COMS10003

# Proof by Mathematical Induction

Kerstin Eder

University of BRISTOL

Department of COMPUTER SCIENCE

# Introduction

- Proof by induction
  - Special proof technique
  - Important proof technique
    - Used to prove algorithms correct
    - Used to prove properties of algorithms and their complexity
    - Used to prove properties of graphs and trees
    - Used to prove programs correct
    - Used to prove hardware correct

# Motivation

- Theorems are mathematical statements that can be shown to be true.
- Some theorems assert properties such as:

*“P(n) is true for all natural numbers n.”*

*e.g.*

$$1+2+3+...+n = n*(n+1)/2$$

- How can we demonstrate this is correct?

# The Principle of Induction

*"P(n) is true for all natural numbers n."*

**Proof by induction** relies on two steps:

- **Base step:**
  - Demonstrate that P(1) is true,
    i.e. set n=1 and show P(1).

# The Principle of Induction

*"P(n) is true for all natural numbers n."*

**Proof by induction** relies on two steps:

- Base step:
  - Demonstrate that P(1) is true.
- **Inductive step:**
  - Show that the implication $P(n) \rightarrow P(n+1)$ is true for all natural numbers n.
  - P(n) is the **inductive hypothesis** or **assumption.**

# The Principle of Induction

Proof by induction relies on two steps:

- Base step:
  - Demonstrate that $P(1)$ is true.
- Inductive step:
  - Show that the implication $P(n) \rightarrow P(n+1)$ is true for all natural numbers $n$.

## Intuition:

- Need to show that $P(n+1)$ can't be false when $P(n)$ is true.
- Assume $P(n)$ and use this to show $P(n+1)$.

# The Principle of Induction

## Intuition:

- Need to show that P(n+1) can't be false when P(n) is true.
- Assume P(n) and use this to show P(n+1).
- Note, we don't assume that P(n) is true for all n.
- We only demonstrate that

  **if** we assume P(n) is true,

  **then** P(n+1) is also true.

# Structure of an inductive proof

- Show that the statement holds for $n=1$, i.e. prove $P(1)$.
- Assume the statement is true for $n=k$, with $k \geq 1$.
  - Note, this is simply a syntactic replacement of $n$ with $k$ in $P(n)$.
- Prove that if $P(k)$ is true, then $P(k+1)$ is true.
- This establishes $P(n)$ for all $n$.

# Loop Invariant Proofs

- Loop invariants help us understand why an algorithm is correct.
- To prove a **loop invariant** we must show:
  - **Initialization:** It is true prior to the first loop iteration.
  - **Maintenance:** If it is true before an iteration of the loop, then it remains true before the next iteration.
  - **Termination:** When the loop terminates, the invariant establishes a property that helps us see that the algorithm is correct.
- Note, this is similar to Mathematical Induction!

# Summary

- Principle of mathematical induction
- Loop invariant proofs