Formal Proofs in FOL (Section 7.3)

Getting started

All proof rules for propositional calculus extend to predicate calculus. *Example:*

...	
$k.\ \forall x\ p(x)$	P
$k{+}1.\ \forall x\ p(x) \rightarrow \exists x\ p(x)$	P
$k{+}2.\ \exists x\ p(x)$	1,2,MP
...	

But we need additional proof rules to reason with most quantified wffs.

Free to Replace

- For a wff $W(x)$ and a term t we say t is free to replace x in $W(x)$ if $W(t)$ has the same bound occurences of variables as $W(x)$.
- *Example:* Let $W(x) = \exists y\ p(x, y)$. Then:
  - $W(y) = \exists y\ p(y, y)$, so y is not free to replace x in $W(x)$.
  - $W(f(x)) = \exists y\ p(f(x), y)$, so $f(x)$ is free to replace x in $W(x)$.
  - $W(c) = \exists y\ p(c, y)$, so c is free to replace x in $W(x)$.
  - $W(x) = \exists y\ p(x, y)$, so x is free to replace x in $W(x)$.

Universal Instantation

Universal Instantiation (UI)

- $\frac{\forall x \ W(x)}{W(t)}$ if t is free to replace x in $W(x)$.
- Special cases that satisfy the restriction:
  - $\frac{\forall x \ W(x)}{W(x)}$
  - $\frac{\forall x \ W(x)}{W(c)}$

Existential Generalization (EG)

Existential Generalization (EG)

- $\frac{W(t)}{\exists x\ W(x)}$ if t is free to replace x in $W(x)$.
- Special cases that satisfy the restriction:
  - $\frac{W(x)}{\exists x\ W(x)}$
  - $\frac{W(c)}{\exists x\ W(x)}$

Existential Instantiation (EI)

If $\exists x\, W(x)$ occurs on some line of a proof, then $W(c)$ may be placed on any subsequent line of the proof, subject to the following restrictions:

- Choose c to be a new constant in the proof and such that c does not occur in the statement to be proven.

Universal Generalization (UG)

If $W(x)$ occurs on some line of a proof, then $\forall x\, W(x)$ may be placed on any subsequent line of the proof, subject to the following restrictions:

- Among the wffs used to obtain $W(x)$, x is not free in any premise and x is not free in any wff obtained by EI.

Broken proofs

- There are lots of ways that quantifier inference rules can be misused. The next several slides show broken proofs.
- *Example:* $\forall x \exists y\ p(x, y) \rightarrow \exists y \forall x\ p(x, y)$ is invalid. Here is an *attempted* proof.

1.	$\forall x \exists y\ p(x, y)$	P
2.	$\exists y\ p(x, y)$	1,UI
3.	$p(x, c)$	2,EI
4.	$\forall x\ p(x, c)$	3,UG No!

Broken proofs

- There are lots of ways that quantifier inference rules can be misused. The next several slides show broken proofs.
- *Example:* $\forall x \exists y\ p(x,y) \to \exists y \forall x\ p(x,y)$ is invalid. Here is an *attempted* proof.

1.	$\forall x \exists y\ p(x,y)$	P
2.	$\exists y\ p(x,y)$	1,UI
3.	$p(x,c)$	2,EI
4.	$\forall x\ p(x,c)$	3,UG No! (x on (3) is free in wff obtained by EI)
5.	$\exists y \forall x\ p(x,y)$	4,EG
NOT QED		1-5, CP

Second Broken Proof

Example: $\exists x\ p(x) \rightarrow \forall x\ p(x)$ is invalid. Here is an *attempted* proof.

1.	$\exists p(x)$	P
2.	$p(x)$	1,EI No!

Second Broken Proof

Example: $\exists x\ p(x) \rightarrow \forall x\ p(x)$ is invalid. Here is an *attempted* proof.

1.	$\exists p(x)$	P
2.	$p(x)$	1,EI No! (x is not a new constant)
3.	$\forall x\ p(x)$	2,UG No!

Second Broken Proof

Example: $\exists x\ p(x) \rightarrow \forall x\ p(x)$ is invalid. Here is an *attempted* proof.

1. $\exists p(x)$	P
2. $p(x)$	1,EI No! (x is not a new constant)
3. $\forall x\ p(x)$	2,UG No! (x on (2) is free in wff obtained by EI)
NOT QED	1-3,CP

Third Broken Proof

Example: $\exists x\ p(x) \wedge \exists x\ q(x) \rightarrow \exists x\ (p(x) \wedge q(x))$ is invalid. Here is an *attempted* proof.

1.	$\exists x\ p(x)$	P
2.	$\exists x\ q(x)$	P
3.	$p(c)$	1,EI
4.	$q(c)$	2,EI No!

Third Broken Proof

Example: $\exists x\ p(x) \land \exists x\ q(x) \to \exists x\ (p(x) \land q(x))$ is invalid. Here is an *attempted* proof.

1. $\exists x\ p(x)$	P
2. $\exists x\ q(x)$	P
3. $p(c)$	1,EI
4. $q(c)$	2,EI No! (c is not a new constant)
5. $p(c) \land q(c)$	3,4,Conj
6. $\exists x\ (p(x) \land q(x))$	5,EG
NOT QED	1-6, CP

Broken Proof (4)

Example: $p(x) \to \forall x\ p(x)$ is invalid. Here is an *attempted* proof.

1.	$p(x)$	P
2.	$\forall x\ p(x)$	1,UG No!

Broken Proof (4)

Example: $p(x) \to \forall x\ p(x)$ is invalid. Here is an *attempted* proof.

1. $p(x)$	P
2. $\forall x\ p(x)$	1,UG No! (x is free in a premise)
NOT QED	1,2,CP

Broken Proof (5)

Example: $\forall x \exists y\ p(x,y) \rightarrow \exists y\ p(y,y)$ is invalid. Here is an *attempted* proof.

1.	$\forall x \exists y\ p(x,y)$	P
2.	$\exists y\ p(y,y)$	1,UI No!

Broken Proof (5)

Example: $\forall x \exists y\ p(x, y) \rightarrow \exists y\ p(y, y)$ is invalid. Here is an *attempted* proof.

1. $\forall x \exists y\ p(x, y)$	P
2. $\exists y\ p(y, y)$	1,UI No!
(y is not free to replace x in $\exists y\ p(x, y)$)	
NOT QED	1,2,CP

Broken Proof (6)

Example: $\forall x\ p(x, f(x)) \rightarrow \exists x\ p(x, x)$ is invalid. Here is an *attempted* proof.

1.	$\forall x\ p(x, f(x))$	P
2.	$p(x, f(x))$	1,UI
2.	$\exists x\ p(x, x)$	2,EG No!

Broken Proof (6)

Example: $\forall x\, p(x, f(x)) \rightarrow \exists x\, p(x, x)$ is invalid. Here is an *attempted* proof.

1. $\forall x\, p(x, f(x))$	P
2. $p(x, f(x))$	1,UI
2. $\exists x\, p(x, x)$	2,EG No!
$(p(x, f(x)) \neq p(x, x)(x/t)$ for any term $t)$	
NOT QED	1-3,CP

Broken Proof (7)

Example: $\forall x\, p(x, f(x)) \to \exists y \forall x\, p(x, y)$ is invalid. Here is an *attempted* proof.

1.	$\forall x\, p(x, f(x))$	P
2.	$\exists y \forall x\, p(x, y)$	1,EG No!

Broken Proof (7)

Example: $\forall x\, p(x, f(x)) \rightarrow \exists y \forall x\, p(x, y)$ is invalid. Here is an *attempted* proof.

1. $\forall x\, p(x, f(x))$	P
2. $\exists y \forall x\, p(x, y)$	1,EG No!
($f(x)$ is not free to replace y in $\forall x\, p(x, y)$)	
NOT QED	1,2,CP

Broken Proof (8)

Example: $\exists x\ p(x) \to p(c)$ is invalid. Here is an *attempted* proof.

1.	$\exists x\ p(x)$	P
2.	$p(c)$	1,EI No!

Broken Proof (8)

Example: $\exists x\ p(x) \rightarrow p(c)$ is invalid. Here is an *attempted* proof.

1. $\exists x\ p(x)$	P
2. $p(c)$	1,EI No!
(c occurs in statement to be proved)	
NOT QED	1,2,CP

Some Valid wffs

Example: $\forall x \forall y\ p(x, y) \to \forall y\ p(y, y)$ is valid. Here is an *attempted* proof.

1.	$\forall x \forall y\ p(x, y)$	P
2.	$\forall y\ p(y, y)$	1,UI No!

Some Valid wffs

Example: $\forall x \forall y\ p(x,y) \rightarrow \forall y\ p(y,y)$ is valid. Here is an *attempted* proof.

1. $\forall x \forall y\ p(x,y)$	P
2. $\forall y\ p(y,y)$	1,UI No!
(y is not free to replace x in $\forall y\ p(x,y)$)	
NOT QED	1,2,CP

But here is a correct proof:

1. $\forall x \forall y\ p(x,y)$	P
2. $\forall y\ p(x,y)$	1,UI
3. $p(x,x)$	2,UI
4. $\forall x\ p(x,x)$	3,UG
5. $p(y,y)$	4,UI
6. $\forall y\ p(y,y)$	5,UG
QED	1-6,CP.

Another Valid wff

Example: $\forall x\,(A(x) \to B(x)) \to (\forall x\, A(x) \to \forall x\, B(x))$ is valid.
Here is a proof.

1. $\forall x\,(A(x) \to B(x))$	P
2. $\quad \forall x\, A(x)$	P [for $\forall x\, A(x) \to \forall x\, B(x)$]
3. $\quad A(x)$	2,UI
4. $\quad A(x) \to B(x)$	1,UI
5. $\quad B(x)$	3,4,MP
6. $\quad \forall x\, B(x)$	5,UG
7. $\forall x\, A(x) \to \forall x\, B(x)$	2-6, CP.
QED	1,7,CP.

Multiple proofs

Prove the following wff is valid using IP. *Example:*
$\forall x\, \neg p(x,x) \wedge \forall x \forall y \forall z\, (p(x,y) \wedge p(y,z) \rightarrow p(x,z)) \rightarrow$
$\forall x \forall y\, \neg(p(x,y) \wedge p(y,x))$.

1.	$\forall x\, \neg p(x,x)$	P
2.	$\forall x \forall y \forall z\, (p(x,y) \wedge p(y,z) \rightarrow p(x,z))$	P
3.	$\quad \exists x \exists y\, (p(x,y) \wedge p(y,x))$	P [for $\forall x \forall y\, \neg(p(x,y) \wedge p(y,$
4.	$\quad p(a,b) \wedge p(b,a)$	3,EI,EI
5.	$\quad p(a,b) \wedge p(b,a) \rightarrow p(a,a)$	2,UI,UI,UI
6.	$\quad p(a,a)$	4,5,MP
7.	$\quad \neg p(a,a)$	1,UI
8.	False	6,7,Contr
9.	$\forall x \forall y\, \neg(p(x,y) \wedge p(y,x))$	3-8,IP
QED		1,2,9,CP.

Multiple proofs

Prove the same wff is valid using CP. *Example:*
$\forall x \neg p(x,x) \wedge \forall x \forall y \forall z\,(p(x,y) \wedge p(y,z) \rightarrow p(x,z)) \rightarrow \forall x \forall y\, \neg(p(x,y) \wedge p(y,x))$.

1.	$\forall x \neg p(x,x)$	P
2.	$\forall x \forall y \forall z\,(p(x,y) \wedge p(y,z) \rightarrow p(x,z))$	P
3.	$\neg p(x,x)$	1,UI
4.	$p(x,y) \wedge p(y,x) \rightarrow p(x,x)$	2,UI,UI,UI
5.	$\neg(p(x,y) \wedge p(y,x))$	3,4,MT
6.	$\forall x \forall y\, \neg(p(x,y) \wedge p(y,x))$	5,UG,UG
QED		1-6,CP.

IP Proof

Use IP to prove that: $\forall x \exists y\ (p(x) \to p(y))$ is valid.

1. $\exists x \forall y\ (p(x) \wedge \neg p(y))$	P [for IP]
2. $\forall y\ (p(c) \wedge \neg p(y))$	1,EI
3. $p(c) \wedge \neg p(c)$	2,UI
4. $p(c)$	3,Simp
5. $\neg p(c)$	3,Simp
6. False	4,5,Contr
QED	1-6,IP.

Group Practice

Break into six groups. I will assign each group one of these proofs.

1. $\forall x\,(A(x) \to C) \to (\exists x\,A(x) \to C)$.
2. $(\exists x\,A(x) \to C) \to \forall x\,(A(x) \to C)$.
3. $(C \to \forall x\,A(x)) \to \forall x\,(C \to A(x))$.
4. $(C \to \exists x\,A(x)) \to \exists x\,(C \to A(x))$.
5. $\exists x\,(C \to A(x)) \to (C \to \exists x\,A(x))$.
6. $\exists x\,(A(x) \to C) \to (\forall x\,A(x) \to C)$.

Solution 1

1. $\forall x\,(A(x) \to C) \to (\exists x\, A(x) \to C)$.

1.	$\forall x\,(A(x) \to C)$	P
2.	$\quad \exists x\, A(x)$	P [for $\exists x\, A(x) \to C$]
3.	$\quad A(d)$	2,EI
4.	$\quad A(d) \to C$	1,UI
5.	$\quad C$	3,4,MP
6.	$\exists x\, A(x) \to C$	2-5,CP
QED		1,6,CP.

Solution 2

2. $(\exists x\, A(x) \to C) \to \forall x\, (A(x) \to C)$.

1.	$\exists x\, A(x) \to C$	P
2.	$\quad A(x)$	P [for $A(x) \to C$]
3.	$\quad \exists x\, A(x)$	2,EG
4.	$\quad C$	1,3,MP
5.	$A(x) \to C$	2-4,CP.
6.	$\forall x\, (A(x) \to C$	5, UG
QED		1,5-6,CP.

Solution 3

3. $(C \to \forall x\, A(x)) \to \forall x\, (C \to A(x))$.

1.	$C \to \forall x\, A(x)$	P
2.	C	P [for $C \to A(x)$]
3.	$\forall x\, A(x)$	1,2,MP
4.	$A(x)$	3,UI
5.	$C \to A(x)$	2-4,CP
6.	$\forall x\, (C \to A(x))$	5,UG
QED		1,5-6, CP.

Solution 4

4. $(C \to \exists x\, A(x)) \to \exists x\, (C \to A(x))$.

1.	$C \to \exists x\, A(x)$	P
2.	$\quad C$	P [for $C \to A(?)$]
3.	$\quad \exists x\, A(x)$	1,2,MP
4.	$\quad A(d)$	3,UI
5.	$C \to A(d)$	2-4,CP
6.	$\exists x\, (C \to A(x))$	5,UG
QED		1,5-6, CP.

Solution 5

5. $\exists x\,(C \to A(x)) \to (C \to \exists x\,A(x))$.

1.	$C \to \exists x\,A(x)$	P
2.	C	P [for $C \to \exists x\,A(x)$]
3.	$C \to A(d)$	1,EI
4.	$A(d)$	2,3,MP
5.	$\exists x\,A(x)$	4,EG
6.	$C \to \exists x\,A(x)$	2-5,CP
QED		1,6,CP.

Solution 6

6. $\exists x\,(A(x) \to C) \to (\forall x\, A(x) \to C)$.

1.	$\exists x\,(A(x) \to C)$	P
2.	$\forall x\, A(x)$	P [for $\forall x\, A(x) \to C$]
3.	$A(d) \to C$	1,EI
4.	$A(d)$	2,UI
5.	C	3,4,MP
6.	$\forall x\, A(x) \to C$	2-5,CP.
QED		1,6,CP.