Discrete Mathematics

Topic 02 — Methods of Mathematical Proof

Lecture 03 — Other Proof Techniques

Dr Kieran Murphy

Department of Computing and Mathematics,
Waterford IT.
(kmurphy@wit.ie)

Autumn Semester, 2021

Outline

- Proof by Contradiction, Construction, Induction . . .

Outline

Proof by Contradiction I

Proof by Contradiction

In a proof by contradiction argument you:

- Assume the negative of the claim
  - So a universal claim will become an existence claim, and an existence claim will become a universal claim.
- Then show that the assumption leads to a contradiction.

Proof by Contradiction (Formal Structure)

Given claim

$$P \implies Q$$

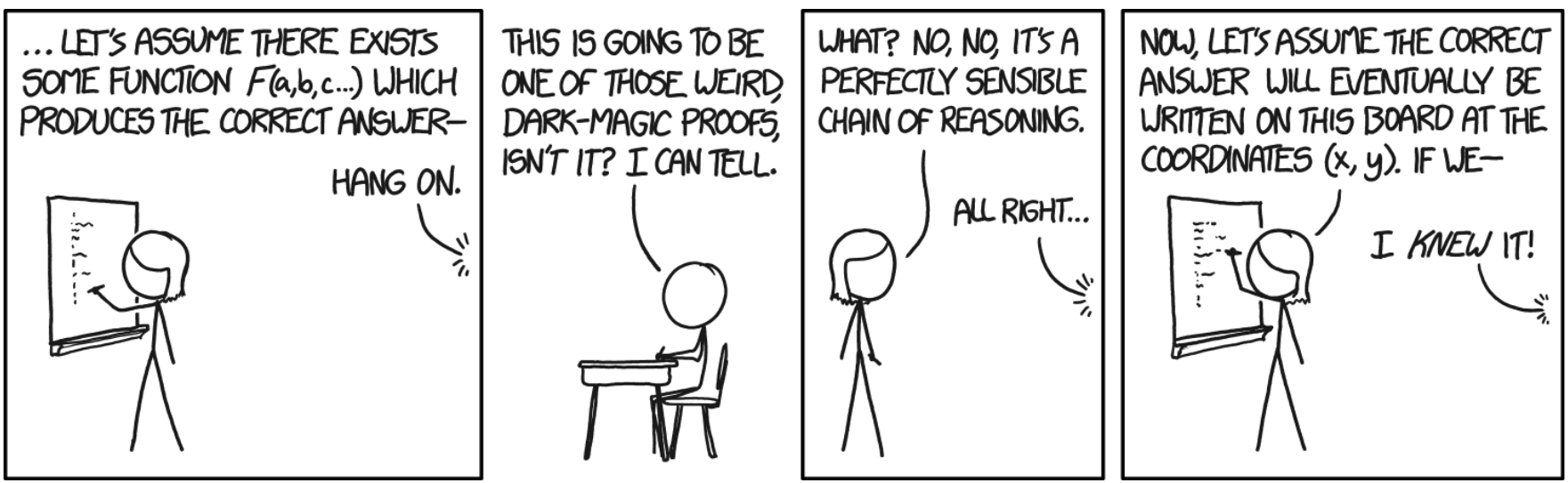
Show that the negative, i.e. $P \Rightarrow \neg Q$, leads to a contradiction, by

1. Assume P.
2. Assume $\neg Q$.
3. Use P and $\neg Q$ to demonstrate a contradiction.

Proof by Contradiction II

Proofs by contradiction can be tricky, you

- Need to be very clear as to what statement you are assuming in order to generate a contradiction.
- In particular, take case when the statement involves a qualifier.



*https://xkcd.com/1724/

Examples

a) Prove that a triangle cannot have more than one right angle.

b) Prove that the $\sqrt{2}$ is irrational.[†]

c) Prove that $\log_2(3)$ is irrational.

d) Let n be an integer. If $3n + 2$ is odd, then n is odd.

e) Prove that there are an infinite number of primes.[‡]

f) There are no integers x and y such that $x^2 = 4y + 2$.

g) The Pigeonhole Principle: If more than n pigeons fly into n pigeon holes, then at least one pigeon hole will contain at least two pigeons. Prove this.

[†] "irrational"= "not rational". A rational number is a number that can be expressed as quotient of two integers p and p which don't have a common factor.

[‡] A prime is an integer greater than one with exactly two divisors.

Outline

Proof by Construction

Proof by Construction

In a proof by construction argument you:

- Are dealing with an existence claim.
- Prove existence of an object by actually constructing it.
- The proof usually involves stating the steps (algorithm) needed to construct the required object.

- This type of proof is more powerful than just an existence proof — this not only proves existence but also create an example.
- Very common in geometry, and graph theory

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 1

Example 1

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Examples

a) Prove that x^n can be computed using only $\log_2(n)$ multiplications when n is a power of 2.

This is a special case of the Montgomery algorithm for computing large integer power quickly — a big deal in cryptography!

b) Prove that the sum of the first n positive integers equals $n(n+1)/2$

Outline

Proof by Induction

Proof by Induction

A proof by induction argument, can be applied when Q, the conclusion in the claim $P \Rightarrow Q$, can be represented as a sequence of related claims, $Q_1, Q_2, Q_3, \ldots$. Then we show, that

- the first claim is true, and
- if any claim is true, then the next claim must also be true.

Proof by Induction (Formal Structure)

Given family of claims, where integer n is 1,2,3,4,...,

$$P \Rightarrow Q_n$$

1. Assume P, (now we need to prove that all of $Q_1, Q_2, Q_3, \ldots$, are true)
2. Prove Q_1. (the basic/initial step)
3. Prove $Q_k \Rightarrow Q_{k+1}$ for arbitrary integer k. (the inductive step)[§]

[§]Instead of attacking the problem directly, we only explain how to get a proof for Q_{k+1} when given a proof for Q_k.

Example 2

Example 2

Suppose an ATM has only twenty euro and fifty euro bills. You can type in the amount you want, and it will figure out how to divide things up into the proper number of twenty and fifty euro bills.
Prove that the ATM can generate any multiple of 10 euro amount ≥ 40.

(by induction).

First we define the proposition (or family of propositions)

$$Q_n : \text{ATM can output } 10n \text{ euro} = 20a + 50b$$

where a and b are nonnegative integers

We want to prove the sequence

$$Q_4, Q_5, Q_6, \ldots$$

Note: In this example we did not start at one (and our stride was 10). □

Example 2

Example 2

Suppose an ATM has only twenty euro and fifty euro bills. You can type in the amount you want, and it will figure out how to divide things up into the proper number of twenty and fifty euro bills.
Prove that the ATM can generate any multiple of 10 euro amount ≥ 40.

(by induction).

First we define the proposition (or family of propositions)

$$Q_n : \text{ATM can output } 10n \text{ euro} = 20a + 50b$$

where a and b are nonnegative integers

We want to prove the sequence

$$Q_4, Q_5, Q_6, \ldots$$

Note: In this example we did not start at one (and our stride was 10). □

Example 2 II

Q_n : $10n = 20a + 50b$ where a and b are nonnegative integers

the basis step, Q_4

$$10(4) \stackrel{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 2 II

Q_n : $10n = 20a + 50b$ where a and b are nonnegative integers

the basis step, Q_4

$$10(4) \stackrel{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 2 II

$$Q_n: \quad 10n = 20a + 50b \qquad \text{where } a \text{ and } b \text{ are nonnegative integers}$$

the basis step, Q_4

$$10(4) \stackrel{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 2 II

Q_n : $10n = 20a + 50b$ where a and b are nonnegative integers

the basis step, Q_4

$$10(4) \stackrel{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 2 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Example 2 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Example 2 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Hence $a \geq 2$, since $10k \geq 40$. To get ten more euro out we replace two twenties by one fifty, i.e.,

$$10k = 20a + 50(0) \implies 10k + 10 = 10(k+1) = 20\underbrace{(a-2)}_{\text{OK, since } a > 2} + 50(1)$$

Example 2 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Hence $a \geq 2$, since $10k \geq 40$. To get ten more euro out we replace two twenties by one fifty, i.e.,

$$10k = 20a + 50(0) \implies 10k + 10 = 10(k+1) = 20\underbrace{(a-2)}_{\text{OK, since } a > 2} + 50(1)$$

We have proven the two steps required in an induction argument, hence we can conclude the sequence of claims are true.

Examples

a) For all integers n, prove that $n^2 + 5n + 6$ is even.

b) Prove that the sum of the first n positive integers equals $n(n+1)/2$

c) Prove for integer $n \geq 4$, that $3^n > 2n^2 + 3n$.