Logik für Informatiker
Formal proofs for propositional logic

Till Mossakowski, Lutz Schröder

WiSe 2011/12
A sentence is a tautology if and only if it evaluates to \textit{TRUE} in all rows of its complete truth table.

Truth tables can be constructed with the program \textit{Boole}.
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 \textsc{true} to each of $P_1, \ldots, P_n$ also assigns \textsc{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.
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 $P_1, \ldots, P_n$ 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.
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 $P_1, \ldots, P_n$ 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.
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 \( P_1, \ldots, P_n \) 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

\[-(P \land Q) \iff (\neg P \lor \neg Q)\]
\[-(P \lor Q) \iff (\neg P \land \neg Q)\]
\[-\neg\neg P \iff P\]

Note: \(\neg\) binds stronger than \(\land\) and \(\lor\). Brackets are needed to override this.
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 $\land$, $\lor$, 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: $P \iff Q$ then the results of substituting one for the other in the context of a larger sentence are also logically equivalent: $S(P) \iff S(Q)$

- 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 $\land$, $\lor$, and $\neg$ can be put into negation normal form by repeated application of the de Morgan laws and double negation.
Substitution of equivalents: If $P$ and $Q$ are logically equivalent: $P \iff Q$ then the results of substituting one for the other in the context of a larger sentence are also logically equivalent: $S(P) \iff S(Q)$

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 $\land$, $\lor$, 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 $\lor$:**

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

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

  $$P \lor (Q \land R) \iff (P \lor Q) \land (P \lor R).$$
Distributive laws

For any sentences $P$, $Q$, and $R$:

- **Distribution of $\land$ over $\lor$**:
  \[ P \land (Q \lor R) \iff (P \land Q) \lor (P \land R). \]

- **Distribution of $\lor$ over $\land$**:
  \[ P \lor (Q \land R) \iff (P \lor Q) \land (P \lor R). \]
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 $\lor$ over $\land$ 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 $\land$ over $\lor$ allows you to transform any sentence in negation normal form into disjunctive normal form.

Some sentences are in both CNF and DNF.
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 $\land$ over $\lor$ 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 $\land$ over $\lor$ 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
Truth-table method leads to \textit{exponentially growing} tables

- 20 atomic sentences $\Rightarrow$ more than 1,000,000 rows

Truth-table method cannot be extended to \textit{first-order logic}

- \textit{Model checking} can overcome the first limitation (up to 1,000,000 atomic sentences)
- \textit{Proofs} can overcome both limitations
1. truth-table method leads to \textit{exponentially growing} tables
   - 20 atomic sentences $\Rightarrow$ more than 1,000,000 rows

2. truth-table method cannot be extended to \textit{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
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 $P \lor Q$. 
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 $P \land Q$, infer $P$.
  - From $P$ and $Q$, infer $P \land Q$.
  - From $P$, infer $P \lor Q$. 

Till Mossakowski, Lutz Schröder

Logic
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 $P \lor Q$. 
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 $P \lor Q$. 
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 \( P \lor Q \).
To prove $S$ from $P_1 \lor \ldots \lor P_n$, 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 $b^c = (\sqrt{2}^\sqrt{2})^\sqrt{2} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$. 
To prove $S$ from $P_1 \lor \ldots \lor P_n$, 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 $b^c = (\sqrt{2^\sqrt{2}})^\sqrt{2} = \sqrt{2^{(\sqrt{2} \cdot \sqrt{2})}} = \sqrt{2^2} = 2$. 
To prove $S$ from $P_1 \lor \ldots \lor P_n$, 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 $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$. 
To prove $S$ from $P_1 \lor \ldots \lor P_n$, 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 $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$. 

 Till Mossakowski, Lutz Schröder Logic
To prove \( S \) from \( P_1 \lor \ldots \lor P_n \), 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 \( b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2 \).
To prove $\neg S$, assume $S$ and prove a contradiction $\bot$.
($\bot$ may be inferred from $P$ and $\neg P$.)
Assume $\text{Cube}(c) \lor \text{Dodec}(c)$ and $\text{Tet}(b)$.
Claim: $\neg(b = c)$.
Proof: Let us assume $b = c$.
Case 1: If $\text{Cube}(c)$, then by $b = c$, also $\text{Cube}(b)$, which contradicts $\text{Tet}(b)$.
Case 2: $\text{Dodec}(c)$ similarly contradicts $\text{Tet}(b)$.
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 inferred from $P$ and $\neg P$.)

Assume $Cube(c) \lor Dodec(c)$ 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 $\neg (b = c)$.
To prove \( \neg S \), assume \( S \) and prove a contradiction \( \bot \).

(\( \bot \) may be inferred from \( P \) and \( \neg P \).)

Assume \( \text{Cube}(c) \lor \text{Dodec}(c) \) and \( \text{Tet}(b) \).

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

Proof: Let us assume \( b = c \).

Case 1: If \( \text{Cube}(c) \), then by \( b = c \), also \( \text{Cube}(b) \), which contradicts \( \text{Tet}(b) \).

Case 2: \( \text{Dodec}(c) \) similarly contradicts \( \text{Tet}(b) \).

In both case, we arrive at a contradiction. Hence, our assumption \( b = c \) cannot be true, thus \( \neg (b = c) \).
To prove $\neg S$, assume $S$ and prove a contradiction $\bot$.
($\bot$ may be infered from $P$ and $\neg P$.)
Assume $Cube(c) \lor Dodec(c)$ 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 inferred from $P$ and $\neg P$.)
Assume $\text{Cube}(c) \lor \text{Dodec}(c)$ and $\text{Tet}(b)$.
Claim: $\neg (b = c)$.
Proof: Let us assume $b = c$.
Case 1: If $\text{Cube}(c)$, then by $b = c$, also $\text{Cube}(b)$, which
contradicts $\text{Tet}(b)$.
Case 2: $\text{Dodec}(c)$ similarly contradicts $\text{Tet}(b)$.
In both case, we arrive at a contradiction. Hence, our assumption
$b = c$ cannot be true, thus $\neg (b = c)$.
To prove $\neg S$, assume $S$ and prove a contradiction $\bot$.
($\bot$ may be inferred from $P$ and $\neg P$.)
Assume $Cube(c) \lor Dodec(c)$ 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 $\neg (b = c)$.
A proof of a contradiction $\bot$ 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.

\[
\begin{array}{l}
\text{Home(max) } \lor \text{ Home(claire)} \\
\neg \text{Home(max)} \\
\neg \text{Home(claire)} \\
\hline \\
\text{Home(max) } \land \text{ Happy(carl)}
\end{array}
\]
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 $P \lor Q$”.
  - an **elimination rule**, e.g. “from $P \land Q$, infer $P$”.
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 $P$”.
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 $P \lor Q$”.
  - an elimination rule, e.g. “from $P \land Q$, infer $P$”. 

Till Mossakowski, Lutz Schröder Logic
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 \( P \)”. 

Conjunction Elimination
($\land$ Elim)

\[
\begin{array}{c}
\vdots \\
\therefore \\
P_i
\end{array}
\]

\[
\begin{array}{c}
P_1 \land \ldots \land P_i \land \ldots \land P_n \\
\vdots \\
\therefore \\
P_i
\end{array}
\]
Conjunction Introduction
(\(\land\) Intro)

\[
P_1 \\
\downarrow \\
P_n \\
\vdots \\
\triangleright P_1 \land \ldots \land P_n
\]
Disjunction Introduction
(∨ Intro)

\[
\begin{array}{c|c}
\hline
P_i \\
\vdots \\
\hline
P_1 \lor \cdots \lor P_i \lor \cdots \lor P_n \\
\hline
\end{array}
\]
Disjunction Elimination
(\lor \text{ Elim})

\[
\begin{align*}
P_1 \lor \ldots \lor P_n \\
\vdots \\
P_1 \\
\vdots \\
S \\
\vdots \\
S \\
\vdots \\
S \\
\vdots \\
S
\end{align*}
\]
In the following two exercises, determine whether the sentences are consistent. If they are, use Tarski's World to build a world where the sentences are both true. If they are inconsistent, use Fitch to give a proof that they are inconsistent (that is, derive $\bot$ from them). You may use $\text{Ana Con}$ in your proof, but only applied to literals (that is, atomic sentences or negations of atomic sentences).

6.15
$\neg (\text{Larger}(a, b) \land \text{Larger}(b, a))$
$\neg \text{SameSize}(a, b)$

6.16
$\neg \text{Smaller}(a, b) \lor \text{Smaller}(b, a)$
$\text{SameSize}(a, b)$

Section 6.4

The proper use of subproofs

Subproofs are the characteristic feature of Fitch-style deductive systems. It is important that you understand how to use them properly, since if you are not careful, you may “prove” things that don’t follow from your premises. For example, the following formal proof looks like it is constructed according to our rules, but it purports to prove that $A \land B$ follows from $(B \land A) \lor (A \land C)$, which is clearly not right.

1. $(B \land A) \lor (A \land C)$
2. $B \land A$
3. $B$
4. $A$
5. $A \land C$
6. $A$
7. $A$
8. $A \land B$

The problem with this proof is step 8. In this step we have used step 3, a step that occurs within an earlier subproof. But it turns out that this sort of justification—one that reaches back inside a subproof that has already ended—is not legitimate. To understand why it’s not legitimate, we need to think about what function subproofs play in a piece of reasoning. A subproof typically looks something like this:
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.
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.
\[ \bot \text{ Introduction} \]
(\bot \text{ Intro})

\[
\begin{array}{c}
\text{P} \\
\vdots \\
\neg \text{P} \\
\vdots \\
\triangle \\
\bot \\
\end{array}
\]
Negation Introduction
(¬ Intro)

\[ \begin{array}{c}
\vdash \neg P \\
\hline
P \\
\vdots \\
\bot
\end{array} \]
Negation Elimination
(¬ Elim)

\[ \begin{array}{c}
\neg\neg P \\
\vdots \\
P \\
\end{array} \]
\[ \bot \text{ Elimination} \]

**(\bot \text{ Elim})**

\[ \begin{array}{c}
\bot \\
\vdots \\
\triangleright \\
\bot
\end{array} \]

\[ \vdash P \]