CS172: Computer Systems II

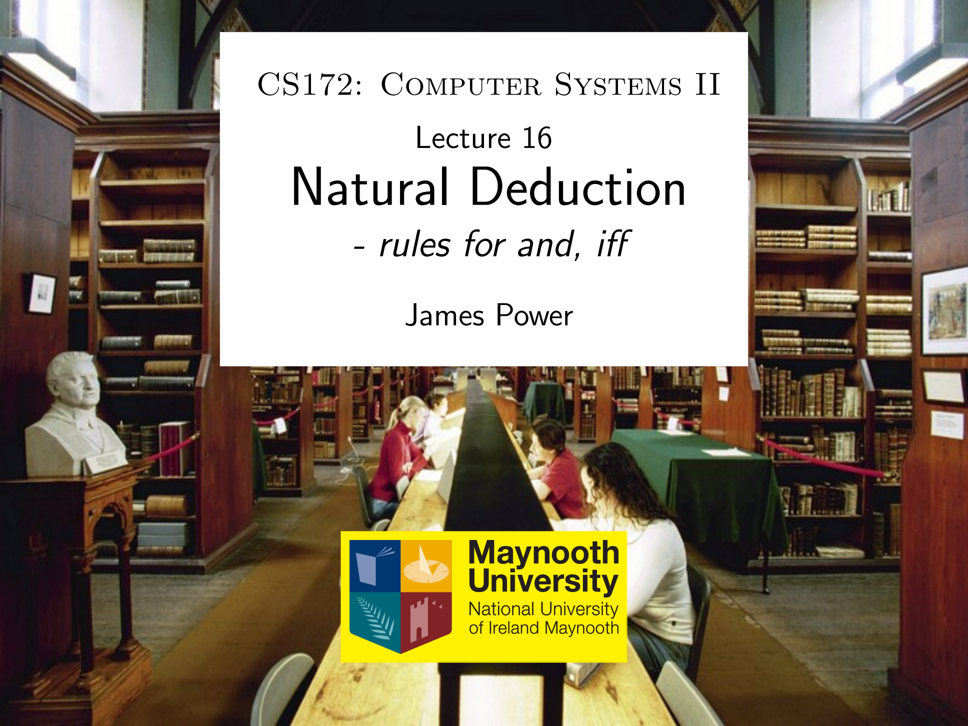
Lecture 16

Natural Deduction

- rules for and, iff

James Power

Maynooth University
National University of Ireland Maynooth



Some notation

Existing notation: "models"

- When we write

$$\varphi_1, \ldots, \varphi_n \models \psi$$

we mean: in any model where $\varphi_1, \ldots, \varphi_n$ are all true, then so is ψ.

Some notation

Existing notation: "models"

- When we write

$$\varphi_1, \ldots, \varphi_n \models \psi$$

we mean: in any model where $\varphi_1, \ldots, \varphi_n$ are all true, then so is ψ.

New notation: "entails"

- We will write

$$\varphi_1, \ldots, \varphi_n \vdash \psi$$

to mean: we can construct a natural deduction proof starting with the premises $\varphi_1, \ldots, \varphi_n$ and finishing with the conclusion ψ.

Another example of a proof

Show that: $P \rightarrow Q, Q \rightarrow R \vdash P \rightarrow R$

Another example of a proof

Show that: $P \to Q, Q \to R \vdash P \to R$

Formal Proof.

1. $P \to Q$ — Premise
2. $Q \to R$ — Premise
3. Suppose P :
4. $\quad Q$ — $\to_{\mathcal{E}}$ lines 3,1
5. $\quad R$ — $\to_{\mathcal{E}}$ lines 4,2
6. $P \to R$ — $\to_{\mathcal{I}}$ lines 3-5

$\square$

Another example of a proof

Show that: $P \to Q, Q \to R \vdash P \to R$

Formal Proof.

1. $P \to Q$ — Premise
2. $Q \to R$ — Premise
3. Suppose P : — (making a local assumption)
4. $\boxed{\textit{indent}}$ Q — $\to_{\mathcal{E}}$ lines 3,1
5. $\boxed{\textit{indent}}$ R — $\to_{\mathcal{E}}$ lines 4,2
6. $P \to R$ — local assumption now discharged by: $\to_{\mathcal{I}}$ lines 3-5

□

- I use **indentation** in lines 4 and 5 to show the *scope* of the local assumption P.

Another example of a proof

Show that: $P \to Q, Q \to R \vdash P \to R$

Formal Proof.

1. $P \to Q$ — Premise
2. $Q \to R$ — Premise
3. Suppose P :
4. $\quad Q$ — $\to_{\mathcal{E}}$ lines 3,1
5. $\quad R$ — $\to_{\mathcal{E}}$ lines 4,2
6. $P \to R$ — $\to_{\mathcal{I}}$ lines 3-5

$\square$

- This proof shows that implies is a *transitive* relation.

Proofs using 'and'

The rules for dealing with conjunction (i.e. 'and') are pretty straightforward:

- Introduction: To prove $A \wedge B$:
  you must prove A and you must also prove B.

- Elimination: If you know $A \wedge B$:
  then you can deduce that A is true,
  also you can deduce that B is true
  (you can deduce both, if you like).

Formal proof rules for 'and'

$$\frac{A \qquad B}{A \wedge B}\wedge_{\mathcal{I}} \qquad\qquad \frac{A \wedge B}{A}\wedge_{\mathcal{E}1} \qquad \frac{A \wedge B}{B}\wedge_{\mathcal{E}2}$$

Formal proof rules for 'and'

$$\frac{A \qquad B}{A \land B}\land_{\mathcal{I}} \qquad\qquad \frac{A \land B}{A}\land_{\mathcal{E}1} \qquad \frac{A \land B}{B}\land_{\mathcal{E}2}$$

- There are *two* elimination rules, so use whichever one suits your proof. You can use both of them if you like.

Example of a proof using 'and'

Show that: $P \land Q \vdash Q \land P$

Example of a proof using 'and'

Show that: $P \wedge Q \vdash Q \wedge P$

Formal Proof.

1	$P \wedge Q$	Premise
2	Q	$\wedge_{\mathcal{E}2}$, line 1
3	P	$\wedge_{\mathcal{E}1}$, line 1
4	$Q \wedge P$	$\wedge_{\mathcal{I}}$, lines 2,3

$\square$

Example of a proof using 'and'

Show that: $P \wedge Q \vdash Q \wedge P$

Formal Proof.

1	$P \wedge Q$	Premise
2	Q	$\wedge_{\mathcal{E}2}$, line 1
3	P	$\wedge_{\mathcal{E}1}$, line 1
4	$Q \wedge P$	$\wedge_{\mathcal{I}}$, lines 2,3

$\square$

This proof shows that 'and' is a *commutative* operator.

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
-
-
-
-
-
-
-
- $\quad\quad \ldots\ldots$
- $A \subseteq (B \setminus C)$

$\square$

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
-
-
-
-
-
-
-
- $\quad\quad \ldots\ldots$
- $(\forall x \cdot (x \in A) \rightarrow (x \in (B \setminus C)))$

$\square$

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
-
-
-
-
-
-
-
- $\qquad \cdots\cdots$
- $(\forall x \cdot (x \in A) \to ((x \in B) \wedge \neg(x \in C)))$

$\square$

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
-
-
-
-
-
-
- $\quad (x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C))$
- $\quad \cdots\cdots$
- $(\forall x \cdot (x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C)))$

□

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
-
-
-
-
-
-
- $(x \in A) \to ((x \in B) \land \neg(x \in C))$ $\qquad \to_{\mathcal{I}}$, lines ...
- $\cdots\cdots$
- $(\forall x \cdot (x \in A) \to ((x \in B) \land \neg(x \in C)))$

$\square$

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
- Suppose $(x \in A)$:
-
-
-
-
- $(x \in B) \wedge \neg(x \in C)$
- $(x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C))$ $\quad\rightarrow_{\mathcal{I}}$, lines ...
- $\cdots\cdots$
- $(\forall x \cdot (x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C)))$

□

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
- Suppose $(x \in A)$:
-
-
-
-
- $(x \in B) \wedge \neg(x \in C)$ $\quad \wedge_{\mathcal{I}}$, lines ...
- $(x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C))$ $\quad \rightarrow_{\mathcal{I}}$, lines ...
- $\cdots\cdots$
- $(\forall x \cdot (x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C)))$

$\square$

(Partial) Example of a proof using 'and' and 'implies'...

Theorem

Suppose that $A \subseteq B$, and A and C are disjoint. Then $A \subseteq (B \setminus C)$.

Proof.

- $\cdots$
- Suppose $(x \in A)$:
- $\cdots\cdots$
- $(x \in B)$
- $\cdots\cdots$
- $\neg(x \in C)$
- $(x \in B) \wedge \neg(x \in C)$ — $\wedge_{\mathcal{I}}$, lines ...
- $(x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C))$ — $\rightarrow_{\mathcal{I}}$, lines ...
- $\cdots\cdots$
- $(\forall x \cdot (x \in A) \rightarrow ((x \in B) \wedge \neg(x \in C)))$

$\square$

Proofs using equivalence (‘iff’)

The rules for dealing with equivalence (i.e. ‘iff’) are also straightforward, and are closely related to the last two set of rules:

- Introduction:
  To prove $A \leftrightarrow B$:
  you must prove $A \rightarrow B$ and you must also prove $B \rightarrow A$.

- Elimination: If you know $A \leftrightarrow B$:
  then you can deduce that $A \rightarrow B$ is true,
  also you can deduce that $B \rightarrow A$ is true
  (you can deduce both, if you like).

Formal proof rules for 'iff'

$$\frac{A \to B \qquad B \to A}{A \leftrightarrow B} \leftrightarrow_{\mathcal{I}} \qquad\qquad \frac{A \leftrightarrow B}{A \to B} \leftrightarrow_{\mathcal{E}1} \qquad \frac{A \leftrightarrow B}{B \to A} \leftrightarrow_{\mathcal{E}2}$$

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even)

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\qquad \leftrightarrow_{\mathcal{I}}$, lines ...

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- (x is even) $\rightarrow$ (x^2 is even)
- (x^2 is even) $\rightarrow$ (x is even)
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\qquad \leftrightarrow_{\mathcal{I}}$, lines ...

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- (x is even) $\rightarrow$ (x^2 is even) $\quad\quad \rightarrow_{\mathcal{I}}$, lines ...
- (x^2 is even) $\rightarrow$ (x is even)
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\quad\quad \leftrightarrow_{\mathcal{I}}$, lines ...

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- Suppose x is even :
- $\quad \cdots\cdots$
- $\quad x^2$ is even
- (x is even) $\rightarrow$ (x^2 is even) $\quad \rightarrow_{\mathcal{I}}$, lines ...
- (x^2 is even) $\rightarrow$ (x is even)
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\quad \leftrightarrow_{\mathcal{I}}$, lines ...

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- Suppose x is even :
- $\quad \cdots\cdots$
- $\quad x^2$ is even
- (x is even) $\rightarrow$ (x^2 is even) $\quad\quad \rightarrow_{\mathcal{I}}$, lines ...
- (x^2 is even) $\rightarrow$ (x is even) $\quad\quad \rightarrow_{\mathcal{I}}$, lines ...
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\quad\quad \leftrightarrow_{\mathcal{I}}$, lines ...

(Partial) Example of a proof using 'iff'

Theorem

Suppose that x is an integer. Then x is even iff x^2 is even.

Proof.

- $\cdots$
- Suppose x is even :
- $\quad\quad \cdots\cdots$
- $\quad\quad x^2$ is even
- (x is even) $\rightarrow$ (x^2 is even) $\quad\quad \rightarrow_{\mathcal{I}}$, lines ...
- Suppose x^2 is even :
- $\quad\quad \cdots\cdots$
- $\quad\quad x$ is even
- (x^2 is even) $\rightarrow$ (x is even) $\quad\quad \rightarrow_{\mathcal{I}}$, lines ...
- $\cdots$
- (x is even) $\leftrightarrow$ (x^2 is even) $\quad\quad \leftrightarrow_{\mathcal{I}}$, lines ...