are tautologically equivalent, if they evaluate to the same truth value in all valuations (rows of the truth table).
- Q is a tautological consequence of $P_1, \ldots, P_n$ if and only if every row that assigns TRUE to each of $P1, \ldots P_n$ also assigns TRUE to Q.
- If Q is a tautological consequence of $P_1, \ldots P_n$, then Q is also a logical consequence of $P_1, \ldots, P_n$.
- Some logical consequences are not tautological ones.

Tautological equivalence and consequence

- Two sentences P and Q are tautologically equivalent, if they evaluate to the same truth value in all valuations (rows of the truth table).
- Q is a tautological consequence of $P_1, \ldots, P_n$ if and only if every row that assigns TRUE to each of $P1, \ldots P_n$ also assigns TRUE to Q.
- If Q is a tautological consequence of $P_1, \ldots P_n$, then Q is also a logical consequence of $P_1, \ldots, P_n$.
- Some logical consequences are not tautological ones.

Tautological equivalence and consequence

- Two sentences P and Q are tautologically equivalent, if they evaluate to the same truth value in all valuations (rows of the truth table).
- Q is a tautological consequence of $P_1, \ldots, P_n$ if and only if every row that assigns TRUE to each of $P1, \ldots P_n$ also assigns TRUE to Q.
- If Q is a tautological consequence of $P_1, \ldots P_n$, then Q is also a logical consequence of $P_1, \ldots, P_n$.
- Some logical consequences are not tautological ones.

de Morgan's laws and double negation

$$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$$

$$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$$

$$\neg\neg P \Leftrightarrow P$$

Note: $\neg$ binds stronger than $\wedge$ and $\vee$. Bracktes are needed to override this.

Negation normal form

- Substitution of equivalents: If P and Q are logically equivalent: $P \Leftrightarrow Q$ then the results of substituting one for the other in the context of a larger sentence are also logically equivalent: $S(P) \Leftrightarrow S(Q)$
- A sentence is in negation normal form (NNF) if all occurrences of $\neg$ apply directly to atomic sentences.
- Any sentence built from atomic sentences using just $\wedge$, $\vee$, and $\neg$ can be put into negation normal form by repeated application of the de Morgan laws and double negation.

Negation normal form

- Substitution of equivalents: If P and Q are logically equivalent: $P \Leftrightarrow Q$ then the results of substituting one for the other in the context of a larger sentence are also logically equivalent: $S(P) \Leftrightarrow S(Q)$
- A sentence is in negation normal form (NNF) if all occurrences of $\neg$ apply directly to atomic sentences.
- Any sentence built from atomic sentences using just $\wedge$, $\vee$, and $\neg$ can be put into negation normal form by repeated application of the de Morgan laws and double negation.

Negation normal form

- Substitution of equivalents: If P and Q are logically equivalent: $P \Leftrightarrow Q$ then the results of substituting one for the other in the context of a larger sentence are also logically equivalent: $S(P) \Leftrightarrow S(Q)$
- A sentence is in negation normal form (NNF) if all occurrences of $\neg$ apply directly to atomic sentences.
- Any sentence built from atomic sentences using just $\wedge$, $\vee$, and $\neg$ can be put into negation normal form by repeated application of the de Morgan laws and double negation.

Distributive laws

For any sentences P, Q, and R:

- Distribution of $\land$ over $\lor$:

$$P \land (Q \lor R) \Leftrightarrow (P \land Q) \lor (P \land R).$$

- Distribution of $\lor$ over $\land$:

$$P \lor (Q \land R) \Leftrightarrow (P \lor Q) \land (P \lor R).$$

Distributive laws

For any sentences P, Q, and R:

- Distribution of $\wedge$ over $\vee$:

  $$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R).$$

- Distribution of $\vee$ over $\wedge$:

  $$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R).$$

Conjunctive and disjunctive normal form

- A sentence is in conjunctive normal form (CNF) if it is a conjunction of one or more disjunctions of one or more literals.
- Distribution of $\lor$ over $\land$ allows you to transform any sentence in negation normal form into conjunctive normal form.

Conjunctive and disjunctive normal form

- A sentence is in conjunctive normal form (CNF) if it is a conjunction of one or more disjunctions of one or more literals.
- Distribution of $\vee$ over $\wedge$ allows you to transform any sentence in negation normal form into conjunctive normal form.

Disjunctive normal form

- A sentence is in disjunctive normal form (DNF) if it is a disjunction of one or more conjunctions of one or more literals.
- Distribution of $\wedge$ over $\vee$ allows you to transform any sentence in negation normal form into disjunctive normal form.
- Some sentences are in both CNF and DNF.

Disjunctive normal form

- A sentence is in disjunctive normal form (DNF) if it is a disjunction of one or more conjunctions of one or more literals.
- Distribution of $\wedge$ over $\vee$ allows you to transform any sentence in negation normal form into disjunctive normal form.
- Some sentences are in both CNF and DNF.

Disjunctive normal form

- A sentence is in disjunctive normal form (DNF) if it is a disjunction of one or more conjunctions of one or more literals.
- Distribution of $\wedge$ over $\vee$ allows you to transform any sentence in negation normal form into disjunctive normal form.
- Some sentences are in both CNF and DNF.

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 $\Rightarrow$ 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

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 $P \wedge Q$, 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 $P \vee Q$.

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 $\bot$.
($\bot$ 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 $\bot$.
($\bot$ 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 $\bot$.
($\bot$ 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 $\bot$.
($\bot$ 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: $\neg(P \land \neg P)$.

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 $P \vee Q$".
  - 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 $P \lor Q$".
  - 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".

Conjunction Elimination ($\wedge$ Elim)

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

Conjunction Introduction (∧ Intro)

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

Disjunction Introduction
(∨ Intro)

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

Disjunction Elimination (∨ Elim)

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

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.
- 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.

⊥ Introduction (⊥ Intro)

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

Negation Introduction (¬ Intro)

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

Negation Elimination ($\neg$ Elim)

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

⊥ Elimination
(⊥ Elim)

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