CHAPTER 1

Proof techniques (section 2.1)

1.1. Theorems and Informal proofs

What we have seen so far:

> **Argument:** $P_1 \wedge \cdots \wedge P_n \;\rightarrow\; Q$
> **Syntax:** how it's written
> **Semantic:** meaning in a given interpretation
> **Valid argument:**
> True for all interpretations
> True because of its very structure

Proofs of valid argument are purely based on syntactical rewriting rules.

Only arguments that are true for all interpretations can be proved.

1.1.1. Theorems. We are now interested to work in a particular subject (say integer arithmetic).

Définition. A *theorem* is an argument that is valid in this particular subject.

Exemple. If x is even and y is even then xy is even.
$E(x)$: x is even
$(\forall x)\ (\forall y)\ [E(x) \wedge E(y) \;\rightarrow\; E(xy)]$

This argument is true in this context, but not universally true.
How to prove it ?
Implicitly, we add new hypothesis which reflects basic facts of this subject.
For example, we add the following hypothesis:

- x is even if and only if there exists y such that $x = 2y$:

$$(\forall x)\ [P(x) \;\leftrightarrow\; (\exists y)\ x = 2y]$$

Using those new hypothesis, it's now possible to write a formal logic proof of the theorem.
See [**?**, Example 4 p. 87]

1.1.2. Formal and informal proofs: Remember that the goal of a proof is to be read by humans (in particular yourself) in order to convince those humans.

The formal proof above is convincing in the sense that you can check that all the steps are valid. However, it's very difficult to extract the meaning of the proof:

- Why does it work ?
- How could I reuse it for a similar problem ?

The problem is that the keys of the proofs are buried under layers of insignificant details.

So, starting from now, we will write *informal proofs*:

DÉFINITION. An *informal proof* is a narrative descriptions, of the ideas and of the important steps of the proof, without extraneous details.

EXEMPLE. A proof of the theorem above could be written as follow:

PROOF. Let x and y be two even integers. We can take n and m such that $x = 2n$ and $y = 2m$.

Then, $xy = 2(2nm)$. Since $2nm$ is an integer, xy is an even number. □

Let see which details we omitted:

(1) Let x and y be two even integers.
    Implicit universal instantiation
(2) We can take n and m such that $x = 2n$ and $y = 2m$.
    Implicit universal instantiation for x and y of the definition of an even number
    Implicit existential instantiation for n and m
(3) Then, $xy = 2(2nm)$
    Implicit use of rules of arithmetic
(4) Since $2nm$ is an integer, xy is an even number:
    Implicit universal instantiation of the definition of an even number
    Implicit universal generalization to get the final result

PROBLEM 1.1.1. Which details can we omit, and which not ?

A reader will be convinced by the proof if he can check that he could translate each step of the proof into one or several steps of a formal proof.

So, this all depends on WHO reads the proof!

You should not write your proof for your instructor, but for yourself, and for everybody else in the class.

A good rule of thumb is to imagine yourself rereading the proof in a few month, and to check that even then, you could possibly translate the proof into a formal one.

The difference between formal and informal proofs is very similar to the difference between assembly and, say, C++ or Java. A C++ program is not usable by itself. It's usable because it's possible to translate it into assembly language.

However, there does not exists, and most likely will never exists, a compiler that transforms informal proofs into formal proofs. English is much to rich a language for this.

1.1.3. Formal and informal theorems: Most of the time, we also won't write theorems as a formal argument, but rather with an English sentence that could be translated into a formal argument:

THÉORÈME. *Let x and y be two integers. [Some definitions: interpretation]*
Assume x and y are even. [Some hypothesis: $P_1 \wedge \cdots \wedge P_n$]
Then, xy is even. [Consequent: Q]

1.1.4. To Prove or not to prove. In textbooks, you can be asked: prove that ...

- you know in advance it's true;
- you just have to figure out how to prove it.

Usually, in real life, you first have to find what to prove.

- you don't even know in advance if it's true.

Two jobs:

- Find the good questions
- Prove or disprove those questions

DÉFINITION. A *conjecture* is a statement that you guess is true, but that you have not proved or disproved yet.

Classical steps:

(1) Explore some examples
(2) Try to see some pattern emerging
(3) Formulate a conjecture
(4) Try to prove (or disprove it)

Steps 1-3 are inductive reasoning, whereas step 4 is deductive reasoning.

Finding the good questions is as important as solving them !

EXEMPLE. Fermat's conjecture.

1.1.5. Some "research" around the factorial.

DÉFINITION. Let n be an integer. The factorial of n is the number $n! := n(n-1)\cdots 1$.

For example, $1! = 1$ and $4! = \dot{4} \cdot 3 \cdot 2 \cdot 1 = 24$.

PROBLEM 1.1.2. How big is $n!$?

1.2. Proof techniques

We want to prove some argument of the form $P \rightarrow Q$.

1.2.1. Disproof by counter example.

CONJECTURE. *If n is a positive integer, then $n! < n^3$.*

1.2.2. Direct proof.

DÉFINITION. *Direct proof*

(1) *Assume P*
(2) Deduce Q

EXEMPLE. Prove that if x and y are even, then xy is even.

EXERCICE 1. Prove that if x and y are even, then $x + y$ is even.

1.2.3. Proof by contraposition.

EXEMPLE. Prove that if n^2 is odd, then n is odd.

Hint: prove instead that if n is even, then n^2 is even.

DÉFINITION. *Proof by contraposition:*

(1) Assume Q' (the consequent is false)
(2) Prove P' (the antecedent is also false)

This technique relies on the fact that $P \rightarrow Q$ is equivalent to $Q' \rightarrow P'$.

EXERCICE 2. Prove that xy is odd if and only if x and y are odd.

1.2.4. Exhaustive proof.

PROBLEM 1.2.1. Can a proof by example be valid ?

Yes, if there is a finite number of cases to be treated.

EXEMPLE. Propositional logic formula (the truth table is finite)

DÉFINITION. *Proof by exhaustion* means that all cases have been exhausted.
(and so are you ...).

EXEMPLE. Drawing a figure without lifting the pencil and without retracing a line.

1.2.5. Some "research" around rational numbers.

DÉFINITION. A number x is *rational* if it can be written as $\frac{p}{q}$, where p and q are integers.

EXEMPLE. $5, \frac{-7}{5}, \frac{1}{-3}, \frac{14}{4}, \frac{7}{2}, \dots$ are rational.

PROBLEM 1.2.2. Properties of rational numbers ?

REMARQUE. If x is rational, it's always possible to choose p and q so that:

- q is positive
- p and q are *relatively prime*
  I.e., the biggest common divisor of p and q is 1.

PROBLEM 1.2.3. Are all numbers rational ?

PROBLEM 1.2.4. Assume x and y are rational.

(1) Is $x + y$ rational ?
(2) Is xy rational ?
(3) Is $\frac{x}{y}$ rational ?

PROBLEM 1.2.5. Is the square root of an integer a rational number ?

PROBLEM 1.2.6. Prove that the square root of 2 is irrational.

1.2.6. Proof by contradiction.

THÉORÈME. *The square root of* 2 *is irrational.*

PROOF. Let's assume the square root of 2 is rational.
Let p and q be two integers such that $\sqrt{2} = \frac{p}{q}$ and p and q are relatively prime.
Then, we have $2 = \left(\frac{p}{q}\right)^2$, and so $2q^2 = p^2$.
Therefore p^2 is even, and we have seen that this implies that p is also even.
Let k be the integer such that $p = 2k$.
Then, we have $2q^2 = p^2 = (2k)^2 = 4k^2$, and so $q^2 = 2k^2$.
It follows that q^2 is even, and so q is also even.
Conclusion: p and q are both even.
That's a contradiction, since p and q are relatively prime! □

DÉFINITION. *Proof by contradiction*

(1) Assume the contrary
(2) Deduce a contradiction

This technique relies on the fact that:

(1) $Q \wedge Q'$ is always false
(2) if $P \to 0$ is true, then P is false.

1.2.7. Serendipity.

EXEMPLE. The chess board problem.

1.3. Summary

Goal	Technique	Name
$P \to Q$	Assume P ; deduce Q.	Direct proof/Deduction method
$P' \to Q'$	Prove $Q \to P$.	Proof by contraposition
Q'	Assume Q; deduce a contradiction.	Proof by contradiction
$P \leftrightarrow Q$	Prove $P \to Q$; prove $Q \to P$.	
$P \wedge Q$	Prove P ; prove Q.	
$P \vee Q$	Prove $P' \to Q$	
$(P_1 \vee P_2) \to Q$	Prove $P_1 \to Q$; prove $P_2 \to Q$	Proof by cases
$(\forall x)\ Q(x)$	Let x; prove $Q(x)$	ui / ug
$(\exists x)\ Q(x)$	Construct a such that $Q(a)$	eg
	Be smart	Serendipity