Formale Methoden der Softwaretechnik
Formal methods of software engineering

Till Mossakowski, Christoph Lüth

SoSe 2011

Propositional Logic

- at the core of many logics, formalisms, programming languages
- used as kind of assembly language for coding problems
- available tools:
  - Boole — learning about truth tables
  - Tarski's world — Henkin-Hintikka game
  - Fitch — natural deduction proofs
  - SPASS — resolution proofs
  - Jitpro — tableau proofs
  - minisat, zChaff — SAT solvers using DPLL
  - Hets — friendly interface to SAT solvers and SPASS

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 $P \vee Q$.

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".

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

P	
Q	
R	
S_1	Justification 1
...	
...	
S_n	Justification n
S	Justification n+1

Fitch rule: Reiteration

Reiteration (Reit):

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

Conjunction Elimination ($\land$ Elim)

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

Conjunction Introduction
($\wedge$ Intro)

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

Disjunction Introduction ($\vee$ Intro)

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

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 $c = \sqrt{2}$.

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

Disjunction Elimination ($\vee$ Elim)

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

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.

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

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

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 $\bot$.
($\bot$ 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 $\neg(b = c)$.

Negation Introduction ($\neg$ Intro)

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

Negation Elimination (¬ Elim)

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

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*.

Home(max) $\vee$ Home(claire)
$\neg$Home(max)
$\neg$Home(claire)

Home(max) $\wedge$ Happy(carl)

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

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

Example proof in fitch

Arguments without premises

A proof without any premises shows that its conclusion is a *logical truth*.
Example: $\neg(P \wedge \neg P)$.

The **Con** rules in Fitch

- **Taut Con** proves all tautological consequences.
- **FO Con** proves all first-order consequences (like $a = c$ follows from $a = b \wedge b = c$).
- **Ana Con** proves (almost) all Tarski's world consequences.

The **Con** rules in Fitch

- **Taut Con** proves all tautological consequences.
- **FO Con** proves all first-order consequences (like $a = c$ follows from $a = b \wedge b = c$).
- **Ana Con** proves (almost) all Tarski's world consequences.

The **Con** rules in Fitch

- **Taut Con** proves all tautological consequences.
- **FO Con** proves all first-order consequences (like $a = c$ follows from $a = b \wedge b = c$).
- **Ana Con** proves (almost) all Tarski's world consequences.

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