More examples of mathematical proofs

Lecture 4

ICOM 4075

Proofs by construction

A **proof by construction** is one in which an **object that proves the truth value of an statement** is built, or found

There are two main uses of this technique:

- Proof that a statement with an **existential quantifier** is **true**
- And disproof by counterexample: this is a proof that a statement with a **universal quantifier**, is **false**

Note the existential quantifier

Example 1

Statement: "There is a prime number between 45 and 54"

Example 1

Statement: "There is a prime number between 45 and 54"

Proof: Search for an object: we examine one by one, the numbers between 45 and 54, until a prime is found. If no prime were found, the statement would be false.

Number	Is it prime?
45	No, because it is divisible by 5
46	No, because is divisible by 2
47	Yes, 47 is divisible only by 1 and 47

Conclusion: the statement is **true** (no need to check the rest of the numbers from 48 to 54)

Note the universal quantifier: "For all a, b, and d integer"

Example 2

<u>Statement</u>: "If d | a · b then d | a or d | b"

Example 2

Statement: "If $d \mid a \cdot b$ then $d \mid a$ or $d \mid b$"

Proof: By counterexample.

1. Let $d = 6$, $a = 2$ and $b = 3$
2. Then, $a \cdot b = 6$ and thus, $d \mid a \cdot b$
3. But $d = 6$ **does not** divide $a = 2$, **and**
4. $d = 6$ **does not** divide $b = 3$

Therefore, the statement is **false**

Example 3

Statement: "Let m and n be integers. Then, there is no integer k such that

$$(3m+2)(3n+2) = 3k+2"$$

WHAT KIND OF STATEMENT IS THIS?

(doesn't look like an implication)

Example 3

Statement: "Let m and n be integers. Then, there is no integer k such that

$$(3m+2)(3n+2) = 3k+2"$$

Let's parse it (don't forget the quantifiers)

A(m, n) : "m and n are integers" and

B(m, n, k) : "(3m+2)(3n+2) = 3k+2"

Statement:

(For all m, n) A(m, n) (For all k) Not B(m, n, k)

Example 3

As suspected, this is not an implication. So, neither a direct nor a contrapositive proof is possible

Also, the statement is "**negative**" in the sense that ensures that **a property is not possible**. This suggest a contradiction: What is wrong if the property **is possible**?

Negation of the statement: (the property is true)

(There are m, n) A(m, n) (There is k) B(m, n, k)

The negation of the statement implies a false statement

<u>Proof</u>:

1. By hypothesis: m, n, and k are integers
2. $(3m+2)(3n+2) = 9mn + 6(m+n) + 4 = 3(3mn + 2(m+n)) + 4$
3. It follows that $3(3mn + 2(m+n)) + 4 = 3k + 2$
4. And thus, $k = 3mn + 2(m+n) - 2/3$
5. So, there is an integer that is equal to the sum of an integer and a negative fraction

THIS IS FALSE !!!

Example 4

Statement: "The sum of an even number and an odd number is always odd"

Again, the same important question:

WHAT KIND OF STATEMENT IS THIS?

Example 4

Statement: "The sum of an even number and an odd number is always odd"

Let's rephrase it:

"If x is even and y is odd, then x + y is odd"

Makes sense?

Yes, indeed. So, the statement is an implication. And the proof is direct

Example 4

Proof:

1. Since x is even, then x = 2k, for some natural k.
2. Since y is odd, then y = 2q + 1, for some natural q.
3. Thus, x + y = 2k + 2q + 1 = 2(k + q) + 1.
4. Since (k + q) is a natural number, x + y is an odd number.

Example 5: just another direct proof

<u>Statement</u>: "If d | (a + b) and d | a, then d | b"

There is no doubt: THIS IS AN IMPLICATION, but…

Example 5: just another direct proof

Statement: "If d | (a + b) and d | a, then d | b"

Be careful: The hypothesis is "d | (a + b) and d | a".

Proof: Direct.

1. Since d | (a + b), k · d = a + b, for some integer k.
2. Since d | a, q · d = a, for some integer q.
3. Thus, k · d = a + b = q · d + b.
4. And therefore, (k – q) · d = b.
5. Since k – q is an integer, d divides b.

Example 6

Statement: "$m \mid n$ and $n \mid m$ if and only if $n = m$ or $n = -m$."

Here is also clear that this is an
IF AND ONLY IF STATEMENT
So you only have to…

Example 6

Statement: “m | n and n | m if and only if n = m or n = - m.”

Recall that: As all if and only if statement, this statement consists of two implications:

(a) “If m | n and n | m then, n = m or n = - m”

(b) “If n = m or n = - m then, m | n and n | m”

We will prove them separately.

Statement (a)

<u>Proof</u>: direct.

1. The hypothesis is: “m | n and n | m”. Therefore,
2. k · m = n and q · n = m for some integers k and q, respectively.
3. By replacing the second equation in the first one we get k · q · n = n.
4. By dividing by n we get k · q = 1.
5. Thus, either k = q = 1 or k = q = -1 . But,
6. If k = q = 1 m = n, and if k = q = -1, then m = -n.

Statement (b)

Proof:

1. The hypothesis is now “n = m or n = - m”.
2. Assume first that n = m.
3. Then, n divides m since $1 \cdot n = m$; and
4. m divides n since $1 \cdot m = n$, as well.
5. Assume now that n = -m.
6. Then, n divides m since $-1 \cdot n = m$; and
7. m divides n since $-1 \cdot m = n$, as well.

Example 7: Recall our first proof by exhaustion

In the previous lecture we had the statement: "If n is an integer and $2 \le n \le 7$, then $q = n^2 + 2$ is not divisible by 4", which we proved to be true by exhaustion, using the table:

n	q	Divisible by 4?
2	6	No
3	11	No
4	18	No
5	27	No
6	38	No
7	51	No

Example 7 (continuation)

In the same lecture we pointed out that the statement:

“If n is an integer, then $n^2 + 2$ is not divisible by 4”

cannot be proved by exhaustion since it involves infinitely many objects (integers).

Next is a proof for this statement.

Example 7 (continuation)

Statement: "If n is an integer then $n^2 + 2$ is not divisible by 4"

Proof: By contradiction. The negation of the statement is:

"n is an integer and $n^2 + 2$ is divisible by 4"

This is now our hypothesis. As a handy remark, recall that since n is an integer, n may be either even or odd

Example 7: the proof

1. Assume first that n is even. Then $n = 2m$, for some integer m
2. Thus, $n^2 + 2 = (2m)^2 + 2 = 4m^2 + 2$
3. Since $n^2 + 2$ is divisible by 4, we have that
4. $4m^2 + 2 = 4k$, for some integer k.
5. By dividing both sides by 2 we get
6. $2m^2 + 1 = 2k$, k and m^2 integers.
7. So, there is an odd number that is equal to an even number (**The conclusion is false**)

Example 7: the proof

1. Assume now that n is odd. Then $n = 2m + 1$, for some integer m
2. Thus, $n^2 + 2 = (2m + 1)^2 + 2 = 4m^2 + 4m + 2$
3. Since $n^2 + 2$ is divisible by 4, we have that
4. $4m^2 + 4m + 2 = 4k$, for some integer k.
5. By dividing both sides by 2 we get
6. $2m^2 + 2m + 1 = 2(m^2 + m) + 1 = 2k$
7. So again, there is an odd number that is equal to an even number

Summary of Lectures 3 and 4

- Revision of the concepts of integer, natural number, divisible numbers, even, odd, and prime numbers.
- Notions of mathematical statement and mathematical proofs
- Types of mathematical proofs and examples:
  - Direct proofs
  - Proof by exhaustion
  - Use of the contrapositive form of the implication
  - Proof by contradiction
  - If and only if proofs
  - Proofs by construction and their use as counterexamples

Exercises: Prove

1. If $(3n)^2$ is even, then n is even.
2. If d | (d · a + b), then d | b.
3. x · y is odd if and only if x is odd and y is odd.
4. Every odd integer between 2 and 26 is either prime or the product of two primes.
5. If x and z are even numbers then, 4 divides $(x - z)^2$

Exercises

6. Is the statement “If d divides (a + b) or d divides a, then d divides b” true or false? Give a proof or provide a counterexample
7. Is the statement “If d divides (a + b + c) and d divides a and b, then d divides c” true or false? Give a proof or provide a counterexample
8. Parse and prove the statement: “For each integer m there is an integer k such that $(4m + 3)^2 = 2k + 9$”
9. Parse and prove: “There is no integer k such that $(4m + 3)^2 = 2(k + 3)$”