

Direct Proof and Counterexample

CS 231
Dianna Xu

1

Vacuous proofs

- Consider an implication: $p \rightarrow q$
- If it can be shown that p is false, then the implication is always true
 - By definition of an implication/conditional
- Note that you are showing that the antecedent is false

2

Vacuous proof example

- Consider the statement:
 - All criminology majors in CS 231 are female
 - Rephrased: If you are a criminology major and you are in CS231, then you are female
- Since there are no criminology majors in this class, the antecedent is false, and the implication is true

3

Trivial proofs

- Consider an implication: $p \rightarrow q$
- If it can be shown that q is true, then the implication is always true
 - By definition of an implication
- Note that you are showing that the consequent is true

4

Trivial proof example

- Consider the statement:
 - If you are in CS231 then you are human (domain is all people)
- Since all people are human, the implication is true regardless

5

Direct proofs

- Consider an implication: $p \rightarrow q$
 - What if p is true, and q may or may not be true?
 - Show that if p is true, then q is true
- To perform a direct proof, assume that p is true, and show that q must be true

6

Definitions of Even and Odd

- n is even: $\exists k \in \mathbb{Z}$ such that $n = 2k$
- n is odd: $\exists k \in \mathbb{Z}$ such that $n = 2k+1$

7

Direct proof example

- Show that the square of an even number is an even number
 - Rephrased: n is even $\rightarrow n^2$ is even
- Proof:
 - n is even: $n = 2k$, for some $k \in \mathbb{Z}$ (definition of even)
 - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
 - $2k^2 \in \mathbb{Z}$
 - As n^2 is 2 times an integer, n^2 is even ■

8

Proving Existential Statements

- To prove a statement of the form
 - $\exists x \in D, Q(x)$
- Constructive: find such an x
- Non-constructive:
 - show that the existence of an x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem – no need to find one
 - assume that there is no such x and show a contradiction

9

Constructive Existence Proof Example

- Show that a square exists that is the sum of two other squares
 - Proof: $3^2 + 4^2 = 5^2$ ■
- Show that a cube exists that is the sum of three other cubes
 - Proof: $3^3 + 4^3 + 5^3 = 6^3$ ■

10

Non-constructive Existence Proof

- Prove that either $2 \times 10^{500} + 15$ or $2 \times 10^{500} + 16$ is not a perfect square
 - A perfect square is the square of an integer
- Proof:
 - The only two perfect squares that differ by 1 are 0 and 1
 - Thus, any other numbers that differ by 1 cannot both be perfect squares
 - Thus, a non-perfect square must exist in any set that contains two numbers that differ by 1 ■
 - Note that we didn't need to specify which one!

Disproving Universal Statements

- Disproving a statement of the form:
 - $\forall x \in D, P(x) \rightarrow Q(x)$
- Equivalent to showing the negation is true:
 - $\exists x \in D, P(x)$ and $\sim Q(x)$
 - Finding such an x is known as finding a counterexample

12

Disproof by Counterexamples

- Every positive integer is the square of another integer
 - $\sqrt{2}$ is not an integer ■
- If the sum of two integers is even, then one of them is even
 - $1+3 = 4$ ■

13

A note on counterexamples

- You can DISPROVE something by showing a single counter example
 - Find an example to show that something is not true
- You cannot PROVE something by example
- Example: prove or disprove that all numbers are even
 - Disproof by counterexample: 1 is not even
 - (Invalid) proof by example: 2 is even

14

Proving Universal Statements

- Exhaustion: list all possibilities

15

Proof by Cases

- Show a statement is true by showing all possible cases are true
- Thus, you are showing a statement of the form: $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$

is true by showing that:

$$[(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q] \Leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$$

16

Proof by cases example

- Prove that $\frac{|a|}{|b|} = \frac{|a|}{|b|}$
 - Note that $b \neq 0$
- Cases:
 - Case 1: $a \geq 0$ and $b > 0$
 - Then $|a| = a$, $|b| = b$, and $\frac{|a|}{|b|} = \frac{a}{b} = \frac{|a|}{|b|}$
 - Case 2: $a \geq 0$ and $b < 0$
 - Then $|a| = a$, $|b| = -b$, and $\frac{|a|}{|b|} = \frac{a}{-b} = \frac{a}{-b} = \frac{|a|}{|b|}$
 - Case 3: $a < 0$ and $b > 0$
 - Then $|a| = -a$, $|b| = b$, and $\frac{|a|}{|b|} = \frac{-a}{b} = \frac{-a}{b} = \frac{|a|}{|b|}$
 - Case 4: $a < 0$ and $b < 0$
 - Then $|a| = -a$, $|b| = -b$, and $\frac{|a|}{|b|} = \frac{-a}{-b} = \frac{-a}{-b} = \frac{|a|}{|b|}$ ■

17

Control the Cases

- Make sure you get ALL the cases
 - The biggest mistake is to leave out some of the cases
- Don't list extra cases
 - We could have 9 cases in the last example
 - Positive
 - Negative
 - Zero
 - Those additional cases wouldn't have added anything to the proof

18

Proving Universal Statements

- Generalizing from the generic particular
 - show that every element of a set satisfies a certain property and that x is an element of such a set

19

Example

- If the sum of any two integers is even, so is their difference
 - Let m and n be particular but arbitrarily chosen integers such that $m+n$ is even
 - $m + n = 2k, k \in \mathbb{Z}$
 - $m - n = m + n - 2n = 2k - 2n = 2(k-n)$
 - $k-n \in \mathbb{Z}$
 - $m-n$ is even ■

20

Mistakes in proofs

- Modus Badus
 - Fallacy of denying the hypothesis (inverse error)
 - Fallacy of affirming the conclusion (converse error)
- Proving a universal by example
 - You can only prove an existential by example!
- Disproving an existential by example
 - You can only disprove a universal by example!

21

Other Pointers

- Directions for writing Proofs
- Common mistakes
- How to get a proof started

22