Section 1.8 Proof Methods (continued)

Comp 232
Instructor: Robert Mearns

1. Proof by Cases method and Proof by Exhaustion method.

a) Sometimes it is not possible to get an argument that works for all values in the Domain. So we separate the values of the Domain into categories (cases) and construct an argument for each category (case).

b) These types of proof are based on the following Equivalence: $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$
First let us prove this Equivalence:

Proof: (Direct)

Consider	$(p \vee q) \rightarrow r$	Given
	$\equiv \neg(p \vee q) \vee r$	$\rightarrow$ with or
	$\equiv (\neg p \wedge \neg q) \vee r$	De Morgan
	$\equiv (\neg p \vee r) \wedge (\neg q \vee r)$	Distributive
	$\equiv (p \rightarrow r) \wedge (q \rightarrow r)$	$\rightarrow$ with or

QED

If we generalize $(p_1 \vee p_2 \vee \ldots\ldots \vee p_n) \rightarrow r \equiv (p_1 \rightarrow r) \wedge (p_2 \rightarrow r) \wedge \ldots\ldots \wedge (p_n \rightarrow r)$
In words: Prove an implication with Or in given ≡ Proving separate implications joined by And

c) Method: Step 1 Split Domain into categories (cases). Then Domain = (case1 $\vee$ case2 $\vee$ ...)
Step 2 To prove (case 1 $\vee$ case 2 $\vee$ ....) $\rightarrow$ conclusion
we prove: (case1 $\rightarrow$ conclusion) $\wedge$ (case2 $\rightarrow$ conclusion) $\wedge$ ...

d) The method is called Proof by Cases. If every member of domain is a separate case the method is also called Proof by Exhaustion

Ex 1: $\forall x \forall y$: $|x| * |y| = |x * y|$, $x,y \in R$ (real numbers)

Recall when we remove absolute value signs: $|x| = x$ if $x \geq 0$

$|x| = -x$ If $x < 0$

Since we do something different depending on whether x, y are positive or negative, we separate into cases.

There are four cases. What are they ? $x \geqslant 0 \wedge y \geqslant 0$

$x \geqslant 0 \wedge y \leqslant 0$

$x \leqslant 0 \wedge y \geqslant 0$

$x \leqslant 0 \wedge y \leqslant 0$

Proof: (By Cases)

Note: the references are similar for each case

Case 1: $x \geq 0 \wedge y \geq 0$		Case 2: $x \geq 0 \wedge y < 0$
Let x=a, y=b where a, $b \geq 0$ $\|x\| \|y\| = \|a\| \|b\| = ab$ $\|xy\| = \|ab\| = ab$ $\rightarrow \forall x \forall y$, $x \geq 0$ $y \geq 0$: $\|x\| \|y\| = \|xy\|$	a,b any R in Case 1 Due to sign of a, b Due to sign of ab Def of $\forall$	Let x=a, y=b where $a \geq 0$, $b < 0$ $\|x\| \|y\| = \|a\| \|b\| = (a)(-b) = -ab$ $\|x\| \|y\| = \|ab\| = -(ab) = -ab$ $\rightarrow \forall x \forall y$, $x \geq 0$ $y < 0$: $\|x\| \|y\| = \|xy\|$
Case 3: $x < 0 \wedge y \geq 0$ Let x=a, y=b where $a < 0$, $b \geq 0$ $\|x\| \|y\| = \|a\| \|b\| = (-a)(b) = -ab$ $\|x\| \|y\| = \|ab\| = -(ab) = -ab$ $\rightarrow \forall x \forall y$, $x < 0$ $y \geq 0$: $\|x\| \|y\| = \|xy\|$		Case 4: $x < 0 \wedge y < 0$ Let x=a, y=b where $a < 0$, $b < 0$ $\|x\| \|y\| = \|a\| \|b\| = (-a)(-b) = ab$ $\|x\| \|y\| = \|ab\| = ab$ $\rightarrow \forall x \forall y$, $x < 0$ $y < 0$: $\|x\| \|y\| = \|xy\|$

Conclusion: $\forall x \forall y$: $|x| * |y| = |x * y|$, $x,y \in R$

Ex 2: Prove that there are no Integer solutions to the equation $2x^2 + 5y^2 = 14$

In symbols we have to prove $\forall x \forall y: \neg (2x^2 + 5y^2 = 14)$, $x, y \in Z$

Proof (Exhaustion)

(i) We need not test negative x, y. Why? Equation includes only ,

(ii) If we start with x=0 (the smallest x) what is the largest y we can use and why ?

y=1: If x=0, y=2 → 2(0) + 5(2) > 14. Hence we need only test y=0,1

(iii) If we start with y=0 (the smallest y) what is the largest x we can use and why?

x=2: If y=0, x=3 → 2(3) + 5(0) > 14. Hence we need only test x=0,1,2

(iv) Hence we can consider all possibilities separately. How many are there ?

Case 1 $x=0, y=0 \rightarrow 2(0)^2 + 5(0)^2 = 0, \rightarrow 2x^2 + 5y^2 = 14$ is False

Case 2 $x=0, y=1 \rightarrow 2(0)^2 + 5(1)^2 = 5, \rightarrow$ "

Case 3 $x=1, y=0 \rightarrow 2(1)^2 + 5(0)^2 = 2, \rightarrow$ "

Case 4 $x=1, y=1 \rightarrow 2(1)^2 + 5(1)^2 = 7, \rightarrow$ "

Case 5 x=2, y=0 → 2(2) + 5(0) = 8, →

Case 6 x=2, y=1 → 2(2) + 5(1) = 13, →

QED Conclusion: There are no integer solutions to the equaion

2. Existence proofs

a) This type of proof is based on propositions : $\exists x\, P(x)$ or $\exists x \exists y\, P(x,y)$ ……

The proof answers the question: Can we find an x or an (x,y) ?

b) There are two kinds of Existence Proof techniques:

Constructive	Non constructive
Find at least one element that makes the proposition = True	Actually Proof by Contradiction Step 1 List all possibilities: $\exists xP(x)$ or $\neg\exists xP(x)$ Step 2 Assume the one not wanted: $\neg\exists xP(x)$, show contradiction Step 3 State remaining possibility: $\exists xP(x)$

Ex 1: $\forall a \forall b \exists x$: $ax + b = 0$, $x, a, b \in R$ $a \neq 0$

Proof (Constructive Existence).

Consider x=	x exists since $a \neq 0$
ax+b =	Now show x satisfies given equation
ax+b = -b+b	Simplify
ax+b = 0	Simplify
Conclusion: $\forall a \forall b \exists x$: ax+b = 0	Def of $\exists$

Ex 2: Integers 1,….10 are placed around a circle, Three groups size three are formed. One integer is alone
Prove there exists at least one group where the sum of its three integers ≥ 17.
In symbols: $\exists n_1 \exists n_2 \exists n_3$: $n_1 + n_2 + n_3 \geq 17$, $n_i \in \{1,2,\ldots..10\}$

Proof (Non constructive Existence. Proof by Contradiction)

Step 1 Either $\exists n_1 \exists n_2 \exists n_3: n_1 + n_2 + n_3 \geq 17$ Or $\neg \exists n_1 \exists n_2 \exists n_3: n_1 + n_2 + n_3 \geq 17$	All poss.conclusions
Step 2 Assume	Assume poss. not wanted
	De Morgan, quantifiers
$\rightarrow \forall n_1 \forall n_2 \forall n_3$: $n_1 + n_2 + n_3 < 17$	Def: $\neg \geq \; \equiv <$
Step 3 For the case that shows the contradiction: Since the assumption is for all integers 1,..10. Form 3 groups with 3 integers in each and let digit 1 be alone (could be 2 or 3 as the lone digit)	
Total sum = 1 + group1 + group2 + group3 < (1+17+17+17) = 52	Using $n_1 + n_2 + n_3 < 17$
$\rightarrow$ Total sum < 52	Transitive
But Total sum = (1+2+3+...+10) = 55	$1+2+3+\ldots+n = \frac{n(n+1)}{2}$
	Remaining poss.
QED Conclusion:	

- 3. Uniqueness Proofs

a) This type of proof is based on propositions like: $!\exists x$: $P(x)$ or $!\exists x!\exists y$: $P(x,y)$

Part 1 Prove Existence (there exists at least one) $\exists x$: $P(x)$ or $\exists x\exists y$: $P(x,y)$

Part 2 Prove Uniqueness (there is exactly one) $!\exists x$: $P(x)$ or $!\exists x\exists y$: $P(x,y)$

b) Part 2 will employ the Proof by Contradiction technique

Ex: Prove $\forall a \forall b\ !\exists x$: $a x + b = 0$, $a \neq 0$, a, b, $x \in R$

Part 1 Existence: Prove $\forall a \forall b\ \exists x$: $a x + b = 0$, $a \neq 0$, a, b, $x \in R$

Proof: (see previous Existence Proof Ex 1:)

Part 2 Uniqueness:

Proof: (by Contradiction)

Step 1 Either $\forall a \forall b\ !\exists x$: $a x + b = 0$, $a \neq 0$

or $\neg\ \forall a \forall b\ !\exists x$: $a x + b = 0$, $a \neq 0$

List all poss. Conclusions

Step 2 Assume $\neg\ \forall a \forall b\ !\exists x$: $a x + b = 0$, $a \neq 0$

$\rightarrow\ \exists a \exists b \neg E!x$: $ax+b = 0$, $a \neq 0$, a, b, $x \in R$

Assume possibility not wanted

Transitive

Subtract b

Since $a \neq 0$, divide by a

$x_2 \neq$ x above

Contradiction

Step 3 Conclusion: $\forall a \forall b \exists !x$: $ax+b = 0$, $a \neq 0$, a, b, $x \in R$

Remaining possibility in line 1

- 4. Summary of Proof Techniques.

Proof Technique Name	**Description**
Couter example (proving proposition ≠ True)	Find one specific example for which proposition ≠ True
Direct	Start with given and use valid logic steps to get to conclusion
Contraposition	- Change Implication into its Contrapositive form. - Use a Direct method on this Contrapositive form
Contradiction	- List all possible outcomes for the conclusion - Assume (1 by 1) the outcomes you do not want - Show each outcome assumed leads to a contradiction
Cases	- Break up the Domain into cases - Prove each case separately using any proof method
Exhaustion	Same as Cases except prove for every individual member of the Domain using any proof method
Existence - constructive	Find one specific example for which proposition = True
Existence - Non constructive	Assume non existence and show this leads to a Contradiction
Uniqueness	Assume two elements exist and then show they must be equal.

5. Beware of the following:

a) Assuming the Conclusion is True You CANNOT assume the conclusion that you are trying to prove.

b) Confusing the Contradiction and Contraposition methods in some examples.

Ex: Suppose we are asked to prove $p \rightarrow q$ by the Contradiction method:

Step 1 List all possibilities for Conclusion: q or $\neg q$

Step 2 Assume the conclusion you do not want: Assume $\neg q$ and look for a contradiction

The contradiction can be: (i) a contradiction of any true fact

or (ii) a contradiction of the true hypothesis: $\neg p$

Step 3 After you get the contradiction, list the remaining possibility to get QED

Note in (ii): If assuming $\neg q$ implies a contradiction of the hypothesis (this is $\neg p$)

we actually have proved: $\neg q \rightarrow \neg p$ which proves $p \rightarrow q$ by Contraposition

Hence we could also do this proof using

c) Vacuous proofs: Some situations make the hypothesis (given) false.

This situation can be handled by recalling the truth table for $p \rightarrow q$:

If hypothesis p = False then the implication $p \rightarrow q$ = T automatically.

Ex: P(x) represents: If $x > 1$ then $x^2 > x$, $x \in R$. Prove P(0) = True

Proof: (This is Vacuous)

P(0) represents: If 0>1, then > 0

The hypothesis 0>1 = False

$\rightarrow$ The implication [If 0>1, the > 0] is True automatically.

$\rightarrow$ P(0) is True.

d) Trivial Proof: If we are trying to prove the implication $p \to q$ is True and we know q = True then this situation can be handled by recalling the truth table for $p \to q$:
If conclusion q = True then implication $p \to q$ = T automatically

Ex: Prove: P(n) represents: If a, b are positive integers and $a \geq b$ then $a^n \geq b^n$. Prove P(0) = True

Proof: (This is Trivial)

P(0) represents: If a,b are positive integets then

Since conclusion $a^0 \geq b^0$ means $1 \geqslant 1$

$\rightarrow$ the conclusion = True

$\rightarrow$ the implication [If a,b are positive integers then] is True automatically.

$\rightarrow$ P(0) is True

QED

e) Summary: Vacuous / Trivial proofs:

When proving an Implication is True

If Hypothesis is known to be False, the implication is True automatically. Vacuous case.

If Conclusion is known to be True, the implication is True automatically. Trivial case.