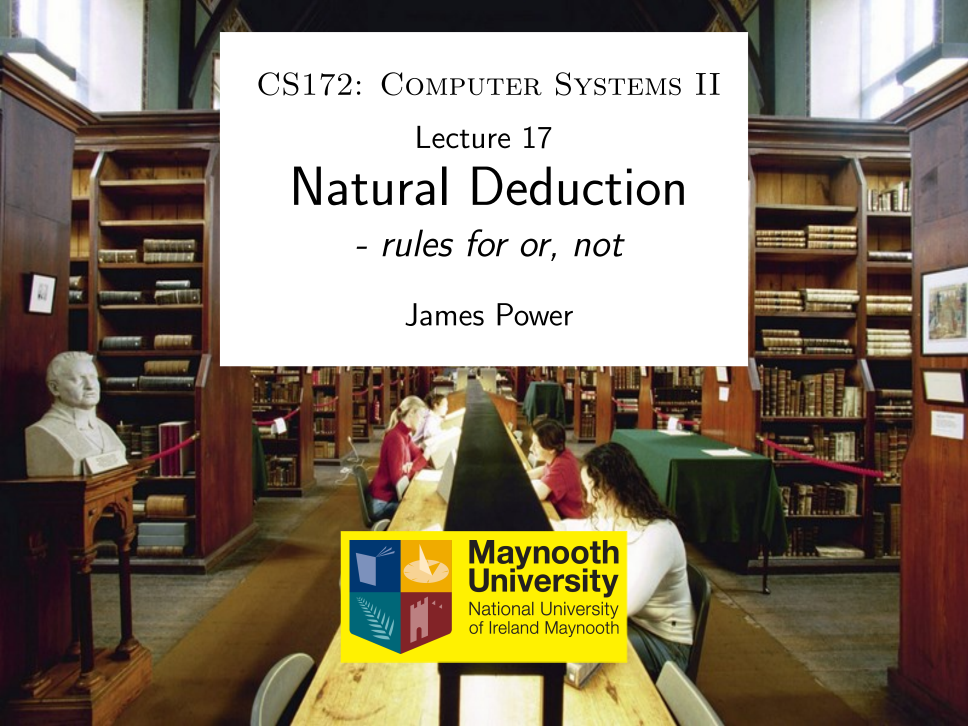


CS172: Computer Systems II

Lecture 17

Natural Deduction

- rules for or, not

James Power

Maynooth University
National University of Ireland Maynooth

Proofs using 'or'

The rules for dealing with disjunction (i.e. 'or'):

- Introduction:
  To prove $A \vee B$:
  you must prove A, or you must prove B (your choice)

Proofs using 'or'

The rules for dealing with disjunction (i.e. 'or'):

- Introduction:
  To prove $A \vee B$:
  you must prove A, or you must prove B (your choice)

- Elimination:
  If you know $A \vee B$:
  Unfortunately you don't know *which* one of them is true,
  so you must prove the theorem both
  - for the case where A is true
  - and also for the case where B is true

  (Proof by cases).

Formal proof rules for 'or'

$$\frac{A}{A \vee B}\ \vee_{\mathcal{I}1} \qquad \frac{B}{A \vee B}\ \vee_{\mathcal{I}2}$$

$$\frac{A \vee B \quad \boxed{\begin{array}{c}\text{Suppose } A: \\ \vdots \\ C\end{array}} \quad \boxed{\begin{array}{c}\text{Suppose } B: \\ \vdots \\ C\end{array}}}{C}\ \vee_{\mathcal{E}}$$

Example of a maths proof using 'or'

Theorem

If $A \subseteq C$ *and* $B \subseteq C$ *then* $(A \cup B) \subseteq C$

Example of a maths proof using 'or'

Theorem

If $A \subseteq C$ *and* $B \subseteq C$ *then* $(A \cup B) \subseteq C$

Proof.

Suppose that $A \subseteq C$ and $B \subseteq C$,
and suppose also that x is some element of $(A \cup B)$.
Thus we know that $x \in A$ or $x \in B$.
  Case 1: If $x \in A$, then since $A \subseteq C$ we know $x \in C$.
  Case 2: If $x \in B$, then since $B \subseteq C$ we know $x \in C$.
Since we know that at least one case is true, we conclude $x \in C$.
But x was an *arbitrary* element of $(A \cup B)$, so we conclude that $(A \cup B) \subseteq C$. $\square$

A more formal version of that proof

Theorem

If $A \subseteq C$ *and* $B \subseteq C$ *then* $(A \cup B) \subseteq C$

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

11. $(A \subseteq C) \wedge (B \subseteq C) \rightarrow ((A \cup B) \subseteq C)$

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $A \subseteq C$ and $B \subseteq C$

10. $\quad (A \cup B) \subseteq C$
11. $(A \subseteq C) \wedge (B \subseteq C) \rightarrow ((A \cup B) \subseteq C)$ $\quad \rightarrow_{\mathcal{I}}$, lines 1-10

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $(x \in A) \to (x \in C)$ and $(x \in B) \to (x \in C)$:

10. $\quad (x \in (A \cup B)) \to (x \in C)$
11. $(A \subseteq C) \wedge (B \subseteq C) \to ((A \cup B) \subseteq C)$ $\qquad \to_{\mathcal{I}}$, lines 1-10

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $(x \in A) \to (x \in C)$ and $(x \in B) \to (x \in C)$:
2. Suppose $x \in (A \cup B)$:

9. Thus $x \in C$
10. $(x \in (A \cup B)) \to (x \in C)$ — $\to_{\mathcal{I}}$, lines 2-9
11. $(A \subseteq C) \wedge (B \subseteq C) \to ((A \cup B) \subseteq C)$ — $\to_{\mathcal{I}}$, lines 1-10

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $(x \in A) \rightarrow (x \in C)$ and $(x \in B) \rightarrow (x \in C)$:
2. Suppose $(x \in A) \vee (x \in B)$:

9. Thus $x \in C$
10. $(x \in (A \cup B)) \rightarrow (x \in C)$ — $\rightarrow_{\mathcal{I}}$, lines 2-9
11. $(A \subseteq C) \wedge (B \subseteq C) \rightarrow ((A \cup B) \subseteq C)$ — $\rightarrow_{\mathcal{I}}$, lines 1-10

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $(x \in A) \rightarrow (x \in C)$ and $(x \in B) \rightarrow (x \in C)$:
2. Suppose $(x \in A) \vee (x \in B)$:
3. Suppose $(x \in A)$:

6. Suppose $(x \in B)$:

9. Thus $x \in C$ — $\vee_{\mathcal{E}}$, lines 2,3-5,6-8
10. $(x \in (A \cup B)) \rightarrow (x \in C)$ — $\rightarrow_{\mathcal{I}}$, lines 2-9
11. $(A \subseteq C) \wedge (B \subseteq C) \rightarrow ((A \cup B) \subseteq C)$ — $\rightarrow_{\mathcal{I}}$, lines 1-10

A more formal version of that proof

Theorem

If $A \subseteq C$ and $B \subseteq C$ then $(A \cup B) \subseteq C$

1. Suppose $(x \in A) \to (x \in C)$ and $(x \in B) \to (x \in C)$:
2. Suppose $(x \in A) \vee (x \in B)$:
3. Suppose $(x \in A)$:
4. But $(x \in A) \to (x \in C)$ — $\wedge_{\mathcal{E}1}$, line 1
5. So $(x \in C)$ — $\to_{\mathcal{E}}$, lines 3,4
6. Suppose $(x \in B)$:
7. But $(x \in B) \to (x \in C)$ — $\wedge_{\mathcal{E}2}$, line 1
8. So $(x \in C)$ — $\to_{\mathcal{E}}$, lines 6,7
9. Thus $x \in C$ — $\vee_{\mathcal{E}}$, lines 2,3-5,6-8
10. $(x \in (A \cup B)) \to (x \in C)$ — $\to_{\mathcal{I}}$, lines 2-9
11. $(A \subseteq C) \wedge (B \subseteq C) \to ((A \cup B) \subseteq C)$ — $\to_{\mathcal{I}}$, lines 1-10

Duality between ‘and’ and 'or’

Note that the introduction/elimination rules for ‘and’ and 'or’ seem to *reflect* each other:

Duality between ‘and’ and ’or’

Note that the introduction/elimination rules for ‘and’ and ’or’ seem to *reflect* each other:

- The introduction rule for ‘or’ and the elimination rule for ‘and’ give you the choice (which to prove/use).
- The elimination rule for ‘or’ and the introduction rule for ‘and’ inist you deal with both possibilities.

Duality between ‘and’ and ’or’

Note that the introduction/elimination rules for ‘and’ and ’or’ seem to *reflect* each other:

- The introduction rule for ‘or’ and the elimination rule for ‘and’ give you the choice (which to prove/use).
- The elimination rule for ‘or’ and the introduction rule for ‘and’ inist you deal with both possibilities.
- ... a little bit similar to the way they interact in de Morgan’s laws

Duality between ‘and’ and ’or’

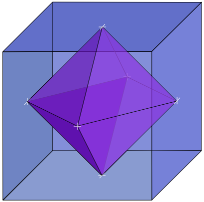
Note that the introduction/elimination rules for ‘and’ and ’or’ seem to *reflect* each other:

- The introduction rule for ‘or’ and the elimination rule for ‘and’ give you the choice (which to prove/use).
- The elimination rule for ‘or’ and the introduction rule for ‘and’ inist you deal with both possibilities.
- ... a little bit similar to the way they interact in de Morgan’s laws

The connectives ‘and’ and ’or’ are not exactly logical opposites: instead we say that are dual to each other.

Other examples of dual concepts:

- for-all and there-exists
- satisfiability and validity
- set theory: union and intersection
- platonic solids: cube and octahedron



Negation

- Dealing with negation is a little awkward...

- To assert "$\neg A$" must be the same as saying "A is false", but we only have rules to prove things that are *true*.

Negation

- Dealing with negation is a little awkward...
- To assert "$\neg A$" must be the same as saying "A is false", but we only have rules to prove things that are *true*.

- The usual approach is to work by means of a contradiction:

  if we assume A and derive a contradiction,
  then it must have been wrong to assume A,
  so deduce $\neg A$

- We use the symbol $\perp$ to denote "contradiction".

Formal proof rule for ‘not’

For the moment we will adopt just an *introduction rule* for negation:

$$\frac{\boxed{\begin{array}{c}\text{Suppose } A: \\ \vdots \\ \perp\end{array}}}{\neg A}\ \neg\mathcal{I}$$

- To prove $\neg A$:

  Assume A, and then derive a contradiction.

Formal proof rule for 'not'

For the moment we will adopt just an *introduction rule* for negation:

$$\dfrac{\boxed{\begin{array}{c}\text{Suppose } A : \\ \vdots \\ \bot\end{array}}}{\neg A}\ \neg\mathcal{I}$$

- To prove $\neg A$:

  Assume A, and then derive a contradiction.

- So how do we derive a contradiction?

Formal proof rules for ‘contradiction’

$$\frac{B \qquad \neg B}{\perp} \perp_{\mathcal{I}} \qquad\qquad \frac{\perp}{B} \perp_{\mathcal{E}}$$

Explanation:

- Introduction:
  You get a contradiction by
  proving both B and $\neg B$, for some formula B.
- Elimination:
  If you have a contradiction in your proof,
  then anything can be deduced.

Formal proof rules for 'contradiction'

$$\frac{B \qquad \neg B}{\perp}\ \perp_{\mathcal{I}} \qquad\qquad \frac{\perp}{B}\ \perp_{\mathcal{E}}$$

Notes

- Introduction:
  The introduction rule for contradiction is also a sort of *elimination rule* for negation:

  If you have a premise of the form $\neg B$,
  try to prove B, and then deduce a contradiction.

- Elimination:
  It's rarely useful to deduce just "anything" from $\perp$.
  Typically this rule is used to tidy up impossible cases in a proof.

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

9. $(x^2 + y = 13) \wedge (y \neq 4) \to (x \neq 3)$

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

9. $(x^2 + y = 13) \land \neg(y = 4) \rightarrow \neg(x = 3)$

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \land \neg(y = 4)$:

8. $\quad \neg(x = 3)$
9. $(x^2 + y = 13) \land \neg(y = 4) \to \neg(x = 3)$ $\quad\to_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:

7. $\perp$
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:
3. $x^2 + y = 13$ — $\wedge_{\mathcal{E}1}$, line 1

7. $\perp$
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:
3. $x^2 + y = 13$ — $\wedge_{\mathcal{E}1}$, line 1
4. $3^2 + y = 13$ — "substitution", lines 2,3
7. $\perp$
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:
3. $x^2 + y = 13$ — $\wedge_{\mathcal{E}1}$, line 1
4. $3^2 + y = 13$ — "substitution", lines 2,3
5. $y = 4$ — "arithmetic", line 4
7. $\bot$
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:
3. $x^2 + y = 13$ — $\wedge_{\mathcal{E}1}$, line 1
4. $3^2 + y = 13$ — "substitution", lines 2,3
5. $y = 4$ — "arithmetic", line 4
6. $\neg(y = 4)$ — $\wedge_{\mathcal{E}2}$, line 1
7. $\bot$
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A formal(-ish) example of a proof using negation

Theorem

If $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$

Proof.

1. Suppose $(x^2 + y = 13) \wedge \neg(y = 4)$:
2. Suppose $x = 3$:
3. $x^2 + y = 13$ — $\wedge_{\mathcal{E}1}$, line 1
4. $3^2 + y = 13$ — "substitution", lines 2,3
5. $y = 4$ — "arithmetic", line 4
6. $\neg(y = 4)$ — $\wedge_{\mathcal{E}2}$, line 1
7. $\perp$ — $\perp_{\mathcal{I}}$, lines 5,6
8. $\neg(x = 3)$ — $\neg_{\mathcal{I}}$, lines 2-7
9. $(x^2 + y = 13) \wedge \neg(y = 4) \rightarrow \neg(x = 3)$ — $\rightarrow_{\mathcal{I}}$, lines 1-8

A less formal example of a proof using negation

Theorem

The square root of 2 is irrational.

A less formal example of a proof using negation

Theorem

The square root of 2 is irrational.

Proof.

- So $\sqrt{2}$ is not rational.

A less formal example of a proof using negation

Theorem

The square root of 2 is irrational.

Proof.

- Suppose that $\sqrt{2}$ *is* rational.
- Contradiction!
- So $\sqrt{2}$ is not rational.

A less formal example of a proof using negation

Theorem

The square root of 2 is irrational.

Proof.

- Suppose that $\sqrt{2}$ *is* rational.
- Then it can be written as a/b for some integers a and b, and we can assume that a and b have no common factors.
- But if $\sqrt{2} = a/b$, then $a^2 = 2b^2$.
- Therefore a^2 must be even. Therefore a must be even.
- This means that b must be odd.
- However if a is even, then a^2 must be a multiple of 4.
- Since $a^2 = 2b^2$, $2b^2$ is also a multiple of 4.
- Therefore b^2 is even, and thus b is even.
- Contradiction!
- So $\sqrt{2}$ is not rational.

A less formal example of a proof using negation

Theorem

The square root of 2 is irrational.

Proof.

- Suppose that $\sqrt{2}$ *is* rational.
- Then it can be written as a/b for some integers a and b, and we can assume that a and b have no common factors.
- But if $\sqrt{2} = a/b$, then $a^2 = 2b^2$.
- Therefore a^2 must be even. Therefore a must be even.
- This means that b must be odd.
- However if a is even, then a^2 must be a multiple of 4.
- Since $a^2 = 2b^2$, $2b^2$ is also a multiple of 4.
- Therefore b^2 is even, and thus b is even.
- Contradiction!
- So $\sqrt{2}$ is not rational.

Elimination rule for 'not' (Classical Logic Only)

- We deferred discussing the elimination rule for negation as it is not accepted in all kinds of logic.
- However, it is accepted in *classical logic*.
- Elimination rule:

$$\frac{\neg\neg A}{A}\,\neg\mathcal{E}$$

Elimination rule for 'not' (Classical Logic Only)

- We deferred discussing the elimination rule for negation as it is not accepted in all kinds of logic.
- However, it is accepted in *classical logic*.
- Elimination rule:

$$\frac{\neg\neg A}{A}\ \neg\mathcal{E}$$

- Do you believe this rule is valid?

Brouwer's Intuitionism

L. E. J. Brouwer
(1881-1966)

- Developed intuitionism (philosophical view of the foundation of mathematics)
- "On the significance of the principle of excluded middle in mathematics, especially in function theory.", 1923.
- Ideas developed into *constructive logic* by Kolmogorov and Heyting ("BHK").
- Close links with the *lambda-calculus* (via the Curry-Howard isomorphism)

Some rules that are equivalent to $\neg_{\mathcal{E}}$

"Law of the Excluded Middle"

$$\frac{\cdot}{A \vee \neg A} \; LEM$$

This is a direct consequence of $\neg_{\mathcal{I}}$ (tricky proof), and is the most famous rule that is rejected by constructive logic.

(Full) "Proof by contradiction"

$$\frac{\boxed{\begin{array}{c}\text{Suppose } \neg A : \\ \vdots \\ \bot\end{array}}}{A} \; PBC$$

This *PBC* rule is just $\neg_{\mathcal{I}}$ followed immediately by $\neg_{\mathcal{E}}$.

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- So a^b is rational

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational)*.
- So a^b is rational

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational).*
- Either b^b is rational or it is not. *LEM*.

- So a^b is rational

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational)*.
- Either b^b is rational or it is not. *LEM*.
- - Suppose b^b is rational:
- - Suppose b^b is not rational:
- So a^b is rational either way. $\vee_{\mathcal{E}}$

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational).*
- Either b^b is rational or it is not. *LEM.*
- \- Suppose b^b is rational:
- Easy: choose $a = b$, *(so a is not rational).*
- and thus $a^b = b^b$ is rational
- \- Suppose b^b is not rational:

- So a^b is rational either way. $\vee_{\mathcal{E}}$

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational)*.
- Either b^b is rational or it is not. *LEM*.
- - Suppose b^b is rational:
- Easy: choose $a = b$, *(so a is not rational)*.
- and thus $a^b = b^b$ is rational
- - Suppose b^b is not rational:
- Then choose $a = b^b = (\sqrt{2}^{\sqrt{2}})$ *(so a is not rational)*.
- So a^b is rational either way. $\vee_{\mathcal{E}}$

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Proof.

- Let $b = \sqrt{2}$ *(so b is not rational).*
- Either b^b is rational or it is not. *LEM*.
- \- Suppose b^b is rational:
- Easy: choose $a = b$, *(so a is not rational).*
- and thus $a^b = b^b$ is rational
- \- Suppose b^b is not rational:
- Then choose $a = b^b = (\sqrt{2}^{\sqrt{2}})$ *(so a is not rational).*
- But now both a and b are irrational,
- and $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = 2$, which is rational.
- So a^b is rational either way. $\vee_{\mathcal{E}}$

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Q: Is this proof OK?

Example of a proof using LEM

Theorem

There exist irrational numbers a and b such that a^b is rational.

Q: Is this proof OK?

A: (classical)
Yes, it follows the rules of natural deduction.

A: (constructive)
No, you haven't given me *actual* irrationals a and b such that a^b is rational.