Sec 1.7 Introduction to Proofs

Monday, June 13, 2016 5:04 PM

Section 1.7 Introduction to Proofs

Comp 232
Instructor: Robert Mearns

1. Preliminary: Where are we headed in this section ?

a) We have now established the Rules of Logic and how they apply to an Argument. We now look at different ways to organize the Arguments and hence establish different forms for Proofs in general.

b) Why do we need Proofs ? We benefit from the fact that once a proof has been constructed we can use the proven result. If proofs did not exist then each time we want to use a fact we would not be sure whether it would always give correct results.

Ex: $[\forall x\ P(x) \wedge \forall x\ Q(x)] \equiv [\forall x\ [P(x) \wedge Q(x)]$ is: T

$[\forall x\ [P(x) \vee Q(x)] \equiv [\forall x\ P(x) \vee \forall x\ Q(x)]$ is: F

$[\ (p \vee q) \wedge (\neg p \vee r)\ ] \rightarrow (q \vee r)$ is: a Tautology: This is the Resolution inference.

We accept these facts because they have been proven using valid arguments

c) In Computer Science one uses proof techniques to:

Test programs to see if they Always give correct output	Test operating systems to see if they are secure	Artificial Intelligence	Test specifications for a new system to see if they are consistent (no contradictions)

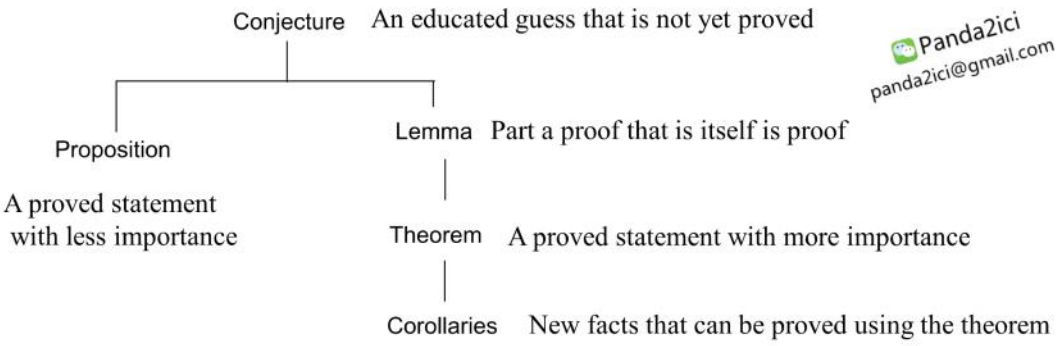
1

2. Vocabulary

a) Proof is another word for argument
b) Axiom is a basic idea that is accepted to start the discussion

Ex: If a = b and b = c then
This Axiom is called the transitive property. In early history it would have been stated as " things that are equal to the same thing are equal to each other "
You have accepted and used this Axiom many times in Mathematics and otherwise.

c) Some other vocabulary is included in the diagram below:



3

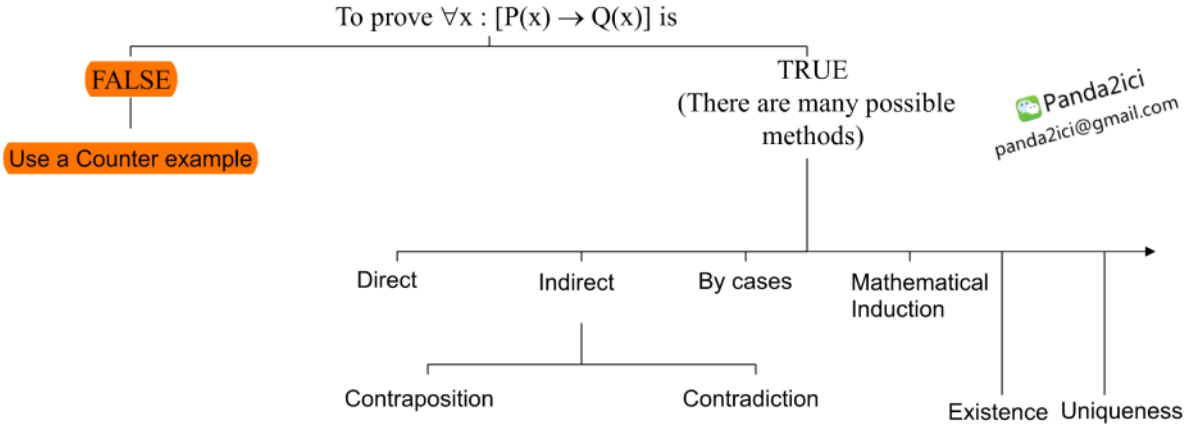
3. Beware that there may be words missing when a conjecture is stated and then turned into a Proposition, Lemma, Theorem or Corollary.

   Ex: x, y and z are Real numbers, $x > y$ and $y > z$ implies $x > z$ actually means:

   $\forall x \forall y \forall z$: [if $x>y$ and $y > z$ then $x>z$] where the Domain for x, y, z is the set of all Real numbers

   Or write: $\forall x \forall y \forall z$: $[P(x,y) \wedge P(y,z) \rightarrow P(x,z)]$, $x, y, z \in R$, where $P(m,n)$ represents: $m>n$

4. There are different methods that can be used to construct a proof:



5. Counter Example

This type of proof structure is based on the following rule of logic:

If we are trying to prove $\neg\forall x: P(x)$

Since $\neg\forall x: P(x) \equiv \exists x: \neg P(x)$ we try to prove $\exists x: \neg P(x)$ instead.

This means we require a search to find at least one case for which P(x) is false.

Ex: $\neg\ \forall x \forall y\ \ x, y \in R:\ |x+y| = |x| + |y|$

Proof (Counter Example method)

Consider Real numbers $x = 5, y = -3$	
$\|x+y\| = \|5\| + \|(-3)\| = \|2\| = 2$	Substitute, simplify LHS of given
$\|x\| + \|y\| = \|5\| + \|-3\| = 5 + 3 = 8$	Substitute, simplify RHS of given
$\rightarrow\ \exists x \exists y\ \ x, y \in R:\ \neg(\|x+y\| = \|x\| + \|y\|)$	Def $\exists$
$\rightarrow\ \neg\forall x \forall y\ \ x, y \in R:\ \neg(\|x+y\| = \|x\| + \|y\|)$	De Morgan for quantifiers
QED	

Note: (i) Do not use $x = 5, y = 3$ as counter example. Why ? $|x+y| = |x| + |y|$

(ii) Summary of final results:

$\neg\ \forall x \forall y\ \ x,y \in R: (\ |x+y| = |x| + |y|\ )$

$\equiv\ \exists x \exists y\ \ x,y \in R: \neg\ (\ |x+y| = |x| + |y|\ )$

$\equiv\ \exists x \exists y\ \ x, y \in R:\ (|x+y| \neq |x| + |y|)$

7

6. Direct proof structure

a) This type of proof structure is based on the following rule of logic.

If we are trying to prove $p \rightarrow q$ = True we must show that: p = T is sufficient for q = T

Method - Start with the hypothesis p (given)
- Use axioms, definitions, previous proven results, rules of logic
- Arrive at the conclusion q.

This is what we did in the arguments in the previous section

b) Before further examples of Direct proof we need some definitions and axioms.

(i) The set of integers is denoted as Z and Z+ denotes positive integers

(ii) Multiplication and addition of integers are both Closed (answers are also integers)
$\forall m \forall n\ m, n \in Z: (m+n \in Z) \wedge (m, n \in Z)$

(iii) Definition: n is an Even integer iff $\exists k,\ k \in Z+ \wedge n=2k$

(iv) Definition: n is an Odd integer iff $\exists k,\ k \in Z+ \wedge n=2k+1$

9

Ex 1: Theorem: If n is an odd integer then n^2 is an odd integer.

Proof (Direct method)

1. Consider any odd integer n	Given
2. $n = 2k+1,\ k \in Z$	Def odd integer
3. $n^2 = (2k+1)^2$	Square both sides
4. $n^2 = (2k+1)(2k+1)$	Def of square
5. $n^2 = 4k^2+4k+1$	Multiply
6. $n^2 = 2(2k^2+2k)+1$	Factor
7. Now $2k^2+2k$ is an integer	$k \epsilon Z$ and multiplication, addition are closed
→ n^2 is an odd integer	Def of odd integer, [n^2 = 2 (integer) + 1 in line 6]
QED	

11

Ex 2: Theorem: If n -1 is an odd integer then n is an even integer.
Proof (Direct method)

1. Consider any odd integer n-1	Given
2. $n-1 = 2k+1,\ k \in Z$	Def odd integer
3. n-1+1=2k+1+1	Add one to both sides
4. n=2k+2	Simplify
5. n=2(k+1)	Factor
6. since (k+1) is an integer	k ,1 ϵ Z and addition is closed
→ n is an even integer	n = 2 (integer) in line 5

Ex 3: Complete the steps of the following direct proof given that a = b.
Proof (Direct method)

1. a=b	Given
2. $a^2 = ab$	Multiply both sides by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides
4. (a+b)(a-b) = b(a-b)	Factor both sides
✕ 5. a + b = b	Divide both sides by (a-b)
6. b + b = b	On LHS substitute a = b which is given
7. 2b = b	Simplify
Conclusion: 2=1	Divide both sides by b

Since a=b → a-b=0

13

Ex 4: Prove that ∀n, n ϵ Z: if n^3 is odd then n is odd. Use the Direct Proof method.

Before this proof we use Backward Reasoning that will tell us how to start this proof because:

If we start with: Let n^3= 2k+1, k ϵ Z , this is valid because of given and def. of odd integer

but then n = $\sqrt[3]{2k+1}$ and we cannot conclude from this that n is odd.

Instead, look at what you need near the end of the proof :

We need to have $n^3 = (2k+1)^3$ with k ∈ Z

so if we take its cube root we get n = 2k+1, k ∈ Z which makes n odd which is what we want.

Question: Since we are given n^3 is odd we would need $(2k+1)^3$ to be odd.

Is $(2k+1)^3$ odd ?

Consider $(2k+1)^3$, k ϵ Z

$= 8k^3 + 12k^2 + 6k + 1$	Multiply
$= 2(4k^3 + 6k^2 + 3k) + 1$	Factor
= 2(Integer) + 1	k ϵ Z, mult., add. closed in Z
→ $(2k+1)^3$ odd	Def of odd integer

Proof (Direct)

1. n^3 is an odd integer	Given
2. Let $n^3 = 2(4k^3 + 6k^2 + 3k) + 1$, $k \in Z$	Closure → 2[Integer]+1,(idea from Back.Reason.)
3. $n^3 = 8k^3 + 12k^2 + 6k + 1$	Multiply
4. $n^3 = (2k+1)^3$	Factor (reverse multiply line in Back. Reason.)
5. n = 2k+1	Cube root
6. Since k is an integer	Line 2
→ n is an odd integer	Def of Odd Integer

15

Ex 5: Definition: (i) The real number r is Rational iff $\exists p \exists q$ p, q $\in Z \wedge r = \frac{p}{q}$, $q \neq 0$

(ii) If a number is not Rational it is Irrational

Prove that the product of two Rational numbers is Rational by Direct method.

Proof (Direct)

1. Consider a, b are Rational	Given
2. Let $a = \frac{p_1}{q_1}, b = \frac{p_2}{q_2}, q_1 \neq 0, q_2 \neq 0$	Def of Rational
3. $ab = \frac{p_1 p_2}{q_1 q_2}$	Multiply and simplify
→ a b is Rational	Closure → $p_1 p_2, q_1 q_2 \in Z$, Def of Rational
QED	

17

7. Contraposition proof structure

This type of proof structure is based on the following rule of logic:
$p \rightarrow q \equiv \neg q \rightarrow \neg p$ (contrapositive form). If a proof of the original form is difficult, if not impossible, then try the proof using the contrapositive form of the original statement.
If the Contrapositive statement = True then the Original statement = True

Method - Start with the negation of the conclusion $\neg$ q as the "new" hypothesis
- Use axioms, definitions, previous proven results, rules of logic to arrive at the "new" conclusion $\neg$ p. (These steps use a Direct Method)
- State the final conclusion in the original form.

Ex: Let P(n), $n \in Z$ represent: (3n+2) is odd integer, Q(n), $n \in Z$ represent: n is an odd integer.
Prove $\forall n, n \in Z$: $P(n) \rightarrow Q(n)$

Proof (Contraposition): $\forall n, n \in Z$: $\neg Q(n) \rightarrow \neg P(n)$	Contrapositive form of Original statement
1. Consider $\neg Q(n) \rightarrow$ n is an even integer.	Negation of the Original Conclusion
2. n = 2k, $k \in Z$	Def even integer
3. 3n+2 = 3(2k)+2	Substitute n = 2k in (3n+2)
4. 3n+2 = 6k+2	Multiply
5. 3n+2 = 2(3k+1)	Factor
6. $\rightarrow$ (3n+2) is an even integer	Add, mult. are closed, 3n+2 = 2(Integer)
7. $\forall n, n \in Z$: $\neg Q(n) \rightarrow \neg P(n)$	
8. $\rightarrow \forall n, n \in Z$: $P(n) \rightarrow Q(n)$	Contrapositive of line 7
QED	

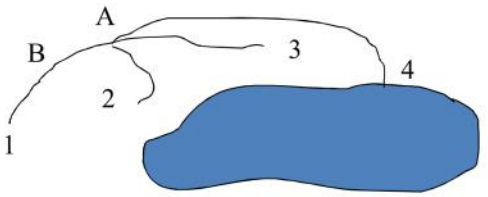
19

8. Contradiction proof structure

a) This type of proof structure is based on the following logic: $(p \vee q) \wedge \neg p \rightarrow q$; $(p \vee q \vee r) \wedge (\neg p \wedge \neg q) \rightarrow r$

b) Consider a non mathematical situation to illustrate the idea of a Contradiction proof structure:

There exists a lake, 4 roads and two persons A, B. The lake cannot be seen from the intersection of the roads where A sits. B approaches the intersection from the left on road 1. A tells the truth.
Step 1 A says "road 2 or road 3 or road 4 leads to the lake": $p \vee q \vee r$
Step 2 B assumes road 2 leads to lake and tests it. Road 2 fails to lead to lake: $\neg p$
Step 3 B assumes road 3 leads to lake and tests it. Road 3 fails to lead to lake: $\neg q$
Conclusion: $(p \vee q \vee r) \wedge (\neg p \wedge \neg q) \rightarrow r$



Tri-cotomy: There exists exactly 3 possibilities, hence test 2 of them before conclusion is known.
Di-cotomy: There exists exactly 2 possibilities, hence test 1 of them before conclusion is known.

c) In a proof by contradiction:
Method Step 1 List all possible Conclusions.
Step 2 Assume each possibility that you **do not want** and show each leads a contradiction.
Step 3 Final Conclusion is: the remaining prossibility from Step 1.

21

Ex 1: Prove: If x ϵ R is Irrational then (3x + 2) is Irrational. Use proof by Contradiction

Proof (Contradiction method)

Step 1	Either (3x+2) is Irrational is T or (3x+2) is Irrational is F	List all possibilities for conclusion
Step 2	Assume (3x+2) is Irrational is F → (3x+2) is Rational	Assume the conclusion you do not want
	$\rightarrow 3x + 2 = \frac{a}{b}, a, b \in Z, b \neq 0$	Definition of Rational
	$\rightarrow 3x = \frac{a}{b} - 2$ $\rightarrow x = \frac{a - 2b}{3b}$	Simplify Algebra
	→ x is Rational → Contradiction	Closure: a+(-2b), 3b are Integers, Def of Rational x is given as Irrational
Step 3	→ (3x+2) is Irrational is T QED	Only possibility remaining

23

Ex 2: Prove: $\forall x \forall y \;\; x,y \in R: [\, x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2} \,]$ In words this says that for all Real numbers at least one of two numbers is greater than or equal their mean (average).

Proof (Contradiction)

Step 1	1. Either $\forall x \forall y: [\, x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2} \,]$ or $\neg\, \forall x \forall y: [\, x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2} \,]$	List all possibilities for the conclusion
Step 2	2. Assume $\neg\, \forall x \forall y: [\, x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2} \,]$	Assume the possibility not wanted
	3. $\rightarrow \exists x \exists y: \neg\, [x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2}]$	De Morgan's Rule for quantifiers
	4. $\rightarrow \exists x \exists y: \{\, \neg\, [x \geq \frac{x+y}{2}] \;\wedge \neg\, [y \geq \frac{x+y}{2}] \,\}$	De Morgan's Rule (Regular)
	5. $\rightarrow \exists x \exists y: \{\, [x < \frac{x+y}{2}] \;\wedge\; [y < \frac{x+y}{2}] \,\}$	$\neg(\geq) \;\equiv\; <$
	6. Let $x = a, y = b$ be the values in line 5	a, b represent values by Def of ∃
	7. $\rightarrow\; a < \frac{a+b}{2} \wedge\; b < \frac{a+b}{2}$	Substitute for x,y in line 5
	8. $\rightarrow a + b < \frac{a+b}{2} + \frac{a+b}{2} = \frac{2(a+b)}{2} = a + b$	Add, simplify
	9. $\rightarrow\; a+b < a+b$	Transitive in line 8
	10. $\rightarrow$ Contradiction	From line 9
Step 3	$\rightarrow \forall x \forall y: [\, x \geq \frac{x+y}{2} \;\vee\; y \geq \frac{x+y}{2} \,]$ QED	Only remaining possibility in line 1

25