Section 7.3 Formal Proofs in Predicate Calculus

All inference rules for propositional calculus extend to predicate calculus.

Example. …

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

…

But we need additional inference rules to reason with most quantified wffs. For example, suppose we want to prove that the following wff is valid.

$$\exists x\, \forall y\, p(x, y) \to \forall y\, \exists x\, p(x, y).$$

We might start with

Proof: 1. $\exists x\, \forall y\, p(x, y)$ $\quad P$

But what do we do for the next line of the proof? We're stuck if we want to use inference rules. We need more inference rules.

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 occurrences 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 Instantiation (UI)

$$\frac{\forall x W(x)}{\therefore W(t)}$$ if t is free to replace x in $W(x)$.

Special cases that satisfy the restriction: $$\frac{\forall x W(x)}{\therefore W(x)} \qquad \frac{\forall x W(x)}{\therefore W(c)}$$

Existential Generalization (EG)

$$\frac{W(t)}{\therefore \exists x W(x)}$$ if t is free to replace x in $W(x)$.

Special cases that satisfy the restriction: $$\frac{W(x)}{\therefore \exists x W(x)} \qquad \frac{W(c)}{\therefore \exists x W(x)}$$

Existential Instantiation (EI)

$$\frac{\exists x W(x)}{\therefore W(c)}$$ if c is a new constant in the proof **and** c does not occur in the statement to be proved.

Universal Generalization (UG)

$$\frac{W(x)}{\therefore \forall x W(x)}$$ if among the wffs used to infer $W(x)$, x is not free in any premise **and** x is not free in any wff constructed by EI.

Restrictions on quantifier inference rules are necessary

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 line 3 is free in wff inferred by EI)
5.	$\exists y\, \forall x\, p(x, y)$	4, EG
	NOT QED	1, 4, CP

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

1.	$\exists x\, p(x)$	P
2.	$p(x)$	1, EI (NO, x is not a new constant in the proof)
3.	$\forall x\, p(x)$	2, UG
	NOT QED	1, 3, CP

Example. $\exists x\, p(x) \wedge \exists x\, q(x) \to \exists x\, (p(x) \wedge q(x))$ 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, c is not a new constant in the proof)
5.	$p(c) \wedge q(c)$	3, 4, Conj
6.	$\exists x\, (p(x) \wedge q(x))$	5, EG
	NOT QED	1, 6, CP

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

Example. $\forall x\, \exists y\, p(x, y) \to \exists y\, p(y, y)$ 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

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

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

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, $f(x)$ is not free to replace y in $\forall x\, p(x, y)$)
	NOT QED	1, 2, CP

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, c occurs in statement to be proved)
	NOT QED	1, 2, CP

Now 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, 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.	$\forall y\, p(y, y)$	4, T
	QED	1, 5, CP.

Quiz. Find an IP proof of the statement.

Example/Quiz. $\forall x\, (A(x) \to B(x)) \to (\forall x\, A(x) \to \forall x\, B(x))$ is valid. Find a proof.

Proof:

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

Example/Quiz. Prove that the following wff is valid using IP.

$$\forall x \neg p(x, x) \land \forall x \forall y \forall z \ (p(x, y) \land p(y, z) \to p(x, z)) \to \forall x \forall y \neg (p(x, y) \land p(y, x)).$$

Proof:

1.	$\forall x \neg p(x, x)$	P
2.	$\forall x \forall y \forall z \ (p(x, y) \land p(y, z) \to p(x, z))$	P
3.	$\exists x \exists y \ (p(x, y) \land p(y, x))$	P for IP, T
4.	$p(a, b) \land p(b, a)$	3, EI, EI
5.	$p(a, b) \land p(b, a) \to p(a, a)$	2, UI, UI, UI
6.	$p(a, a)$	4, 5, MP
7.	$\neg p(a, a)$	1, UI
8.	$p(a, a) \land \neg p(a, a)$	6, 7, Conj
9.	false	8, T
	QED	1, 2, 9, IP.

Quiz. Find a CP proof of the statement.

Proof:

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

Example/Quiz. Prove that the following wff is valid: $\forall x \exists y \ (p(x) \to p(y))$.

1.	$p(x)$	P
2.	$\exists x \ p(x)$	1, EG
3.	$p(c)$	2, EI
4.	$p(x) \to p(c)$	1, 2, CP
5.	$\exists y \ (p(x) \to p(y))$	4, EG
6.	$\forall x \exists y \ (p(x) \to p(y))$	5, UG
	QED.	

Quiz. Find an IP proof.

Group Quiz. Divide the class into six subgroups and assign each group one of the following six wffs to prove using CP (no IP and no T's). Assume that x does not occur free in C.

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

Solutions.

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

Proof:

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

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

Proof:

1.	$\exists x\,A(x) \to C$	P
2.	$\quad A(x)$	P
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, 6, CP.

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

Proof:		
1.	$C \to \forall x\, A(x)$	*P*
2.	C	*P*
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, 6, CP.

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

Proof:		
1.	$C \to \exists x\, A(x)$	*P*
2.	C	*P*
3.	$\exists x\, A(x)$	1, 2, MP
4.	$A(d)$	3, EI
5.	$C \to A(d)$	2, 4, CP
6.	$\exists x\, (C \to A(x))$	5, EG
	QED	1, 6, CP.

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

Proof:		
1.	$\exists x\, (C \to A(x))$	*P*
2.	C	*P*
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.

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

Proof:		
1.	$\exists x\, (A(x) \to C)$	*P*
2.	$\forall x\, A(x)$	*P*
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.