Propositional Calculus

Simon Foster & Jim Woodcock

University of York

PROF

8th December 2021

Overview

Outline

Propositions and Truth Tables

- Propositional language = variables + truth-functional connectives.
- Examples: $\neg P$, $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$, $P \Leftrightarrow Q$.
- Propositional variables range over truth-valued statements.
- Three semantic questions about propositions:
  1. Given a truth assignment to variables: is proposition P true or false?
  2. Is there a truth assignment that makes P true?
  3. Which truth assignments make P true?
- Semantics: one technique to answer these questions:
  - Truth tables (Peirce, 1893; Wittgenstein, 1921; Post, 1921).

Proof System

A proof system answers the following questions:

1. Which propositions must be true, for any assignment?
2. What are the laws for reasoning about propositions:

   equalities and inequalities.
3. How do we reason logically?

   entailment and arguments.
4. How do we write a formal proof so that it can be checked?

Propositions

Atomic propositions

- Proposition: some statement such as the following

  4 is a prime number.

  2 is an even integer, but 3 is not.

  My program always halts, if it runs for long enough.

- Fundamental property: either *true* or *false*, but not both.

Compound propositions: fundamental property

- Truth value determined by sub-propositions and connectives.

Outline

Logical Connectives

$\neg$	negation	not
$\wedge$	conjunction	and
$\vee$	disjunction	or
$\Rightarrow$	implication	implies
$\Leftrightarrow$	equivalence	if and only if (is equivalent to)

order of precedence

$$\neg P \wedge Q \vee R \Leftrightarrow Q \Rightarrow P \wedge R$$

is equivalent to

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

Terminology: antecedent $\Rightarrow$ consequent.

Outline

Propositions and Truth Tables

- Logical connectives construct more compound propositions.
- Connectives are functions of component truth values.
- Truth tables evaluate truth value of compound propositions.

	P	Q	$P \wedge Q$	
1 :	t	t	t	$t \wedge t = t$
2 :	t	f	f	$t \wedge f = f$
3 :	f	t	f	$f \wedge t = f$
4 :	f	f	f	$f \wedge f = f$

- Answers all three semantic questions:

1. Given a truth assignment: is the proposition true or false? *See rows (1)–(4).*
2. Is there a truth assignment that makes it true? *Yes, row (1).*
3. Which truth assignments make it true? *Only row (1).*

Truth Tables for Propositional Connectives

P	Q	$P \wedge Q$
t	t	t
t	f	f
f	t	f
f	f	f

P	Q	$P \Rightarrow Q$
t	t	t
t	f	f
f	t	t
f	f	t

P	$\neg P$
t	f
f	t

P	Q	$P \vee Q$
t	t	t
t	f	t
f	t	t
f	f	f

P	Q	$P \Leftrightarrow Q$
t	t	t
t	f	f
f	t	f
f	f	t

Using Truth Tables: Example

- Example proposition: $\neg(P \wedge \neg Q)$.
- List all propositional variables.
- List all situations for propositional variables: 2^k combinations, for k variables.
- Tabulate result in each situation.

P	Q	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$
t	t	f	f	t
t	f	t	t	f
f	t	f	f	t
f	f	t	f	t

Final Result

- Extract the truth table: inputs and output:

P	Q	$\neg(P \wedge \neg Q)$
t	t	t
t	f	f
f	t	t
f	f	t

P	Q	$P \Rightarrow Q$
t	t	t
t	f	f
f	t	t
f	f	t

- This is the same truth table as that for $P \Rightarrow Q$.
- We have formally proved the equivalence of the two propositions:

$$\neg(P \wedge \neg Q) \;\Leftrightarrow\; P \Rightarrow Q$$

Tautologies and Contradictions

- Tautology: proposition that is *true* everywhere.
- Contradiction: proposition that is *false* everywhere.
- Contingency: proposition that is neither a tautology nor a contradiction.
- Duality: the negation of a contradiction is a tautology and vice versa.

Outline

Identities

Tautologies with equivalence as the main connective.

1.	$P \Leftrightarrow P \vee P$	idempotence of $\vee$
2.	$P \Leftrightarrow P \wedge P$	idempotence of $\wedge$
3.	$P \vee Q \Leftrightarrow Q \vee P$	commutativity of $\vee$
4.	$P \wedge Q \Leftrightarrow Q \wedge P$	commutativity of $\wedge$
5.	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	associativity of $\vee$
6.	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	associativity of $\wedge$
7.	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	De Morgan's Law (1)
8.	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	De Morgan's Law (2)
9.	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	distributivity of $\wedge$ over $\vee$
10.	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	distributivity of $\vee$ over $\wedge$

Identities

11.	$P \vee \mathit{true} \Leftrightarrow \mathit{true}$	zero for $\vee$
12.	$P \wedge \mathit{true} \Leftrightarrow P$	unit for $\wedge$
13.	$P \vee \mathit{false} \Leftrightarrow P$	unit for $\vee$
14.	$P \wedge \mathit{false} \Leftrightarrow \mathit{false}$	zero for $\wedge$
15.	$P \vee \neg P \Leftrightarrow \mathit{true}$	excluded middle
16.	$P \wedge \neg P \Leftrightarrow \mathit{false}$	contradiction
17.	$P \Leftrightarrow \neg\neg P$	double negation
18.	$(P \Rightarrow Q) \Leftrightarrow \neg P \vee Q$	implication
19.	$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$	equivalence
20.	$(P \wedge Q \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$	exportation
21.	$(P \Rightarrow Q) \wedge (P \Rightarrow \neg Q) \Leftrightarrow \neg P$	absurdity
22.	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$	contraposition

Equational Reasoning

- As we've already seen: if $P \Leftrightarrow Q$, then P and Q have the same truth table.
- The fact that they have the same semantics justifies writing $P = Q$.
- Equivalence is transitive: $(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R) \Rightarrow (P \Leftrightarrow R)$.
- These two facts justify our presentation of equational reasoning:

$$
\begin{array}{l}
\quad (P_1 \Leftrightarrow P_2) \\
\wedge\ (P_2 \Leftrightarrow P_3) \\
\qquad \vdots \\
\wedge\ (P_{n-1} \Leftrightarrow P_n)
\end{array}
\qquad\qquad
\begin{array}{rl}
P_1 & = P_2 \\
& = P_3 \\
& \vdots \\
& = P_{n-1} \\
& = P_n
\end{array}
$$

Presenting Proofs using Identities

Classic equational reasoning presentation

$$\begin{aligned} \neg\,(P \Rightarrow Q) &= \neg\,(\neg\,P \vee Q) && \text{implication} \\ &= \neg\,\neg\,P \wedge \neg\,Q && \text{De Morgan's Law (1)} \\ &= P \wedge \neg\,Q && \text{double negation} \end{aligned}$$

Width-saving presentation

$$\begin{aligned} & \neg\,(P \Rightarrow Q) && \text{implication} \\ = \;& \neg\,(\neg\,P \vee Q) && \text{De Morgan's Law (1)} \\ = \;& \neg\,\neg\,P \wedge \neg\,Q && \text{double negation} \\ = \;& P \wedge \neg\,Q \end{aligned}$$

Saving even more width

$$\begin{aligned} & \neg\,(P \Rightarrow Q) \\ = \;& \quad \{\text{ implication }\} \\ & \neg\,(\neg\,P \vee Q) \\ = \;& \quad \{\text{ De Morgan's Law (1) }\} \\ & \neg\,\neg\,P \wedge \neg\,Q \\ = \;& \quad \{\text{ double negation }\} \\ & P \wedge \neg\,Q \end{aligned}$$

Example: Using Identities to Simplify by Hand

	$(P \Rightarrow Q) \vee (P \Rightarrow R) \Rightarrow (Q \vee R)$	implication, twice
$=$	$(\neg P \vee Q) \vee (\neg P \vee R) \Rightarrow (Q \vee R)$	comm, assoc, idemp $\vee$
$=$	$\neg P \vee (Q \vee R) \Rightarrow (Q \vee R)$	implication
$=$	$\neg(\neg P \vee (Q \vee R)) \vee (Q \vee R)$	De Morgan's Law (1)
$=$	$(\neg\neg P \wedge \neg(Q \vee R)) \vee (Q \vee R)$	double negation
$=$	$(P \wedge \neg(Q \vee R)) \vee (Q \vee R)$	commutativity of $\vee$
$=$	$(Q \vee R) \vee (P \wedge \neg(Q \vee R))$	distributivity of $\vee$ over $\wedge$
$=$	$((Q \vee R) \vee P) \wedge ((Q \vee R) \vee \neg(Q \vee R))$	excluded middle
$=$	$((Q \vee R) \vee P) \wedge \mathit{true}$	unit for $\wedge$
$=$	$(Q \vee R) \vee P$	commutativity of $\vee$
$=$	$P \vee (Q \vee R)$	

Example: An Absorption Law

- Consider a proposed identity: $(P \wedge \neg Q) \vee Q = P \vee Q$.
- Do you know or are you willing to believe this identity?
- It represents a tautology. Consider the truth table:

P	Q	$\neg Q$	$P \wedge \neg Q$	$(P \wedge \neg Q) \vee Q$	$P \vee Q$
t	t	f	f	t	t
t	f	t	t	t	t
f	t	f	f	t	t
f	f	t	f	f	f

- The two sides of the equation have identical truth tables.
- Therefore they are equivalent.

Algebraic proof

$$(P \wedge \neg Q) \vee Q \;=\; P \vee Q$$

$$\begin{aligned}
(P \wedge \neg Q) \vee Q &= Q \vee (P \wedge \neg Q) && \text{commutativity of } \vee \\
&= (Q \vee P) \wedge (Q \vee \neg Q) && \text{distributivity of } \vee \text{ over } \wedge \\
&= (Q \vee P) \wedge \mathit{true} && \text{excluded middle} \\
&= Q \vee P && \text{unit for } \wedge \\
&= P \vee Q && \text{commutativity of } \vee
\end{aligned}$$

Logical Proofs in Software Engineering

- Refinement is the main development process in formal methods.
- This is the verifiable transformation of one model or program into another.
- An abstract specification is transformed into an executable program.
- Stepwise refinement allows this process to be done in stages.
- Abstract model M_i is refined into concrete model M_{i+1}.
- Requirements specification $\longrightarrow$ final software.
- Each refinement step involves implication: $S \Leftarrow P$.
- Each concrete behaviour must also be an abstract behaviour.
- This is the fundamental idea in this course. Requires implication tautologies.

Inequalities

Tautologies with implication as the main connective.

1.	$P \Rightarrow P \vee Q$	addition
2.	$P \wedge Q \Rightarrow P$	simplification
3.	$P \wedge (P \Rightarrow Q) \Rightarrow Q$	modus ponens
4.	$(P \Rightarrow Q) \wedge \neg Q \Rightarrow \neg P$	modus tollens
5.	$\neg P \wedge (P \vee Q) \Rightarrow Q$	disjunctive syllogism
6.	$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$	hypothetical syllogism
7.	$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$	transitivity of $\Rightarrow$
8.	$(P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow ((P \wedge R) \Rightarrow (Q \wedge S))$	coupling
9.	$(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R) \Rightarrow (P \Leftrightarrow R)$	transitivity of $\Leftrightarrow$

Implication Order on Truth Values

- The contradiction "*false*" is a very strong constraint: it can't be satisfied!
- The tautology "*true*" is very weak: it's satisfied by any truth assignment!
- Recall "P implies Q" : $P \Rightarrow Q$.
- Read this as "P is stronger than (or equal to) Q".
- False is stronger than true. True is weaker than false.
- Each truth value is as strong as itself (reflexivity).

Ordering

- Truth table for implication:

P	Q	$P \Rightarrow Q$
t	t	t
t	f	f
f	t	t
f	f	t

- Is *true* stronger than or equal to *true*? $(true \Rightarrow true) = true$ yes!
- Is *true* stronger than or equal to *false*? $(true \Rightarrow false) = false$ no!
- Is *false* stronger than or equal to *true*? $(false \Rightarrow true) = true$ yes!
- Is *false* stronger than or equal to *false*? $(false \Rightarrow false) = true$ yes!
- Programs are stronger (more determined) than specifications.
- Spec: $S = (x' > x)$. Program: $P = (x := x + 1)$.
- Refinement: $(\forall x, x' \bullet P \Rightarrow S)$. That is, $\forall x, x' \bullet x' = x + 1 \Rightarrow x' > x$.

Outline

Arguments

- Argument: chain of reasoning from premises to conclusion.
- Given a set of propositions $P_1, P_2, \ldots, P_n$: the premises.
- Logical argument leads to a valid proposition Q: the conclusion.
- Entailment: claim that premises entail conclusion: $P_1, P_2, \ldots, P_n \vdash Q$
- Entailment $P_1, P_2, \ldots, P_n \vdash Q$ is either valid or invalid.
- Valid: Q is true whenever all premises $P_1, P_2, \ldots, P_n$ are true.
- Invalid: an entailment that isn't valid.
- Entailment is closely related to implication:
  - Entailment is valid, except where premises are true and conclusion is false.
  - Implication is true, except where antecedent is true and consequent is false.

Example

- This argument is a fallacy (it's invalid): $P \Rightarrow Q, Q \vdash P$
- Demonstration of invalidity here follows directly from a truth table.
- Truth table involves all premises and the conclusion:

	$P \Rightarrow Q$	Q	P
1 :	***t***	***t***	***t***
2 :	*f*	*f*	*t*
3 :	***t***	***t***	***f***
4 :	*t*	*f*	*f*

- There are two situations where the premises are both true: rows (1) and (3).
- Rows (2) and (4) are irrelevant (at least one false premise).
- Row (1) is a valid argument, but row (3) is an invalid argument.
- Therefore the entailment is invalid and $P \Rightarrow Q, Q \vdash P$ is a fallacy.

Example Application

- Consider the following conjecture, for rational x:

  if $x^2 - 3 * x + 2 < 0$ then $x > 0$

- The conditional is an implication: $x^2 - 3 * x + 2 < 0 \Rightarrow x > 0$.
- It's obvious that it's a theorem, isn't it?
- But how will you prove it? What argument will you use?

- We show three possible arguments:

  1. Assume the implication's antecedent, then prove its consequent.
  2. Take the contrapositive. Now follow argument (1).
  3. Negate the conjecture, then show this is a contradiction.

Outline

Summary

- Overview of the propositional calculus.
- Meaning, truth tables, laws, identities, weakening, strengthening.
- Writing proofs: structure with an appropriate argument and give hints.
- Formal proof: every step justified by a law.
- Laws from propositional calculus or from a formal theory (e.g., arithmetic).
- Next lecture: Natural deduction in the propositional calculus.