Formal Methods in software development

a.y. 2017/2018

Prof. Anna Labella

The need of formal declarative sentences

cfr. M. Huth – M. Ryan ch.1

- Logic in computer science

Modelling and reasoning about systems

Composing sentences: connectives

- Sentences are expressions that assume truth values
- Inductive definition of complex sentences via connectives

Examples of sentences and of connectives

- Mary wants to go to the picnic
- Today sun is shining….
- Sun is shining and Mary is going to the picnic
- If it is raining Mary gets wet
- If it is raining and Mary has an umbrella, then Mary does not get wet

Natural deduction calculus1

Propositional variables p, q, r…..

Connectives $\neg$ $\wedge$ $\vee$ $\rightarrow$

Intuitive meaning:

$\neg$ p is true iff p is not true

p $\wedge$ q is true iff p and q are both true

p $\vee$ q is true iff one between p and q is true

p $\rightarrow$ q is true iff, supposing p true, q is true

Natural deduction calculus1

Convention 1.3 $\neg$ binds more tightly than $\vee$ and $\wedge$, and the latter two bind more tightly than $\to$. Implication $\to$ is *right-associative*: expressions of the form $p \to q \to r$ denote $p \to (q \to r)$.

Natural deduction calculus 2

Sequents

$$\varphi_1, \varphi_2, \varphi_3, \ldots.. \vdash \psi$$

A sequent is *valid* if we can “prove” it

For this reason we introduce proof rules

Natural deduction calculus 2

What is a proof:

A proof is a finite sequence of elementary steps given by proof rules beginning with the left part of the sequent and ending with the right part

Natural deduction calculus 3

Proof rules involving conjunction

$$\frac{\phi \qquad \psi}{\phi \land \psi} \quad \land\text{i.}$$

$$\frac{\phi \land \psi}{\phi} \quad \land\text{e1}$$

$$\frac{\phi \land \psi}{\psi} \quad \land\text{e2.}$$

Exercises

Prove

- $p \wedge q,\ r \vdash p \wedge r$
- $p \wedge q \vdash q \wedge p$
- $(p \wedge q) \wedge r \vdash p \wedge (q \wedge r)$

Natural deduction calculus 4

Proof rules involving double negation

$$\frac{\neg\neg\phi}{\phi} \quad \neg\neg\, e$$

$$\frac{\phi}{\neg\neg\phi} \quad \neg\neg\, i$$

Exercise

Prove

- $\neg\neg(p \wedge q), r \vdash \neg\neg p \wedge r$

Natural deduction calculus 5

Modus Ponens

$$\frac{\phi \quad \phi \rightarrow \psi}{\psi} \qquad \rightarrow e$$

Natural deduction calculus 6

Modus Tollens (derived rule)

$$\frac{\phi \rightarrow \psi \quad \neg \psi}{\neg \phi} \quad \text{MT}$$

Exercises

Prove

- $p \rightarrow q, (p \rightarrow q) \rightarrow r \vdash r$
- $p, p \rightarrow (p \rightarrow q) \vdash q$
- $q \rightarrow (p \rightarrow r), \neg r, q \vdash \neg p$

Natural deduction calculus 7

Implies introduction

$$\frac{\boxed{\begin{array}{c}\phi\\ \cdot\\ \cdot\\ \\ \psi\end{array}}}{\phi \;\to\; \psi} \qquad \to i$$

Natural deduction calculus 8

Use of assumptions

1.	$p \rightarrow q$	premise
2.	$\neg q$	assumption
3.	$\neg p$	MT
4.	$\neg q \rightarrow \neg p$	$\rightarrow$i (2,3)

$p \rightarrow q \vdash \neg q \rightarrow \neg p$

$(p \rightarrow q), \neg q \vdash \neg p$

Exercise

Prove

- $\vdash (q \rightarrow r) \rightarrow ((\neg q \rightarrow \neg p) \rightarrow (p \rightarrow r))$

Natural deduction calculus 9

Metatheorem

$\varphi_1, \varphi_2, \varphi_3, \ldots\ldots \vdash \psi$

Is equivalent to

$\vdash (\varphi_1 \rightarrow (\varphi_2 \rightarrow (\varphi_3 \rightarrow \ldots\ldots \rightarrow \psi)))$

Proof by induction

Natural deduction calculus 10

Rules involving disjunction

$$\frac{\phi}{\phi \vee \psi} \quad \vee i1$$

$$\frac{\psi}{\phi \vee \psi} \quad \vee i2$$

Natural deduction calculus 11

Introducing disjunction

$$\frac{\phi \vee \psi \qquad \boxed{\begin{array}{c}\phi \\ \\ \\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\psi \\ \\ \\ \chi\end{array}}}{\chi}\ \vee e$$

Exercises

Prove

- $p \vee q \vdash q \vee p$
- $(p \vee q) \vee r \vdash p \vee (q \vee r)$
- $\vdash p \rightarrow (q \rightarrow p)$
- $p \rightarrow q \vdash \neg q \rightarrow \neg p$

- The Copy rule

Natural deduction 12

About negation and $\perp$

$$\frac{\perp}{\phi} \quad \perp e$$

$$\frac{\phi \wedge \neg \phi}{\perp} \quad \neg e$$

$$\frac{\boxed{\begin{array}{c}\phi \\ \vdots \\ \perp\end{array}}}{\neg \phi} \quad \neg i$$

Natural deduction calculus 13

Derived rules

$$\frac{\phi \rightarrow \psi \quad \neg \psi}{\neg \phi} \quad \text{MT}$$

$$\frac{}{\phi \vee \neg \phi} \quad \text{LEM}$$

$$\frac{\phi}{\neg \neg \phi} \quad \neg \neg \text{i}$$

$$\frac{\boxed{\begin{array}{c} \neg \phi \\ \vdots \\ \perp \end{array}}}{\phi} \quad \text{RAA}$$

Natural deduction calculus 14

Derived rules

$$\frac{\phi \rightarrow \psi \quad \neg\psi}{\neg\phi} \quad \text{MT}$$

1	$\phi \rightarrow \psi$	premise
2	$\neg\psi$	premise
3	ϕ	assumption
4	ψ	$\rightarrow$e 1, 3
5	$\perp$	$\neg$e 4, 2
6	$\neg\phi$	$\neg$i 3–5

Natural deduction calculus 15

Derived rules

$$\frac{}{\phi \vee \neg\phi} \text{ LEM}$$

1	$\neg(\phi \vee \neg\phi)$	assumption
2	ϕ	assumption
3	$\phi \vee \neg\phi$	$\vee i_1$ 2
4	$\bot$	$\neg e$ 3, 1
5	$\neg\phi$	$\neg i$ 2–4
6	$\phi \vee \neg\phi$	$\vee i_2$ 5
7	$\bot$	$\neg e$ 6, 1
8	$\neg\neg(\phi \vee \neg\phi)$	$\neg i$ 1–7
9	$\phi \vee \neg\phi$	$\neg\neg e$ 8

Natural deduction calculus 16

Derived rules

$$\frac{\phi}{\neg\neg\phi} \quad \neg\neg i$$

1	ϕ	premise
2	$\neg\phi$	assumption
3	$\bot$	$\neg e$ 1, 2
4	$\neg\neg\phi$	$\neg i$ 2–3

	introduction	*elimination*
$\wedge$	$\dfrac{\phi \quad \psi}{\phi \wedge \psi}\wedge\mathrm{i}$	$\dfrac{\phi \wedge \psi}{\phi}\wedge\mathrm{e}_1 \qquad \dfrac{\phi \wedge \psi}{\psi}\wedge\mathrm{e}_2$
$\vee$	$\dfrac{\phi}{\phi \vee \psi}\vee\mathrm{i}_1 \qquad \dfrac{\psi}{\phi \vee \psi}\vee\mathrm{i}_2$	$\dfrac{\phi \vee \psi \quad \boxed{\begin{array}{c}\phi\\ \vdots\\ \chi\end{array}} \quad \boxed{\begin{array}{c}\psi\\ \vdots\\ \chi\end{array}}}{\chi}\vee\mathrm{e}$
$\rightarrow$	$\dfrac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \psi\end{array}}}{\phi \rightarrow \psi}\rightarrow\mathrm{i}$	$\dfrac{\phi \quad \phi \rightarrow \psi}{\psi}\rightarrow\mathrm{e}$
$\neg$	$\dfrac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \bot\end{array}}}{\neg\phi}\neg\mathrm{i}$	$\dfrac{\phi \quad \neg\phi}{\bot}\neg\mathrm{e}$
$\bot$	(no introduction rule for $\bot$)	$\dfrac{\bot}{\phi}\bot\mathrm{e}$
$\neg\neg$		$\dfrac{\neg\neg\phi}{\phi}\neg\neg\mathrm{e}$

Some useful derived rules:

$$\dfrac{\phi \rightarrow \psi \quad \neg\psi}{\neg\phi}\mathrm{MT} \qquad \dfrac{\phi}{\neg\neg\phi}\neg\neg\mathrm{i}$$

$$\dfrac{\boxed{\begin{array}{c}\neg\phi\\ \vdots\\ \bot\end{array}}}{\phi}\mathrm{PBC} \qquad \dfrac{}{\phi \vee \neg\phi}\mathrm{LEM}$$

Natural deduction calculus 18

Provably equivalent formulas ϕ and ψ,
if we can prove both

$\phi \vdash \psi$ and $\psi \vdash \phi$

Natural deduction calculus 19

Important remark (or metatheorem):

The proof is obtained from the formula to be proved
Hence it is automatic

Exercises

1. Use $\neg$, $\rightarrow$, $\wedge$ and $\vee$ to express the following declarative sentences in propositional logic; in each case state what your respective propositional atoms p, q, etc. mean:
   * (a) If the sun shines today, then it won't shine tomorrow.
   (b) Robert was jealous of Yvonne, or he was not in a good mood.
   (c) If the barometer falls, then either it will rain or it will snow.
   * (d) If a request occurs, then either it will eventually be acknowledged, or the requesting process won't ever be able to make progress.
   (e) Cancer will not be cured unless its cause is determined and a new drug for cancer is found.
   (f) If interest rates go up, share prices go down.
   (g) If Smith has installed central heating, then he has sold his car or he has not paid his mortgage.
   * (h) Today it will rain or shine, but not both.
   * (i) If Dick met Jane yesterday, they had a cup of coffee together, or they took a walk in the park.
   (j) No shoes, no shirt, no service.
   (k) My sister wants a black and white cat.

Exercises

2. The formulas of propositional logic below implicitly assume the binding priorities of the logical connectives put forward in Convention 1.3. Make sure that you fully understand those conventions by reinserting as many brackets as possible. For example, given $p \wedge q \rightarrow r$, change it to $(p \wedge q) \rightarrow r$ since $\wedge$ binds more tightly than $\rightarrow$.

* (a) $\neg p \wedge q \rightarrow r$
  (b) $(p \rightarrow q) \wedge \neg(r \vee p \rightarrow q)$
* (c) $(p \rightarrow q) \rightarrow (r \rightarrow s \vee t)$
  (d) $p \vee (\neg q \rightarrow p \wedge r)$
* (e) $p \vee q \rightarrow \neg p \wedge r$
  (f) $p \vee p \rightarrow \neg q$
* (g) Why is the expression $p \vee q \wedge r$ problematic?