Logical Formalism (🇫🇷 *Formalisation logique*)

Introduction

Adrien Pommellet, LRE

September 3, 2024

What Are Mathematics?

- Performing **calculations** has very little to do with actual science.
- Neither does **rote learning** nor **random guesses**.
- The point of mathematics is to find **true statements**.

Why Logics?

- Everyday language is too ambiguous, hence not suitable for mathematics.
- The meaning of each word has to be defined rigorously; vague statements shall not be tolerated.
- We shall learn how to write proper **proofs**.

Logics and Proofs

Mathematics is of the utmost importance in the field of computer science.

Indeed, consider the following uses:

Proving algorithms. Does an algorithm indeed **solve** a given problem?

Measuring complexity. How **efficient** is a given algorithm? What's the worst case scenario?

Writing correct programs. A **rigorous** proof is somewhat similar to a flawless program in many ways.

Tangible Goals

- Identify in a mathematical statement the relevant **types**, **quantifications**, and **relations**.
- Formalise a statement as a **propositional formula**.
- **Parse** the structure of a complex mathematical statement as the composition of related sub-statements.
- Apply a relevant **proof pattern**[1]: by contradiction, by double implication, by double inclusion, by bijection, by contraposition, by induction, by analysis and synthesis.
- Find the appropriate **representation** among a variety of equipotent encodings in order to count a set.

[1] *motif de preuve*

Course Overview

- The full course is split into six **lectures** of two hours each.
- The matching slides can be found on **Moodle**.
- There are four **tutorials** of two hours each. For each tutorial, a matching exercise sheet with a fair amount of extra material can be downloaded on **Moodle**, with the exception of the last one that is a **mock-up exam**.
- Attend the lectures, prepare the exercise sheet, attend the tutorial, then try to do the extra exercises.

The Dreaded Exams

- A programming assignment (**3 points**) + a mid-term Moodle exam (**3 points**) + a final written exam (**14 points**).
- Mostly short problems with an emphasis on **rigorous proofs**.
- The final exam will be **hand graded**.

Good luck!

Logical Formalism

Mathematical Objects

Adrien Pommellet, LRE

September 4, 2024

Variables

- We will learn how to manipulate mathematical objects, be they simple or complex.
- We will name them unambiguously using **variables**: two different objects must be named differently.
- A **rule of thumb**: two similar objects should have similar names.

E The statement "$n, m \in \mathbb{N}$ and $x, y \in \mathbb{R}$" is easier to parse than "$n, x \in \mathbb{N}$ and $y, m \in \mathbb{R}$".

Sets (🇫🇷 *Ensembles*)

Collecting objects

- We need to be able to **gather** and manipulate objects.
- A **set** is merely a well-defined collection of objects.

E $\mathbb{N}$, $\mathbb{R}$, the prime numbers $\mathbb{P}$, the points of a line, etc.

Sets

Representing sets

- Each object in a set can appear **only once**: there are no duplicates.
- A finite set containing n elements can be written $\{x_1, \ldots, x_n\}$. This indexing is a purely arbitrary choice and may be **unordered**.
- The set $\{x\}$ containing only the element x is called a **singleton**. It should not be mistaken with x itself.

E $\{0, 1, 2\}$ and $\{2, 1, 0, 2\}$ represent the same set, but the latter notation is clumsy.

Sets

Shaky foundations

Set theory is somewhat flawed because of the **catalogue paradox**.

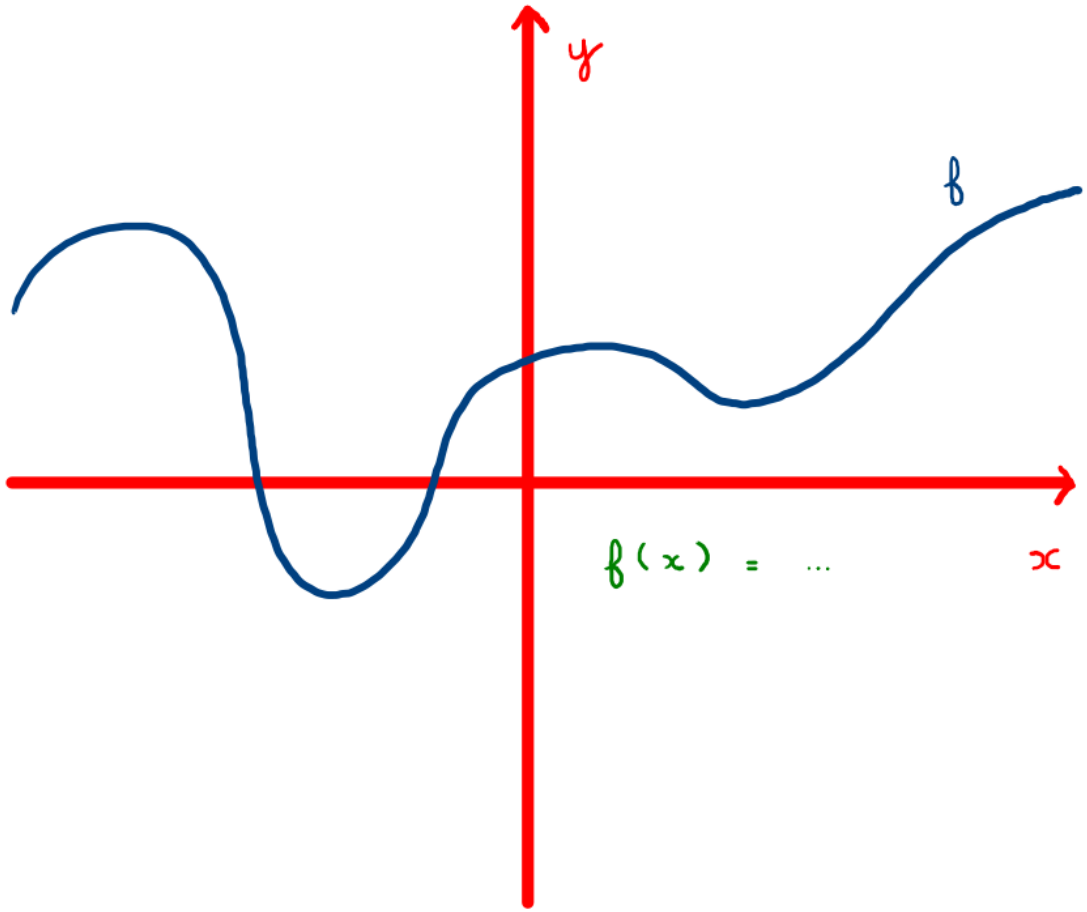
Consider a library that follows **three rules**:

1. Each library section features a catalogue listing its contents.
2. Some catalogues list themselves, others do not.
3. A special catalogue lists all the catalogues that do not list themselves.

? The paradox consists in the following question: **does the special catalogue list itself**?

Functions

What is a function?



Functions

An engineer's answer

A function takes an input of a **given type** and returns a **single** value of another (possibly different) **type**.

Functions

Implementing a specification

Consider the following C++ function:

```
int f(std::vector<int> v) {
  int m;
  for (int i = 0; i < v.size(); i++)
    if (v[i] > v[m]) m = i;
  return m;
}
```

It **should** return the index of the highest value element of an integer vector.

Can you find at least two issues with this implementation?

Functions

Check the inputs

The empty vector should not be a valid input.

```
int f(std::vector<int> v) {
  assert(v.size() != 0);
  int m = 0;
  for (int i = 0; i < v.size(); i++)
    if (v[i] > v[m]) m = i;
  return m;
}
```

One should be wary of the function's **domain**: the **actual** set of input values the function can use as an input.

Functions

Restricting the output

Note that `f` only ever outputs nonnegative[1] integers. We may therefore restrict its output type.

```
unsigned int f(std::vector<int> v) {
  assert(v.size() != 0);
  unsigned int m = 0;
  for (unsigned int i = 0; i < v.size(); i++)
    if (v[i] > v[m]) m = i;
  return m;
}
```

A function's **image** may be smaller than its theoretical type.

[1] *positif*

Functions

Be wary of specifications

- What is the expected output on the input `[2,3,1,3]`?
- Function `f` returns the **smallest** index of the highest value element of the integer vector `v`.
- The original specification is poorly written as it fails to define the answer **unambiguously**.
- We must ensure that a given input only yields[2] a **single** output.

[2] *conduit à*

Functions

More than equations

- A function is not necessarily defined by an equation or an **explicit** formula. Consider computer programs.
- Definitions written using mathematical constraints may not always guarantee that an input always yields a **single** output.
- We must also be wary of respecting the input and the output types.

Practical Application

Exercise 1. Are the following objects functions? If they are, describe their domain and image.

1. Minimum.
2. Derivation.
3. Anti-derivation (computing the primitive).
4. The `C` function `malloc`.

Answer I

1. Assuming we are considering **non-empty** sets of integers, it is a function that takes a **set** as input and returns **its smallest value**. Not every set of (signed) integers admits a minimum[3]: only sets with a lower bound do.
   Note that it is possible to write a function that takes a set as input and returns a value.
2. It is a function defined on **differentiable** real functions that returns real functions.
   Note that it is possible to write a function that takes a function as an input and returns a function.

[3] *Tout ensemble d'entiers n'admet pas **forcément** un minimum.*

Answer II

3. It is not a function as a real function may admit an infinite number of primitives.
   Consider $f : x \in \mathbb{R} \mapsto 1$. Both $g : x \in \mathbb{R} \mapsto x \in \mathbb{R}$ and $h : x \in \mathbb{R} \mapsto x + 1 \in \mathbb{R}$ are primitives of f.
4. `malloc` takes an `unsigned int` as an input and returns a `void *` pointer. However, it is not a function in the **mathematical sense** of the term: indeed, two calls with the same input value may return different addresses depending on the execution context.
   What is `malloc(32)`? There is no universal answer to this question.

Propositions

Propositions are merely statements on mathematical objects to which we assign a truth value.

The following principle applies:

Law of the excluded middle (🇫🇷 *tiers exclu*)

A proposition P is either **true** or **false**.

This axiom states that there are only two possible and mutually exclusive truth values.

Propositions

Logical connectors

We can combine existing propositions P and Q to build new propositions using the following Boolean connectors:

$P \implies Q$. **If** P is true **then** Q must be true as well.

$P \wedge Q$. **Both** P and Q are true.

$P \vee Q$. **At least one** of the two propositions P and Q is true.

$\neg P$. P is **false**.

$P \iff Q$. P and Q have the **same truth value**: they're either both true or both false.

Proofs

Rigorous arguments

A **mathematical proof** is an argument logically guaranteeing that a proposition is true.

Proofs

The logical implication $\implies$

- Mathematical truths are often expressed as **theorems**: if a hypothesis P is true, then a conclusion Q must be true as well.
- To this end, we consider propositions of the form $P \implies Q$.
- What would be a **rigorous** proof of such a proposition?

? Q being true and P being false does not contradict $P \implies Q$.

Proofs

Proof patterns

Do not write random proofs but structure them instead through the (mandatory) explicit use of **proof patterns**.

Logical Connectors

A proof pattern for $\implies$

Goal. Prove that $P \implies Q$ is true.

If P is true ...

Flow from the hypothesis to the conclusion. Write a linear series of deductions until you reach the conclusion.

Remember your definitions. Express the hypothesis P in a detailed manner by making the definitions explicit.

Write common properties. Can you think of some obvious, immediate consequences of P as a starting point?

...then Q is true.

Practical Application

Exercise 2. Prove that if $n \in \mathbb{N}$ is even[4], then n^2 is even as well.

[4] *pair*

Answer

Goal. Prove that $\boxed{n \in \mathbb{N} \text{ is even}} \implies \boxed{n^2 \text{ is even}}$. Explicit the goal.

Let $n \in \mathbb{N}$ be an **even** integer. Explicit the hypothesis.
There exists $k \in \mathbb{N}$ such that $n = 2k$.
Thus $n^2 = 4k^2 = 2 \cdot 2k^2$, hence n^2 is **even**. Explicit the conclusion.

Proof patterns

A somewhat common mistake

Assume that $1 = 2$ is true.

Then $0 \times 1 = 0 \times 2$ is true.
Thus $0 = 0$ is true.
But $0 = 0$ is indeed true.
~~Therefore $1 = 2$ is true.~~
Therefore $\boxed{1 = 2} \implies \boxed{0 = 0}$ is true.

Proof patterns

A contractual operation

- The formula $P \implies Q$ is purely **contractual**: it does not mean that P **causes** Q, but instead that Q must be true whenever P is.
- As a consequence, if P is false, then $P \implies Q$ is **always true**, regardless of Q's truth value.
- However, if both P and $P \implies Q$ are true, then Q is **indeed true**.

E Here, the implication $(1 = 2) \implies (0 = 0)$ and the conclusion $(0 = 0)$ are **true** despite the original hypothesis $(1 = 2)$ being **false**.

Proof patterns

A similar mistake

Prove that for all $x, y \in \mathbb{R}$, $\boxed{xy \geq 0} \implies \boxed{x + y \geq 2 \times \sqrt{xy}}$.

If we assume $xy \geq 0$, note that:

$$\begin{aligned} & x + y \geq 2 \times \sqrt{xy} \\ \implies & (x+y)^2 \geq 4xy \\ \implies & x^2 + 2xy + y^2 \geq 4xy \\ \implies & x^2 - 2xy + y^2 \geq 0 \\ \implies & (x-y)^2 \geq 0 \end{aligned}$$

But $(x-y)^2 \geq 0$ is obviously true.

~~Therefore the property is true.~~

Consider the counter-example $x = y = -1$.

A Property of the Implication

An actual proof

Prove that for all $x, y \in \mathbb{R}$, $\boxed{xy \geq 0} \implies \boxed{|x+y| \geq 2 \times \sqrt{xy}}$.

Let $x, y \in \mathbb{R}$ such that $xy \geq 0$. Then:

$$\begin{aligned}
(x-y)^2 &\geq 0 \\
x^2 - 2xy + y^2 &\geq 0 \\
x^2 + 2xy + y^2 &\geq 4xy \\
(x+y)^2 &\geq 4xy \\
|x+y| &\geq 2 \times \sqrt{xy}
\end{aligned}$$

Thus the property holds.

Logical Formalism

More Proof Patterns

Adrien Pommellet, LRE

September 4, 2024

Disjunction, conjunction, equivalence

Richer proofs

- Theorems may feature the operators $\wedge$ and $\vee$ as well.
- You may have to **rewrite** a proposition to make the $\wedge$ and $\vee$ operators more apparent.
- Note that the mathematical $\vee$ should not be mistaken for the common, everyday or.

E The sentence *'Pay a fine or go to jail.'* features an **exclusive** or.

Disjunction, conjunction, equivalence

A proof pattern for $\wedge$ as a conclusion

Goal. Prove that $P \implies (Q \wedge R)$ is true.

Suppose that P is true ...

Split a complex goal into subgoals. Split the proof into more manageable subproofs by detailing the original goal.

Subgoal 1. Prove that Q is true.

Subgoal 2. Prove that R is true.

Disjunction, conjunction, equivalence

A proof pattern for $\wedge$ as a hypothesis

Goal. Prove that $(P \wedge Q) \implies R$ is true.

If P is true ...
... and Q is true ...
... then R is true.

Disjunction, conjunction, equivalence

A proof pattern for $\vee$ as a hypothesis

Goal. Prove that $(P \vee Q) \implies R$ is true.

Subgoal 1. Prove that $P \implies R$ is true.

If P is true ...
...then R is true.

Subgoal 2. Prove that $Q \implies R$ is true.

If Q is true ...
...then R is true.

Disjunction, conjunction, equivalence

The logical equivalence $\iff$

In order to prove equivalences of the form $P \iff Q$, we will rely on the following property:

Double implication

$P \iff Q$ is true if and only if $P \implies Q$ and $Q \implies P$ are true.

Disjunction, conjunction, equivalence

A proof pattern for $\iff$

Goal. Prove that $P \iff Q$ is true.

Subgoal 1. Prove that $P \implies Q$ is true.

If P is true ...
...then Q is true.

Subgoal 2. Prove that $Q \implies P$ is true.

If Q is true ...
...then P is true.

Patterns Based on Negation

Proof by contradiction I

We consider a **proof pattern** relying on the negation $\neg$.

Goal. Prove that P is true.

Assume that $\neg P$ is true . . .

. . . then prove something that contradicts another property we know or assumed to be true.

Therefore P cannot be false, thus must be true.
This is a consequence of the law of the excluded middle.

Practical Application

Exercise 1. Prove that $\sqrt{2}$ is irrational. Remember that $k \in \mathbb{Q}$ if and only if $\exists p, q \in \mathbb{Z}$ such that $k = \frac{p}{q}$ and p, q are **relatively prime**.

Answer

Goal. Prove that $\sqrt{2}$ is irrational.

Assume that $\sqrt{2}$ is rational.

$\exists p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$ and p, q are relatively prime.
Note that $2 = \frac{p^2}{q^2}$. Thus $p^2 = 2 \cdot q^2$ is even, then p^2 is even.
As a consequence, p is **even**. We admit this property.
$\exists k \in \mathbb{Z}$ such that $p = 2k$. Thus, $2 = \frac{4k^2}{q^2}$, hence $q^2 = 2k^2$.
Therefore, q^2 is **even**, thus q as well.
Finally, p and q are both even, hence admit a **common divider** different from 1, despite being relatively prime. This is impossible.

By **contradiction**, $\sqrt{2}$ is irrational.

Patterns Based on Negation

Proof by contradiction II

Goal. Prove that $P \implies Q$ is true.

If P is true ...

Assume that $\neg Q$ is true ...

... then prove something that contradicts P or a true property.

Therefore Q cannot be false, thus must be true.

Patterns Based on Negation

Common logical equivalences

The following equivalences are **well-known results**:

$$
\begin{aligned}
\neg\neg P &\iff P \\
P \wedge (Q \vee R) &\iff (P \wedge Q) \vee (P \wedge R) \\
P \vee (Q \wedge R) &\iff (P \vee Q) \wedge (P \vee R) \\
\neg(P \vee Q) &\iff \neg P \wedge \neg Q \\
\neg(P \wedge Q) &\iff \neg P \vee \neg Q \\
P \implies Q &\iff \neg P \vee Q \\
\neg(P \implies Q) &\iff P \wedge \neg Q \\
P \implies Q &\iff \neg Q \implies \neg P
\end{aligned}
$$

Practical Application

Exercise 2. Are the following properties true in the general case? If they're not, use **counter-examples** to falsify them.

$$\begin{aligned}
\neg(P \implies Q) &\iff \neg P \implies \neg Q \\
P \implies Q &\iff \neg P \implies \neg Q \\
P \iff (Q \wedge R) &\iff (P \iff Q) \wedge (P \iff R) \\
(P \wedge Q) \implies R &\iff (P \implies R) \wedge (Q \implies R)
\end{aligned}$$

Answer

1. Consider $P_1 =$ "It rains." and $Q_1 =$ "I brought my umbrella.". Both $P_1 \implies Q_1$ and $\neg P_1 \implies \neg Q_1$ are true. Thus:
   $\neg(P \implies Q) \not\Longleftrightarrow \neg P \implies \neg Q$.
2. Consider $P =$ "'I am human." and $Q =$ "I will die.". $P_2 \implies Q_2$ is true but not $\neg P_2 \implies \neg Q_2$. Thus:
   $P \implies Q \not\Longleftrightarrow \neg P \implies \neg Q$.
3. Let T be a quadrilateral. Consider $P_3 =$ "T is a square", $Q_3 =$ "T'is a lozenge", and $R_3 =$ "T is a rectangle". $(P_3 \iff Q_3)$ and $(P_3 \iff Q_3)$ are false but $P_3 \iff (Q_3 \wedge R_3)$ is true. Thus:
   $P \iff (Q \wedge R) \not\Longleftrightarrow (P \iff Q) \wedge (P \iff R)$
   But $\Longleftarrow$ is true in the general case.
4. Similar to 3.
   Again, $\Longleftarrow$ is true in the general case.

Patterns Based on Negation

Proof by contraposition

Knowing that $(P \implies Q) \iff (\neg Q \implies \neg P)$ yields an alternative **proof pattern** for implications that relies on $\neg$.

Goal. Prove that $P \implies Q$ is true.

Equivalent goal. Prove that $\neg Q \implies \neg P$ is true.

If $\neg Q$ is true ...
... then $\neg P$ is true.

Practical Application

Exercise 3. Prove that for $n \in \mathbb{N}$, if n^2 is even, then n is even as well.

Answer

Goal. Prove that for $n \in \mathbb{N}$, $\boxed{n^2 \text{ is even}} \implies \boxed{n \text{ is even}}$.

Equivalent goal. Prove that for $n \in \mathbb{N}$, $\boxed{n \text{ is odd}} \implies \boxed{n^2 \text{ is odd}}$.

Assume $n \in \mathbb{N}$ is odd. There exists $k \in \mathbb{N}$ such that $n = 2k + 1$.
Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$.
Thus n^2 is odd.

Patterns Based on Negation

Contradiction or contraposition

- Do not mistake the two patterns!
- Proof by **contraposition** comes in handy when $\neg Q$ is easier to express and yields more interesting consequences than starting from P. One can then prove $\neg Q \implies \neg P$.
- Proof by **contradiction** helps when $\neg Q$ is easier to express than Q. Then one can work from $P \wedge \neg Q$ and look for a contradiction.

Case Disjunction

Applying the law of the excluded middle

- We know that for any proposition R, $R \vee \neg R$ is always true.
- As a consequence, $P \wedge (R \vee \neg R) \iff P$: true propositions are neutral elements for $\wedge$.
- Thus, $P \implies Q$ is true if and only if **both** $(P \wedge R) \implies Q$ and $(P \wedge \neg R) \implies Q$ are true.

Case Disjunction

A new proof pattern

If we can intuit the right R, we can apply a new **proof pattern**:

Goal. Prove that $P \implies Q$ is true.

Consider a proposition R.

Subgoal 1. Prove that $(P \wedge R) \implies Q$.

If P and R are true ...
...then Q is true.

Subgoal 2. Prove that $(P \wedge \neg R) \implies Q$.

If P is true and R is false ...
...then Q is true.

Case Disjunction

A proof pattern for $\vee$ as a conclusion

Goal. Prove that $P \implies (Q \vee R)$ is true.

If P is true ...

Use a **case disjunction**. Q can either be true or false; in both cases, we want $Q \vee R$ to be true.

Assume that Q is true.

Then obviously $Q \vee R$ is true. No further proof is needed.

Assume that Q is false.

If P is true and Q is false ...
... then R must be true.

Practical Application

Exercise 4. Prove that $\forall n \in \mathbb{N}$, $\frac{n(n+1)}{2} \in \mathbb{N}$.

Answer

Goal. Prove that $\forall n \in \mathbb{N}, \frac{n(n+1)}{2} \in \mathbb{N}$.

Subgoal 1. Prove that property if $\boxed{n \text{ is even}}$.

There exists $k \in \mathbb{N}$ such that $n = 2k$.
Thus $\frac{n(n+1)}{2} = \frac{2k(2k+1)}{2} = k(2k+1) \in \mathbb{N}$.

Subgoal 2. Prove that property if $\boxed{n \text{ is odd}}$.

There exists $k \in \mathbb{N}$ such that $n = 2k+1$.
Thus $\frac{n(n+1)}{2} = \frac{(2k+1)(2k+2)}{2} = (2k+1)(k+1) \in \mathbb{N}$.

How to Use Proof Patterns

- The **structure** of the proposition to prove will often yield an obvious proof pattern. E.g. an equivalence requires a double implication.
- If said structure is not obvious, explicit all the **hypotheses** and their matching **definitions**.
- Use the right proof patterns and sub-goals to design a **proof skeleton** then fill in its blanks. Do not rush, write the skeleton first.
- You know the hypotheses and the conclusion. To find the intermediate steps, review **relevant properties** that can be immediately deduced from the hypotheses or result in the conclusion.

See you next class!

Logical Formalism

Set Theory

Adrien Pommellet, LRE

September 4, 2024

Operations on Sets

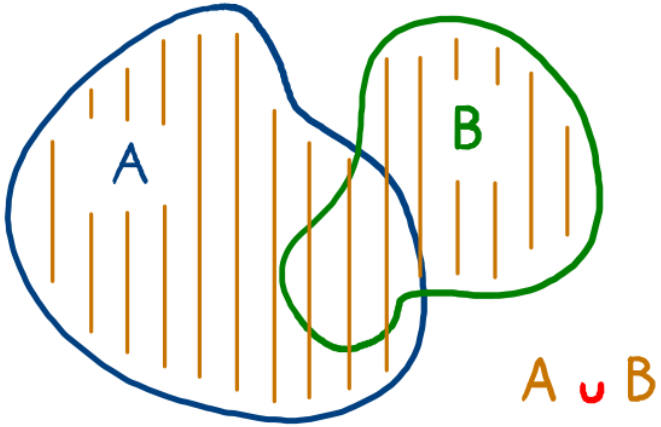
The $\in$ predicate

- Formally, a set E is matched to a **predicate** $\in$ such that x **belongs** to E if and only if the statement $x \in E$ is true.
- We also introduce the predicate $x \notin E \iff \neg(x \in E)$.
- We define the **empty set** $\emptyset$ such that no element belongs to $\emptyset$: the proposition $x \in \emptyset$ is always false.

Operations on Sets

The union $\cup$

Given two sets A and B, we introduce their **union** $A \cup B$ such that $x \in A \cup B$ if and only if $(x \in A) \vee (x \in B)$.

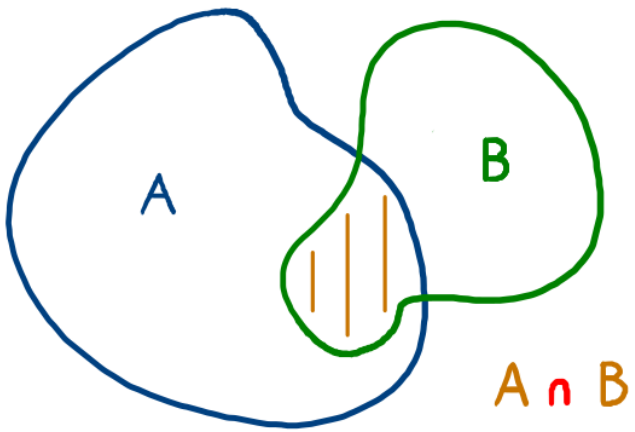


E Consider $\mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_-$. Note that 0 belongs to **both** $\mathbb{Z}_+$ and $\mathbb{Z}_-$.

Operations on Sets

The Intersection $\cap$

Given two sets A and B, we introduce their **intersection** $A \cap B$ such that $x \in A \cap B$ if and only if $(x \in A) \wedge (x \in B)$.

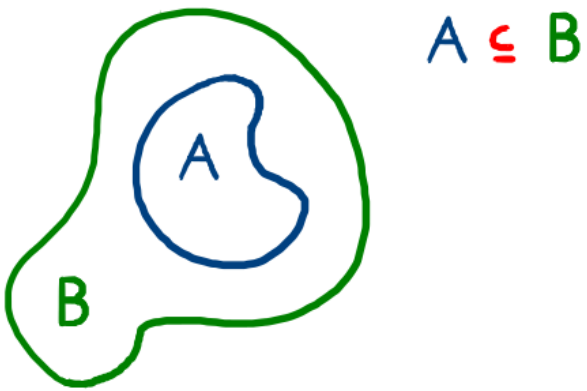


E The intersection of two distinct lines in $\mathbb{R}^2$ is either $\emptyset$ or a singleton.

Operations on Sets

The subset relation $\subseteq$

Given two sets A and B, we introduce the **subset relation**: $A \subseteq B$ if and only if $(x \in A) \implies (x \in B)$.



E You should already know that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Operations on Sets

The simple inclusion pattern

The logical implication $\implies$ yields the following **proof pattern**:

Goal. Prove that $A \subseteq B$.

Let $x \in A \ldots$
$\ldots$ then $x \in B$.

Practical Application

Exercise 1. Let $A = \{a, b, c\}$ and $B = \{a, d\}$. Explicit the sets:

$$A \cup A$$
$$A \cap A$$
$$A \cup B$$
$$A \cap B$$
$$A \cap B \cup \{e\}$$

Answer

$$
\begin{aligned}
A \cup A &= \{a, b, c\} \\
A \cap A &= \{a, b, c\} \\
A \cup B &= \{a, b, c, d\} \\
A \cap B &= \{a\} \\
A \cap (B \cup \{e\}) &= \{a\} \\
(A \cap B) \cup \{e\} &= \{a, e\}
\end{aligned}
$$

There is no **canonical precedence rule** on $\cup$ and $\cap$. Always use parentheses.

Operations on Sets

Equality of sets

- Given two sets A and B, we introduce the **equality relation**: $A = B$ if and only if $(x \in A) \iff (x \in B)$.
- Remember that $(P \iff Q) \iff (P \implies Q) \wedge (Q \implies P)$.
- As a consequence, $(A = B) \iff (A \subseteq B) \wedge (B \subseteq A)$.

Operations on Sets

The double inclusion pattern

Goal. Prove that $A = B$.

Subgoal 1. Prove that $A \subseteq B$.

Let $x \in A$ ...
... then $x \in B$.

Subgoal 2. Prove that $B \subseteq A$.

Let $x \in B$ ...
... then $x \in A$.

Set Theory

Power sets

- Given a set E, we introduce $\mathcal{P}(E)$, the **power set** of E such that $X \in \mathcal{P}(E) \iff X \subseteq E$.
- $\mathcal{P}(E)$ is a **set of sets**.
- Note that $\emptyset \in \mathcal{P}(E)$ and $E \in \mathcal{P}(E)$ for any set E.

Practical Application

Exercise 2. Explicit the set $\mathcal{P}(\{a, b, c\})$.

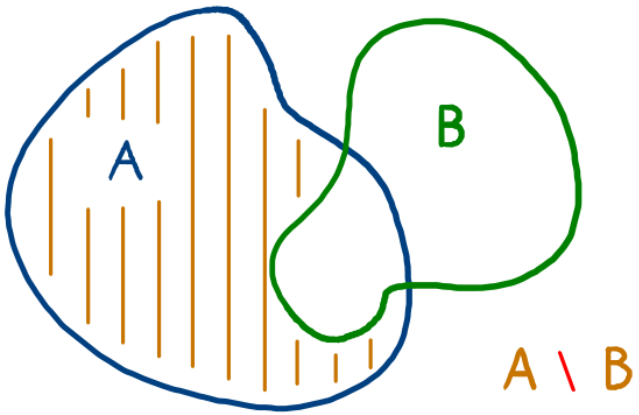
Answer

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Set Theory

The set subtraction $\setminus$

Given two sets A and B, we introduce the **subtraction** $A \setminus B$ of A by B such that $x \in A \setminus B$ if and only if $(x \in A) \wedge (x \notin B)$.

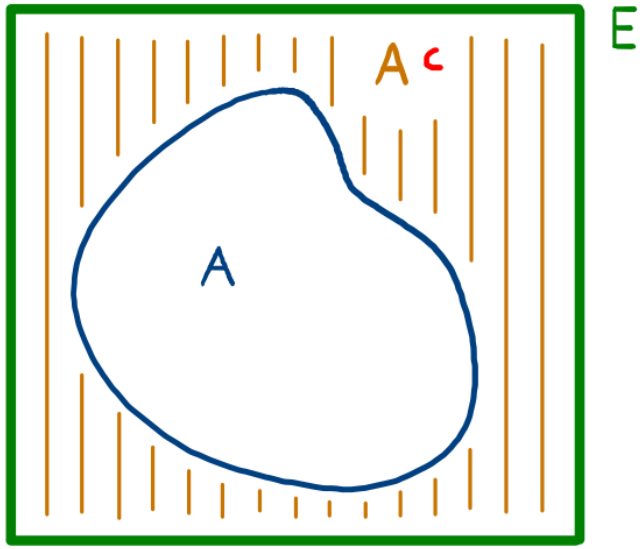


E B isn't necessarily a subset of A: $\{0, 1, 2, 3\} \setminus \{1, 3, 4\} = \{0, 2\}$.

Set Theory

The complement $\complement$

Given an **implicit** set E and a subset $A \subseteq E$, the **complement** of A with regard to E is the set $A^{\complement} = E \setminus A$.



E Given $A = \{0\}$, $A^{\complement} = \mathbb{N}^*$ **with regard to** $\mathbb{N}$ and $A^{\complement} = \mathbb{R}^*$ **with regard to** $\mathbb{R}$.

Properties of Sets

Sets and propositional logic

Sets

$$A \cup B$$
$$A \cap B$$
$$A \subseteq B$$
$$A = B$$
$$A^{\complement}$$

Logical Operators

$$P \vee Q$$
$$P \wedge Q$$
$$P \implies Q$$
$$P \iff Q$$
$$\neg P$$

Properties of Sets

Common equalities

The following properties on sets hold, assuming $A, B, C \in \mathcal{P}(E)$:

$$
\begin{aligned}
A^{\complement\complement} &= A \\
A \cup A^{\complement} &= E \\
A \setminus B &= A \cap B^{\complement} \\
(A \cup B)^{\complement} &= A^{\complement} \cap B^{\complement} \\
(A \cap B)^{\complement} &= A^{\complement} \cup B^{\complement} \\
\emptyset^{\complement} &= E \\
A \subseteq B &\iff A \cap B^{\complement} = \emptyset \\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C)
\end{aligned}
$$

Practical Application

Exercise 3. Are the following properties true in the general case, assuming $A, B, C \in \mathcal{P}(E)$? If they're not, use **counter-examples** to falsify them.

$$
\begin{aligned}
A = B &\iff A \cup C = B \cup C \\
A = B &\iff A \cap B = A \\
A \cup B = C &\iff A \cup C = B \\
A \subseteq B \cup C &\iff (A \subseteq B) \vee (A \subseteq C) \\
A \subseteq B \cap C &\iff (A \subseteq B) \wedge (A \subseteq C) \\
A = B &\iff A \setminus C = B \setminus C \\
(A \subseteq C) \wedge (B \subseteq C) &\implies A \subseteq B \\
A \cup B = C &\iff A = C \setminus B \\
A \cup B + A \cap B = A + B &\iff A \cup B = A + B - A \cup B
\end{aligned}
$$

Answer I

$$
\begin{array}{rcl}
A = B & \not\Longleftrightarrow & A \cup C = B \cup C \\
\mathbb{N} \neq \mathbb{Z} & \text{but} & \mathbb{N} \cup \mathbb{R} = \mathbb{Z} \cup \mathbb{R} = \mathbb{R} \\
\dots & \Longrightarrow & \dots \\
A = B & \not\Longleftrightarrow & A \cap B = A \\
\mathbb{N} \neq \mathbb{Z} & \text{but} & \mathbb{N} \cap \mathbb{Z} = \mathbb{N} \\
\dots & \Longrightarrow & \dots \\
A \cup B = C & \not\Longleftrightarrow & A \cup C = B \\
\mathbb{R}_+ \cup \mathbb{R}_- = \mathbb{R} & \text{but} & \mathbb{R}_+ \cup \mathbb{R} \neq \mathbb{R}_- \\
A \subseteq B \cup C & \not\Longleftrightarrow & (A \subseteq B) \vee (A \subseteq C) \\
\mathbb{R} \subseteq \mathbb{R}_+ \cup \mathbb{R}_- & \text{but} & (\mathbb{R} \not\subseteq \mathbb{R}_+) \wedge (\mathbb{R} \not\subseteq \mathbb{R}_-) \\
\dots & \Longleftarrow & \dots
\end{array}
$$

Answer II

$$
\begin{array}{rcl}
A \subseteq B \cap C & \iff & (A \subseteq B) \wedge (A \subseteq C) \\
A = B & \not\Longleftrightarrow & A \setminus C = B \setminus C \\
\mathbb{N} \neq \mathbb{Z} & \text{but} & \mathbb{N} \setminus \mathbb{R} = \mathbb{Z} \setminus \mathbb{R} = \emptyset \\
\dots & \implies & \dots \\
(A \subseteq C) \wedge (B \subseteq C) & \not\Longrightarrow & A \subseteq B \\
(\mathbb{R}_+ \subseteq \mathbb{R}) \wedge (\mathbb{R}_- \subseteq \mathbb{R}) & \text{but} & \mathbb{R}_+ \not\subseteq \mathbb{R}_- \\
A \cup B = C & \not\Longleftrightarrow & A = C \setminus B \\
A \cup A = A & \text{but} & A \neq A \setminus A \text{ if } A \neq \emptyset \\
A \cup B + A \cap B = A + B & \iff & A \cup B = A + B - A \cup B \\
+ \text{ is undefined} & & - \text{ is undefined}
\end{array}
$$

Practical Application

Exercise 4. Are the following equalities true in the general case, assuming $A, B, C \in \mathcal{P}(E)$? If they're not, use **counter-examples** to falsify them.

$$
\begin{aligned}
(A \setminus B) \cup B &= A \\
(A \cup B) \setminus B &= A \\
(A \cup B \cup B) \setminus B &= A \cup B \\
(A \setminus B) \cup (A \cap B) &= A \\
\emptyset \cup A &= E \cap A \\
\emptyset \cap A &= E \cup A \\
A + B - B &= A \\
A \cup B \cup B &= A + 2B \\
A \cup B &= (A \cup B) \setminus (A \cap B)
\end{aligned}
$$

Answer I

$$
\begin{aligned}
(A \setminus B) \cup B &\neq A \\
(\mathbb{Z} \setminus \mathbb{R}_+) \cup \mathbb{R}_+ &\neq \mathbb{Z} \\
\dots &\supseteq \dots \\
(A \cup B) \setminus B &\neq A \\
(\mathbb{N} \cup \mathbb{R}) \setminus \mathbb{R} = \emptyset &\neq \mathbb{N} \\
\dots &\subseteq \dots \\
(A \cup B \cup B) \setminus B &\neq A \cup B \\
(\mathbb{N} \cup \mathbb{R} \cup \mathbb{R}) \setminus \mathbb{R} = \emptyset &\neq \mathbb{N} \cup \mathbb{R} = \mathbb{R} \\
\dots &\subseteq \dots
\end{aligned}
$$

Answer II

$$
\begin{aligned}
(A \setminus B) \cup (A \cap B) &= A \\
A = \emptyset \cup A &= E \cap A = A \\
\emptyset = \emptyset \cap A &\neq E \cup A = E \\
A + B - B &= A \\
A \cup B \cup B &= A + 2B \\
& \quad 2B \text{ is undefined} \\
A \cup B &\neq (A \cup B) \setminus (A \cap B) \\
& \quad \text{consider } A \cap B \neq \emptyset
\end{aligned}
$$

A Last Few Definitions

The Cartesian product $\times$

- We consider **ordered pairs** of objects. We use the notation (x, y).
- Do not mistake the pair (x, y) for the set (also called an unordered pair) $\{x, y\}$.
- Given two sets U and V, we introduce their **Cartesian product** $U \times V$ such that $(x, y) \in U \times V$ if and only if $(x \in U) \wedge (y \in V)$.

E Consider $\mathbb{R}^2 = (\mathbb{R}_+ \times \mathbb{R}_+) \cup (\mathbb{R}_+ \times \mathbb{R}_-) \cup (\mathbb{R}_- \times \mathbb{R}_-) \cup (\mathbb{R}_- \times \mathbb{R}_+)$.

A Last Few Definitions

Qualifying sets

- A common way to define a set is to select all the elements of a set **verifying a given proposition**.
- Formally, given a proposition $P(x)$ and a set E, we can introduce a subset S of E such that $x \in S \iff (x \in E) \wedge P(x)$.
- We often write $S = \{x \in E \mid P(x)\}$ instead.

E For $a, b \in \mathbb{R}$, the set $S = \{(x, y) \in \mathbb{R}^2 \mid y = a \cdot x + b\}$ is a line of the real plane $\mathbb{R}^2$.

Logical Formalism

Quantified Logic

Adrien Pommellet, LRE

September 4, 2024

Logical Quantifiers

Quantifying variables

- Some propositions may depend on one or more **variables**.
- Consider the proposition $P(n) =$ "*n is odd or even*". It is true if n is an integer, but makes no sense for reals.
- How can we express that a property **holds for an entire set**?

Logical Quantifiers

The Universal quantifier $\forall$

- We introduce the **universal** logical quantifier $\forall$ such that, given a set E, $\forall x \in E$ means "for all x belonging to the set E".
- Hence, given a proposition P that depends on a variable x, we can design a new proposition $\forall x \in E, P(x)$.
- We say that $P(x)$ is **quantified** by $\forall x \in E$.

E The proposition $\forall x \in \mathbb{R}, x^2 \geq 0$ is true.

Logical Quantifiers

A generic proof pattern for $\forall$

We can prove universally quantified propositions thanks to the following **proof pattern**:

Goal. Prove that $\forall x \in E, P(x)$.

Let $x \in E$ ...
... then $P(x)$ is true.

Practical Application

Exercise 1. Prove that $\forall n, m \in \mathbb{N}, n^2 + m^2 \geq 2nm$.

Answer

Goal. Prove that $\forall n, m \in \mathbb{N}, \boxed{n^2 + m^2 \geq 2nm}$.

Let $n, m \in \mathbb{N}$.
Note that $(n - m)^2 \geq 0$.
But $(n - m)^2 = n^2 + m^2 - 2nm$.
Thus $n^2 + m^2 - 2nm \geq 0$, hence $n^2 + m^2 \geq 2nm$.

Logical Quantifiers

A proof pattern for $\forall$ in a conclusion

Some propositions may feature an universal quantifier in their **conclusion** but not in their hypotheses:

Goal. Prove that $P \implies (\forall x \in E, Q(x))$.

Assume that P is true.
Let $x \in E$ ...
...then $Q(x)$ is true.

Logical Quantifiers

A proof pattern for $\forall$ in a hypothesis

It may help to consider **particular cases** of a more general, universally quantified property:

Goal. Prove that $(\forall x \in E, P(x)) \implies Q$.

Assume that $\forall x \in E, P(x)$ is true.
Consider one or more particular $x_0, x_1 \ldots \in E$.
Obviously, $P(x_0), P(x_1) \ldots$ are true ...
... then Q is true.

Practical Application

Exercise 2. Prove that, if $a, b, c \in \mathbb{R}$ are such that $\forall x \in \mathbb{R}$, $a \cdot x^2 + b \cdot x + c = 0$, then $a = b = c = 0$.

Answer

Goal. Prove that $\forall a, b, c \in \mathbb{R}$, $\boxed{\forall x \in \mathbb{R}, \boxed{a \cdot x^2 + b \cdot x + c = 0}} \implies \boxed{a = b = c = 0}$.

Consider $a, b, c \in \mathbb{R}$.
Assume that $\forall x \in \mathbb{R}$, $a \cdot x^2 + b \cdot x + c = 0$.
For $x = 0$, $a \cdot 0^2 + b \cdot 0 + c = 0$, thus $c = 0$.
For $x = -1$, $a \cdot (-1)^2 + b \cdot (-1) = 0 = a - b$. Thus $a = b$.
For $x = 1$, $a \cdot 1^2 + a \cdot 1 = 0 = a + a = 2a$. Thus $a = 0$.
Finally, $a = b = c = 0$.

Logical Quantifiers

The existential quantifier $\exists$

- We introduce the **existential** logical quantifier $\exists$ such that, given a set E, $\exists x \in E$ means "there exists an x belonging to the set E".
- Hence, given a proposition P that depends on a variable x, we can design a new proposition $\exists x \in E, P(x)$.
- Again, $P(x)$ is **quantified** by $\exists x \in E$.

E The proposition $\exists x \in \mathbb{R}, x^2 = 2$ is true.

Logical Quantifiers

A generic proof pattern for $\exists$

We can prove existentially quantified propositions thanks to the following **proof pattern**:

Goal. Prove that $\exists x \in E, P(x)$.

Exhibit a particular value $x_0 \in E$ ...
... then $P(x_0)$ is true.

Logical Quantifiers

A proof pattern for $\exists$ in a hypothesis

We manipulate an **exemplar** verifying the existentially quantified hypothesis:

Goal. Prove that $(\exists x \in E, P(x)) \implies Q$.

Assume that $\exists x \in E, P(x)$ is true.
Consider a particular $x_0 \in E$ such that $P(x_0)$ is true ...
... then Q is true.

Logical Quantifiers

A proof pattern for $\exists$ in a conclusion

We exhibit an **particular value** in the set E verifying the existentially quantified conclusion:

Goal. Prove that $P \implies (\exists x \in E, Q(x))$.

Assume that P is true.
Exhibit a particular value $x_0 \in E$ ...
... $Q(x_0)$ is proven true.

Practical Application

Exercise 3. Prove that, if $a, b \in \mathbb{R}$ and $a \neq 0$, then $\exists x \in \mathbb{R}$ such that $a \cdot x + b = 0$.

Answer

Goal. Prove that $\forall a, b \in \mathbb{R}, \boxed{a \neq 0} \implies \boxed{\exists x \in \mathbb{R}, \boxed{a \cdot x + b = 0}}$.

Consider $a, b \in \mathbb{R}$.
Assume $a \neq 0$.
Consider $x = -\frac{b}{a} \in \mathbb{R}$ that is well-defined because $a \neq 0$.
Then $ax + b = a \cdot (-\frac{b}{a}) + b = -b + b = 0$.

Logical Quantifiers

The Unique Existential Quantifier $\exists!$

- Note that if $\exists x \in E, P(x)$ holds true, we know that **at least one** element x of E verifies $P(x)$.
- But there may be **more than one element** in E satisfying P.
- We introduce the **unique existential** logical quantifier $\exists!$ such that $\exists! x \in E$ means "there exists exactly one x belonging to the set E".

E The proposition $\exists! x \in \mathbb{R}_+, x^2 = 2$ is true.

Logical Quantifiers

A proof pattern for $\exists!$

We usually prove $\exists! x \in E, P(x)$ in two steps: existence first, then unicity.

Goal. Prove that $\exists! x \in E, P(x)$.

Subgoal 1. Prove that $\exists x \in E, P(x)$.

As described previously ...

Subgoal 2. Prove that $\forall x_1, x_2 \in E, \boxed{P(x_1) \wedge P(x_2)} \implies \boxed{x_1 = x_2}$.

We can rely on the usual **implication pattern**, a **proof by contradiction**, or a **proof by contraposition** ...

Practical Application

Exercise 4. Prove that, if $a, b \in \mathbb{R}$ and $a \neq 0$, then $\exists! x \in \mathbb{R}$ such that $a \cdot x + b = 0$.

Answer I

Goal. Prove that $\forall a, b \in \mathbb{R}, \boxed{a \neq 0} \implies \boxed{\exists! x \in \mathbb{R}, \boxed{a \cdot x + b = 0}}$.

Consider $a, b \in \mathbb{R}$.
Assume $a \neq 0$.

Subgoal 1. Prove that $\boxed{\exists x \in \mathbb{R}, \boxed{a \cdot x + b = 0}}$.

This has already be done previously.

Answer II

Subgoal 2. Prove that $\forall x_1, x_2 \in \mathbb{R}, \boxed{a \cdot x_1 + b = 0 = a \cdot x_2 + b} \implies \boxed{x_1 = x_2}$.

Suppose $a \cdot x_1 + b = 0 = a \cdot x_2 + b$.
As a consequence, $a \cdot x_1 = a \cdot x_2$.
Since $a \neq 0$, $x_1 = x_2$.

Properties of Logical Quantifiers

Quantifying the empty set

- The proposition $\forall x \in \emptyset, P(x)$ is **always true**, regardless of P.
- Indeed, there are no x in $\emptyset$ to which the constraint $P(x)$ applies.
- The proposition $\exists x \in \emptyset, P(x)$ is **always false**, regardless of P.
- As a consequence, $\exists x \in E \iff E \neq \emptyset$.

Logical Quantifiers

A proof pattern for $\emptyset$

The last property yields the following proof pattern:

Goal. Prove that $E = \emptyset$.

Let us suppose that $E \neq \emptyset$.
Consider $\exists x \in E \ldots$
$\ldots$ then prove something that is blatantly false.
Thus by **contradiction** $E = \emptyset$.

Properties of Logical Quantifiers

Multiple quantifiers

- We can build propositions with **multiple quantifiers**, as an example $\forall x \in E, \exists y \in F, \forall z \in G, P(x, y, z)$.
- A variable should appear within the **scope**[1] of its quantifier. Avoid propositions of the form $P(x) \wedge (\exists x \in E, Q(x))$.
- A variable can only be quantified **once** in a given proposition.

[1] *portée*

Practical Application

Exercise 5. Express **formally** the following property: any non-empty subset of $\mathbb{N}$ admits a minimum.

Answer

- What is a minimum of a set E? It is an element m that belongs to the set E and is smaller than or equal to every other element of E.
- For every non-empty subset E of $\mathbb{N}$, a minimum must exist.
- These remarks yield the following formalization:

$$\forall E \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}, \boxed{\exists m \in E, \boxed{\forall n \in E, \boxed{m \leq n}}}$$

See you next class!

Logical Formalism

Functions

Adrien Pommellet, LRE

September 17, 2024

Defining Functions

Binary relations

- We want to properly define **relations between objects**.
- Formally, a **binary relation** on a set E is a subset $R \subseteq E \times E$.
- We associate it with the **binary predicate** $\sim_R$ such that $x \sim_R y$ is true if and only if $(x, y) \in R$.

E

Consider the **divisibility** relation $|$ on $\mathbb{N}$: $(2, 4) \in |$ can also be written $2 \mid 4$.

Defining Functions

Beware of symmetry

Please note that $x \sim_R y$ may not imply $y \sim_R x$. There is an **order** to binary relations.

Some binary relations **may fail** to verify the following property:

Symmetry

If $\forall x, y \in E, (x \sim_R y) \iff (y \sim_R x)$, then R is said to be **symmetric**.

E $\quad 3 \mid 6$ but $6 \nmid 3$.

Defining Functions

A formal definition

Function

Given two sets E and F, a **function** is a binary relation $f \subseteq E \times F$ (also written $f : E \to F$) such that $\forall x \in E$, there exists **exactly** one $y \in F$ such that $(x, y) \in f$.

We then write $y = f(x)$; x is an **antecedent** of y, and y, the **image** of x.

E The set $\{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$ is **not** a function, as a single antecedent can have two images.

Defining Functions

An mathematician's answer

A function takes an input in a **set** E and returns a **single** value in a (possibly different) **set** F.

Defining Functions

Domains

Domain

Given a function $f : E \to F$, E is called the **domain** $\mathrm{Dom}(f)$ of f.

The set of all functions $E \to F$ is written F^E.

E Consider the logarithm function: $\mathrm{Dom}(\log) = \mathbb{R}_+^*$ and $\log \in \mathbb{R}^{\mathbb{R}_+^*}$.

Defining Functions

Images

Image

The subset $\mathrm{Im}(f) = \{y \in F \mid \exists x \in E, (x, y) \in f\}$ of F is called the **image** of a function $f : E \to F$.

- It is possible that $F \neq \mathrm{Im}(f)$.

  E Consider $\exp : \mathbb{R} \to \mathbb{R}$. Then $\mathrm{Im}(\exp) = \mathbb{R}_+^*$.

- Indeed, the **notation** $f : E \to F$ does **not** mean that $F = \mathrm{Im}(f)$.
- An element y of F may admit zero, one, or many antecedents.

  E Consider $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$. 0 has one antecedent, 1 has two, -1 has none.

Defining Functions

A proof pattern for functions

Goal. Prove that the relation f is a **function** $E \to F$.

Subgoal 1. Prove that an image always **exists**.

Let $x \in E$ ...
... then $\exists y \in F$, $(x, y) \in f$.

Subgoal 2. Prove that the image is **unique**.

Let $(x, y), (x, z) \in f$ ...
... then $y = z$.

Practical Application

Exercise 1. Are the following binary relations **functions**?

$$
\begin{aligned}
F_1 &= \{(x,y) \in \mathbb{R}_+ \times \mathbb{R} \mid x = \cos(y)\} \\
F_2 &= \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 3\} \\
F_3 &= \{(x,y) \in \mathbb{R}^2 \mid y = x^2\} \\
F_4 &= \{(E,F) \in \mathcal{P}(\mathbb{N})^2 \mid E \subseteq F\} \\
F_5 &= \{(E,F) \in \mathcal{P}(\mathbb{N})^2 \mid F = E^{\complement}\} \\
F_6 &= \{((E_1,E_2),F) \in \mathcal{P}(\mathbb{N})^2 \times \mathcal{P}(\mathbb{N}) \mid F = E_1 \cap E_2\} \\
F_7 &= \{(x,y) \in \mathbb{Q} \times \mathbb{Z} \mid \exists z \in \mathbb{Z}^*, x = \frac{y}{z}\} \\
F_8 &= \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid m \text{ divides } n\}
\end{aligned}
$$

Answer I

$$
\begin{aligned}
F_1 &= \{(x,y) \in \mathbb{R}_+ \times \mathbb{R} \mid x = \cos(y)\} \text{ is not a function.} \\
& \quad (1,0), (1, 2 \cdot \pi) \in F_1 \\
F_2 &= \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 3\} \text{ is not a function.} \\
& \quad (0, \sqrt{3}), (0, -\sqrt{3}) \in F_2 \\
F_3 &= \{(x,y) \in \mathbb{R}^2 \mid y = x^2\} \text{ is a function } \mathbb{R} \to \mathbb{R}. \\
F_4 &= \{(E,F) \in \mathcal{P}(\mathbb{N})^2 \mid E \subseteq F\} \text{ is not a function.} \\
& \quad (\emptyset, \{0\}), (\emptyset, \{1\}) \in F_4
\end{aligned}
$$

Answer II

$$
\begin{aligned}
F_5 &= \{(E,F) \in \mathcal{P}(\mathbb{N})^2 \mid F = E^{\complement}\} \text{ is a function } \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N}). \\
F_6 &= \{((E_1,E_2),F) \in \mathcal{P}(\mathbb{N})^2 \times \mathcal{P}(\mathbb{N}) \mid F = E_1 \cap E_2\} \\
&\quad \text{is a function } \mathcal{P}(\mathbb{N})^2 \to \mathcal{P}(\mathbb{N}). \\
F_7 &= \{(x,y) \in \mathbb{Q} \times \mathbb{Z} \mid \exists z \in \mathbb{Z}^*, x = \frac{y}{z}\} \text{ is not a function.} \\
&\quad (\frac{1}{2},1),(\frac{1}{2},2) \in F_7 \text{ as } \frac{1}{2} = \frac{2}{4} \\
F_8 &= \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid m \text{ divides } n\} \text{ is not a function.} \\
&\quad (6,2),(6,3) \in F_8
\end{aligned}
$$

Practical Application

Exercise 2. Consider a function $f : E \to F$. Are the following binary relations **always** functions?

$$
\begin{aligned}
g_1 &= \{(y, x) \in F \times E \mid f(x) = y\} \\
g_2 &= \{(y, X) \in F \times \mathcal{P}(E) \mid \forall x \in E, x \in X \iff f(x) = y\} \\
h_1 &= \{(X, Y) \in \mathcal{P}(E) \times \mathcal{P}(F) \mid \forall x \in E, x \in X \implies f(x) \in Y\} \\
h_2 &= \{(X, Y) \in \mathcal{P}(E) \times \mathcal{P}(F) \mid Y = \{f(x) \mid x \in X\}\}
\end{aligned}
$$

Answer

1. g_1 may not be a function. Consider $f : x \in \mathbb{R} \to x^2 \in \mathbb{R}^+$. Then $(1, 1) \in g_1$ and $(1, -1) \in g_1$.
2. g_2 is a function such that $g_2(y) = \{x \in E \mid y = f(x)\}$. First note that $\forall y \in F, (y, \{x \in E \mid y = f(x)\}) \in g_2$. Then prove by double inclusion that if $(y, X) \in g_2$, $X = \{x \in E \mid y = f(x)\}$.
   Almost always use the double inclusion pattern to prove set equality.
3. h_1 may not be a function. Consider $f : x \in \mathbb{R} \to x \in \mathbb{R}$. Then $(\{1\}, \{1\}) \in h_1$ and $(\{1\}, \{1, 2\}) \in h_1$.
4. h_2 is a function as $\forall X \in \mathcal{P}(E)$, $h_2(X) = \{f(x) \mid x \in X\}$ is defined explicitly.

Properties of Functions

Composing functions

Can we **chain functions together** to produce a new composite function?

Function composition

Given two functions $f : E \to F$ and $g : F \to G$, there exists an unique function $g \circ f : x \in E \mapsto g(f(x)) \in G$.

Associativity law

Consider three functions $f : E \to F$, $g : F \to G$, and $h : G \to H$. Then $(h \circ g) \circ f = h \circ (g \circ f)$. We say that the operator $\circ$ is **associative**.

Properties of Functions

Injections

Note that a function may match the **same image** to **two different antecedents**. We thus consider the following definition:

Injective function

A function $f : E \to F$ is said to be **injective** or one-to-one if and only if $\forall x, y \in Dom(f)$, $f(x) = f(y) \implies x = y$.

E Consider $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$. Then f is **not** injective: indeed, $f(1) = f(-1) = 1$.

Properties of Functions

A proof pattern for injectivity

We want to prove an **unicity** property.

Goal. Prove that a function $f : E \to F$ is injective.

Consider any $x, y \in \mathrm{Dom}(f)$.
Assume that $f(x) = f(y)$ ...
... then $x = y$.

Conversely, an element of a function's destination set may admit **no antecedent**. Formally:

Surjective function

A function $f : E \to F$ is said to be **surjective** if and only if $\forall y \in F$, $\exists x \in E$, $y = f(x)$.

E Consider $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$. Then f is **not** surjective: indeed, the number -1 has no antecedent.

Properties of Functions

A proof pattern for surjectivity

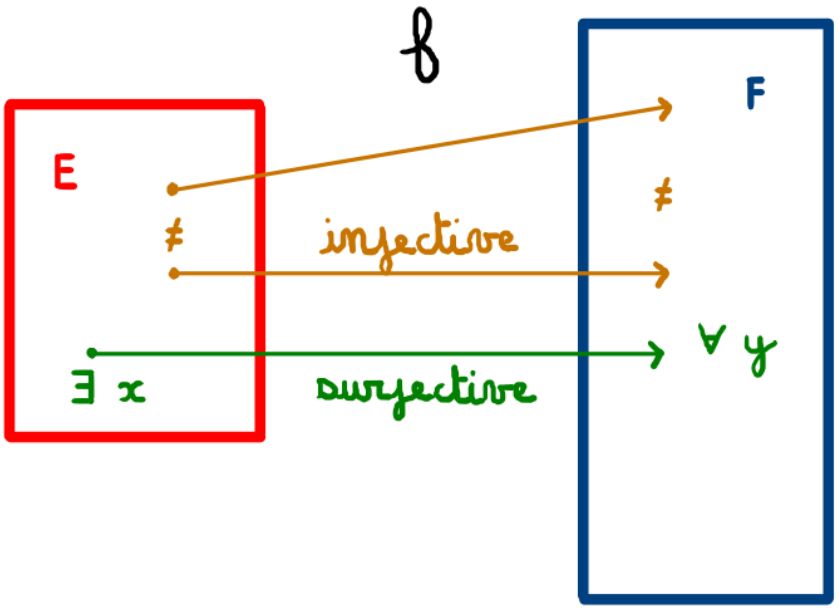
We want to prove an **existential** property.

Goal. Prove that a function $f : E \to F$ is surjective.

Consider any $y \in F$ ...
... then exhibits x such that $y = f(x)$.

Properties of Functions

A summary



Practical Application

Exercise 3. Let $(a, b) \in \mathbb{R}^* \times \mathbb{R}$. Prove that $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = a \cdot x + b$ is both **injective** and **surjective**.

Answer

Goal. Prove that $f : \mathbb{R} \to \mathbb{R}$ is **injective**.

Consider $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$.
$a \cdot x_1 + b = a \cdot x_2 + b$, thus $a \cdot x_1 = a \cdot x_2$.
Since $a \neq 0$, $x_1 = x_2$.

Goal. Prove that $f : \mathbb{R} \to \mathbb{R}$ is **surjective**.

Let $y \in \mathbb{R}$.
Consider $x = \frac{y-b}{a}$ that is well-defined because $a \neq 0$.
Then $f(x) = a \cdot \frac{y-b}{a} + b = y$.

Bijections

A definition

A function can be a **one-to-one correspondence** that matches to each element of F an unique antecedent in E.

Bijection function

A function $f : E \to F$ is said to be **bijective** if and only if f is **injective** and **surjective**.

The sets E and F are then said to be **equipotent**.

E As an example, the function $\exp : \mathbb{R} \to \mathbb{R}_+^*$ is a **bijection**.

Bijections

Invertible functions

Intuitively, a one-to-one correspondence should go **both ways**. Formally:

Invertibility of bijections

A function $f : E \to F$ is a bijection **if and only** if there exists an function $f^{-1} : F \to E$ such that $f \circ f^{-1} = \mathrm{Id}_F$ and $f^{-1} \circ f = \mathrm{Id}_E$.

The function f is said to be **invertible**, and the **inverse** f^{-1} is a bijection as well. Moreover, f^{-1} is **unique**.

Intuitively, f^{-1} **undoes** whatever operation f performed, assuming it is revertible in the first place.

Bijections

An alternative proof pattern for bijections

Goal. Prove that $f : E \to F$ is a bijection.

Introduce a **candidate** $g \subseteq F \times E$ for the inverse function.
First **prove** that g is indeed a function $F \to E$. Then:

Subgoal 1. Prove that $f \circ g = \mathrm{Id}_F$.

Let $y \in F$ ...
...then $f(g(y)) = y$.

Subgoal 2. Prove that $g \circ f = \mathrm{Id}_E$.

Let $x \in E$ ...
...then $g(f(x)) = x$.

Practical Application

Exercise 4. Let E be a set. Prove that function $f : \mathcal{P}(E) \to \mathcal{P}(E)$ such that $\forall X \in \mathcal{P}(E)$, $f(X) = X^{\complement}$ is a **bijection**.

Answer

We have already mentioned that f is a function earlier.
Note that $\forall X \in \mathcal{P}(E)$, $f(f(X)) = (X^{\complement})^{\complement} = X$.
Thus f is its own **inverse**, hence a bijection.
A function that is its own inverse is called an **involution**.

Logical Formalism

Parsing Complex Propositions

Adrien Pommellet, LRE

September 17, 2024

Formalizing Properties

A web of relations

A proposition only makes sense if one understands the **types** of its variables and the **relations** between them.

Formalizing Properties

An example I

In order to formalize a proposition, one has to describe the **various objects involved**.

- Consider a sequence $(U_n)_{n\geq 0} \in \mathbb{R}^{\mathbb{N}}$ of real numbers.
- How can we formalize (U_n) having a **finite limit**?
- Intuitively, there is a real number such that (U_n) is as close to this value as we want it to be past a certain point.

Formalizing Properties

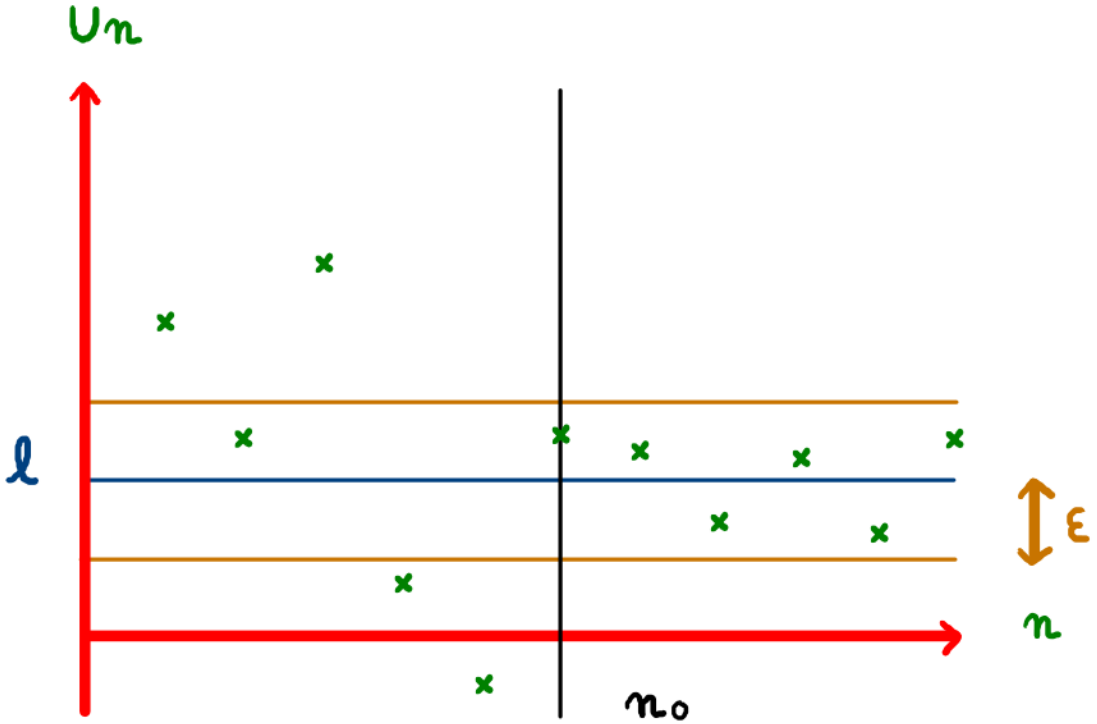
An example II

We **always** need to **name** these variables and **explicit the sets** they belong to before using them in a proposition.

- Let $\ell \in \mathbb{R}$ be the (one and only) limit of (U_n).
- In order to express the distance $|U_n - \ell|$ becoming as small as we want it to be, we consider an upper bound $\varepsilon > 0$.
- This bound only applies past a certain rank $n_0 \in \mathbb{N}$.

Formalizing Properties

An example III



Formalizing Properties

An example IV

The resulting formula is the following:

$$\exists \ell \in \mathbb{R}, \boxed{\forall \varepsilon > 0, \boxed{\exists n_0 \in \mathbb{N}, \boxed{\forall n \geq n_0, |U_n - \ell| < \varepsilon}}}$$

- The limit ℓ only depends on (U_n).
- The distance ε can be any value we want.
- Rank n_0 depends on (U_n), ℓ, and ε: the closer we want to be to the limit, the further we may have to go.

Formalizing Properties

Understanding quantifier dependencies

An existentially quantified variable **depends** on all the other variables that were quantified prior to its definition.

Properties of Logical Quantifiers

Permuting quantifiers

- We may **permute** adjacent quantifiers of the same type (assuming F's definition does not depend on x):

$$\forall x \in E, \quad \forall y \in F, \quad P(x,y) \iff \forall y \in F, \quad \forall x \in E, \quad P(x,y)$$
$$\exists x \in E, \quad \exists y \in F, \quad P(x,y) \iff \exists y \in F, \quad \exists x \in E, \quad P(x,y)$$

- But we can't permute adjacent quantifiers of different types!

$$\forall x \in E, \quad \exists y \in F, \quad P(x,y) \not\Longleftrightarrow \exists y \in F, \quad \forall x \in E, \quad P(x,y)$$

E "Every single human being has a mother." is **not equivalent** to "There exists a woman mother to every single human being.".

Properties of Logical Quantifiers

Negating quantifiers

- The negation of an universal quantifier is a **counter-example**:

$$\neg(\forall x \in E, P(x)) \iff \exists x \in E, \neg P(x)$$

- The negation of an existential quantifier is an **universal negation**:

$$\neg(\exists x \in E, P(x)) \iff \forall x \in E, \neg P(x)$$

- Propagate the negation **one quantifier** at a time:

$$\begin{aligned}\neg(\forall x \in E,\ \exists y \in F,\ P(x,y)) &\iff \exists x \in E,\ \neg(\exists y \in F,\ P(x,y)) \\ &\iff \exists x \in E,\ \forall y \in F,\ \neg P(x,y)\end{aligned}$$

Practical Application

Exercise 1. Write the **negation** of $(U_n)_{n\geq 0} \in \mathbb{R}^{\mathbb{N}}$ having a finite limit.

Answer

$$\forall \ell \in \mathbb{R},\ \exists \varepsilon > 0,\ \forall n_0 \in \mathbb{N},\ \exists n \geq n_0,\ |U_n - \ell| \geq \varepsilon$$

Handling higher-order functions

A tricky problem

We will study the following problem:

2023, final exam

Given two sets E and F and a function $f : E \to F$. Let us define the function $g : X \in \mathcal{P}(E) \mapsto \{y \in F \mid \exists x \in X, y = f(x)\} \in \mathcal{P}(F)$.

Prove that f is **injective** if and only if $\forall A, B \in \mathcal{P}(E)$, $(A \cap B = \emptyset) \implies (g(A) \cap g(B) = \emptyset)$.

Handling higher-order functions

Understanding the definitions of the objects involved

- Note that g is a function that takes a **set** as input and returns a **set**.
- The set $g(X)$ is known as the **image** of set X by function f.
  As an example, on finite sets, $g(\{x_1, \ldots, x_n\}) = \{f(x_1), \ldots, f(x_n)\}$.
- **Do not mistake the input and output types** of f and g: you can't apply f to sets and g to variables in E.
- Remember the meaning of **injectivity**: different inputs always yield different outputs.

Handling higher-order functions

A common parsing failure

An **improper** way to parse the exercise is the following:

$$\boxed{f \text{ is injective}}$$

$$\iff \quad \boxed{\forall A, B \in \mathcal{P}(E), \boxed{A \cap B = \emptyset}}$$

$$\implies \quad \boxed{g(A) \cap g(B) = \emptyset}$$

- Do we mean $P \iff (Q \implies R)$ or $(P \iff Q) \implies R$?
- Third line makes no sense if A and B are **unquantified**.
- Second line is **always false** unless E is empty.

Handling higher-order functions

The proper reading

The right way to read the proposition is the following:

$$\boxed{f \text{ is injective}} \tag{P}$$

$$\iff \quad \boxed{\forall A, B \in \mathcal{P}(E), \boxed{\boxed{A \cap B = \emptyset} \implies \boxed{g(A) \cap g(B) = \emptyset}}} \tag{Q}$$

We have to prove an equivalence $P \iff Q$. From there, we **must** use proof patterns.

Practical Application

Exercise 2. Write a **proof skeleton**.

Answer I

Left to right

Subgoal 1. Prove that $P \implies Q$.

Assume that f is injective.

Subgoal 2. $\forall A, B \in \mathcal{P}(E), \boxed{A \cap B = \emptyset} \implies \boxed{g(A) \cap g(B) = \emptyset}$.

Let $A, B \in \mathcal{P}(E)$ such that $A \cap B = \emptyset$.
Let us prove that $g(A) \cap g(B) = \emptyset$ by **contradiction**.

Assume that $g(A) \cap g(B) \neq \emptyset$.

Then $\exists x \in g(A) \cap g(B) \ldots$
This is how far we can get, using **only** proof patterns.

Answer II

Right to left

Subgoal 3. Prove that $Q \implies P$.

Assume that $\forall A, B \in \mathcal{P}(E), (A \cap B = \emptyset) \implies (g(A) \cap g(B) = \emptyset)$.
Note that the property applies to **any** pair of subsets in $\mathcal{P}(E)$, and not to a particular pair (A, B).
Consider $x_1, x_2 \in E$ such that $f(x_1) = f(x_2)$.
Let us prove that $x_1 = x_2$ ...

Practical Application

Exercise 3. Finish the proof of Subgoal 1.

Answer I

- Assume that $A \cap B = \emptyset$.
- Therefore $A \neq B$. ✗ What if $A = B = \emptyset$?
- As f is injective, $f(A) \neq f(B)$. ✗ f cannot take a set as input.
- As a consequence, $g(A) \neq g(B)$.
- Finally, $g(A) \cap g(B) = \emptyset$. ✗ $\{1, 2\} \cap \{1, 3\} = \{1\} \neq \emptyset$.

This is not a proof. This is **utter drivel**, worthy of exactly **zero** points.

Answer II

Use your **intuition**: what is the set $g(X)$? The image by f of the elements of X. What can we say of an element that is **both** in $g(A)$ and $g(B)$?

Answer III

- Assume $\exists x \in g(A) \cap g(B)$.
  Let's go back to the proof by contradiction we outlined previously.
- By definition of g, as $x \in g(A)$, there exists $a \in A$, $f(a) = x$.
  Writing the definition of g helps us furthering the proof.
- In a similar fashion, there exists $b \in B$, $f(b) = x$.
- As a consequence, $f(a) = f(b)$.
- Since f is injective, $a = b$. Use an hypothesis.
- Thus $a \in A \cap B$.
- But $A \cap B = \emptyset$. Try using **all** the hypotheses!
- Therefore, there is a **contradiction** and $g(A) \cap g(B) = \emptyset$.

Handling higher-order functions

Properties of a higher-order function

- How can a property on g (a function on **subsets** of E) result in a property on f (a function on **elements** of E)?
- Function g cannot take an element of E as input, and conversely, f cannot take a set as input.
- However, given $x \in E$, the singleton $\{x\}$ is an element of $\mathcal{P}(E)$.
- Moreover, note that $g(\{x\}) = \{f(x)\}$.

Practical Application

Exercise 4. Finish the proof of Subgoal 3.

Answer

- Consider $x_1, x_2 \in E$ such that $f(x_1) = f(x_2)$.
- Note that $g(\{x_1\}) = \{f(x_1)\} = \{f(x_2)\} = g(\{x_2\})$.
- We know that $\forall A, B \in \mathcal{P}(E), (g(A) \cap g(B) \neq \emptyset) \implies (A \cap B \neq \emptyset)$ by **contraposition** of the hypothesis.
  This property applies to **any** A and B in $\mathcal{P}(E)$.
- As $g(\{x_1\}) \cap g(\{x_2\}) = \{f(x_1)\} \neq \emptyset$, $\{x_1\} \cap \{x_2\} \neq \emptyset$.
- Thus $x_1 = x_2$ and f is **injective**.
  Two singletons only intersect if they are equal.

See you next class!

Logical Formalism

Inductive Proofs (🇫🇷 *Preuve par récurrence*)

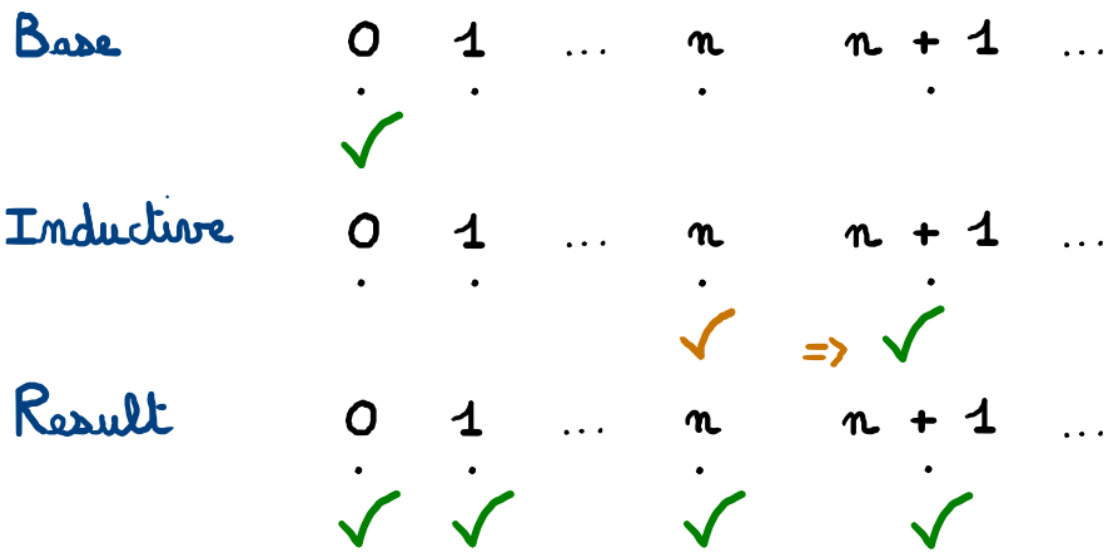
Adrien Pommellet, LRE

September 17, 2024

The Induction Principle (🇫🇷 *Principe de récurrence*)

Spreading the gospel

Induction is a way to prove **hereditary properties** on **integers**.



The Induction Principle

Inductive proofs

- First, we want to prove that a given property P holds for a small integer called the **base case**.
- Then, we show that the property can spread through the **inductive case**: if P holds for an integer n, then P must hold for $n + 1$ as well.
- Finally, we conclude that P holds for all integers.

The Induction Principle

Formalizing the principle

Let us formalize **inductive** proofs.

Induction theorem

Consider a proposition P on natural integers and $n_0 \in \mathbb{N}$ such that:

- $P(n_0)$ holds.
- $\forall n \geq n_0,\ P(n) \implies P(n+1)$.

Then $\forall n \geq n_0, P(n)$.

The Induction Principle

The inductive proof pattern

Goal. Prove that $\forall n \geq n_0, P(n)$.

We are going to use a proof by **simple induction** (🇫🇷 *récurrence simple*) on n.

Base case. Prove that $P(n_0)$ holds.

Don't forget it! And use the right index n_0.

Use the hypotheses. They often directly yield $P(n_0)$.

Inductive case. Prove that $\forall n \geq n_0, \boxed{P(n)} \implies \boxed{P(n+1)}$.

Assume that $P(n)$ holds for some $n \geq n_0$ ...

Find a relation between $P(n)$ and $P(n+1)$. Then apply $P(n)$.

... then $P(n+1)$ holds.

Practical Application

Exercise 1. Prove that $\forall n \in \mathbb{N}^*$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Answer I

Goal. Prove that $\forall n \in \mathbb{N}^*$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

We will prove it by **simple induction** on n.

Base case. Prove that the property holds at rank 1.

$1 = \frac{1(1+1)}{2}$, thus the property holds for $n = 1$.

Answer II

Inductive case. Assume that the property holds at rank n. Let us prove it holds at rank $n+1$.

For $n \in \mathbb{N}^*$, assume that $1+2+\ldots+n = \frac{n(n+1)}{2}$. Then:

$$\begin{aligned} & 1+2+\ldots+n+(n+1) \\ = & \frac{n(n+1)}{2}+(n+1) \qquad \text{by hypothesis} \\ = & \frac{n(n+1)+2(n+1)}{2} \\ = & \frac{(n+1)(n+2)}{2} \end{aligned}$$

Proving the Induction Principle

Laying out the proof

- Our goal is to prove the proposition:

$$(P(n_0) \wedge (\forall n \geq n_0, P(n) \implies P(n+1))) \implies (\forall n \geq n_0, P(n))$$

- To do so, we will **use a proof by contradiction**.
- We assume that $\exists u \geq n_0$ such that $P(u)$ does not hold.
- As a consequence, the set $H = \{n \geq n_0 \mid \neg P(n)\}$ is **not empty** as it contains u.

Proving the Induction Principle

Sealing the deal

- As it happens, the set $\mathbb{N}$ is **well-ordered**: any non-empty subset of $\mathbb{N}$ admits a smallest element.
- Let m be the smallest element of H. We consider a **case disjunction**:

  Suppose $m = n_0$. $P(m)$ holds by hypothesis, but so does $\neg P(m)$ as $m \in H$. Hence, there is a **contradiction**.

  Suppose $m > n_0$. Since m is minimal, $m - 1 \notin H$. Thus $P(m-1)$ holds. But $P(m-1) \implies P(m)$ by hypothesis, thus $P(m)$ holds. Hence, another **contradiction**.
- Thus, H is empty. As a consequence, $\forall n \geq n_0, P(n)$.

Practical Application

Exercise 2. Prove that $\forall n \in \mathbb{N}^*$, $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2 \cdot n+1)}{6}$.

Answer I

Goal. Prove that $\forall n \in \mathbb{N}^*$, $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2 \cdot n+1)}{6}$.

We will prove it by **simple induction** on n.

Base case. Prove that the property holds at rank 1.

$1^2 = \frac{1(1+1)(2 \cdot 1+1)}{6} = 1$, thus the property holds for $n = 1$.

Answer II

Inductive case. Assume that the property holds at rank n. Let us prove it holds at rank $n+1$.

For $n \in \mathbb{N}^*$, assume that $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2 \cdot n+1)}{6}$. Then:

$$\begin{aligned}
& 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 \\
= \quad & \frac{n(n+1)(2 \cdot n+1)}{6} + (n+1)^2 \qquad \text{by hypothesis} \\
= \quad & (n+1)\left(\frac{n(2 \cdot n+1)}{6} + (n+1)\right) \\
= \quad & (n+1) \cdot \frac{2 \cdot n^2 + n + 6 \cdot n + 6}{6} \\
= \quad & (n+1) \cdot \frac{(n+2)(2 \cdot n+3)}{6} \\
= \quad & \frac{(n+1)((n+1)+1)(2 \cdot (n+1)+1)}{6}
\end{aligned}$$

Practical Application

Exercise 3. Prove that $\forall n \in \mathbb{N}^*$, $\forall x \in \mathbb{R}$, $|\sin(n \cdot x)| \leq n \cdot |\sin(x)|$.
Remember that $\forall a, b \in \mathbb{R}$, $\sin(a + b) = \cos(a)\sin(b) + \sin(a)\cos(b)$.

Answer I

Goal. Prove that $\forall n \in \mathbb{N}^*$, $\forall x \in \mathbb{R}$, $|\sin(n \cdot x)| \leq n \cdot |\sin(x)|$.

We will prove it by **simple induction** on n.

Base case. Prove that the property holds at rank 1.

Obviously, $|\sin(x)| \leq |\sin(x)|$, thus the property holds for $n = 1$.

Answer II

Inductive case. Assume that the property holds at rank n. Let us prove it holds at rank $n+1$.

For $n \in \mathbb{N}^*$, assume that $|\sin(n \cdot x)| \leq n \cdot |\sin(x)|$.
Note that $\sin((n+1)x) = \cos(n \cdot x)\sin(x) + \sin(n \cdot x)\cos(x)$.

$$
\begin{aligned}
& |\sin((n+1)x)| \\
= \quad & |\cos(n \cdot x)\sin(x) + \sin(n \cdot x)\cos(x)| \\
\leq \quad & |\cos(n \cdot x)\sin(x)| + |\sin(n \cdot x)\cos(x)| \\
\leq \quad & |\sin(x)| + |\sin(n \cdot x)| \\
\leq \quad & |\sin(x)| + n \cdot |\sin(x)| && \text{by hypothesis} \\
\leq \quad & (n+1) \cdot |\sin(x)|
\end{aligned}
$$

Common Mistakes

Something is missing

- Let us prove by induction on n that $\forall n \in \mathbb{N}^*$, $9 \mid 10^n + 1$.
- Let us suppose that for a given $n \in \mathbb{N}^*$, $9 \mid 10^n + 1$. Then $\exists k \in \mathbb{N}$, $10^n + 1 = 9k$. Therefore, $10 \times (10^n + 1) = 10 \times 9k$, and $10^{n+1} + 10 = 90k$.

  Finally, $10^{n+1} + 1 = 90k - 9 = 9 \times (10k - 1)$, thus $9 \mid 10^{n+1} + 1$.
- Thus we have proven this property by induction. Or have we?

The base case is missing! Obviously, $9 \nmid 11$, $9 \nmid 101$, etc. This property is **false**.

Common Mistakes

I'm the best teacher

Let us prove by induction on n that any class of $n \in \mathbb{N}$ students always unanimously agrees with me.

Base case. In a class of 0 students, the property holds: there's no one there that can contradict me in the first place.

Inductive case. Assume that the property holds for any class of n students for a given $n \in \mathbb{N}$. Consider a class of $n+1$ students. If I remove a student n_1 from the class, the remaining n students all agree with me **by induction hypothesis**.

And if I bring n_1 back but remove another student n_2 (that already agrees with me), then the remaining n students also agree with me **by induction hypothesis**, including n_1. Thus, the entire class of $n+1$ students agrees with me.

Common Mistakes

I'm the worst teacher

This property is **false**, but why?

- The inductive case assumes that there are two different students in the class. To do so, $n + 1$ must be greater than or equal to 2, hence, we have to assume $n \geq 1$ in the **inductive case**.
- But the base case is $n = 0$. Thus, the proof is not correct.
- Always make sure that the **minimal value** of n required by the inductive case matches the base case.

Logical Formalism

Advanced Inductive Proofs

Adrien Pommellet, LRE

September 17, 2024

Deeper Inductions (🇫🇷 *Récurrence d'ordre supérieur*)

Extending the induction depth

The inductive case of a recursive proof may depend on **more than the immediate predecessor**.

Depth k induction theorem

Consider a proposition P on natural integers, $n_0 \in \mathbb{N}$ and $k \in \mathbb{N}^*$ such that:

- $P(n_0), \ldots, P(n_0 + k - 1)$ hold.
- $\forall n \geq n_0$, $(P(n) \wedge \ldots \wedge P(n + k - 1)) \Rightarrow P(n + k)$.

Then $\forall n \geq n_0, P(n)$.

The proof is similar to the original induction theorem.

Deeper Inductions

The depth k inductive proof pattern

Goal. Prove that $\forall n \geq n_0, P(n)$.

We are going to use a proof by **induction of depth** k.

Base case. Prove that $P(n_0), \ldots, P(n_0 + k - 1)$ hold.

Use the right k. And prove all the k base cases.

Inductive case. Prove that $\forall n \geq n_0, \boxed{P(n) \wedge \ldots \wedge P(n + k - 1)} \implies \boxed{P(n + k)}$.

Assume that $P(n), \ldots, P(n + k - 1)$ hold for some $n \geq n_0$ ...

Find a relation. Note that all the k hypotheses may not be used.

... then $P(n + k)$ holds.

Practical Application

Exercise 1. Fibonacci's sequence is defined as follows: $F_0 = 1$, $F_1 = 1$, and $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$. Prove that $\forall n \in \mathbb{N}$, $F_n \leq (\frac{5}{3})^n$.

Answer I

Goal. Prove that $\forall n \in \mathbb{N}$, $F_n \leq (\frac{5}{3})^n$.

We will use an **induction of depth** 2 on n.

Bases cases. Prove that the property holds at ranks 0 and 1.

Obviously, $F_0 = 1 \leq (\frac{5}{3})^0$ and $F_1 = 1 \leq (\frac{5}{3})^1$, thus the property holds for $n = 0$ and $n = 1$.

Answer II

Inductive case. Assume that the property holds at rank n and $n+1$. Let us prove it holds at rank $n+2$.

For $n \in \mathbb{N}$, assume that $F_n \leq (\frac{5}{3})^n$ and $F_{n+1} \leq (\frac{5}{3})^{n+1}$. Then:

$$\begin{aligned}
& F_{n+2} \\
= \quad & F_n + F_{n+1} \\
\leq \quad & (\tfrac{5}{3})^n + (\tfrac{5}{3})^{n+1} \quad \text{by hypothesis} \\
\leq \quad & (\tfrac{5}{3})^n (1 + \tfrac{5}{3}) \\
\leq \quad & (\tfrac{5}{3})^n \cdot \tfrac{8}{3} \\
\leq \quad & (\tfrac{5}{3})^n \cdot (\tfrac{5}{3})^2 \quad \text{as } \frac{8}{3} = \frac{24}{9} < \frac{25}{9} \\
\leq \quad & (\tfrac{5}{3})^{n+2}
\end{aligned}$$

Practical Application

Exercise 2. Prove that for all integers $n \geq 8$, $\exists a, b \in \mathbb{N},\ n = 3 \cdot a + 5 \cdot b$.

Trying Our Luck

Let us prove by **simple induction** on n that $\forall n \in \mathbb{N}$ such that $n \geq 8$, $\exists a, b \in \mathbb{N},\ n = 3 \cdot a + 5 \cdot b$.

Base case. Obviously, $8 = 3 + 5$, thus the property holds for $n = 8$.

Inductive case. For $n \in \mathbb{N}$, assume that the property holds for n. Then

$\exists a, b \in \mathbb{N},\ n = 3 \cdot a + 5 \cdot b$.

Thus $n + 1 = n + 10 - 9 = 3 \cdot (a - 3) + 5 \cdot (b + 2)$.

But we cannot claim that $a - 3 \in \mathbb{N}$.

Be wary of the actual property you want to prove.

Answer I

Goal. Prove that for all integer $n \geq 8$, $\exists a, b \in \mathbb{N}$, $n = 3 \cdot a + 5 \cdot b$.

We will use an **induction of depth** 3 on n.

Bases cases. Prove that the property holds at ranks 8, 9, and 10.

Obviously, $8 = 3 + 5$, $9 = 3 \cdot 3$, $10 = 5 \cdot 2$, thus the property holds for $n = 8$, $n = 9$ and $n = 10$.

Answer II

Inductive case. Assume that the property holds at rank n, $n+1$ and $n+2$. Let us prove it holds at rank $n+3$.

For $n \in \mathbb{N}$, assume that the property holds for n, $n+1$, and $n+2$.
In particular, $\exists a, b \in \mathbb{N}$, $n = 3 \cdot a + 5 \cdot b$.
Then $n + 3 = 3 \cdot (a+1) + 5 \cdot b$.

The Strong Induction Principle (🇫🇷 *Récurrence Forte*)

A new method

What if, instead of looking for the immediate predecessors of the inductive case, our proof may rely on any **previous case**?

Strong induction theorem

Consider a proposition P on natural integers and $n_0 \in \mathbb{N}$ such that:

- $P(n_0)$ holds.
- $\forall n \geq n_0$, $(\forall k \in \{n_0, \ldots, n\}, P(k)) \Rightarrow P(n+1)$.

Then $\forall n \geq n_0, P(n)$.

The Strong Induction Principle

The strong inductive proof pattern

Goal. Prove that $\forall n \geq n_0, P(n)$.

We are going to use a proof by **strong induction** on n.

Base case. Prove that $P(n_0)$ holds.

Similar to simple inductive proofs ...

Inductive case. Prove that $\forall n \geq n_0, \boxed{\forall k \in \{n_0, \ldots, n\}, P(k)} \implies \boxed{P(n+1)}$.

Assume that for some $n \geq n_0$, $\forall k \in \{n_0, \ldots, n\}$, $P(k)$ holds ...

Associate $P(n+1)$ with one or more $P(k)$ for $n_0 \leq k \leq n$. Then apply the induction hypothesis.

... then $P(n+1)$ holds.

Practical Application

Exercise 3. Prove that every integer $n \geq 2$ can be decomposed into a product of prime numbers.

Answer I

Goal. Prove that every integer $n \geq 2$ can be decomposed into a product of prime numbers.

We will use a **strong induction** on n.

Base case. Prove that the property holds at rank 2.

Obviously, since 2 is prime, the property holds for $n = 2$.

Answer II

Inductive case. For $n \in \mathbb{N}$, assume that the property holds for any integer $2 \leq k \leq n$. Prove that it holds at rank $n+1$.

Consider $n+1$. Either $n+1$ is prime (and the property holds) or $\exists p, q \in \mathbb{N}$, $p, q \geq 2$, such that $n+1 = p \cdot q$.
Note that $2 \leq p, q \leq n$, thus we can apply the **induction hypothesis**: p and q can be decomposed into a products of prime factors. Then so does $n+1$, since $n+1$ is the product of p and q.

Practical Application

Exercise 4. Consider the following recursive sequence: $u_0 = 1$ and $\forall n \in \mathbb{N},\ u_{n+1} = \frac{u_0 + \ldots + u_n}{n+1}$. Prove that $\forall n \in \mathbb{N},\ u_n = 1$.

Answer I

Goal. Prove that $\forall n \in \mathbb{N},\ u_n = 1$.

We will use a **strong induction** on n.

Base case. Prove that the property holds at rank 0.

Obviously, $u_0 = 1$, thus the property holds for $n = 0$.

Answer II

Inductive case. For $n \in \mathbb{N}$, assume that the property holds for any integer $0 \leq k \leq n$. Prove that it holds at rank $n+1$.

For $n \in \mathbb{N}$, assume that for any integer $0 \leq k \leq n$, $u_k = 1$. Then:

$$\begin{aligned} & u_{n+1} \\ = & \frac{u_0 + \ldots + u_n}{n+1} \\ = & \frac{1 + \ldots + 1}{n+1} \quad \text{by hypothesis} \\ = & \frac{n+1}{n+1} \\ = & 1 \end{aligned}$$

Picking the Right Pattern

Simple induction. There is a direct relation between $P(n+1)$ and $P(n)$.

Induction of depth k. There exists a **known** k such that a relation between $P(n), \ldots, P(n+k-1)$ and $P(n+k)$ can be established. Note that k **must not** depend on n.

Strong induction. We can determine a relation between $P(n)$ and one or more strictly smaller cases $P(i)$, where the rank i **may be unknown** and depend on n.

The Generalized Induction Principle

Some order relations

- The induction principle consists in **starting** from a base case and **spreading** a property from smaller elements to bigger elements.
- In order to prove this principle, we had to consider the **minimal** element of a set of integers.
- We will formalize what being smaller or bigger means in a generic case.

The Generalized Induction Principle

Introducing order relations

We consider another class of **binary relations** that is somewhat similar to the **lesser or equal** relation $\leq$ on real numbers.

Antisymmetry

A binary relation R on a set E is said to be **antisymmetric** if and only if $\forall x, y \in E, ((x \sim_R y) \wedge (y \sim_R x)) \Leftrightarrow (x = y)$.

Order relation

A binary relation $\preceq$ is said to be an **order relation** if it is **reflexive**, **antisymmetric**, and **transitive**.

The Generalized Induction Principle

Properties of order relations

Some order relations may verify further properties:

Total order

An order relation $\preceq$ on E is said to be **total** if $\forall x, y \in E$, $x \preceq y$ or $y \preceq x$.

Well-founded order

An order relation $\preceq$ on E is said to be **well-founded** if any non-empty subset F of E admits a **minimal element** x, that is, such that $x \in F$ and there is no $y \in F \setminus \{x\}$ such that $y \preceq x$.

E The **usual order** $\leq$ on $\mathbb{N}$ is indeed total and well-founded.

The Generalized Induction Principle

Some order relations

- $\leq$ and $\geq$ are total order relations on $\mathbb{R}$. However, they're not well-founded.
- The **inclusion** $\subseteq$ is a well-founded order relation on the power set $\mathcal{P}(\mathbb{N})$. It is however not total: $\{1\} \not\subseteq \{2\}$ and $\{2\} \not\subseteq \{1\}$.
- A set may admit **more than one minimal element**: $\{1\}$ and $\{2\}$ are both minimal elements of $\{\{1\}, \{2\}, \{1, 2\}\}$ with regards to $\subseteq$.
- The **divisibility** relation $\mid$ on $\mathbb{N}^*$ such that $x \mid y$ if and only if x divides y is a well-founded order relation. However, it is not total.

The Generalized Induction Principle

Extending the principle

We can apply the induction principle to generic **ordered sets**.

Generalized induction theorem

Consider a set E, a **well-founded** order relation $\preceq$ on E and a proposition P on E such that:

- $P(x)$ holds for any minimal $x \in E$.
- Given $x \in E$, if $\forall y \in E$ such that $(y \preceq x) \wedge (y \neq x)$, $P(y)$ holds, then $P(x)$ holds.

Then $\forall x \in E, P(x)$.

See you next class!

Logical Formalism

Bijections and Cardinality

Adrien Pommellet, LRE

September 3, 2024

Intuiting Bijections

Encoding integers

Decimal encoding					$5 \cdot 10^1$	$7 \cdot 10^0$
Binary encoding	$1 \cdot 2^5$	$1 \cdot 2^4$	$1 \cdot 2^3$	$0 \cdot 2^2$	$0 \cdot 2^1$	$1 \cdot 2^0$
Ternary encoding			$2 \cdot 3^3$	$0 \cdot 3^2$	$1 \cdot 3^1$	$0 \cdot 3^0$

Intuiting Bijections

From an decimal encoding to a binary encoding

Function. To each decimal encoding, we can match an unique (little endian) binary encoding.

Domain. Finite, non-empty sequences of integers in $\{0, \ldots, 9\}$ that do not start with 0 (with the exception of 0 itself).

Image. Finite, non-empty sequences of Booleans that do not start with 0 (with the exception of 0 itself).

Injectivity. Two different decimal encodings yield different binary encodings.

Surjectivity. To each binary sequence corresponds an original decimal encoding.

Invertibility of bijections is a natural consequence of interpreting **equipotent** sets as various **encodings** of the same objects.

Practical Application

Exercise 1. How can we **practically** encode sets of integers in $\mathcal{P}(\mathbb{N})$? Discuss the possible drawbacks of the various implementations.

Answer I

It is a non-trivial problem. First, let us focus on **finite** sets.

Listing the elements. $[0, 3, 2, 5]$ encodes $\{0, 2, 3, 5\}$. So does $[5, 0, 3, 5, 2]$, though: it is therefore **not** a bijection.

Sorted lists without repetitions. $[0, 2, 3, 5]$ encodes $\{0, 2, 3, 5\}$. It is indeed a bijection, although **inserting** new elements may prove tricky as the list must be kept sorted.

Bit vectors. 101101 encodes $\{0, 2, 3, 5\}$. It is a bijection and a situational encoding: 1111 is a compact representation of $\{0, 1, 2, 3\}$, but $10^{999}1$ **inefficiently** encodes $\{0, 1000\}$.

Answer II

There is **no** exhaustive, finite encoding of **infinite** sets. The following solutions can be situationally useful:

Regular expressions. $[0-9]^*(0+5)$ encodes the multiples of 5. It is, however, a purely **syntactic** encoding, that does not equate 0123 with 123.

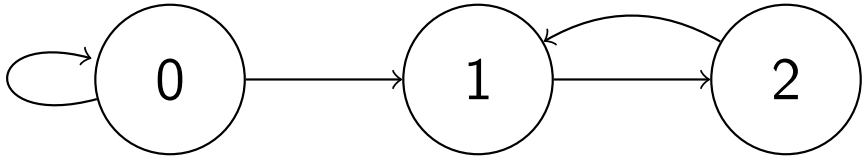
Constraints. Encode a set E as a conjunction of equations and inequalities whose set of solutions is exactly E. It is **not** a bijection.

Programs. Consider the binary encoding of an assembly program recognizing the set E. It is **not** a bijection either.

Intuiting Bijections

Encoding graphs

How can we **encode** directed graphs with three vertices?



Adjacency matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Edge set

$$\{(0,0),(0,1)$$
$$(1,2),(2,1)\}$$

$$f : \{0,1,2\} \to \mathcal{P}(\{0,1,2\})$$

$$\begin{aligned} f(0) &= \{0,1\} \\ f(1) &= \{2\} \\ f(2) &= \{1\} \end{aligned}$$

Practical Application

Exercise 2. What is the number of directed graphs with three vertices?

Answer

- The set of directed graphs with three vertices is **equipotent** to the set of 3×3 binary matrices.
- The number of directed graphs with three vertices is thus equal to the number of 3×3 binary matrices. We will prove it later.
- There are $2^9 = 512$ possible 3×3 binary matrices, thus, 512 possible graphs.

Intuiting Bijections

Why do we bother?

Use the right encoding for the problem being considered, e.g. **counting** the number of elements in a set.

Finite Sets

What is a finite set?

- Some sets are **infinite**, others are **finite**.
- Not all finite sets are defined by an **explicit** enumeration of the form $\{x_1, \ldots, x_n\}$.
- How can we **count** the number of elements of such sets?

Finite Sets

Finiteness

We define the **finite** sets as follows:

Finiteness

Let E be a set. E is said to be **finite** if either:

- $E = \emptyset$;
- $\exists n \in \mathbb{N}^*$ such that $\{1, \ldots, n\}$ and E are equipotent.

Intuitively, every element of E can be assigned **an unique index** in $\{1, \ldots, n\}$ thanks to a bijection $\{1, \ldots, n\} \to E$.

Note that these two cases are **mutually exclusive**: it can be proven that a non-empty set E is never equipotent to $\emptyset$.

Finite Sets

Cardinality

We define the **size** of a set formally as follows:

Cardinality

Let E be a non-empty finite set. Then $\exists! n \in \mathbb{N}^*$ such that $\{1, \ldots, n\}$ and E are equipotent. This integer is called the **cardinality** $\mathrm{Card}(E) = n$ of E.

Moreover, we define $\mathrm{Card}(\emptyset) = 0$.

This **unicity** property is hardly trivial, but out of the scope of this class.

Finite Sets

The fundamental cardinality property

Properties on **bijections** yield the following result:

Equipotent sets

Let E and F be two finite sets. If E and F are **equipotent** then $\mathrm{Card}(E) = \mathrm{Card}(F)$.

We **admit** this property.

Counting with Bijections

Finding the right encoding

- If two sets E and F are equipotent, we can consider them to be merely two **representations** of the same object.
- Designing a bijection is in essence finding a way to **encode** relevant information.
- Some encodings may be **easier to count** than others and may allow us to **determine the cardinality of a complex equipotent set**.

Counting with Bijections

A proof pattern for equipotence

Goal. Prove that E and F are equipotent.

Introduce a **candidate** relation f.

Subgoal 1. Prove that f is a well-defined **function** $E \to F$.

As discussed earlier.

Subgoal 2. Prove that f is a bijection.

Apply the definition. Prove that f is **injective** and **surjective**.

Find the inverse. Exhibit g such that $g = f^{-1}$.

Counting with Bijections

Composing bijections

Functional **composition** can be applied to bijections.

Composition of bijections

Consider two bijections $f : E \to F$ and $g : F \to G$. Then $g \circ f : E \to G$ is a bijection as well.

Indeed, note that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

$$\begin{tikzcd} E \arrow[r, "f"'] & F \arrow[l, bend right, "f^{-1}"'] \arrow[r, "g"'] & G \arrow[l, bend right, "g^{-1}"'] \end{tikzcd}$$

Practical Application

Exercise 3. Let E and F be two finite sets such that $\mathrm{Card}(E) = \mathrm{Card}(F)$. Prove that E and F are **equipotent**.

Answer

If $\mathrm{Card}(E) = \mathrm{Card}(F) = n$, there exist two bijections $f : \{1, \ldots, n\} \to E$ and $g : \{1, \ldots, n\} \to F$.

$$\begin{tikzcd}
E \arrow[rr, "h = g \circ f^{-1}"] & & F \\
& \{1, \ldots, n\} \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Consider then function $h = g \circ f^{-1}$ from E to F. Then h is a **bijection**, as it admits an inverse $f \circ g^{-1}$. Thus E and F are **equipotent**.

Counting the Power Set

Subset analysis

- The analysis and enumeration of various finite structures is known as **combinatorics**.
- A simple finite structure that can be derived from any finite set E is its **power set** $\mathcal{P}(E)$.
- We would like to count the number of subsets of E.

Counting the Power Set

A important result

If a set E is finite, then intuitively its **power set** $\mathcal{P}(E)$ is also finite as well. But what is its exact cardinality?

Cardinality of the power set

Let E be a finite set such that $\text{Card}(E) = n$. Then $\text{Card}(\mathcal{P}(E)) = 2^n$.

For that reason, the power set of E is often written 2^E, hence the name.

Counting the Power Set

Designing the right bijection

E	e_1	e_2	e_3	...	e_n
F	$\in$	$\notin$	$\in$		$\notin$
	in	out	in		out
$\{0, 1\}^n$	1	0	1		0

Counting the Power Set

A quick proof

- Let $E = \{e_1, \ldots, e_n\}$ be a finite set of cardinality n and $\mathbb{B} = \{0, 1\}$ the Boolean set.
- We define a function $f : \mathcal{P}(E) \to \mathbb{B}^n$ such that $f(X) = (x_1, \ldots, x_n)$, where $x_i = 1$ (resp. 0) if and only if $e_i \in X$ (resp. $e_i \notin X$).
- The function f is **surjective**; indeed, given $(x_1, \ldots, x_n) \in \mathbb{B}^n$, the subset $X = \{e_i \mid i \in \{1, \ldots, n\}, x_i = 1\} \in \mathcal{P}(E)$ is such that $f(X) = (x_1, \ldots, x_n)$.
- The function f is also **injective**; indeed, given $X, Y \in \mathcal{P}(E)$, if $f(X) = f(Y)$, then $x \in X \iff x \in Y$, thus $X = Y$.
- $\mathcal{P}(E)$ and $\mathbb{B}^n$ are **equipotent**, thus $\mathrm{Card}(\mathcal{P}(E)) = \mathrm{Card}(\mathbb{B}^n)$.
- Finally, $\mathrm{Card}(\mathcal{P}(E)) = 2^n$.

We intuit the cardinality of $\mathbb{B}^n$.

Logical Formalism

Applied Combinatorics

Adrien Pommellet, LRE

September 17, 2024

Counting Sets

Union

We first introduce the following property on the union:

Cardinality of a disjoint union

Let E and F be two finite sets such that $\text{Card}(E) = n$, $\text{Card}(F) = m$, and $E \cap F = \emptyset$. Then $\text{Card}(E \cup F) = n + m$.

We can intuit a proof of this property.

Counting Sets

Class struggle

- Consider two **disjoint** groups of students: group A contains n students, group B, m students.
- Each student in group A (resp. B) is **uniquely identified** by a number between 1 and n (resp. m).
- If we merge the two groups, how can we give each student an unique identifier between 1 and $n + m$?

Preserve the original identifiers of group A and **offset** the identifiers of group B by n.

Counting Sets

Inclusion and complementary

The following set-theoretic properties also hold:

Cardinality and inclusion

Let E and F be two finite sets such that $\mathrm{Card}(E) = n$, $\mathrm{Card}(F) = m$, and $E \subseteq F$. Then $n \leq m$.

Cardinality of the complement

Let E and F be two finite sets such that $\mathrm{Card}(E) = n$, $\mathrm{Card}(F) = m$, and $E \subseteq F$. Then $\mathrm{Card}(E^{\complement}) = \mathrm{Card}(F \setminus E) = m - n$.

Practical Application

Exercise 1. Prove these two properties.

Answer

- Since $E \subseteq F$, we consider the **disjoint** union $E \cup (F \setminus E) = F$. Then:

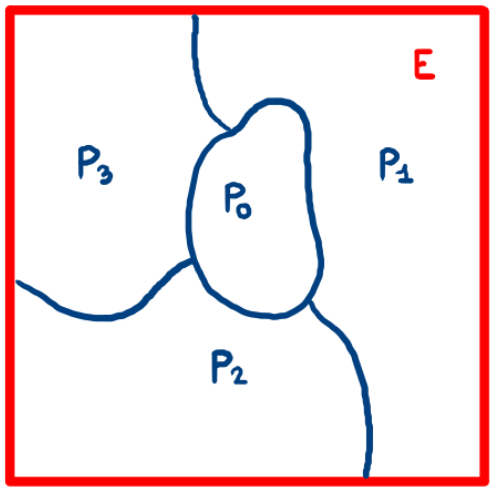
$$\begin{aligned} \mathrm{Card}(E) + \mathrm{Card}(F \setminus E) &= \mathrm{Card}(F) \\ n + \mathrm{Card}(F \setminus E) &= m \\ n &\leq m \end{aligned}$$

- Since $E \subseteq F$, we consider the **disjoint** union $E \cup E^{\complement} = F$. Then:

$$\begin{aligned} \mathrm{Card}(E) + \mathrm{Card}(E^{\complement}) &= \mathrm{Card}(F) \\ n + \mathrm{Card}(E^{\complement}) &= m \\ \mathrm{Card}(E^{\complement}) &= m - n \end{aligned}$$

Partitions

An intuition



$\mathcal{P} = \{ P_0, P_1, P_2, P_3 \}$

Partitions

A proper definition

We introduce a set-theoretic definition:

Partition of a set

A (possibly infinite) set of sets $\mathfrak{P}$ is said to be a **partition** of E if it verifies the following properties:

Non-empty subset. $\forall X \in \mathfrak{P}, X \subseteq E$ and $X \neq \emptyset$.

Disjointness. $\forall X, Y \in \mathfrak{P}, (X \neq Y) \implies (X \cap Y = \emptyset)$.

Coverage. $\forall x \in E, \exists X \in \mathfrak{P}, x \in X$.

? The last two properties yield the conclusion $\forall x \in E, \exists! X \in \mathfrak{P}, x \in X$.

Partitions

A direct proof pattern

Goal. Prove that $\mathfrak{P}$ is a **partition** of E.

Subgoal 1. Prove that $\forall X \in \mathfrak{P}, X \subseteq E$ and $X \neq \emptyset$.

Let $X \in \mathfrak{P}$. Prove that $X \subseteq E$ and $X \neq \emptyset$.

Subgoal 2. Prove that $\forall X, Y \in \mathfrak{P}, \boxed{X \neq Y} \implies \boxed{X \cap Y = \emptyset}$.

By contradiction, consider $X, Y \in \mathfrak{P}$ such that $\exists x \in X \cap Y$. Then prove that $X = Y$.

Subgoal 3. Prove that $\forall x \in E, \exists X \in \mathfrak{P}, x \in X$.

Let $x \in E$. Exhibit $P \in \mathfrak{P}$ such that $x \in P$.

Partitions

Cardinality of partitions

Cardinality of disjoint unions yields the following property:

A property of partitions

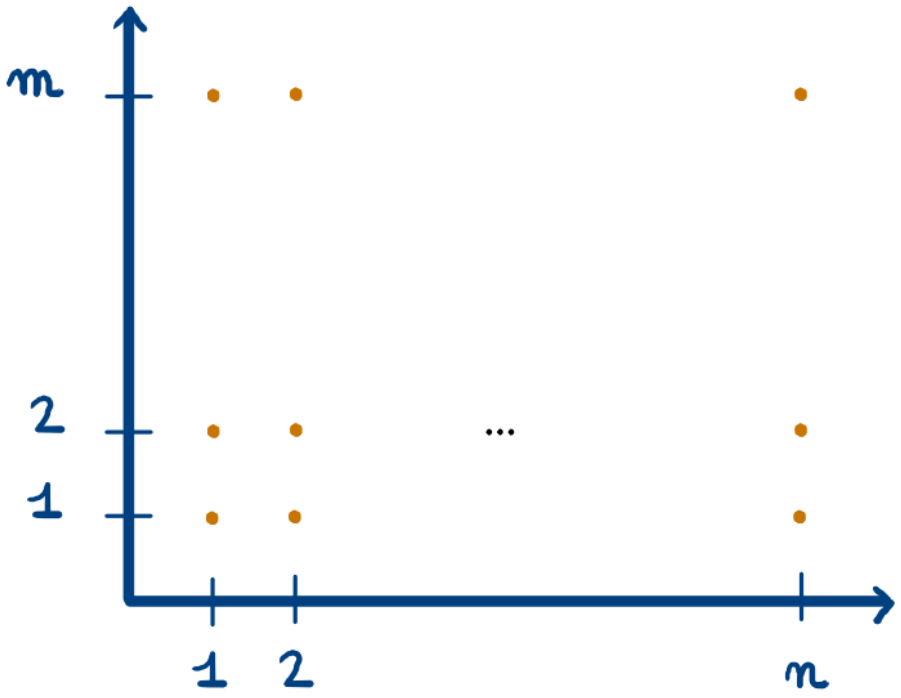
Consider a partition $\mathfrak{P} = \{P_1, \ldots, P_n\}$ of a finite set E. Then the equality $\mathrm{Card}(E) = \mathrm{Card}(P_1) + \ldots + \mathrm{Card}(P_n)$ holds.

It can be proven by **simple induction**.

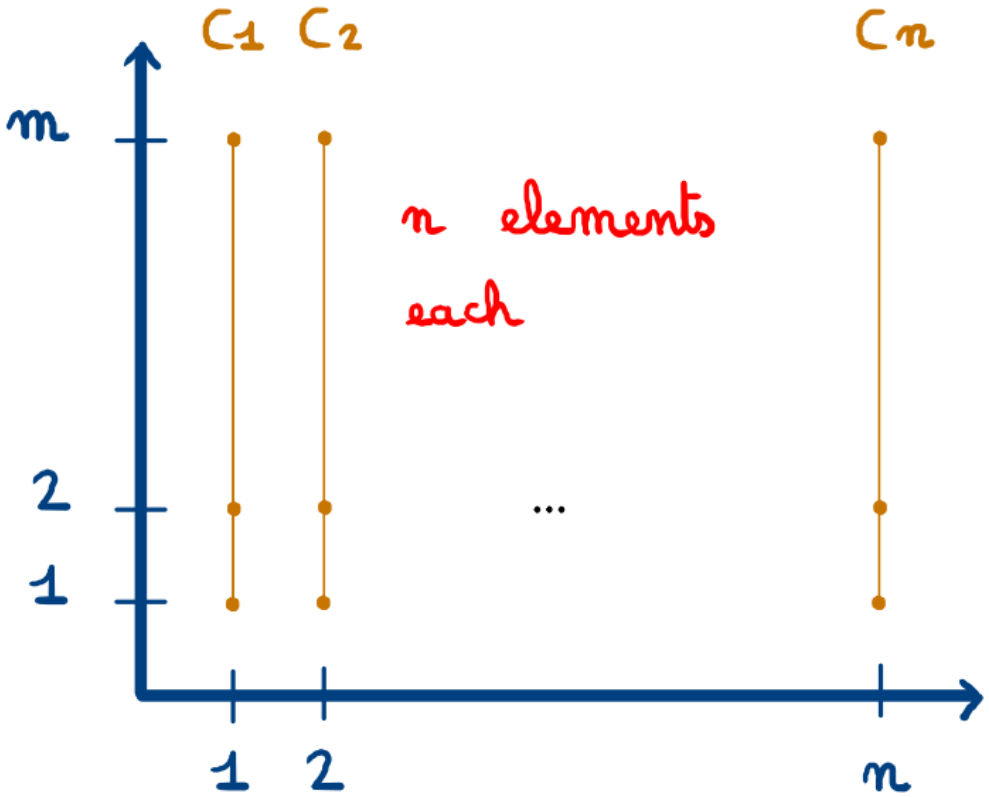
Thus, if we known $\mathrm{Card}(P_1), \ldots, \mathrm{Card}(P_n)$, we can compute $\mathrm{Card}(E)$.

Practical Application

Exercise 2. Intuit a proof of $\mathrm{Card}(\{1, \ldots, n\} \times \{1, \ldots, m\}) = n \cdot m$. Try to rely on an adequately defined partition.



Answer



Still Counting Sets

Cartesian product

Another **set-theoretic** operation we can consider is the Cartesian product:

Cardinality of a Cartesian product

Let E and F be two finite sets such that $\mathrm{Card}(E) = n$ and $\mathrm{Card}(F) = m$. Then $\mathrm{Card}(E \times F) = n \cdot m$.

An inductive generalization

Consider an arbitrary number $n \geq 2$ of finite sets $E_1, \ldots, E_n$. Then the equality $\mathrm{Card}(E_1 \times \ldots \times E_n) = \mathrm{Card}(E_1) \cdot \ldots \cdot \mathrm{Card}(E_n)$ holds.

Practical Application

Exercise 3. O'Zaman, EPITA's favourite kebab joint, offers **2 breads**, pita and wrap, **3 meats**, chicken, beef and lamb, and **4 sauces**, algerian, ketchup, yogurt, and mayonaise.

- What is the number of full (with bread, meat, and sauce) sandwiches?
- What is the number of partial sandwiches without **either** sauce or meat?
- What is the number of full sandwiches without chicken **or** without ketchup?

Answer

Let B, M, and S be three sets of respective size 2, 3, and 4.

- $\text{Card}(B \times S \times M) = \text{Card}(B) \times \text{Card}(S) \times \text{Card}(M) = 2 \cdot 3 \cdot 4 = 24$.
- $\text{Card}(B \times M \cup B \times S) = \text{Card}(B \times M) + \text{Card}(B \times S) = 6 + 8 = 14$.
- Note that the negation of "not containing chicken or not containing ketchup" is "containing **both** chicken and ketchup".
  There are $\text{Card}(B \times \{\text{chicken}\} \times \{\text{ketchup}\}) = 2$ such sandwiches.
  Thus there are $24 - 2 = 22$ sandwiches without chicken or without ketchup.

Still Counting Sets

Counting subsets of size k

We would like to count the number of subsets of E of a **given size**.

The set of k-combinations

Let E be a set such that $\text{Card}(E) = n$. For any $k \in \mathbb{N}$, the set $\mathcal{P}_k(E)$ contains all the k-**combinations**, i.e. the subsets of E of cardinality k.

Cardinality of combinations

For any $k \in \mathbb{N}$, $\text{Card}(\mathcal{P}_k(E)) = \frac{n!}{k! \cdot (n-k)!}$ if $k \leq n$ and 0 otherwise. This value does not depend on E, only on its size, and is denoted C_n^k or $\binom{n}{k}$.

We **admit** this property.

Practical Application

Exercise 4. Consider the binary alphabet $\Sigma = \mathbb{B}$.

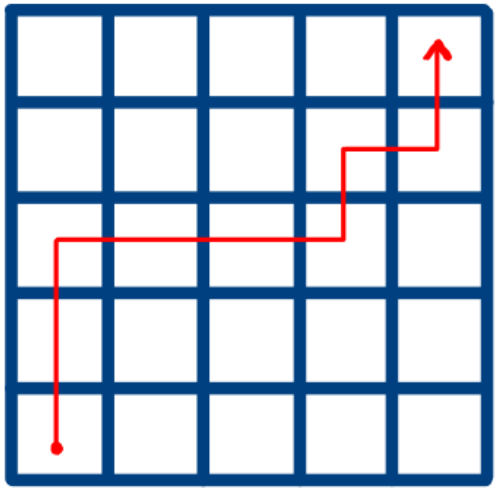
1. What is the number of possible binary words of length 4?
2. What is the number of possible binary words of length 4 containing exactly i bits of value 1 for a given $i \in \{0, \ldots, 4\}$.
3. What is the total number of 1 of all possible binary words of length 4?

Answer

1. $\text{Card}(\mathbb{B}^4) = 2^4 = 16$.
2. Let $W_i \subseteq \mathbb{B}^4$ be the set of all binary words containing i bits of value 1. Then $\text{Card}(W_i) = C_4^i$, as we pick i bits of value 1 among 4.
3. Note that the set $\{W_0, \ldots, W_4\}$ partitions $\mathbb{B}^4$, as its components are disjoint, non-empty, and cover $\mathbb{B}^4$.
   Thus, there is a grand total of $\sum_{i=0}^{4} i \cdot \text{Card}(W_i) = \sum_{i=0}^{4} i \cdot C_4^i = 32$ bits of value 1 in $\mathbb{B}^4$.

Practical Application

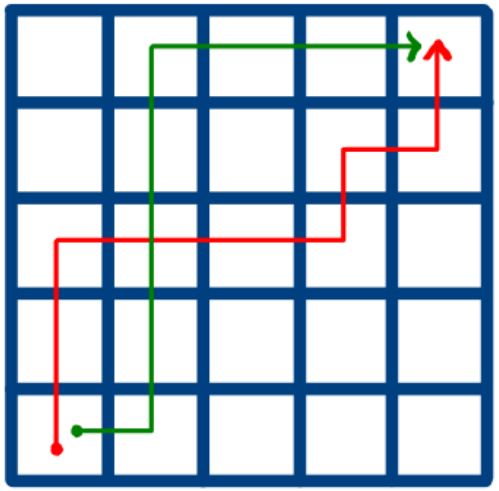
Exercise 5. Compute the number of paths from the bottom left corner to the top right corner of a 5×5 grid without ever moving down or left.



*From **Professor Layton and the Unwound Future**, a game for children over the age of 7.*

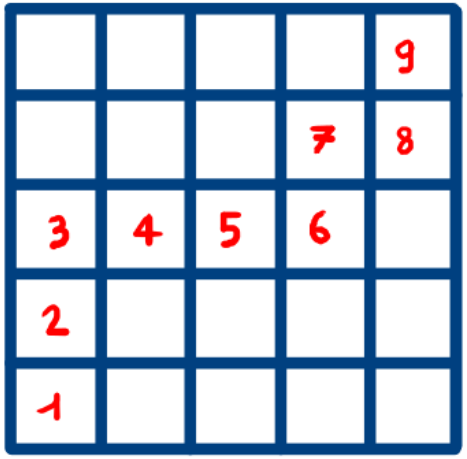
Answer I

First, note that each path goes exactly through 9 cells.



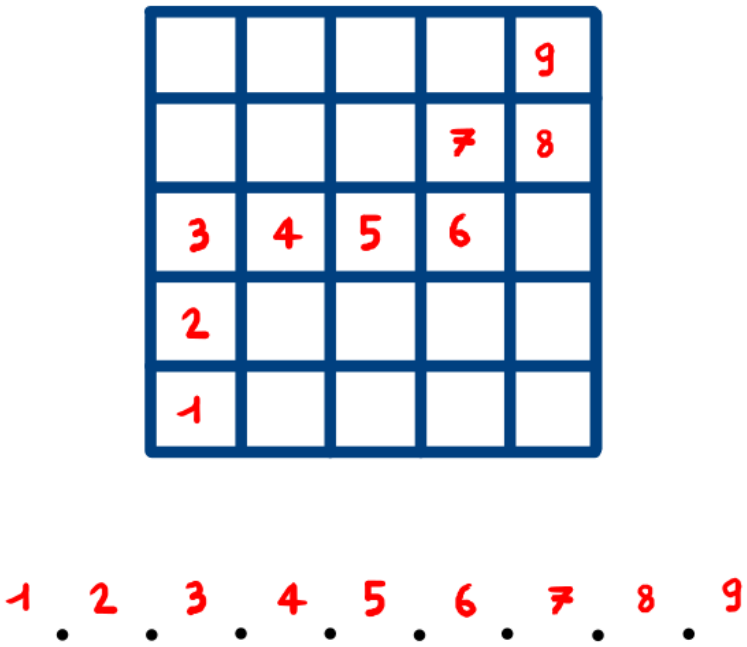
Answer II

More precisely, each path must move up 4 times and move right 4 times. The knowledge of these moves **accurately defines** the path



Answer III

Defining a path consists in picking four $\rightarrow$ positions among eight possible $\bullet$ positions. The remaining positions are implicitly filled with $\uparrow$. Hence, there are $\binom{8}{4} = 70$ paths.



Practical Application

Exercise 6. Prove that $\forall n \in \mathbb{N}$, the equality $2^n = \sum_{k=0}^{n} C_n^k$ holds by considering a partition of a $\mathcal{P}(E)$ for a set E of size n.

Answer

- Consider the set $\{\mathcal{P}_0(E), \ldots, \mathcal{P}_n(E)\}$. We can prove (left as an exercise) it is indeed a **partition** of $\mathcal{P}(E)$: its components are non-empty, disjoint, and cover $\mathcal{P}(E)$.
- Thus, $\mathrm{Card}(\mathcal{P}(E)) = \sum_{k=0}^{n} \mathrm{Card}(\mathcal{P}_k(E))$.
- Moreover, $\mathrm{Card}(\mathcal{P}(E)) = 2^n$ and $\mathrm{Card}(\mathcal{P}_k(E)) = C_n^k$ for any $k \in \{1, \ldots, n\}$.
- Finally, $2^n = \sum_{k=0}^{n} C_n^k$.

Tools for Combinatorics

Set-theoretic operations. Express a set as the disjoint union (a partition), the complementary, or the Cartesian product of **simpler sets**.

Bijections. Prove that a set is **equipotent** to a set whose cardinality is easier to compute.

Canonical properties. Know **by heart** the respective cardinalities 2^n and C_n^k of the sets $\mathcal{P}(E)$ and $\mathcal{P}_k(E)$.

See you next class!

Logical Formalism

Advanced Proof Patterns

Adrien Pommellet, LRE

September 20, 2024

Analysis and Synthesis

Finding unknown values

- Solving an equation actually consists in proving an **equivalence** of the form $f(x) = 0 \iff x \in S$.
- But the set S of solutions may initially be unknown. We thus need to **find** a proper candidate S before proving the equivalence.
- More generally, we face a similar issue when determining or finding an **unknown** value or relation, as opposed to proving a given conclusion from a **known** set of hypotheses.

Analysis and Synthesis

A new proof pattern

Goal. Given $P(x)$ of variable x, find a set S such that $P(x) \iff x \in S$.

Analysis step. Assume that $P(x)$ is true ...

... from there prove that $x \in R$ for some set R.

Find a proper subset $S \subseteq R$.

Synthesis step. Assume that $x \in R$.

~~... from there deduce $P(x)$. The equivalence holds for $S = R$.~~
Maybe $\exists y \in R$ such that $P(y)$ doesn't hold.
Prove that if $x \in R \setminus S$ then $\neg P(x)$.
Also prove that if $x \in S$ then $P(x)$.

Practical Application

Exercise 1. Solve in $\mathbb{R}$ the equation $x = \sqrt{2 - x}$.

Answer

Goal. Find the set $S \subseteq \mathbb{R}$ such that $x \in S \iff x = \sqrt{2-x}$.

Analysis step. Let $x \in \mathbb{R}$. Suppose that $x = \sqrt{2-x}$.

Then $x^2 = 2 - x$, hence $x^2 - 2 + x = 0$.
This equation admits two roots $x = 1$ and $x = -2$.
Thus $x \in \{-2, 1\}$.

Synthesis step. Assume $x \in \{-2, 1\}$.

Note that $1 = \sqrt{2-1}$ but $-2 \neq \sqrt{2-(-2)}$.
Finally, 1 is the only solution and $S = \{1\}$.

Using Bijections

Straight from the past

We will **step by step** solve the following problem:

2021, third mid-term exam

Let E be a set of cardinality n and $A \in \mathcal{P}(E)$ a subset of E of cardinality k. Let $\mathcal{P}_A(E)$ be the set of all subsets of E that contain A.

Prove that $\mathcal{P}_A(E)$ and $\mathcal{P}(E \setminus A)$ are **equipotent**.

Then determine the **cardinality** of $\mathcal{P}_A(E)$

Using Bijections

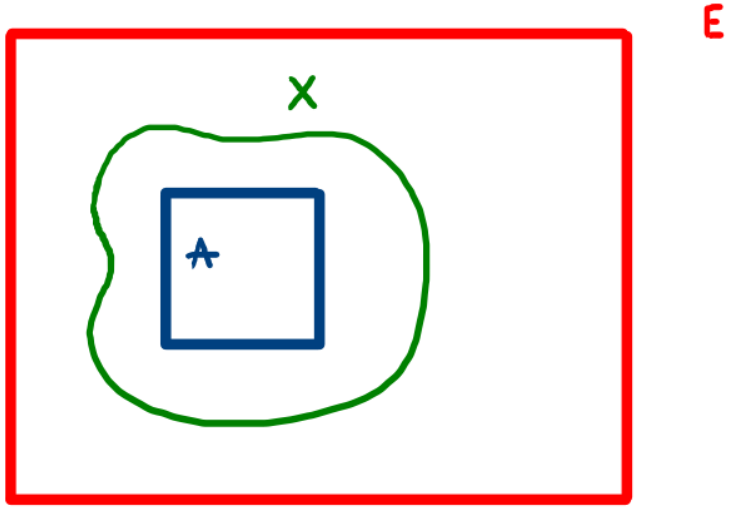
Beware of typing issues

- We need to exhibit a **bijection** $f : \mathcal{P}_A(E) \to \mathcal{P}(E \setminus A)$.
- You must **type** f correctly: it must take a subset of E containing A as an input, and return a subset of $E \setminus A$ as an output.
- Don't mistake its input as an element $x \in E$.
- You may have to prove $f(X)$ is always in $\mathcal{P}(E \setminus A)$.

Using Bijections

What is the input?

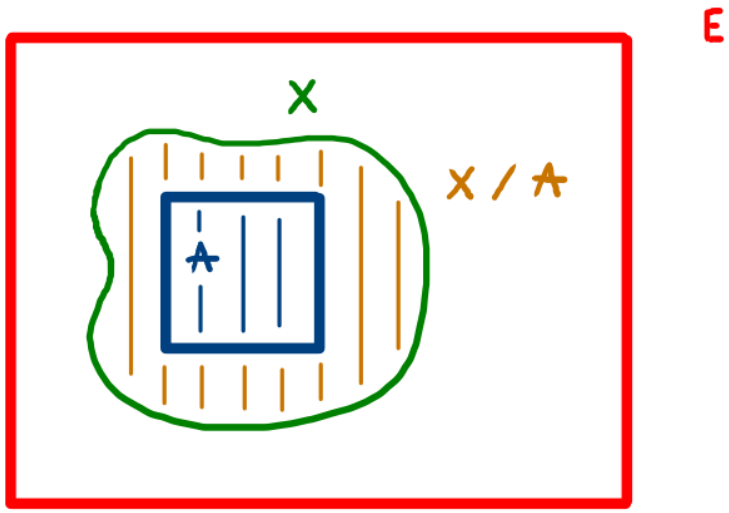
Consider a subset X of E that contains A. Can you associate it with a subset that does **not** contain A?



Using Bijections

What is the output?

If we **already** know that X contains A, the only **additional** data we need to characterize it are the elements of $X \setminus A$.



Using Bijections

An intuition

- Think in terms of **knowledge**: knowing that X is a subset of E that contains A, what is the least amount of data you need to find X?
- All the elements of A are in X, but the other remaining members of X may not be in A. Thus, knowing the latter set $X \setminus A$ is enough.
- Moreover, $X \setminus A$ is a subset of $E \setminus A$ as $X \subseteq E$.
- Our candidate bijection will be $f : X \in \mathcal{P}_A(E) \mapsto X \setminus A$. Note that $f(X) \in \mathcal{P}(E \setminus A)$.

Using Bijections

Proving the bijection I

- There are two ways to show that f is bijective: either prove that f is both injective and surjective, or exhibit the **inverse** function.
- The latter is simpler if we can intuit the right inverse function.
- If f **removes** some elements from X, then the only way to revert f is to **add** these elements back.

Using Bijections

Proving the bijection II

- Consider $g : Y \in \mathcal{P}(E \setminus A) \mapsto Y \cup A$. Since $Y \subseteq E$, $Y \cup A \in \mathcal{P}_A(E)$ and g is therefore a function $\mathcal{P}(E \setminus A) \to \mathcal{P}_A(E)$.
- $\forall Y \in \mathcal{P}(E \setminus A), f \circ g(Y) = (Y \cup A) \setminus A = Y$ because $Y \cap A = \emptyset$.
- $\forall X \in \mathcal{P}_A(E), g \circ f(X) = (X \setminus A) \cup A = X$ because $A \subseteq X$.
- Thus $g = f^{-1}$ and f is **invertible**, hence a **bijection**.

Using Bijections

Computing the cardinality

- $\mathcal{P}(E \setminus A)$ and $\mathcal{P}_A(E)$ are **equipotent**, thus have the same cardinality.
- But, since $A \subseteq E$, $\mathrm{Card}(E \setminus A) = \mathrm{Card}(E) - \mathrm{Card}(A) = n - k$.
- As a consequence, $\mathrm{Card}(\mathcal{P}(E \setminus A)) = 2^{n-k}$, and we conclude that $\mathrm{Card}(\mathcal{P}_A(E)) = 2^{n-k}$.

Using Bijections

What should one write during the exam?

- We define $f : X \in \mathcal{P}_A(E) \mapsto X \setminus A$. Since $X \subseteq E$, $X \setminus A \in \mathcal{P}(E \setminus A)$. Thus f is a **function** $\mathcal{P}_A(E) \to \mathcal{P}(E \setminus A)$.
- Consider $g : Y \in \mathcal{P}(E \setminus A) \mapsto Y \cup A$. Since $Y \subseteq E$, $Y \cup A \in \mathcal{P}_A(E)$. Thus g is a **function** $\mathcal{P}(E \setminus A) \to \mathcal{P}_A(E)$.
- $\forall Y \in \mathcal{P}(E \setminus A), f \circ g(Y) = (Y \cup A) \setminus A = Y$ because $Y \cap A = \emptyset$. And $\forall X \in \mathcal{P}_A(E), g \circ f(X) = (X \setminus A) \cup A = X$ because $A \subseteq X$. As a consequence, $g = f^{-1}$ and f is **invertible**, hence a **bijection**.
- $\mathcal{P}(E \setminus A)$ and $\mathcal{P}_A(E)$ are **equipotent**, therefore have the same cardinality. $\mathrm{Card}(E \setminus A) = \mathrm{Card}(E) - \mathrm{Card}(A) = n - k$ since $A \subseteq E$, thus $\mathrm{Card}(\mathcal{P}(E \setminus A)) = 2^{n-k}$.
- Finally, $\mathrm{Card}(\mathcal{P}_A(E)) = 2^{n-k}$.

Practical Application

Exercise 2. Let E be a set of cardinality n, let $\mathcal{S}_n$ be the set of bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$ and let $\mathcal{F}$ be the set of bijections $E \to \{1, \ldots, n\}$.

Sketch a proof of $\mathcal{F}$ and $\mathcal{S}_n$ being equipotent. How could you use it to determine $\mathrm{Card}(\mathcal{F})$?

Answer

- Our goal is to find a bijection $\varphi : \mathcal{F} \to \mathcal{S}_n$.
- First, we define a **function** φ such that, for any bijection $f : E \to \{1, \ldots, n\}$, $\varphi(f)$ is a bijection $\{1, \ldots, n\} \to \{1, \ldots, n\}$.
- Do not mess up the typing: φ takes a **function** as an argument and returns a **function**.
- We then prove that φ is a **bijection** by exhibiting an inverse function $\psi : \mathcal{S}_n \to \mathcal{F}$ such that:
  - $\forall f \in \mathcal{F}$, $\psi \circ \varphi(f) = f$.
  - $\forall \sigma \in \mathcal{S}_n$, $\varphi \circ \psi(\sigma) = \sigma$.
- Having proved that $\mathcal{F}$ and $\mathcal{S}_n$ are **equipotent**, we conclude that $\mathrm{Card}(\mathcal{F}) = \mathrm{Card}(\mathcal{S}_n)$.
  And it is known that $\mathrm{Card}(\mathcal{S}_n) = n!$ (number of **permutations**).

Stuck?

Determine the type of the objects. What are the **mathematical objects** being used? Integers, sets, functions, sets of sets, sets of functions? Look for usual definitions if needs be.

Understand what is being asked of you. Your **goal** can be to solve an equation, to prove an equivalence, to find a bijection, etc.

Sketch an early proof. This goal may often result in an **obvious first pattern** that you do not even have to guess.

Now it's time to work. Only **later** can you intuit relations between the various objects involved, look for simpler sub-goals, etc.

Logical Formalism

Tips and Mistakes

Adrien Pommellet, LRE

September 18, 2024

Common Logical Mistakes

Incorrect contrapositions

A property of real sequences

Consider two sequences of real numbers $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ in $\mathbb{R}^{\mathbb{N}}$. If both sequences admit a limit, then so does their product $(U_n \cdot Vn)_{n\geq 0}$.

~~Thus, the contraposition holds: if their product $(U_n \cdot Vn)_{n\geq 0}$ admits a limit, then so do $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$.~~

Consider $U_n = V_n = (-1)^n$. $U_n \cdot V_n = 1$, thus $(U_n \cdot V_n)$ admits a limit, but neither (U_n) nor (V_n) do.

The actual contraposition is: if their product $(U_n \cdot Vn)_{n\geq 0}$ **does not** admit a limit, then $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$, or both do not either.

Common Logical Mistakes

The strong law of small numbers

Let us prove that $\forall n \in \mathbb{N}$, $P(n)$ is true.

- $P(0)$ is true.
- $P(1)$ is true.
- $P(2)$ is true.
- $P(3)$ is true.

~~Thus we can obviously see that P is always true.~~

This is not a proper induction but instead **an utter waste of time**.

Common Logical Mistakes

False inductive proofs I

Wrong base case. Trying to prove that $\forall n \in \mathbb{N}^*$, $P(n)$ holds yet considering the base case $n = 0$ or $n = 2$.

Forgetting a base case. Assuming both $P(n)$ and $P(n+1)$ are true to prove $P(n+2)$, yet only considering a single base case $P(0)$ instead of proving both $P(0)$ and $P(1)$.

Wrong variable. Trying to prove that for a fixed, given k, $\forall n \in \mathbb{N}$, $P(n, k)$ is always true by induction on k instead of n, even when k isn't even an integer.

Common Logical Mistakes

False inductive proofs II

Wrong induction depth. Relying on both $P(n)$ and $P(n-1)$ to prove $P(n+1)$ yet using a simple induction.

Wrong rank. Relying on $P(n-k)$ during the inductive step, but not assuming that $n \geq k$.

Wrong induction hypothesis. Assuming that $\forall n \in \mathbb{N}$, $P(n)$ is true in the induction hypothesis. This is the very property you are trying to prove!

Common Logical Mistakes

A typing issue

A bijection on functions

Let $n, p \in \mathbb{N}^*$ such that $p \leq n$, let $\mathcal{F}$ be the set of **injective** functions $\{1, \ldots, p\} \to \{1, \ldots, n\}$, and let $\mathcal{A}_n^p$ be the subset of $\{1, \ldots, n\}^p$ of p-tuples whose components are all distinct.

Prove that $\mathcal{F}$ and $\mathcal{A}_n^p$ are **equipotent**.

Consider the function $\varphi : f \in \mathcal{F} \mapsto (f(1), \ldots, f(p))$. Note that $\varphi(f) \in \mathcal{A}_n^p$ due to f being injective. We will prove that φ is a bijection.

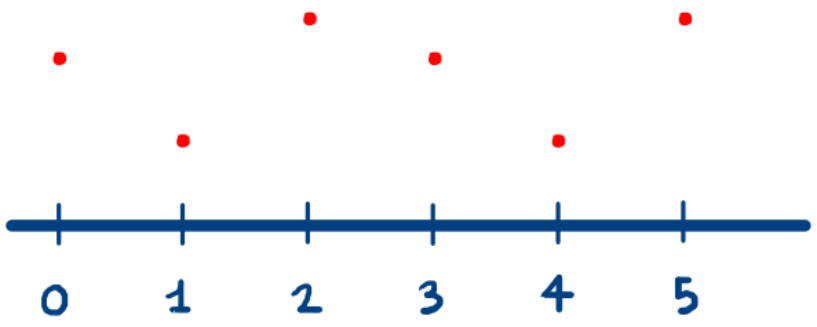
~~First, φ is injective: indeed, consider $f \in \mathcal{F}$; f is by hypothesis injective.~~

Note that φ is a **function that takes a function as an argument**: its argument being injective doesn't make it injective as well!

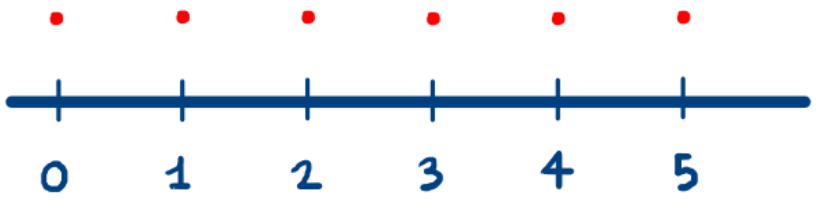
Common Logical Mistakes

Edge cases

Is it true that a **periodic** sequence cannot have a limit?



Actually, a periodic sequence admits a limit if and only if it is **constant**.



Practical Application

Exercise 1. Find **counter-examples** to the following made-up properties:

$$
\begin{aligned}
(x^{n+1} + \frac{1}{x^{n+1}}) &= (x^n + \frac{1}{x^n}) \cdot (x + \frac{1}{x}) \\
(a \leq x) \wedge (b \leq y) &\implies a - b \leq x - y \\
E \setminus A = F \setminus A &\implies E = F \\
\mathrm{Card}(\mathcal{P}(E \setminus A)) &= \mathrm{Card}(\mathcal{P}(E)) - \mathrm{Card}(\mathcal{P}(A))
\end{aligned}
$$

Practical Application

$$
\begin{aligned}
2 = (1^{1+1} + \frac{1}{x^{1+1}}) &\quad \neq \quad (1^1 + \frac{1}{1^1}) \cdot (1 + \frac{1}{1}) = 4 \\
(0 \leq 1) \wedge (0 \leq 2) &\quad \not\Longrightarrow \quad 0 - 0 \leq 1 - 2 \\
\{1, 2\} \setminus \{1, 3\} = \{2, 3\} \setminus \{1, 3\} &\quad \not\Longrightarrow \quad \{1, 2\} = \{2, 3\} \\
2 = \mathsf{Card}(\mathcal{P}(\{1\} \setminus \emptyset)) &\quad \neq \quad \mathsf{Card}(\mathcal{P}(\{1\})) - \mathsf{Card}(\mathcal{P}(\emptyset)) = 1
\end{aligned}
$$

Proper Reasoning

Remember common definitions and properties

A common pattern

Let $\{P_1, \ldots, P_n\}$ be a **partition** of a finite set E.

Compute $\text{Card}(E)$.

We defined a partition $\{P_1, \ldots, P_n\}$ of a set E as a set of **disjoint non-empty subsets** of E such that $P_1 \cup \ldots \cup P_n = E$.

We have proved that $\forall i \in \{1, \ldots n\}$, if $P_i \subseteq E$ and E is finite, then P_i is finite as well ; thus $\text{Card}(P_i)$ is **well-defined**.

Moreover, we have also proved that if $P_1 \cup \ldots \cup P_n = E$ and the sets $P_1, \ldots, P_n$ are disjoint, then $\text{Card}(E) = \text{Card}(P_1) + \ldots + \text{Card}(P_n)$.

Proper Reasoning

Use all the hypotheses

A property on functions

Let E be a finite set such that $\text{Card}(E) \geq 2$, and let F be a non-empty set. Prove that any **constant** function $f : E \to F$ is not injective.

A function is constant if and only if $\forall x, y \in E,\ f(x) = f(y)$.

By hypothesis, $\text{Card}(E) \geq 2$, thus there exists $n \geq 2$ and a bijection $g : \{1, \ldots, n\} \to E$. Note that $g(1) \neq g(2)$.

However, $f(g(1)) = f(g(2))$. Thus f is **not injective**.

Note that this property wouldn't hold if E was of cardinality 1.

Proper Reasoning

Settle on a proof method

Pick a specific proof method and make it **explicit**. As an example:

- We will prove by simple induction that $\forall n \in \mathbb{N}$, $P(n)$ holds...
- We will prove by contradiction that $Q(x)$ is true. If we assume that $\neg Q(x)$ holds...
- Let us prove that $E = F$ by double inclusion...
- Let us prove that $A \iff B$ by double implication. If we assume that A is true...

Proper Reasoning

Follow the problem's logic

Another common pattern

Prove that E and F are **equipotent**.

Then determine $\mathrm{Card}(E)$.

What's a common consequence of E and F being equipotent? That $\mathrm{Card}(E)$ is equal to $\mathrm{Card}(F)$.

Thus, we can use $\mathrm{Card}(F)$ to compute $\mathrm{Card}(E)$. Use previous results and look for common patterns in order to answer further questions.

Practical Application

Exercise 2. Let E be a set and $A, B, \in \mathcal{P}(E)$ be two subsets. Prove that $A \cap B = A \cap B^{\complement}$ if and only $A = \emptyset$.

Answer

Goal. Prove that $A \cap B = A \cap B^{\complement} \iff A = \emptyset$.

Subgoal 1. Prove that $A = \emptyset \implies A \cap B = A \cap B^{\complement}$.

Suppose that $A = \emptyset$. Then $A \cap B = \emptyset = A \cap B^{\complement}$.

Subgoal 2. Prove that $A \cap B = A \cap B^{\complement} \implies A = \emptyset$.

Assume that $A \cap B = A \cap B^{\complement}$. Suppose $\exists x \in A$.
By **case disjunction**, $x \in B$ or $x \in B^{\complement}$.
If $x \in B$, then $x \in A \cap B = A \cap B^{\complement}$, hence $x \notin B$, **absurd**.
If $x \notin B$, then $x \in A \cap B^{\complement} = A \cap B$, hence $x \in B$, **absurd**.
Therefore, by **contradiction**, $A = \emptyset$.

Practical Application

Exercise 3. Let E be a set and $A, B, \in \mathcal{P}(E)$ be two subsets. Prove that $(A \cap B^{\complement}) \cup (A^{\complement} \cap B) = B$ if and only $A = \emptyset$

Answer I

Goal. Prove that $(A \cap B^{\complement}) \cup (A^{\complement} \cap B) = B \iff A = \emptyset$.

Subgoal 1. Prove that $A = \emptyset \implies (A \cap B^{\complement}) \cup (A^{\complement} \cap B) = B$.

Suppose that $A = \emptyset$.
Then $A^{\complement} = E$.
Thus $(\emptyset \cap B^{\complement}) \cup (E \cap B) = \emptyset \cup B = B$.

Answer II

Subgoal 2. $(A \cap B^{\complement}) \cup (A^{\complement} \cap B) = B \implies A = \emptyset$.

Assume $(A \cap B^{\complement}) \cup (A^{\complement} \cap B) = B$.

Subgoal 3. Prove that $A \cap B = A \cap B^{\complement}$.

$A \cap ((A \cap B^{\complement}) \cup (A^{\complement} \cap B)) = A \cap B$
$(A \cap A \cap B^{\complement}) \cup (A \cap A^{\complement} \cap B) = A \cap B$
$(A \cap B^{\complement}) \cup (\emptyset \cap B) = A \cap B$
$(A \cap B^{\complement}) \cup \emptyset = A \cap B$
Finally, $A \cap B^{\complement} = A \cap B$.

The **previous exercise** yields $A = \emptyset$.

A Final Word

- The point of a proof is to **convince an informed reader**.
- Explicit your **objective** as early as you can. We will prove that $\forall x \in E, P(x)$ holds.
- Mention the **proof pattern** or method you're using. Let us prove this property by contraposition.
- If it's an **induction**, specify its **nature** (simple, of order k, or strong). Let us write a proof by induction of depth 3.
- You can admit **obvious** properties. Obviously, $A \cup A = A$.
- If you can't prove a property, feel free to **admit** it and write the rest of the proof. We admit that such an x exists. Let us now prove its unicity.

That's all folks!