Outline: Inductive mathematical proofs

- Three basic steps in induction
- First principle of mathematical induction
- Second principle of mathematical induction
- **Text book Section 2.2**

Mathematical Induction

- Telling secrets example
  - Suppose a “good” secret-keeper only tells one person who didn’t previously know….
  - What happens if every one is good at keeping secrets?
- Conclusion above holds no matter how many people there are.

Mathematical Induction

Mathematical induction is a particularly useful proof technique in computer science. It is used to prove some property true about all the integers greater than or equal to some fixed value.

Let P(n) be some property.

First Principle of Induction: Suppose we want to prove $\forall n$ P(n).

1. Prove P(1) — *Base case*
2. For arbitrary k ≥ 1,
   Assuming P(k), — *Inductive hypothesis*
   Prove P(k+1) — Inductive step

(Step 2 proves $(\forall x)P(x) \rightarrow P(x+1)$)

More on Mathematical Induction

- You are not assuming the conclusion.
  - Goal is a universal formula
    - but what is assumed is an instance…
- Base case can vary.
  - If P(5), then you have shown $\forall n \geq 5$, P(n)

Proof Technique using Mathematical Induction

- **Step A:** (Base Case) Prove that property P holds for 1 (or whatever the base value is).
- **Step B:** (Inductive Assumption or Hypothesis) Assume property P holds for n = k, where k $\geq$ base case.
- **Step C:** (Inductive Step) On the basis of this assumption, prove that property P holds for n = k + 1.

Example #1

- Prove that:

1 + 2 + 3 + … + n = n(n+1)/2

Example #2

- Prove that:

$2^n > n^2$ for $n \geq$???

Second Principle of Mathematical Induction

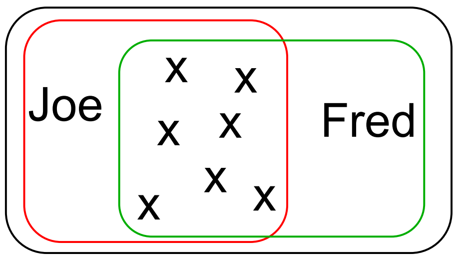
- In order to prove P(n) is true for all n≥1
  1. Prove P(1)
  2. For arbitrary k≥1, assuming *P(r) is true for 1≤r≤k*,
     Prove P(*k*+1)

Stronger than assuming just P(k)

- Example: Prove that any postage ≥ ??? cents can be created by a combination of 3 cents and 5 cents stamps.

Mathematical Induction: Fallacy

- Are all horses the same color?
- $(\forall n \geq 1)$ P(n), where
  - P(n) $\equiv$ Any group of *n* horses is all the same color.
- Base case: P(1) is true, any group of one horse is all the same color. (clearly true).
- Inductive case: Suppose P(k) = any group of k horses is all the same color.



- Black group has k+1 horses
- Red and Green groups have k horses, and so by I.H. are all the same color.
- $\therefore$ Black group is all same color

- Fallacy: we assumed k > 1, implicitly, but cannot