Natural Deduction
(Propositional Calculus)

COMP2600 — Formal Methods for Software Engineering

Jeremy Dawson

Australian National University
Semester 2, 2011

Contrasting Major Proof Techniques

There are three major styles of proof in logic and mathematics.

- Model based computation:
  For propositional logic, this is the use of truth tables.
- Algebraic proof:
  Relies on simplification rules.
- Deductive reasoning:
  The application of rules of inference.

The logical operators

- $p \wedge q$: "p *and* q" : true iff both p and q are true
- $p \vee q$: "p *or* q" : true iff either p or q (or both) is true
- $p \rightarrow q$: "p *implies* q", or "*if* p *then* q" :
  true iff either p is false or q is true (or both of these)
- $\neg p$: "*not* p" : true iff p is false
- $p \leftrightarrow q$: "p *is equivalent to* q", true when p and q are either both false or both true (actually it is just $p = q$, as boolean values)

The logical operators defined by truth tables

We can express the logical operators using truth tables

p	q	$p \vee q$	$p \wedge q$	$p \rightarrow q$	$\neg p$	$p \leftrightarrow q$
T	T	T	T	T	F	T
T	F	T	F	F	F	F
F	T	T	F	T	T	F
F	F	F	F	T	T	T

We can use these tables to calculate the truth values of logical expressions

Model based computation

Statement to be proved: $(p \wedge (q \vee r)) \rightarrow ((p \wedge q) \vee r))$

For all 8 (= 2^3) possibilities of p, q, r, calculate truth value of the statement

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$(p \wedge q) \vee r)$	$(p \wedge (q \vee r)) \rightarrow ((p \wedge q) \vee r))$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	T
F	T	T	T	F	F	T	T
F	T	F	T	F	F	F	T
F	F	T	T	F	F	T	T
F	F	F	F	F	F	F	T

Testing whether proposition valid or not

Likewise we can test whether the proposition
$((p \rightarrow q) \wedge (q \rightarrow r)) \leftrightarrow \neg(r \rightarrow p)$ is *valid*, ie, true for *all* truth-values of p, q, r

p	q	r	$r \rightarrow p$	$\neg(r \rightarrow p)$	$q \rightarrow r$	$p \rightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow r)$	result
T	T	T	T	F	T	T	T	F
T	T	F	T	F	F	T	F	T
T	F	T	T	F	T	F	F	T
T	F	F	T	F	T	F	F	T
F	T	T	F	T	T	T	T	T
F	T	F	T	F	F	T	F	T
F	F	T	F	T	T	T	T	T
F	F	F	T	F	T	T	T	F

So it is not true for the cases (*"counterexamples"*) p, q, r all $True$, or all $False$

Algebraic Proof

Statement to be proved: $(p \wedge (q \vee r)) \rightarrow ((q \rightarrow s) \vee p)$

Calculate that it is equal to T (true) using various logical rules

$(p \wedge (q \vee r)) \rightarrow ((q \rightarrow s) \vee p)$	
$\equiv \neg(p \wedge (q \vee r)) \vee ((q \rightarrow s) \vee p)$	$a \rightarrow b \equiv \neg a \vee b$
$\equiv (\neg p \vee \neg(q \vee r)) \vee ((q \rightarrow s) \vee p)$	$\neg(a \wedge b) \equiv \neg a \vee \neg b$
....	
$\equiv (p \vee \neg p) \vee (\neg(q \vee r) \vee (q \rightarrow s))$	assoc & commut
$\equiv T \vee (\neg(q \vee r) \vee (q \rightarrow s))$	$a \vee \neg a \equiv T$
$\equiv T$	$T \vee a \equiv T$

We will not be using this technique in this course

The notion of a Deductive Reasoning proof

- A proof is a sequence of *steps*.
- Each step is a *logical sentence*.
- Each step is either:
  - an *axiom* or an *assumption*; or
  - a statement which follows from previous steps via a valid *rule of inference*.

Deductive Reasoning

Statement to be proved: $(p \wedge (q \vee r)) \rightarrow ((q \rightarrow s) \vee p)$

1	$p \wedge (q \vee r)$	Assumption
2	p	$\wedge$-E, 1
3	$(q \rightarrow s) \vee p$	$\vee$-I, 2
4	$(p \wedge (q \vee r)) \rightarrow ((q \rightarrow s) \vee p)$	$\rightarrow$-I, 1–3

Which rules are axioms?

- There are many valid rules of inference.
- Many sets of inference rules are used as bases for proof.
- Gentzen's set of rules are well-known and people associate them with *natural deduction.*
- For each connective, there is an introduction and an elimination rule.

Conjunction – Rules

$\wedge$-I (and introduction)

$$\frac{p \qquad q}{p \wedge q}$$

$\wedge$-E (and elimination)

$$\frac{p \wedge q}{p} \qquad\qquad \frac{p \wedge q}{q}$$

Commutativity of Conjunction (derived rule)

$$\frac{p \wedge q}{q \wedge p}$$

1	$p \wedge q$	
2	p	$\wedge$-E, 1
3	q	$\wedge$-E, 1
4	$q \wedge p$	$\wedge$-I, 2, 3

Implication – Rules

$\rightarrow$-I (implies introduction)

$$\frac{\begin{matrix}[\,p\,] \\ \vdots \\ q\end{matrix}}{p \rightarrow q}$$

This notation means that by *assuming* p, you can *prove* q

$\rightarrow$-E (implies elimination)

$$\frac{p \qquad p \rightarrow q}{q}$$

Transitivity of implication (derived rule)

To prove

$$\frac{p \rightarrow q \qquad q \rightarrow r}{p \rightarrow r}$$

1	$p \rightarrow q$	
2	$q \rightarrow r$	
3	$\quad p$	
4	$\quad q$	$\rightarrow$-E, 1, 3
5	$\quad r$	$\rightarrow$-E, 2, 4
6	$p \rightarrow r$	$\rightarrow$-I, 3–5

Lines 1 and 2 are the assumptions given,
you may use these throughout the proof

Line 3 is an assumption made within the proof,
you may use it only within its scope (lines 3 to 5)

Notation: justification of a step – IMPORTANT

1	$p \rightarrow q$	
2	$\quad p$	
3	$\quad q$	$\rightarrow$-E, 1, 2
4	$p \rightarrow q$	$\rightarrow$-I, 2–3

This is a rather silly proof, we succeed in proving what we started with.

But it illustrates the meaning of the line number notation: (IMPORTANT!)

- $\rightarrow$-E,1,2 means that rule $\rightarrow$-E proves line 3 from lines 1 and 2
- $\rightarrow$-I,2-3 means rule $\rightarrow$-I proves line 4 from the fact that we could assume line 2 and (using that assumption) prove line 3

Rules involving assumptions – IMPORTANT

- If a statement is inside the scope of an assumption, then it depends on that assumption.

1	$p \rightarrow q$	
2	$q \rightarrow r$	
3	$\quad p$	
4	$\quad q$	$\rightarrow$-E, 1, 3
5	$\quad r$	$\rightarrow$-E, 2, 4
6	$q \wedge r$ *WRONG*	$\wedge$-I, 4, 5

Given $p \rightarrow q$ and $q \rightarrow r$, I then assumed p and proved $q \wedge r$,
but $q \wedge r$ depends on p.

- You can assume anything, but it might not be useful.

1	$p \wedge q$	
2	q	$\wedge$-E, 1
3	$(p \wedge q) \rightarrow q$	$\rightarrow$-I, 1–2


(Photo: Hans Hillewaert CCSA2.5)

1	p $\wedge$ You are a giraffe	
2	You are a giraffe	$\wedge$-E, 1
3	p $\wedge$ You are a giraffe $\rightarrow$ You are a giraffe	$\rightarrow$-I, 1–2

Disjunction – Rules

$\vee$-I (or introduction)

$$\frac{p}{p \vee q} \qquad \frac{p}{q \vee p}$$

$\vee$-E (or elimination)

$$\frac{p \vee q \quad \begin{matrix}[p] \\ \vdots \\ r\end{matrix} \quad \begin{matrix}[q] \\ \vdots \\ r\end{matrix}}{r}$$

$\vee$-E template (it's a bit tricky)

1	$p \vee q$	
2	p	
$\vdots$	$\vdots$	
a	r	
b	q	
$\vdots$	$\vdots$	
c	r	
d	r	$\vee$-E, 1, 2–a, b–c

Commutativity of Disjunction (derived rule)

$$\frac{p \vee q}{q \vee p}$$

1	$p \vee q$	
2	p	
3	$q \vee p$	$\vee$-I, 2
4	q	
5	$q \vee p$	$\vee$-I, 4
6	$q \vee p$	$\vee$-E, 1, 2–3, 4–5

Negation – Rules

Idea: assume the opposite of what you want to prove and find a contradiction — so your assumption must have been wrong

¬-I (not introduction)

$$\frac{\begin{array}{c}[p]\\ \vdots \\ q \wedge \neg q\end{array}}{\neg p}$$

¬-E (not elimination)
(eliminates ¬ from an *assumption*)

$$\frac{\begin{array}{c}[\neg p]\\ \vdots \\ q \wedge \neg q\end{array}}{p}$$

Double negation introduction (derived rule)

$$\frac{p}{\neg\neg p} \qquad \frac{\text{It is raining}}{\text{It is not the case that is is not raining}}$$

1	p	
2	$\quad \neg p$	
3	$\quad p \wedge \neg p$	∧-I, 1, 2
4	$\neg\neg p$	¬I, 2–3

Contradiction elimination (derived rule)

$$\frac{p \wedge \neg p}{q}$$

1	$p \wedge \neg p$	
2	$\quad \neg$(You are a giraffe)	
3	$\quad p \wedge \neg p$	R, 1
4	You are a giraffe	¬E, 2–3

(Photo: Hans Hillewaert CCSA2.5)

Double negation elimination (derived rule)

$$\frac{\neg\neg p}{p}$$

1	$\neg\neg p$	
2	$\quad \neg p$	
3	$\quad \neg p \wedge \neg\neg p$	∧-I, 1, 2
4	p	¬E, 2–3

Equivalence

$p \leftrightarrow q$ means p is true if and only if q is true

We can make the definition

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

which would naturally give us these rules

introduction rule:

$$\frac{p \rightarrow q \qquad q \rightarrow p}{p \leftrightarrow q}$$

elimination rules:

$$\frac{p \leftrightarrow q}{p \rightarrow q} \qquad \frac{p \leftrightarrow q}{q \rightarrow p}$$

Equivalence — Rules

Alternatively we can get rules which don't involve the $\rightarrow$ symbol

$\leftrightarrow$-I ($\leftrightarrow$ introduction)

$$\frac{\begin{array}{cc} [p] & [q] \\ \vdots & \vdots \\ q & p \end{array}}{p \leftrightarrow q}$$

$\leftrightarrow$-E ($\leftrightarrow$ elimination)

$$\frac{p \leftrightarrow q \qquad p}{q} \qquad \frac{p \leftrightarrow q \qquad q}{p}$$

Note the similarities to the $\rightarrow$-I and $\rightarrow$-E rules

Which rule to use next?

- Guided by the "form" of your goal, and what you already have proved
- "form" — ie, look at the connective: $\wedge, \vee, \rightarrow, \neg$
- always can consider using $\neg$-E (not elimination) rule
- to prove $p \vee q$, $\vee$-I (or introduction) may not work

$$\frac{p}{p \vee q} \qquad \frac{q}{p \vee q}$$

p may not be necessarily true, q may not be necessarily true

To prove $p \vee q$, sometimes you need to do this:

- First step, using $\neg$-E, assume $\neg(p \vee q)$ (hoping to prove some contradiction)
- When is $\neg(p \vee q)$ true ? When both p and q false!
- From $\neg(p \vee q)$ how to prove $\neg p$? (next slide)
- Having proved both $\neg p$ and $\neg q$, prove some further contradiction
- Exercise: prove $\dfrac{\neg p \rightarrow q}{p \vee q}$

Not-or elimination (derived rule)

$$\frac{\neg(p \vee q)}{\neg p}$$

1	$\neg(p \vee q)$	
2	$\quad p$	
3	$\quad p \vee q$	$\vee$-I, 2
4	$\quad (p \vee q) \wedge \neg(p \vee q)$	$\wedge$-I, 1, 3
5	$\neg p$	$\neg$I, 2–4

Proving a contrapositive rule

In the same way, whenever you can prove any $\frac{p}{q}$

then you can prove $\frac{\neg q}{\neg p}$

1	$\neg q$	
2	$\quad p$	
3	$\quad q$	your proof of q from p
4	$\quad q \wedge \neg q$	$\wedge$-I, 1, 3
5	$\neg p$	$\neg$I, 2–4

Law of the excluded middle (derived)

$$p \vee \neg p$$

"Everything must either be or not be." – Russell

1	$\quad \neg(p \vee \neg p)$	
2	$\quad \neg p$	$\neg\vee$-E (previous slide), 1
3	$\quad \neg\neg p$	$\neg\vee$-E (previous slide), 1
4	$\quad \neg p \wedge \neg\neg p$	$\wedge$-I, 2, 3
5	$p \vee \neg p$	$\neg$E, 1–4