Proofs by Induction (Recap)

COMS10018 - Algorithms

Dr Christian Konrad

Proofs by Induction and Loop Invariants

Proofs by Induction

- Correctness of an algorithm often requires proving that a property holds throughout the algorithm (e.g. loop invariant)
- This is often done by induction
- We will use proofs by induction for proving loop invariants (soon) and for solving recurrences (later)

Proofs by Induction

Structure of a Proof by Induction

1. **Statement to Prove:**
   $P(n)$ holds for all $n \in \mathbb{N}$
   (or $n \in \mathbb{N} \cup \{0\}$)
   (or n integer and $n \geq k$)
   (or similar)

2. **Induction hypothesis:**
   Assume that $P(n)$ holds
3. **Induction step:**
   Prove that $P(n+1)$ also holds
   If domino n falls then domino $n+1$ falls as well

4. **Base case:** Prove that $P(1)$ holds
   Domino 1 falls

Structure of a Proof by Induction

- **Statement to prove:** For example, for all $n \geq k$ $P(n)$ is true

$$\forall n \geq 0 \ : \ \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \ .$$

- **Base case:** Prove that $P(k)$ holds

$$n = 0 \ : \ \sum_{i=0}^{0} i = 0 = \frac{0 \cdot (0+1)}{2} \ . \checkmark$$

- **Induction hypothesis:** Assume that P holds for some n (Strong induction: for all m with $k \leq m \leq n$)
- **Induction step:** Prove that $P(n+1)$ holds

$$\sum_{i=0}^{n+1} i = n+1+\sum_{i=0}^{n} i = n+1+\frac{n(n+1)}{2} = \frac{(n+1)(n+2)}{2} \ . \checkmark$$

Geometric Series

Geometric Series: Let n be an integer and let $x \neq 1$. Then:

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

Proof. (by induction on n)

- *Base case.* $(n = 0)$
  $\sum_{i=0}^{0} x^i = x^0 = 1$ and $\frac{x^{n+1}-1}{x-1} = \frac{x-1}{x-1} = 1$. ✓
- *Induction Step.* Suppose the formula holds for n. We will prove that it also holds for $n + 1$:

$$\begin{aligned} \sum_{i=0}^{n+1} x^i &= x^{n+1} + \sum_{i=0}^{n} x^i = x^{n+1} + \frac{x^{n+1} - 1}{x - 1} \\ &= \frac{x^{n+1}(x-1) + x^{n+1} - 1}{x - 1} = \frac{x^{n+2} - 1}{x - 1} . \checkmark \end{aligned}$$

□

Spot the Flaw

Example: $a^n = 1$, for every $a \neq 0$ and n nonnegative integer

1. Base case ($n = 0$): $a^0 = 1$
2. Induction hypothesis: $a^m = 1$, for every $0 \leq m \leq n$ (strong induction)
3. Induction step:

$$a^{n+1} = a^{2n-(n-1)} = \frac{a^{2n}}{a^{n-1}} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1 \ldots .$$

Problem: a^1 is computed as $\frac{a^0 a^0}{a^{-1}}$ and induction hypothesis does not holds for $n = -1$!