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

Negation — Truth table

P	¬P
TRUE	FALSE
FALSE	TRUE

Conjunction — Truth table

P	Q	$P \wedge Q$
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

Disjunction — Truth table

P	Q	$P \vee Q$
TRUE	TRUE	TRUE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

Formalisation

- Sometimes, natural language double negation means logical single negation
- The English expression *and* sometimes suggests a temporal ordering; the FOL expression $\wedge$ never does.
- The English expressions *but*, *however*, *yet*, *nonetheless*, and *moreover* are all stylistic variants of *and*.
- Natural language disjunction can mean *invlusive-or* ($\vee$) or *exclusive-or*: $A \textit{ xor } B \Leftrightarrow (A \vee B) \wedge (\neg A \vee \neg B)$

Logical necessity

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *logically possible*, if it is true in some circumstances (worlds),
- *logically impossible*, if it is true in no circumstances (worlds).

Logical necessity

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *logically possible*, if it is true in some circumstances (worlds),
- *logically impossible*, if it is true in no circumstances (worlds).

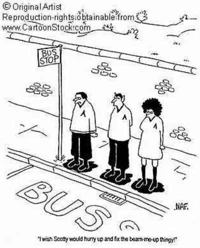
Logical necessity

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *logically possible*, if it is true in some circumstances (worlds),
- *logically impossible*, if it is true in no circumstances (worlds).

Logically possible

Logically and physically possible



Logically impossible

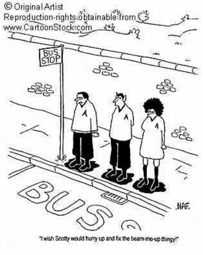
$P \wedge \neg P$ $a \neq a$

Logically necessary

$P \vee \neg P$ $a = a$

Logically possible

Logically and physically possible



Logically impossible

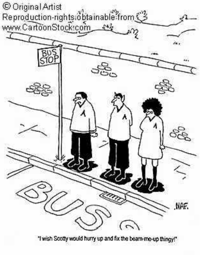
$P \wedge \neg P$ $a \neq a$

Logically necessary

$P \vee \neg P$ $a = a$

Logically possible

Logically and physically possible



Logically impossible

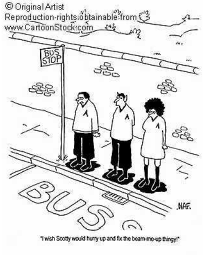
$P \wedge \neg P$ $\qquad a \neq a$

Logically necessary

$P \vee \neg P$ $\qquad a = a$

Logically possible

Logically and physically possible

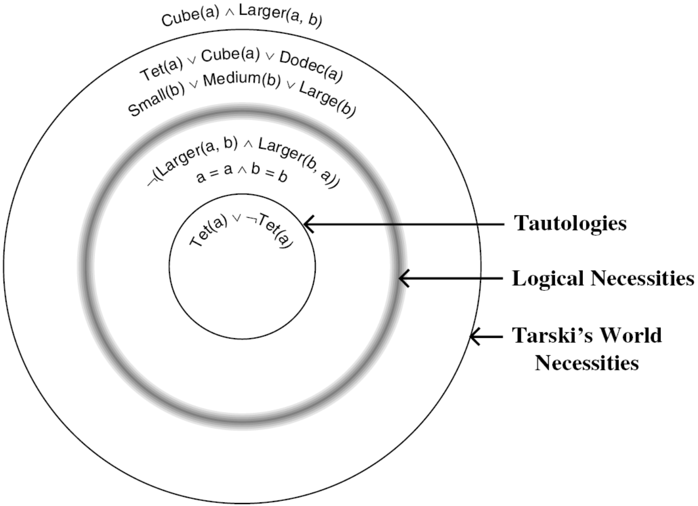


Logically impossible

$P \wedge \neg P$ $\qquad a \neq a$

Logically necessary

$P \vee \neg P$ $\qquad a = a$


Cube(a) ∧ Larger(a, b)
Tet(a) ∨ Cube(a) ∨ Dodec(a)
Small(b) ∨ Medium(b) ∨ Large(b)
¬(Larger(a, b) ∧ Larger(b, a))
a = a ∧ b = b
Tet(a) ∨ ¬Tet(a)
Tautologies
Logical Necessities
Tarski's World
Necessities

The truth table method (Boole)

- 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 $\wedge$ over $\vee$:*

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

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

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

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* $\land$:

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

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.

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.

The Henkin-Hintikka game (Tarski's world)

"Checkmate!"

The Henkin-Hintikka game

Is a sentence true in a given world?

- Players: *you* and the *computer* (Tarski's world)
- You claim that a sentence is true (or false), Tarski's world will claim the opposite
- In each round, the sentence is *reduced* to a simpler one
- When an *atomic sentence* is reached, its truth can be directly inspected in the given world

You have a *winning strategy* exactly in those cases where your claim is *correct*.

Negation — Game rule

Form	Your commitment	Player to move	Goal
$\neg P$	either	—	Replace $\neg P$ by P and switch commitment

Conjunction — Game rule

Form	Your commitment	Player to move	Goal
$P \wedge Q$	TRUE	Tarski's World	Choose one of P, Q that is false.
	FALSE	you	

Disjunction — Game rule

Form	Your commitment	Player to move	Goal
$P \vee Q$	TRUE	you	Choose one of P, Q that is true.
	FALSE	Tarski's World	

Logic, Boolean logic and Tarski's world

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *TW-necessary*, if it is true in all worlds of Tarski's world,
- a *tautology*, if it is true in all valuations of the atomic sentences with $\{\mathrm{TRUE}, \mathrm{FALSE}\}$.

Logic, Boolean logic and Tarski's world

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *TW-necessary*, if it is true in all worlds of Tarski's world,
- a *tautology*, if it is true in all valuations of the atomic sentences with $\{\mathrm{TRUE}, \mathrm{FALSE}\}$.

Logic, Boolean logic and Tarski's world

A sentence is

- *logically necessary*, or *logically valid*, if it is true in all circumstances (worlds),
- *TW-necessary*, if it is true in all worlds of Tarski's world,
- a *tautology*, if it is true in all valuations of the atomic sentences with $\{\mathrm{TRUE}, \mathrm{FALSE}\}$.