DMA: Induction

Laura Mančinska,
Institut for Matematiske Fag

UNIVERSITY OF COPENHAGEN

Plan for today

- Induction as a proof technique
- Examples

- Strong induction
- Examples

- Ask me questions

Reading: Notes on Absalon (can also take a look Section 2.4 from KBR)

Suppose we want to prove a mathematical statement or formula

How do we show that

$$1 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Try different values of n:

$n = 1$ $\quad 1 \stackrel{?}{=} \frac{1(1+1)(2\cdot1+1)}{6}$ ✓

$n = 2$ $\quad 1 + 2^2 \stackrel{?}{=} \frac{2(2+1)(2\cdot2+1)}{6} = \frac{2\cdot3\cdot5}{6}$ ✓

$n = 3$ $\quad 1 + 2^2 + 3^2 \stackrel{?}{=} \frac{3(3+1)(2\cdot3+1)}{6} = \frac{3\cdot4\cdot7}{6} = 14$ ✓

$n = 4$ $\quad 1 + 2^2 + 3^2 + 4^2 \stackrel{?}{=} \frac{4(4+1)(2\cdot4+1)}{6} = \frac{4\cdot5\cdot9}{6} = 30$ ✓

Infinitely many. Cannot try them all.

Is it enough to check for only some values of n?

- Fermat conjectured that all numbers of the form $F_n = 2^{2^n} + 1$ are prime.
  - $F_1 = 2^{2^1} + 1 = 5$
  - $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$
  - $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$
  - Fermat checked up to $n = 4$

- 100 years later, Euler noticed that
  $$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

- There are no known Fermat primes F_n with $n > 4$ (checked up to $n = 32$; F_{33} has about 2.6 billion digits)

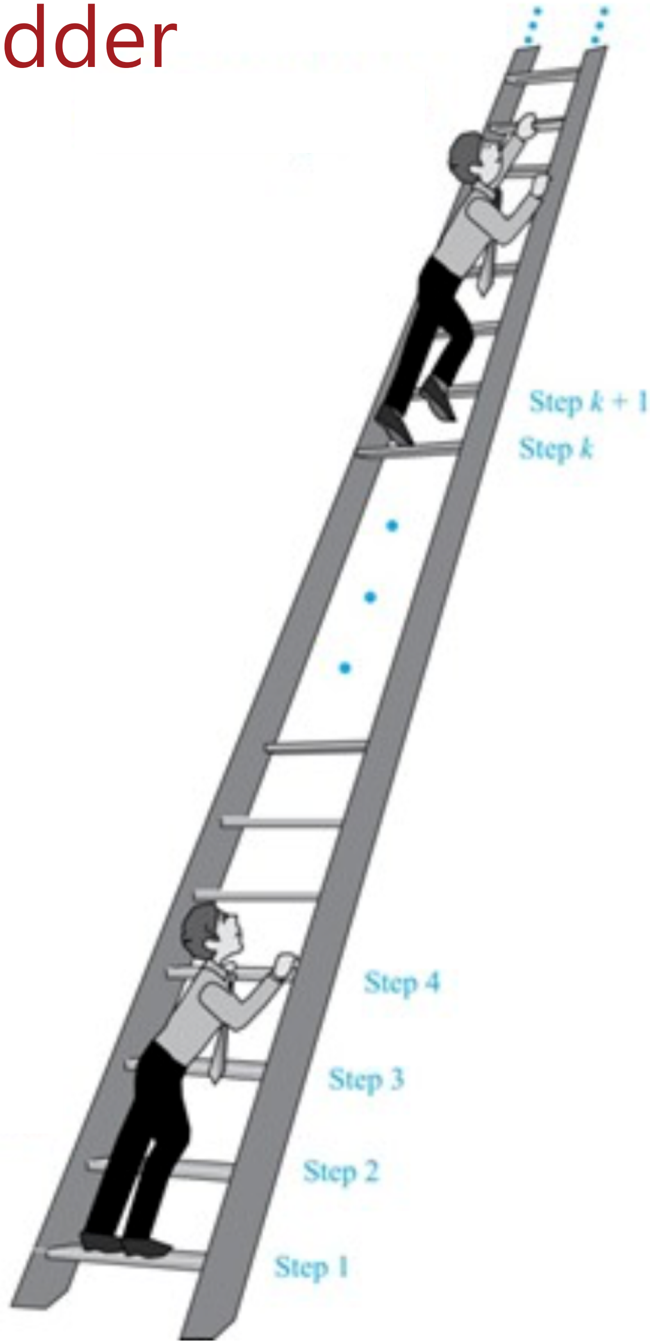
-

Mathematical induction

Analogy: climbing an infinite ladder

- Suppose you can reach the first rung
- If you are on a particular rung k you can get on the next rung $k + 1$

(Not the same as just assuming you can get from rung 1 to 2)



The principle of mathematical induction

Let $P(n)$ be a predicate (statement) defined for integers $\{n_0, n_0 + 1, \dots\}$. If

1. $P(n_0)$ is true and

2. for any $n \geq n_0$, we have that $P(n)$ being true implies that $P(n+1)$ is true

then

- $P(n)$ is true for all integers $n \geq n_0$.

Terminology

1. Is called basis step or base case
2. Is called inductive step.

Using induction to prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \text{ for all } n \in \mathbb{Z}^+$$

- Predicate $P(n)$: $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

- Base case: Check that $P(1)$ holds.

$$\frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{1(2)(3)}{6} = 1 = 1^2$$

- Inductive step:

Assume that $P(n)$ holds for some $n \geq 1$ (Induction hypothesis)

Show that this implies that $P(n+1)$ holds.

Structure of an inductive proof

- State that the proof uses induction.
- Define an appropriate predicate $P(n)$.
- Prove that $P(n_0)$ is true.
- Prove that $P(n)$ implies $P(n+1)$ for all $n \geq n_0$.
- Invoke the principle of mathematical induction.

Invariants

An invariant is a property that is preserved throughout a program or a procedure

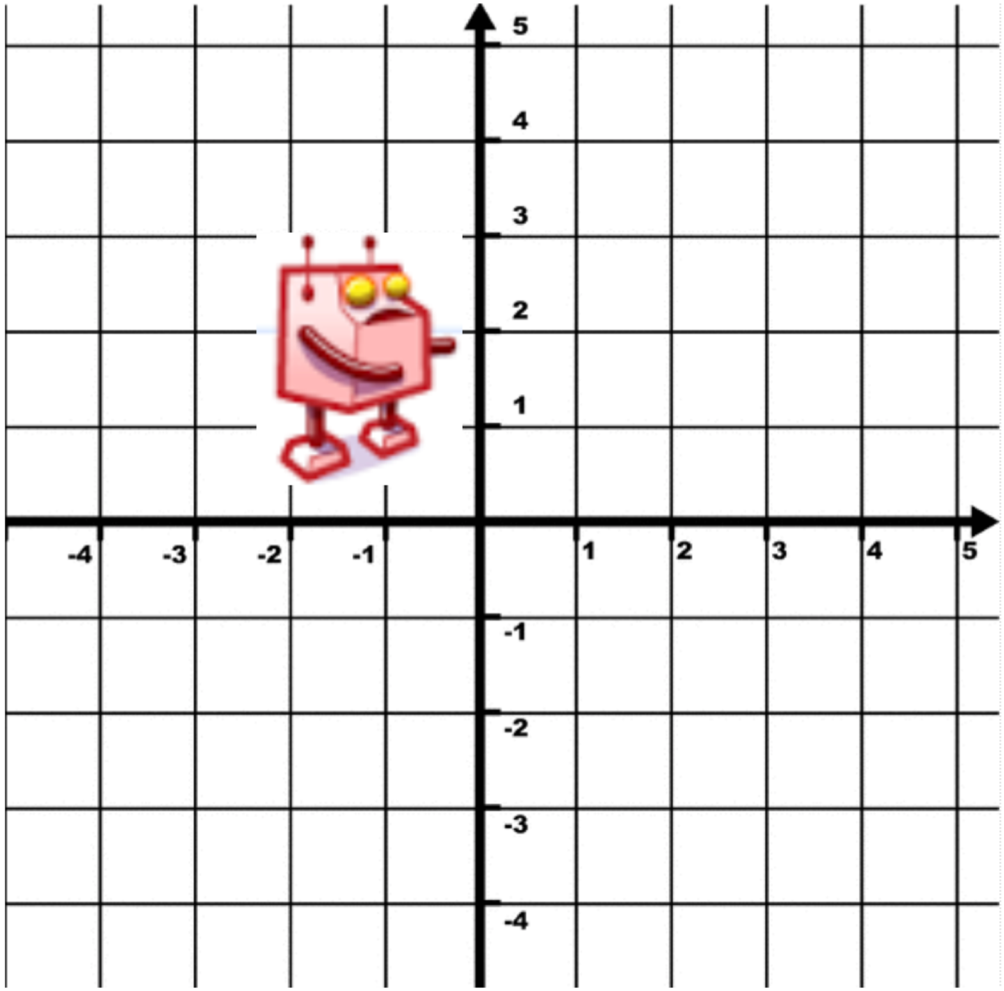
- $xy = z$ after every iteration of a **for**-loop.
- Temperature of a nuclear reactor doesn't exceed a critical value.

Invariants: Diagonally moving robot on a plane

Robot starts at (0,0)

If the robot is at (x, y) after step k, then in step $k+1$ it can go to either

- $(x+1, y+1)$ or
- $(x+1, y-1)$ or
- $(x-1, y+1)$ or
- $(x-1, y-1)$



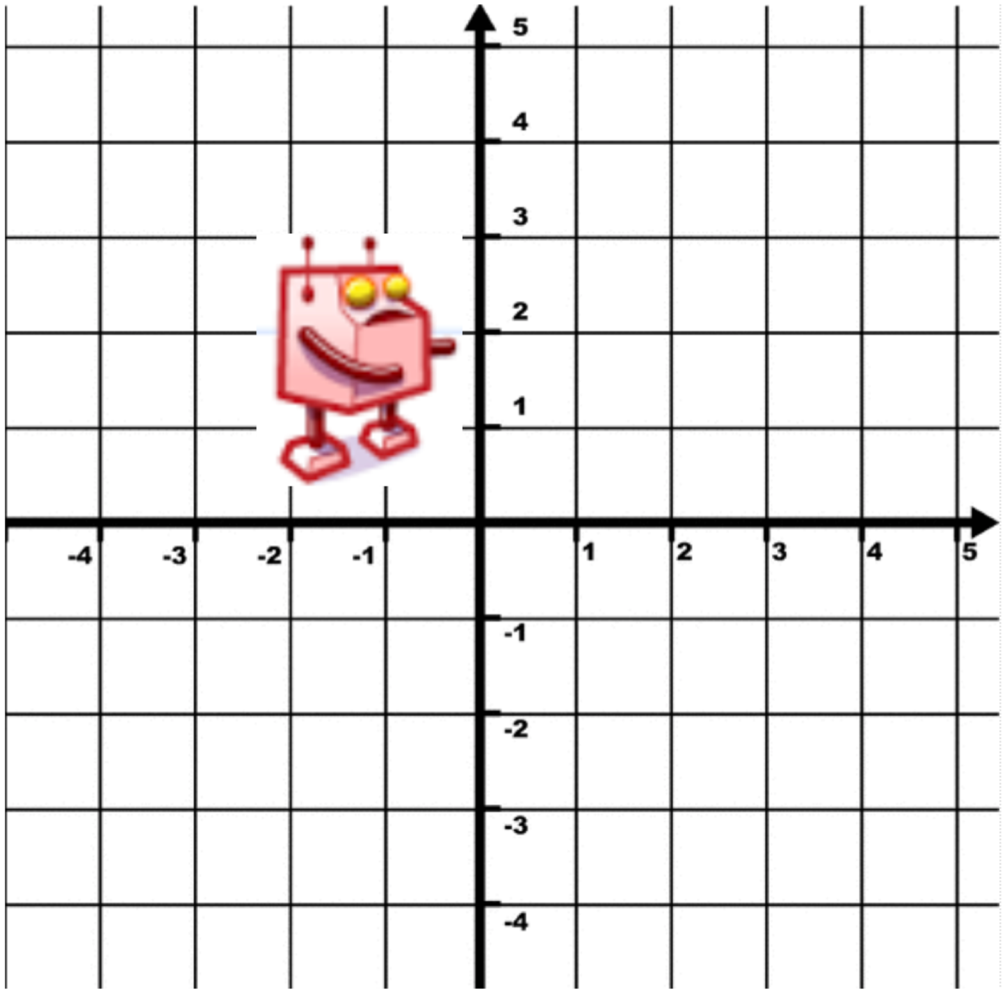
Can the robot be at (1,0) after some number of steps?

Invariants: Diagonally moving robot on a plane

Robot starts at (0,0)

If the robot is at (x, y) after step k, then in step k it can go to either

- $(x + 1, y + 1)$ or
- $(x + 1, y - 1)$ or
- $(x - 1, y + 1)$ or
- $(x - 1, y - 1)$



Warm-up:
How can the robot reach (2,0), (3,1), (4,-2)?

All horses are the same color

$P(n)$: in any set of n horses, all horses have the same color.

Base case: $P(1)$ is true since in a set with only one horse, all (one) horses are of the same color.

Inductive step: Suppose $P(n)$ is true for some $n \geq 1$ **(IH)** So any set of of n horses only contains same-color horses. Let us argue that $P(n+1)$ is true. Let

$$\{h_1, h_2, \dots, h_{n+1}\}$$

be a set of $n+1$ horses.

Have we shown that all horses have the same color?

Strong induction

The principle of strong induction

Let $P(n)$ be a predicate (statement) defined for integers $\{n_0, n_0 + 1, \dots\}$. If

1. $P(n_0)$ is true and
2. for any $n \geq n_0$, we have that $P(n_0), \dots, P(n)$ all being true implies that $P(n+1)$ is true

then

- $P(n)$ is true for all integers $n \geq n_0$.

Strong induction example 1: Prime factorization

Thm. Every integer $n \geq 2$ can be expressed as a product of primes, that is,

$$n = p_1^{a_1}\, p_2^{a_2} \cdots\, p_k^{a_k}$$

where all the p_i's are primes and $a_i \in \mathbb{Z}^+$ for all i.

Proof(by strong induction):

- Let $P(n)$ be the statement that integer $n \geq 2$ can be expressed as a product of primes.
- Base case: $P(2)$: 2 can be expressed as a product of primes $2 = 2$ (true).
- Inductive step: Assume that all of $P(2), \ldots, P(n)$ are true for some $n \geq 2$ (Strong Induction Hypothesis)

The Strong of Inductia: making change

- Inductia's currency is Strongs (Sg)
- They only have 3- and 5- Strong coins

- Which of these amounts can Inductians make:

  4, 5, 6, 7, 8, 9, 10, 11?

Claim. Inductians can make any integer amount $n \geq 8$.

Proof by strong induction.

Let $P(n)$ be the statement that Inductians can make n using their coins.

The Strong of Inductia: proof continued

- Base case: $P(8), \dots, P(11)$ holds:
  - 8=3+5
  - 9=3+3+3
  - 10=5+5
  - 11=3+3+5
- Inductive step. Assume that all of $P(8), P(9), \dots, P(n)$ are true for some $n \geq 11$. (Strong Induction Hypothesis)
- Let us show that $P(n+1)$ holds.
- How can Inductians make $n+1$ with their 3- and 5-Strong coins?

Splitting the chocolate bar

- We have $n \times m$ chocolate bar.
- How many breaks (each being horizontal or vertical) are needed to split it into 1×1 pieces?

- Warm-up: How many breaks are needed to split a bar of size
  - 1×1
  - 2×1
  - 2×2
  - 2×3
  - 3×1
- Can you guess the # of breaks needed for an $n \times m$ bar.

Splitting the chocolate bar

- $n \times m$ chocolate bar.
- We will use induction on the value of nm (call it k)

- Let $P(k)$ be the statement that any bar of size $n \times m$ where $nm = k$ needs $k - 1$ breaks.

- Basis case: $k = 1$. Only one $n \times m$ bar with $nm = 1$ (i.e., the 1×1 bar). Needs 0 breaks.
- Inductive step: Assume that all of $P(1), \dots, P(k)$ hold for some $k \geq 1$. (SIH) We want to show that $P(k+1)$ holds.