# How to prove?

- Informal approach to proofs, in this course.
- We exhibit it through examples & ideas.

- **Theorem 1** (Euclid, 300 B.C.): $\forall n$, $\exists$ prime $> n$.

Pf:
- Assume that there is no prime above some bound, say $n$. [$P \subseteq \{1, 2, \dots, n\}$ ↖ primes]
- Consider $m := n! + 1$.

$\Rightarrow$ None of the primes ($\leq n$) divide $m$.

$\Rightarrow$ $m$ is prime ($& > n$) $\Rightarrow$ ↯ $\Rightarrow$ Thm 1. □

$\Rightarrow$ Set of primes $\mathbb{P}$ is $\infty$.

"Proof" example: Recall the infinite geometric sum formula:

$$S := \ldots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots$$

$$= \frac{x^{-1}}{1 - x^{-1}} + \frac{1}{1-x} = \frac{1}{x-1} + \frac{1}{1-x} = 0.$$

↳ Not a proof, as geometric sum application has <u>opposite</u> assumptions.

▷ $S \to \infty$.

- What is a Proof?

→ Proof is a series of mathematical statements, where every step is derived from the previous one by:
axioms, definitions, hypotheses (premises), theorems.

- Axioms of geometry were first made explicit in Euclid's books.
  - → Unique line between two points.
  - → Unique circle given center & radius.

▷ $n$ is odd $\Rightarrow$ $n^2$ is odd.

Pf: Assume $n$ is odd.

$\Leftarrow\!\!\Rightarrow$ $n =: 2k+1$

$\Leftarrow\!\!\Rightarrow$ $n^2 = (2k+1)^2 = 4(k^2+k)+1$

$\Leftarrow\!\!\Rightarrow$ $n^2 =: 2k'+1$

$\Leftarrow\!\!\Rightarrow$ $n^2$ is odd. □

→ Note the bi-directional & uni-directional implications.

– (Premise, conclusion) pair we write as "$p \Rightarrow q$". Read as: "$p$ implies $q$".

- "$p \iff q$" denotes <u>equivalence</u> of $p$ & $q$.
- "$p \impliedby q$" is <u>converse</u> of "$p \implies q$".

- <u>Exercise:</u> $n$ is odd <u>iff</u> $n^2$ is odd.
  → (if & only if)
  - "$p \implies q$" is "$q$ if $p$" is "$p$ only if $q$".
  - "$p \impliedby q$" is "$p$ if $q$" is "$q$ only if $p$".
  - "$p \iff q$" is "$p$ iff $q$".
  - "if $p$ then $q$".

<u>Exercise:</u> Write "Every prime $> 2$ is odd".

# Proofs techniques / Paradigms

- **Direct Proofs** : To prove "$p \Rightarrow q$" start from $p$ & end in $q$ ; statement by statement.

Ex: All squares are of the form $4k$ or $4k+1$.

**Indirect proofs:** Ex: $4k+2$, $4k+3$ are not squares.

- **Contrapositive proofs:** To prove "$p \Rightarrow q$"; start from $\neg q$ (negation/NOT $q$) & conclude with $\neg p$.

Ex: "$n>3$ is prime" $\Rightarrow$ "$n+1$ is non-square".

($p$ $q$)

(Contrapositive) pf: $n+1 = x^2$

$\Rightarrow$ $n = x^2-1 = (x-1)(x+1)$

$\Rightarrow$ $n$ is composite.

$\Rightarrow$ "$\neg q \Rightarrow \neg p$"

$\Rightarrow$ "$p \Rightarrow q$". □

Ex: Is there a direct proof?

- Warning: What about "$\neg p \Rightarrow \neg q$"?
Then you only prove the converse of "$p \Rightarrow q$".

## Contradiction

- eg primes are ∞ly many proof.
- To prove proposition $p$, assume $\neg p$ & arrive at False. $[\neg p \Rightarrow \text{False}] \Rightarrow p$.

▷ $\sqrt{2}$ is irrational.

Pf: $\sqrt{2} = a/b$ [Assume $a, b \in \mathbb{N}_{>0}$ & coprime]

$\Rightarrow a^2 = 2b^2 \Rightarrow a$ is even $\Rightarrow a = 2c$

$\Rightarrow 4c^2 = 2b^2 \Rightarrow 2c^2 = b^2 \Rightarrow b$ is even

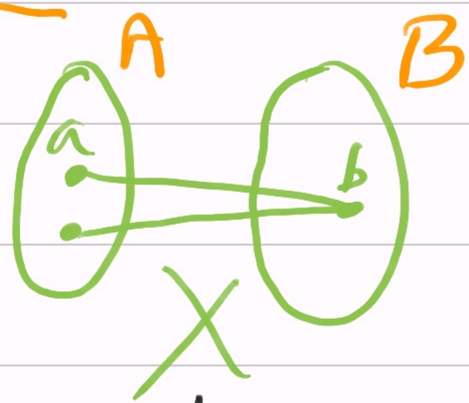
$\Rightarrow$ ↯

$\Rightarrow a, b$ don't exist, $\Rightarrow \sqrt{2} \notin \mathbb{Q}$. □

Exercise: $\pi$ is irrational.

## Cardinality

- Bijection $\varphi: A \to B$ is a function which is injective & surjective.
  - one-to-one
  - $\text{Img}(\varphi) = B$ or $\varphi(A) = B$.




**Defn:**

- $|A| = |B|$ if bijection $\varphi: A \to B$ exists.
  - $|A| \leq |B|$ if $\exists\, B' \subsetneq B$, bijection $\varphi: A \to B'$.

▷ $|\mathbb{N}| = |\mathbb{Z}|$.

$\mathbb{N} := \{0, 1, 2, \dots\}$ ; $\mathbb{N}_{>0}$

Pf: case 1: $n \geq 0 \xrightarrow{\varphi} 2n$ (even nos.)

case 2: $n < 0 \xrightarrow{\varphi} 2(-n)-1$ (odd nos.)

$\Rightarrow \varphi : \mathbb{Z} \longrightarrow \mathbb{N}$ is a function ; injection ; surjection

$\Rightarrow \varphi$ is a bijection.

$\Rightarrow |\mathbb{N}| = |\mathbb{Z}|$. □

- What about $|\mathbb{N}|$ & $|\mathbb{R}|$ ?
- Defn: For set $S$, the set of subsets (powerset) is $2^S := \{T \mid T \subseteq S\}$.

— Compare with $f_T : S \to \{0,1\}$.

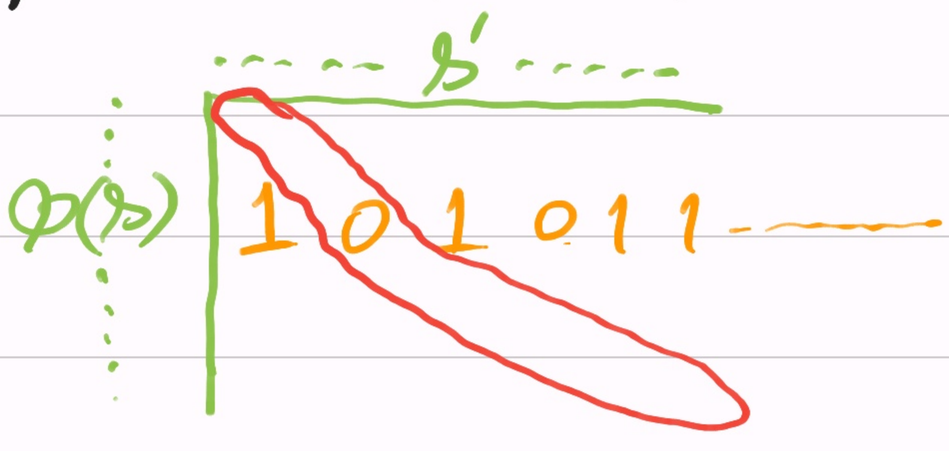
**Theorem** (Cantor 1891): $|S| < |2^S|$, for set $S$.

**Proof:** . Let $\varphi : S \to 2^S$ be a bijection.

[diagonalization argument:]

- Define a schematic matrix, for $S =: \{s \mid s \in S\}$.

▷ $\{0,1\}^{S \times S}$-matrix:




**Defn:** $(\text{Row } \varphi(s))_{s'} = 1$ iff $s' \in \varphi(s)$.

- Consider the binary tuple

$$\underline{D} := ( [\varphi(s), s] \mid s \in S )$$

- Consider $\neg\underline{D} := ( \overline{[\varphi(s), s]} \mid s \in S )$.

- $\neg D$ defines a subset $T \subseteq S$.

Qn: What's the preimage of $T$ under the bijection $\varphi: S \to 2^S$ ?

- Say, $s_0 \in S$ : $\varphi(s_0) = T$.

$$\Rightarrow [\varphi(s_0), s_0] = (T)_{s_0} = \overline{[\varphi(s_0), s_0]}$$

$\Rightarrow \lightning$.

$\Rightarrow |S| < |2^S|$. $\square$

**Corollary:** $|\mathbb{N}| < |2^{\mathbb{N}}| = |\mathbb{R}| < |2^{\mathbb{R}}| \ldots$

**Qn:** Generalize Cantor to show that
∃ problem for which ∄ no C-program?

## Quantification

- We use two quantifiers over domains:
  - Existential: $(\exists\, x \in S\,,\ [\text{condn}])$
  - Universal: $(\forall x \in S,\ [\text{condn}])$
    ⇝ Example / Thm / Counterexample.

▷ $\neg [\exists x \in S,\ P(x)] \equiv [\forall x \in S,\ \neg P(x)]$.

▷ $\neg [\forall x \in S,\ Q(x)] \equiv [\exists x \in S,\ \neg Q(x)]$.

## Induction

- Mathematical induction is like going over natural numbers $\mathbb{N}$: $n = 0, 1, 2, 3, \ldots$.
  - → The uncountable version of this is called: Tranfinite induction.

- Suppose you want to show: $[\forall x \in \mathbb{N},\ P(x)]$.

Then, an inductive pf. has two steps:

- Base case: $P(0)$ is true.
- Induction step: $[P(n) \Rightarrow P(n+1)]$.

▷[Induction] These two $\Rightarrow$ $[\forall x \in \mathbb{N}, P(x)]$.

-Eg. $\forall n \geq 0$, $2^n \geq n+1$.

Pf: Base: $1 = 2^0 \geq 0+1$.

Induction step: Assume $2^m \geq m+1$.

$\Rightarrow$ $2^{m+1} \geq 2\cdot(m+1) \geq ? \; m+2$ ✓

$\Rightarrow$ done. □

**Theorem:** $\forall n \in \mathbb{N}$, $\exists$ binary representation

$P(n) \to$ $n =: b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \cdots + b_r \cdot 2^r$ ;

s.t. $b_i \in \{0,1\}$ & $r \in \mathbb{N}$. ↖(minimal $r$)

**Pf:** **Base case:** $[P(0)]$ $n = 0 =: b_0$ & $r = 0$.

**Induction Step:** Assume $P(m')$, i.e.

$m' = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_s \cdot 2^s$.

$\Rightarrow 2m'+1 = ?$ or $2m' = ?$

**Case 1:** $[c_0 = 0]$ $2m'+1 = 1 + c_0 \cdot 2 + c_1 \cdot 2^2 + \cdots + c_s \cdot 2^{s+1}$

$\Rightarrow$ done.

**Case 2:** $[c_0 = 1]$ $2m' = 0 + c_0 \cdot 2 + c_1 \cdot 2^2 + \cdots + c_s \cdot 2^{s+1}$.

$\Rightarrow$ done.

□

Exercise: Is this representation unique?

— Induction can be multi-dimensional, i.e. $\mathbb{N}^d$.

Theorem: Consider a bivariate function $f(m,n)$, s.t. $f(m+1,n) = f(m,n) + 2(m+n)+1$ &
$f(m,n+1) =$ " &
$f(0,0) = 0$.
$\Rightarrow f = (m+n)^2$. ← $P(m,n)$ [Q: Why this $f$?]

Pf: • Want to show: $P(m,n)$ is true.

Base case: $[P(0,0)]$ $0 = f(0,0) = (0+0)^2 = 0$.

- Induction step: "move in each direction once"

(1) $[P(m,n) \Rightarrow P(m+1,n)]$ : Assume $f(m,n) = (m+n)^2$.

$\Rightarrow f(m+1,n) \overset{\text{given}}{=} f(m,n) + 2(m+n) + 1$

$= (m+n)^2 + 2(m+n) + 1 = (m+n+1)^2$.

$\Rightarrow P(m+1,n)$ is true.

(2) $[P(m,n) \Rightarrow P(m,n+1)]$: Assume $f(m,n) = (m+n)^2$.

$\Rightarrow f(m,n+1) \overset{\text{given}}{=} f(m,n) + 2(m+n) + 1$

$= (m+n+1)^2 \Rightarrow P(m,n+1)$ is true.

$\Rightarrow f = (m+n)^2$ always true. $\square$

- Exercise: Is $f$ unique ?

## Logic

— Math. statements $\equiv$ Propositions.

— Simplest kind of propositions :

AND: $p \wedge q$ ; OR: $p \vee q$ ; NOT: $\neg p$.

- Implication: "$p \Rightarrow q$" $\equiv$ $(\neg p \vee q)$.

- Check it by a truth-table:

| $p$ | $q$ | $p \Rightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

- Rules of inference :

- $p \Rightarrow (p \vee q)$
- $[p \wedge (p \Rightarrow q)] \Rightarrow [q]$
- $[\neg q \wedge (p \Rightarrow q)] \Rightarrow [\neg p]$
- $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow [p \Rightarrow q]$.

- $[\forall x \in S, P(x)] \Rightarrow P(s)$ [Instantiation]
- $P(s) \Rightarrow [\exists x \in S,\ P(x)]$ [from defn]
- $\neg [\forall x, P(x)] \Leftrightarrow [\exists x, \neg P(x)]$