Maths for Computer Science
Proof techniques

Denis TRYSTRAM
Lecture notes MoSIG1

sept. 2024

Context

The main idea of this preliminary lecture is to **introduce the methodology to prove results in Discrete Mathematics** (in the field of combinatorics, summations, counting, graph theory, etc.). We will show how to handle simple results with basic tools that do not require too sophisticated background in Maths.

A subsequent goal is to strengthen the intuition while *doing* Maths.

The holy grail of Mathematics: proving theorems

Schema of classical proofs.

- A *proof* is a sequence of *statements*.
  - The first statement must be an axiom or another proved theorem.
  - Each subsequent statement must be either an axiom or the result of applying a rule of inference to the statements that are already present in the sequence.
- A *theorem* is the last statement of a proof.

Within this formalism: **a theorem is any assertion that is proved.**

A difficulty is that assertions often require some modeling to be turned into mathematical statements.

Overview of proving techniques

- Contradiction *contradictio in contrarium*
- Induction / Recurrences
- Geometric proofs
- Combinatoric proofs
- Algebraic proofs
- Bijections between sets and Pigeon holes
- Unconventional proofs. All means are good!
- Proofs by computers
- Double counting principle (*Fubini*)

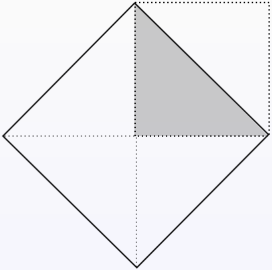
Overview of proving techniques

- Contradiction *contradictio in contrarium*
- Induction / Recurrences
- Geometric proofs
- Combinatoric proofs
- Algebraic proofs
- Bijections between sets and Pigeon holes
- Unconventional proofs. All means are good!
- Proofs by computers
- Double counting principle (*Fubini*)

Always gain intuition before starting for a better understanding of the maths object behind and for choosing a path for solving.

Proof by contradiction

A particular case of Pythagorian theorem for unit isosceles triangles..



Let prove that $\sqrt{2}$ is irrational[1].

[1] that can not be expressed as a ratio of two integers

Proof by contradiction

Assume $\sqrt{2}$ is rational, this means it can be written as $\frac{p}{q}$.
There exists a pair of p and q which have no common divisors.

Proof by contradiction

Assume $\sqrt{2}$ is rational, this means it can be written as $\frac{p}{q}$.
There exists a pair of p and q which have no common divisors.

Thus, $2.q^2 = p^2$.
p^2 is *even* (divisible by 2) then p is also even (the square of an odd number is odd). This means that $p = 2m$ for some positive integer m, which allows us to rewrite:
$2.q^2 = 4.m^2$, after simplification: $q^2 = 2.m^2$
Thus, q must be even.

Proof by contradiction

Assume $\sqrt{2}$ is rational, this means it can be written as $\frac{p}{q}$.
There exists a pair of p and q which have no common divisors.

Thus, $2.q^2 = p^2$.
p^2 is *even* (divisible by 2) then p is also even (the square of an odd number is odd). This means that $p = 2m$ for some positive integer m, which allows us to rewrite:
$2.q^2 = 4.m^2$, after simplification: $q^2 = 2.m^2$
Thus, q must be even.
Both q and p have a common factor (2), which contradicts the assumption that they both share no common prime divisor.

Proof by recurrence

Based on induction principle

Proving that a statement $P(n)$ involving integer n is true.

- **Basis.** Solve the statement for the small values of n.
- **Induction step.** Prove the statement for n assuming it is correct for any $m \leq n - 1$.

Example

Prove the following assertion P(n)

$\forall n$, the nth perfect square is the sum of the first n odd integers.

$$n^2 = 1 + 3 + 5 + \cdots + (2n-3) + (2n-1)$$

Example

Prove the following assertion P(n)

$\forall n$, the nth perfect square is the sum of the first n odd integers.

$$n^2 \;=\; 1 \;+\; 3 \;+\; 5 \;+\cdots+\; (2n-3) \;+\; (2n-1)$$

Proof.

Let us proceed according to the standard format of an inductive argument.

- **Basis.** Because $1 \cdot 1 = 1$, proposition $\mathbf{P}(1)$ is true.
- **Induction step.** Let us assume, for the sake of induction, that assertion $\mathbf{P}(m)$ is true for all positive integers strictly smaller than n.

Consider now the summation

$$1 + 3 + 5 + \cdots + (2n-3) + (2n-1)$$

Because $\mathbf{P}(n-1)$ is true, we know that

$$\begin{aligned} 1 + 3 + \cdots + (2n-1) &= \big(1 + 3 + \cdots + (2n-3)\big) + (2n-1) \\ &= \big(1 + 3 + \cdots + (2(n-1)-1)\big) + (2n-1) \\ &= (n-1)^2 + (2n-1) \end{aligned}$$

By direct calculation, we now find that

$$(n-1)^2 + (2n-1) \;=\; (n^2 - 2n + 1) + (2n-1) \;=\; n^2.$$

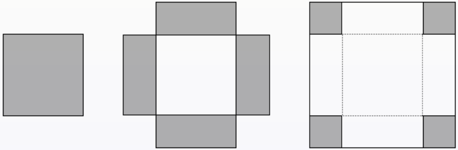
The Principle of (finite) Induction tells us that $\mathbf{P}(n)$ is true for all integer n.

A (old and simple) geometrical proof

- This example has been provided by Al Khwarizmi (XIIth century).
- The solution of the equation $x^2 + 10x = 39$ is determined by means of the surfaces of elementary pieces.

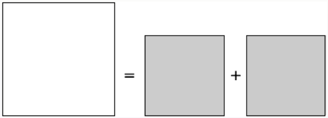
A (old and simple) geometrical proof

We first represent graphically the left hand side $x^2 + 4\frac{5}{2}x$.

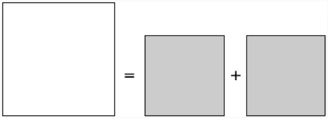


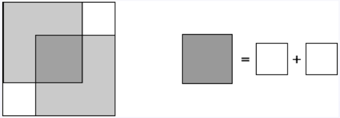
- The surface of the cross is equal to the right hand side.
- Adding the 4 little squares in the border leads to a total surface of $39 + 4\frac{25}{4} = 64$, which is the square of 8.
- We finally deduce the result by the length of a side: $x = 8 - 2\frac{5}{2} = 3$.

Another view of $\sqrt{2}$ is irrational



Another view of $\sqrt{2}$ is irrational





Algebraic proofs

Let consider an example introduced by Lewis carroll[2]

- Two friends are meeting a week-end for hiking.
- They leave their hotel at 3pm and come back at 9pm.
- The only information they have is about walking speed: 4 km/h on the flat, 3 km/h uphill and 6 km/h downhill.
- Could you find out how far they have travelled in total?

[2] Alice in wonderland

Pigeon's holes (relations between sets)

The idea here is to establish a correspondence between two sets (pigeons and boxes).

Principle

If there are more pigeons than boxes, thus, at least one box contains more than one pigeon[3].

[3] we may also think about socks...

Pigeon's holes (relations between sets)

The idea here is to establish a correspondence between two sets (pigeons and boxes).

Principle

If there are more pigeons than boxes, thus, at least one box contains more than one pigeon[3].

Let consider the following problem:

- You are attending a party with n couples. In order to create a nice social atmosphere, the host requests that each attendees shake the hand of every person that he/she does not know.
- Some attendees shake the same number of hands.

[3] we may also think about socks...

Pigeon's holes

- Here, the boxes are the number of times someone shake hands. The persons are the pigeons.
- There are $2n$ persons at the party.
- The number of people that each attendee does not known is $\{0, 1, ..., 2n-2\}$ which contains $2n-1$ elements.

All means are good.

- The problem of friends and strangers at a party.

Assertion

In any gathering of six people, at least one of the following assertions is true.

A. There is a group of three people who know each other.
B. There is a group of three people none of whom knows either of the others.

- Where (and how) to start the proof?!?

If we cannot reduce the provable world to sequences of assertions, then what is our goal?
Using evocative terms, the french mathematician René Thom tells us.

Est rigoureuse toute démonstration, qui, chez tout lecteur suffisamment instruit et préparé, suscite un état d'évidence qui entraîne l'adhésion.

Proof by computers.

The 4-colors theorem (which was a famous conjecture).
Coloring planar graphs using no more than 4 colors.

Constraint: 2 neighbor vertices must have different colors.

Proof by computers.

The 4-colors theorem (which was a famous conjecture).
Coloring planar graphs using no more than 4 colors.

Constraint: 2 neighbor vertices must have different colors.

Easy to color a planar graph in 6 colors.

Preliminary: coloring in 6

Proposition. Every planar graph G is 6-colorable.

Proof (sketch)

1. Remove from graph G a vertex v of smallest degree d_v, together with all its incident edges
   We guarantee that $d_v \leq 5$.
2. inductively color the vertices of the graph left after the removal of v (denoting the smaller graph by G').
   For planar graphs, we use an inductive assumption that can be colored with ≤ 6 colors.
3. Reattach v via its d_v edges and then color v.
   Note that the coloring guarantee in this result allows us to use $d_v + 1$ colors to color G. Because v has degree d_v, it can have no more than d_v neighboring vertices in G', so our access to $d_v + 1$ colors guarantees that we can successfully color v.

Extensions: coloring in 4

- Intermediate step: coloring in 5 colors.
- For 4 colors, the initial proof needed to check the property on more than a thousand of basic configurations!
  It needs a computer.

Double counting

- The informal idea is to establish a one-to-one correspondence between elements of a set (integers).
- This is an important technique widely used in combinatorics

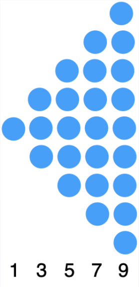
Principle of the double counting[4]

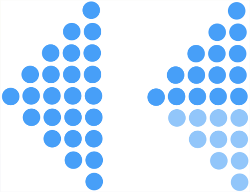
Enumerate the elements of a set by two different methods, one leading to an evidence.

[4] also called Fubini's principle in memory of the mathematician Guido Fubini 1879-1943

Example: compute the sum of odds

- S_n is represented by tokens arranged by columns as follows.





- Rearrange the tokens in order to get an evidence (a perfect square)