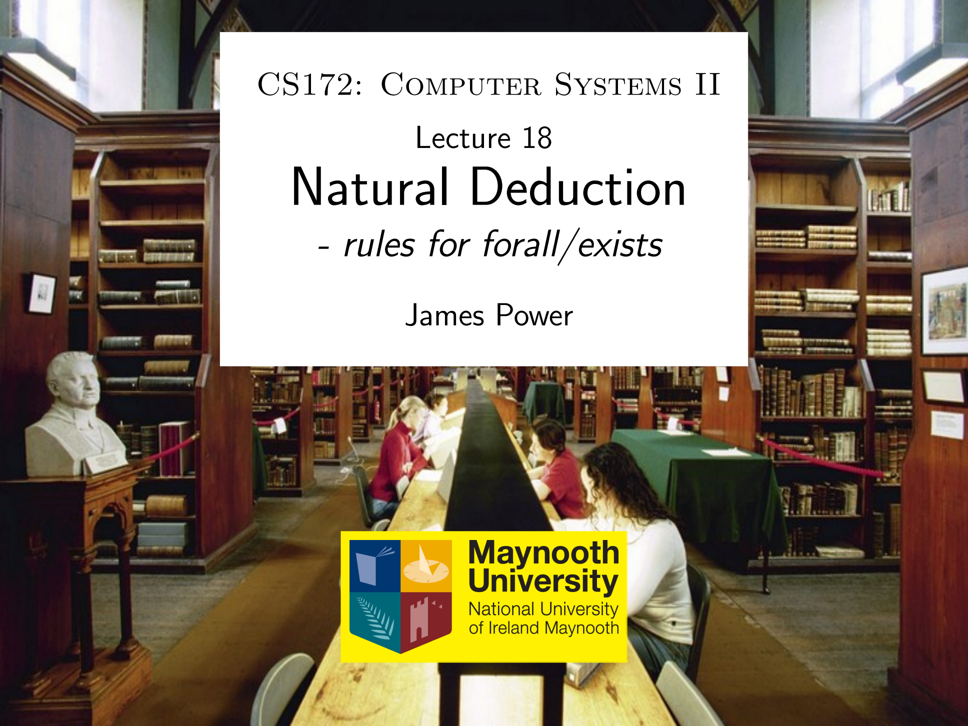


CS172: Computer Systems II

Lecture 18

Natural Deduction

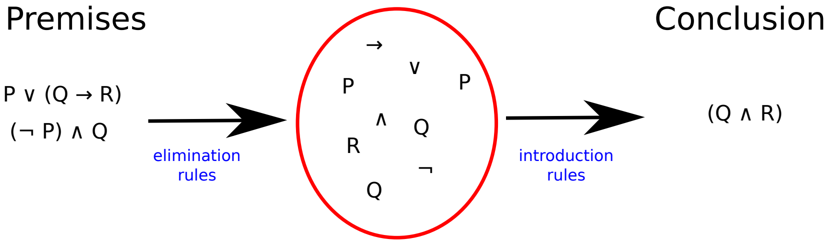
- rules for forall/exists

James Power

Maynooth University
National University of Ireland Maynooth

Dealing with predicate logic

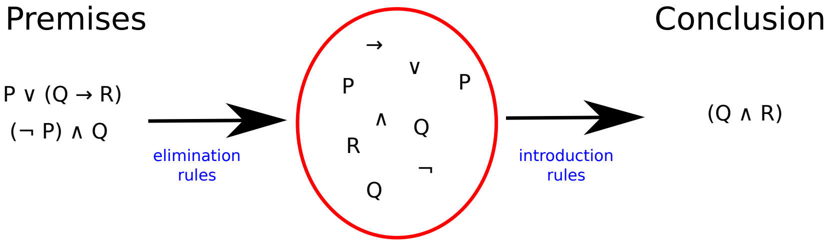
Reminder:



- For **propositional logic** we used the elimination/introduction rules to break down and build up formula based on the *connectives*.

Dealing with predicate logic

Reminder:



- For **propositional logic** we used the elimination/introduction rules to break down and build up formula based on the *connectives*.
- For **predicate logic** we will use the elimination/introduction rules to break down and build up formula based on the *quantifiers*.

Dealing with quantifiers

- Example #1:
  if we had a **premise** like $(\forall x \cdot Px \vee Qx)$ then we'd need to:
  - Somehow "remove" the quantifier to get $Px \vee Qx$
  - The use the ordinary rules for propositional logic (presumably $\vee_{\mathcal{E}}$), since it's now just a disjunction.

Dealing with quantifiers

- Example #1:

  if we had a **premise** like $(\forall x \cdot Px \vee Qx)$ then we'd need to:
  - Somehow "remove" the quantifier to get $Px \vee Qx$
  - The use the ordinary rules for propositional logic (presumably $\vee_{\mathcal{E}}$), since it's now just a disjunction.

- Example #2:

  if we had a **conclusion** like $(\forall x \cdot Px \wedge Qx)$ then we'd need to:
  - First show $Px \wedge Qx$ using the ordinary rules for propositional logic (presumably $\wedge_{\mathcal{I}}$)
  - Then "put back" the quantifier to get the conclusion we want.

Be careful with the use of variables

- The introduction and elimination rules for predicate logic allow us to "remove" and "put back" the quantifiers.
- This will have the side-effect of introducing *unquantified variables* into our proof.
- The introduction and elimination rules have **strict conditions** on what you can do with the variables: these conditions are essential to make sure that the system works correctly.

It's all about the variables.

Formal proof rules for 'for all'

$$\frac{\boxed{\begin{array}{c}\text{Suppose } i: \\ \vdots \\ Pi\end{array}}}{(\forall x \cdot Px)}\ \forall_{\mathcal{I}} \qquad\qquad \frac{(\forall x \cdot Px)}{Pi}\ \forall_{\mathcal{E}}$$

Very Important:

- Introduction rule: In $\forall_{\mathcal{I}}$ the variable i must be a **new variable** that will be *local* to the sub-proof.
- Elimination rule: In $\forall_{\mathcal{E}}$, i is any **current variable** that is *already* in scope in the proof.

Formal proof rules for 'for all'

$$\dfrac{\boxed{\begin{array}{c}\text{Suppose } i: \\ \vdots \\ Pi\end{array}}}{(\forall x \cdot Px)}\ \forall_{\mathcal{I}} \qquad\qquad \dfrac{(\forall x \cdot Px)}{Pi}\ \forall_{\mathcal{E}}$$

Notes:

- Introduction rule: to *generalise* a statement, the variable must not be constrained through involvment in any undischarged assumptions.
- Elimination rule: Here, the $\forall$ statement is acting like a *template*, allowing you to deduce new facts for all your existing variables.

Example of a formal proof with ‘for all’

Theorem

$$\frac{\textit{All politicians are rich.} \quad \textit{All students are politicians.}}{\textit{All students are rich.}}$$

Example of a formal proof with ‘for all’

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\forall y \cdot Sy \rightarrow Py) \qquad \vdash \qquad (\forall z \cdot Sz \rightarrow Rz)$

Proof.

□

Example of a formal proof with 'for all'

Theorem

$(\forall x \cdot Px \to Rx), \quad (\forall y \cdot Sy \to Py) \quad \vdash \quad (\forall z \cdot Sz \to Rz)$

Proof.

1. $(\forall x \cdot Px \to Rx)$ Premise
2. $(\forall y \cdot Sy \to Py)$ Premise

10. $(\forall z \cdot Sz \to Rz)$

□

Example of a formal proof with 'for all'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\forall\, y \cdot Sy \rightarrow Py) \qquad \vdash \qquad (\forall\, z \cdot Sz \rightarrow Rz)$

Proof.

1. $(\forall\, x \cdot Px \rightarrow Rx)$ — Premise
2. $(\forall\, y \cdot Sy \rightarrow Py)$ — Premise
3. Suppose i :

9. $\quad Si \rightarrow Ri$
10. $(\forall\, z \cdot Sz \rightarrow Rz)$ — $\forall_{\mathcal{I}}$, lines 3-10

□

Example of a formal proof with 'for all'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\forall\, y \cdot Sy \rightarrow Py) \quad \vdash \quad (\forall\, z \cdot Sz \rightarrow Rz)$

Proof.

1. $(\forall\, x \cdot Px \rightarrow Rx)$ — Premise
2. $(\forall\, y \cdot Sy \rightarrow Py)$ — Premise
3. Suppose i :
4.   Suppose Si :

8. Ri
9. $Si \rightarrow Ri$ — $\rightarrow_{\mathcal{I}}$, lines 4-8
10. $(\forall\, z \cdot Sz \rightarrow Rz)$ — $\forall_{\mathcal{I}}$, lines 3-10

□

Example of a formal proof with 'for all'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\forall y \cdot Sy \rightarrow Py) \qquad \vdash \qquad (\forall z \cdot Sz \rightarrow Rz)$

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ — Premise
2. $(\forall y \cdot Sy \rightarrow Py)$ — Premise
3. Suppose i :
4. Suppose Si :
5. $Si \rightarrow Pi$ — $\forall_{\mathcal{E}}$, lines 3,2

8. Ri
9. $Si \rightarrow Ri$ — $\rightarrow_{\mathcal{I}}$, lines 4-8
10. $(\forall z \cdot Sz \rightarrow Rz)$ — $\forall_{\mathcal{I}}$, lines 3-10

□

Example of a formal proof with 'for all'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\forall\, y \cdot Sy \rightarrow Py) \qquad \vdash \qquad (\forall\, z \cdot Sz \rightarrow Rz)$

Proof.

1	$(\forall\, x \cdot Px \rightarrow Rx)$	Premise
2	$(\forall\, y \cdot Sy \rightarrow Py)$	Premise
3	Suppose i :	
4	Suppose Si :	
5	$Si \rightarrow Pi$	$\forall_{\mathcal{E}}$, lines 3,2
6	Pi	$\rightarrow_{\mathcal{E}}$, lines 4,5
8	Ri	
9	$Si \rightarrow Ri$	$\rightarrow_{\mathcal{I}}$, lines 4-8
10	$(\forall\, z \cdot Sz \rightarrow Rz)$	$\forall_{\mathcal{I}}$, lines 3-10

□

Example of a formal proof with 'for all'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\forall y \cdot Sy \rightarrow Py) \qquad \vdash \qquad (\forall z \cdot Sz \rightarrow Rz)$

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ — Premise
2. $(\forall y \cdot Sy \rightarrow Py)$ — Premise
3. Suppose i :
4. Suppose Si :
5. $Si \rightarrow Pi$ — $\forall_{\mathcal{E}}$, lines 3,2
6. Pi — $\rightarrow_{\mathcal{E}}$, lines 4,5
7. $Pi \rightarrow Ri$ — $\forall_{\mathcal{E}}$, lines 3,1
8. Ri
9. $Si \rightarrow Ri$ — $\rightarrow_{\mathcal{I}}$, lines 4-8
10. $(\forall z \cdot Sz \rightarrow Rz)$ — $\forall_{\mathcal{I}}$, lines 3-10

□

Example of a formal proof with 'for all'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\forall\, y \cdot Sy \rightarrow Py) \quad \vdash \quad (\forall\, z \cdot Sz \rightarrow Rz)$

Proof.

1. $(\forall\, x \cdot Px \rightarrow Rx)$ — Premise
2. $(\forall\, y \cdot Sy \rightarrow Py)$ — Premise
3. Suppose i :
4.   Suppose Si :
5. $Si \rightarrow Pi$ — $\forall_{\mathcal{E}}$, lines 3,2
6. Pi — $\rightarrow_{\mathcal{E}}$, lines 4,5
7. $Pi \rightarrow Ri$ — $\forall_{\mathcal{E}}$, lines 3,1
8. Ri — $\rightarrow_{\mathcal{E}}$, lines 6,7
9. $Si \rightarrow Ri$ — $\rightarrow_{\mathcal{I}}$, lines 4-8
10. $(\forall\, z \cdot Sz \rightarrow Rz)$ — $\forall_{\mathcal{I}}$, lines 3-10

□

Example of a mathematical proof with ‘for all’

Theorem

If $A \cap B = A$ *then* $A \subseteq B$.

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ *then* $A \subseteq B$.

Proof.

10. $(A \cap B = A) \rightarrow (A \subseteq B)$

$\square$

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(A \cap B = A)$:

9. $\quad (A \subseteq B)$
10. $(A \cap B = A) \rightarrow (A \subseteq B)$ $\quad \rightarrow_{\mathcal{I}}$, lines 1-10

□

Example of a mathematical proof with ‘for all’

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(\forall x \cdot (x \in A \wedge x \in B) \leftrightarrow (x \in A))$:

9. $\quad (\forall x \cdot x \in A \rightarrow x \in B)$
10. $(A \cap B = A) \rightarrow (A \subseteq B)$ $\quad \rightarrow_{\mathcal{I}}$, lines 1-10

$\square$

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(\forall x \cdot (x \in A \land x \in B) \leftrightarrow (x \in A))$:
2. Suppose i :

8. $i \in A \to i \in B$
9. $(\forall x \cdot x \in A \to x \in B)$ — $\forall_{\mathcal{I}}$, lines 2-8
10. $(A \cap B = A) \to (A \subseteq B)$ — $\to_{\mathcal{I}}$, lines 1-10

$\square$

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(\forall x \cdot (x \in A \wedge x \in B) \leftrightarrow (x \in A))$:
2. Suppose i :
3. Suppose $i \in A$:

7. $i \in B$
8. $i \in A \rightarrow i \in B$ — $\rightarrow_{\mathcal{I}}$, lines 3-7
9. $(\forall x \cdot x \in A \rightarrow x \in B)$ — $\forall_{\mathcal{I}}$, lines 2-8
10. $(A \cap B = A) \rightarrow (A \subseteq B)$ — $\rightarrow_{\mathcal{I}}$, lines 1-10

□

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(\forall x \cdot (x \in A \wedge x \in B) \leftrightarrow (x \in A))$:
2. Suppose i :
3. Suppose $i \in A$:
4. $(i \in A \wedge i \in B) \leftrightarrow (i \in A)$ — $\forall_{\mathcal{E}}$, lines 2,1
7. $i \in B$
8. $i \in A \rightarrow i \in B$ — $\rightarrow_{\mathcal{I}}$, lines 3-7
9. $(\forall x \cdot x \in A \rightarrow x \in B)$ — $\forall_{\mathcal{I}}$, lines 2-8
10. $(A \cap B = A) \rightarrow (A \subseteq B)$ — $\rightarrow_{\mathcal{I}}$, lines 1-10

□

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1. Suppose $(\forall x \cdot (x \in A \wedge x \in B) \leftrightarrow (x \in A))$:
2. Suppose i :
3. Suppose $i \in A$:
4. $(i \in A \wedge i \in B) \leftrightarrow (i \in A)$ — $\forall_{\mathcal{E}}$, lines 2,1
5. $(i \in A) \rightarrow (i \in A \wedge i \in B)$ — $\leftrightarrow_{\mathcal{E}2}$, line 4
7. $i \in B$
8. $i \in A \rightarrow i \in B$ — $\rightarrow_{\mathcal{I}}$, lines 3-7
9. $(\forall x \cdot x \in A \rightarrow x \in B)$ — $\forall_{\mathcal{I}}$, lines 2-8
10. $(A \cap B = A) \rightarrow (A \subseteq B)$ — $\rightarrow_{\mathcal{I}}$, lines 1-10

□

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ then $A \subseteq B$.

Proof.

1	Suppose $(\forall x \cdot (x \in A \wedge x \in B) \leftrightarrow (x \in A))$:	
2	Suppose i :	
3	Suppose $i \in A$:	
4	$(i \in A \wedge i \in B) \leftrightarrow (i \in A)$	$\forall_{\mathcal{E}}$, lines 2,1
5	$(i \in A) \rightarrow (i \in A \wedge i \in B)$	$\leftrightarrow_{\mathcal{E}2}$, line 4
6	$(i \in A \wedge i \in B)$	$\rightarrow_{\mathcal{E}}$, lines 3,5
7	$i \in B$	
8	$i \in A \rightarrow i \in B$	$\rightarrow_{\mathcal{I}}$, lines 3-7
9	$(\forall x \cdot x \in A \rightarrow x \in B)$	$\forall_{\mathcal{I}}$, lines 2-8
10	$(A \cap B = A) \rightarrow (A \subseteq B)$	$\rightarrow_{\mathcal{I}}$, lines 1-10

$\square$

Example of a mathematical proof with 'for all'

Theorem

If $A \cap B = A$ *then* $A \subseteq B$*.*

Proof.

1	Suppose $(\forall x \cdot (x \in A \land x \in B) \leftrightarrow (x \in A))$:	
2	Suppose i :	
3	Suppose $i \in A$:	
4	$(i \in A \land i \in B) \leftrightarrow (i \in A)$	$\forall_{\mathcal{E}}$, lines 2,1
5	$(i \in A) \to (i \in A \land i \in B)$	$\leftrightarrow_{\mathcal{E}2}$, line 4
6	$(i \in A \land i \in B)$	$\to_{\mathcal{E}}$, lines 3,5
7	$i \in B$	$\land_{\mathcal{E}2}$, line 6
8	$i \in A \to i \in B$	$\to_{\mathcal{I}}$, lines 3-7
9	$(\forall x \cdot x \in A \to x \in B)$	$\forall_{\mathcal{I}}$, lines 2-8
10	$(A \cap B = A) \to (A \subseteq B)$	$\to_{\mathcal{I}}$, lines 1-10

$\square$

Formal proof rules for 'there exists'

$$\frac{Pi}{(\exists\, x \cdot Px)}\ \exists_{\mathcal{I}}$$

$$\frac{(\exists\, x \cdot Px) \qquad \boxed{\begin{array}{c}\text{Suppose } i : \\ \text{Suppose } Pi : \\ \vdots \\ C\end{array}}}{C}\ \exists_{\mathcal{E}}$$

Very Important:

- Introduction rule: In $\exists_{\mathcal{I}}$, i is any **current variable** that is *already* in scope in the proof.
- Elimination rule: In $\exists_{\mathcal{E}}$, the variable i must be a **new variable** that will be *local* to the sub-proof.

Formal proof rules for 'there exists'

$$\frac{Pi}{(\exists\, x \cdot Px)}\ \exists_{\mathcal{I}}$$

$$\frac{(\exists\, x \cdot Px) \qquad \boxed{\begin{array}{l}\text{Suppose } i : \\ \text{Suppose } Pi : \\ \qquad \vdots \\ \qquad C\end{array}}}{C}\ \exists_{\mathcal{E}}$$

Notes:

- Introduction rule: easy to use, there are essentially no conditions.
- Elimination rule: A little like $\vee_{\mathcal{E}}$ in shape.

  If we know $(\exists\, x \cdot Px)$, then we know there is something for which P holds: the rule says "let's call it i, and proceed with the proof".

Example of a formal proof with 'there exists'

Theorem

$$\frac{\textit{All politicians are rich.} \quad \textit{Some students are politicians.}}{\textit{Some students are rich.}}$$

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\exists z \cdot Sz \wedge Rz)$

Proof.

Example of a formal proof with ‘there exists’

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\exists z \cdot Sz \wedge Rz)$

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ Premise
2. $(\exists y \cdot Sy \wedge Py)$ Premise

11. $(\exists z \cdot Sz \wedge Rz)$

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \qquad \vdash \qquad (\exists z \cdot Sz \wedge Rz)$

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ — Premise
2. $(\exists y \cdot Sy \wedge Py)$ — Premise
3. Suppose i :
4. Suppose $Si \wedge Pi$:

10. $\quad (\exists z \cdot Sz \wedge Rz)$
11. $(\exists z \cdot Sz \wedge Rz)$ — $\exists_{\mathcal{E}}$, lines 3-10

Example of a formal proof with 'there exists'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\exists\, y \cdot Sy \wedge Py) \qquad \vdash \qquad (\exists\, z \cdot Sz \wedge Rz)$

Proof.

1	$(\forall\, x \cdot Px \rightarrow Rx)$	Premise
2	$(\exists\, y \cdot Sy \wedge Py)$	Premise
3	Suppose i :	
4	Suppose $Si \wedge Pi$:	
5	$\quad Si$	$\wedge_{\mathcal{E}1}$, line 4
6	$\quad Pi$	$\wedge_{\mathcal{E}2}$, line 4
10	$\quad (\exists\, z \cdot Sz \wedge Rz)$	
11	$(\exists\, z \cdot Sz \wedge Rz)$	$\exists_{\mathcal{E}}$, lines 3-10

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\exists z \cdot Sz \wedge Rz)$

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ — Premise
2. $(\exists y \cdot Sy \wedge Py)$ — Premise
3. Suppose i :
4. Suppose $Si \wedge Pi$:
5. $\quad Si$ — $\wedge_{\mathcal{E}1}$, line 4
6. $\quad Pi$ — $\wedge_{\mathcal{E}2}$, line 4
7. $\quad Pi \rightarrow Ri$ — $\forall_{\mathcal{E}}$, lines 3,1

10. $\quad (\exists z \cdot Sz \wedge Rz)$
11. $(\exists z \cdot Sz \wedge Rz)$ — $\exists_{\mathcal{E}}$, lines 3-10

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \to Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\exists z \cdot Sz \wedge Rz)$

Proof.

1. $(\forall x \cdot Px \to Rx)$ — Premise
2. $(\exists y \cdot Sy \wedge Py)$ — Premise
3. Suppose i :
4. Suppose $Si \wedge Pi$:
5. Si — $\wedge_{\mathcal{E}1}$, line 4
6. Pi — $\wedge_{\mathcal{E}2}$, line 4
7. $Pi \to Ri$ — $\forall_{\mathcal{E}}$, lines 3,1
8. Ri — $\to_{\mathcal{E}}$, lines 6,7

10. $(\exists z \cdot Sz \wedge Rz)$
11. $(\exists z \cdot Sz \wedge Rz)$ — $\exists_{\mathcal{E}}$, lines 3-10

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \qquad \vdash \qquad (\exists z \cdot Sz \wedge Rz)$

Proof.

1	$(\forall x \cdot Px \rightarrow Rx)$	Premise
2	$(\exists y \cdot Sy \wedge Py)$	Premise
3	Suppose i :	
4	Suppose $Si \wedge Pi$:	
5	$\quad Si$	$\wedge_{\mathcal{E}1}$, line 4
6	$\quad Pi$	$\wedge_{\mathcal{E}2}$, line 4
7	$\quad Pi \rightarrow Ri$	$\forall_{\mathcal{E}}$, lines 3,1
8	$\quad Ri$	$\rightarrow_{\mathcal{E}}$, lines 6,7
9	$\quad Si \wedge Ri$	$\wedge_{\mathcal{I}}$, lines 5,8
10	$\quad (\exists z \cdot Sz \wedge Rz)$	
11	$(\exists z \cdot Sz \wedge Rz)$	$\exists_{\mathcal{E}}$, lines 3-10

Example of a formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\exists z \cdot Sz \wedge Rz)$

Proof.

1	$(\forall x \cdot Px \rightarrow Rx)$	Premise
2	$(\exists y \cdot Sy \wedge Py)$	Premise
3	Suppose i :	
4	Suppose $Si \wedge Pi$:	
5	$\quad Si$	$\wedge_{\mathcal{E}1}$, line 4
6	$\quad Pi$	$\wedge_{\mathcal{E}2}$, line 4
7	$\quad Pi \rightarrow Ri$	$\forall_{\mathcal{E}}$, lines 3,1
8	$\quad Ri$	$\rightarrow_{\mathcal{E}}$, lines 6,7
9	$\quad Si \wedge Ri$	$\wedge_{\mathcal{I}}$, lines 5,8
10	$\quad (\exists z \cdot Sz \wedge Rz)$	$\exists_{\mathcal{I}}$, line 9
11	$(\exists z \cdot Sz \wedge Rz)$	$\exists_{\mathcal{E}}$, lines 3-10

Example of a wrong formal proof with 'there exists'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\exists\, y \cdot Sy \wedge Py) \quad \vdash \quad (\forall\, z \cdot Sz \wedge Rz)$ *Not valid!*

Example of a wrong formal proof with 'there exists'

Theorem

$(\forall x \cdot Px \rightarrow Rx), \quad (\exists y \cdot Sy \wedge Py) \quad \vdash \quad (\forall z \cdot Sz \wedge Rz)$ *Not valid!*

Proof.

1. $(\forall x \cdot Px \rightarrow Rx)$ — Premise
2. $(\exists y \cdot Sy \wedge Py)$ — Premise
3. Suppose i :
4. Suppose $Si \wedge Pi$:
5. $\quad Si$ — $\wedge_{\mathcal{E}1}$, line 4
6. $\quad Pi$ — $\wedge_{\mathcal{E}2}$, line 4
7. $\quad Pi \rightarrow Ri$ — $\forall_{\mathcal{E}}$, lines 3,1
8. $\quad Ri$ — $\rightarrow_{\mathcal{E}}$, lines 6,7
9. $\quad Si \wedge Ri$ — $\wedge_{\mathcal{I}}$, lines 5,8
10. $\quad (\forall z \cdot Sz \wedge Rz)$ — $\forall_{\mathcal{I}}$, line 9
11. $(\forall z \cdot Sz \wedge Rz)$ — $\exists_{\mathcal{E}}$, lines 3-10

Example of a wrong formal proof with 'there exists'

Theorem

$(\forall\, x \cdot Px \rightarrow Rx), \quad (\exists\, y \cdot Sy \wedge Py) \quad \vdash \quad (\forall\, z \cdot Sz \wedge Rz)$ *Not valid!*

Proof.

1	$(\forall\, x \cdot Px \rightarrow Rx)$	Premise
2	$(\exists\, y \cdot Sy \wedge Py)$	Premise
3	Suppose i :	
4	Suppose $Si \wedge Pi$:	
5	$\quad Si$	$\wedge_{\mathcal{E}1}$, line 4
6	$\quad Pi$	$\wedge_{\mathcal{E}2}$, line 4
7	$\quad Pi \rightarrow Ri$	$\forall_{\mathcal{E}}$, lines 3,1
8	$\quad Ri$	$\rightarrow_{\mathcal{E}}$, lines 6,7
9	$\quad Si \wedge Ri$	$\wedge_{\mathcal{I}}$, lines 5,8
10	$\quad (\forall\, z \cdot Sz \wedge Rz)$	Wrong! $\forall_{\mathcal{I}}$, line 9
11	$(\forall\, z \cdot Sz \wedge Rz)$	$\exists_{\mathcal{E}}$, lines 3-10

Another example of a mathematical proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Another example of a mathematical proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Here $x \mid y$ means that "x divides into y (with remainder zero)".

Another example of a mathematical proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Here $x \mid y$ means that "x divides into y (with remainder zero)".

Proof.

- For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

$\square$

Another example of a mathematical proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Here $x \mid y$ means that "x divides into y (with remainder zero)".

Proof.

- Suppose i, j and k are any integers.
- If $i \mid j$ and $j \mid k$ then $i \mid k$.
- For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$. $\forall_{\mathcal{I}}$

□

Another example of a mathematical proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Here $x \mid y$ means that "x divides into y (with remainder zero)".

Proof.

- Suppose i, j and k are any integers.
-     Suppose $i \mid j$ and $j \mid k$.
-         ...
-         ...
-         Then $i \mid k$
-     If $i \mid j$ and $j \mid k$ then $i \mid k$. $\rightarrow_{\mathcal{I}}$
- For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$. $\forall_{\mathcal{I}}$

$\square$

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive?

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric?

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗   Antisymmetric?

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓
- Transitive?

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓
- Transitive? ✓

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓
- Transitive? ✓
- Total?

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓
- Transitive? ✓
- Total? ✗ Partial ✓

Aside: the divisibility relation

- Here $x \mid y$ means that "x divides into y (with remainder zero)".
- Here $x \mid y$ means that "$(\exists\, n \cdot n * x = y)$".

Revision: is the divisibility relation over integers:

- Reflexive? ✓
- Symmetric? ✗ Antisymmetric? ✓
- Transitive? ✓
- Total? ✗ Partial ✓

Thus the divisibility relation over the integers is a *partial order*.

… back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- Suppose $i \mid j$ and $j \mid k$.

- Then $i \mid k$

□

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- $(\exists\, n \cdot n * i = j)$
- $(\exists\, n \cdot n * j = k)$

- $(\exists\, n \cdot n * i = k)$

$\square$

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ *and* $b \mid c$ *then* $a \mid c$*.*

Proof.

- $(\exists n \cdot n * i = j)$
- $(\exists n \cdot n * j = k)$
- Suppose u :
- Suppose $u * i = j$:
- $(\exists n \cdot n * i = k)$

$\square$

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- $(\exists\, n \cdot n * i = j)$
- $(\exists\, n \cdot n * j = k)$
- Suppose u :
- Suppose $u * i = j$:
- Suppose v :
- Suppose $v * j = k$:

- $(\exists\, n \cdot n * i = k)$

□

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- $(\exists\, n \cdot n * i = j)$
- $(\exists\, n \cdot n * j = k)$
- Suppose u :
- Suppose $u * i = j$:
- Suppose v :
- Suppose $v * j = k$:
- $v * (u * i) = k$ "substitute $(u * i)$ for j"
- $(\exists\, n \cdot n * i = k)$

$\square$

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- $\quad (\exists\, n \cdot n * i = j)$
- $\quad (\exists\, n \cdot n * j = k)$
- $\qquad$ Suppose u :
- $\qquad$ Suppose $u * i = j$:
- $\qquad$ Suppose v :
- $\qquad$ Suppose $v * j = k$:
- $\qquad\quad v * (u * i) = k$ "substitute $(u * i)$ for j"
- $\qquad\quad (v * u) * i = k$ "associativity of $*$"
- $(\exists\, n \cdot n * i = k)$

□

... back to that proof

Theorem

For any integers a, b and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

- $(\exists n \cdot n * i = j)$
- $(\exists n \cdot n * j = k)$
- Suppose u :
- Suppose $u * i = j$:
- Suppose v :
- Suppose $v * j = k$:
- $v * (u * i) = k$ — "substitute $(u * i)$ for j"
- $(v * u) * i = k$ — "associativity of $*$"
- $(\exists n \cdot n * i = k)$ — $\exists_{\mathcal{I}}$ with n for $(v * u)$

$\square$