CS 441: Proof by induction

PhD. Nils Murrugarra-Llerena
nem177@pitt.edu
University of Pittsburgh

[Motivation] Proof by Induction

💻 The Problem: Proving a Recursive Function is Correct

Consider a recursive function to compute the factorial of a non-negative integer n.

```
function factorial(n):
  if n == 0:
    return 1
  else:
    return n * factorial(n - 1)
```

How can we be certain that this function is correct for *every* non-negative integer? We can't test it on every possible number. This is where induction comes in.

Today's topics

- Proof By Induction
- Examples
  - Equations
  - Inequalities
  - Sets

We've learned a lot of proof methods…

Basic proof methods

- Direct proof, contradiction, contraposition, cases, …

Proof of quantified statements

- Existential statements (i.e., ∃x P(x))
  - Finding a single example suffices
- Universal statements (i.e., ∀x P(x)) can be harder to prove
  - $$\sum_{j=0}^{n} ar^j = \begin{cases} \frac{ar^{n+1}-a}{r-1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r = 1 \end{cases}$$
  - $$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

Bottom line: We need new tools!

Mathematical induction lets us prove universally quantified statements!

Goal: Prove $\forall x \in \mathbf{N}\ P(x)$.

Intuition: If P(0) is true, then P(1) is true. If P(1) is true, then P(2) is true…

Procedure:

1. Prove $P(0)$
2. Show that $P(k) \rightarrow P(k+1)$ for any arbitrary k
3. Conclude that $P(x)$ is true $\forall x \in \mathbf{N}$

$$\begin{array}{l} P(0) \\ \text{For arb. } k,\ P(k) \rightarrow P(k+1) \\ \hline \therefore \forall x \in \mathbf{N}\ P(x) \end{array}$$

Analogy: Climbing a ladder

Proving P(0):

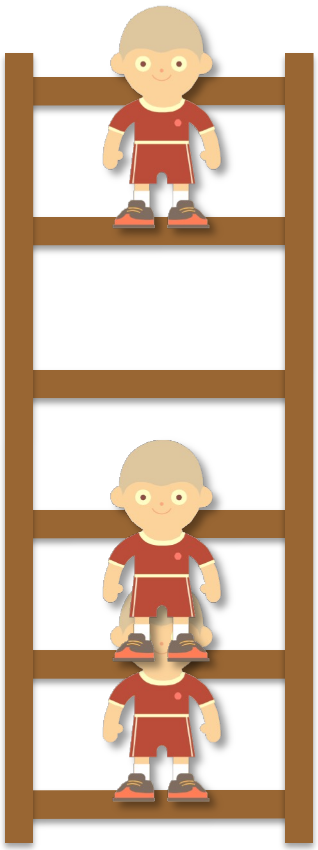
- You can get on the first rung of the ladder

Proving P(k) → P(k+1):

- If you are on the kth step, you can get to the (k+1)th step

∴ ∀x P(x)

- You can get to any step on the ladder



Analogy: Playing with dominoes

Proving P(0):

- The first domino falls

Proving P(k) → P(k+1):

- If the kth domino falls, then the (k+1)th domino will fall

∴ ∀x P(x)

- All dominoes will fall!

All of your proofs should have the same overall structure

$P(x) \equiv$	***Define the property that you are trying to prove***
Base case:	***Prove the "first step onto the ladder." Typically, but not always, this means proving P(0) or P(1).***
Inductive Hypothesis:	***Assume that P(k) is true for an arbitrary k***
Inductive step:	***Show that P(k) → P(k + 1). That is, prove that once you're on one step, you can get to the next step. This is where many proofs will differ from one another.***
Conclusion:	***Since you've proven the base case and P(k) → P(k + 1), the claim is true!*** ❑

Prove that $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

P(n) ≡	$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$
Base case:	P(1): 1(1+1)/2 = 1 ✔
I.H.:	Assume that P(k) holds for an arbitrary positive integer k
Inductive step:	We will now show that P(k) → P(k+1)

- 1+2+…+k = k(k+1)/2 — by I.H.
- 1+2+…+k+(k+1) = k(k+1)/2 + (k+1) — k+1 to both sides
- 1+2+…+k+(k+1) = k(k+1)/2 + 2(k+1)/2
- 1+2+…+k+(k+1) = (k^2 + 3k + 2)/2
- 1+2+…+k+(k+1) = (k+1)(k+2)/2 — factoring

Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{Z}^+(P(n))$ by mathematical induction ❑

Induction cannot give us a formula to prove, but can allow us to verify conjectures

Mathematical induction is not a tool for discovering new theorems, but rather a powerful way to prove them

Example: Make a conjecture about the sum of the first n odd positive numbers, then prove it.

- 1 = 1
- 1 + 3 = 4
- 1 + 3 + 5 = 9
- 1 + 3 + 5 + 7 = 16
- 1 + 3 + 5 + 7 + 9 = 25

The sequence 1, 4, 9, 16, 25, … appears to be the sequence $\{n^2\}$

Conjecture: The sum of the first n odd positive integers is n^2

Prove that the sum of the first n positive odd integers is n^2

$P(n) \equiv$ The sum of the first n positive odd numbers is n^2
Base case: $P(1)$: $1 = 1$ ✔
I.H.: Assume that $P(k)$ holds for an arbitrary positive integer k
Inductive step: We will now show that $P(k) \rightarrow P(k+1)$ • $1+3+\ldots+(2k-1) = k^2$ — by I.H. • $1+3+\ldots+(2k-1)+(2k+1) = k^2+2k+1$ — 2k+1 to both sides • $1+3+\ldots+(2k-1)+(2k+1) = (k+1)^2$ — factoring ***Note: The kth odd integer is 2k-1, the (k+1)th odd integer is 2k+1***
Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{Z}^+ \big(P(n)\big)$ by mathematical induction ❑

Prove that the sum $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n

P(n) ≡ $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Base case: P(0): $2^0 = 1$ ✔

I.H.: Assume that P(k) holds for an arbitrary natural number k

Inductive step: We will now show that P(k) → P(k+1)

- $1+2+\ldots+2^k = 2^{k+1}-1$ — by I.H.
- $1+2+\ldots+2^k+2^{k+1} = 2^{k+1}-1+2^{k+1}$ — 2^{k+1} to both sides
- $1+2+\ldots+2^k+2^{k+1} = 2^{k+1}+2^{k+1}-1$ — associative law
- $1+2+\ldots+2^k+2^{k+1} = 2\times2^{k+1}-1$ — def'n of ×
- $1+2+\ldots+2^k+2^{k+1} = 2^{k+2}-1$ — def'n of exp.

Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{N}(P(n))$ by mathematical induction ❏

Why does mathematical induction work?

This follows from the well ordering axiom

- i.e., Every set of positive integers has a least element

We can prove that mathematical induction is valid using a proof by contradiction.

- Assume that $P(1)$ holds and $P(k) \rightarrow P(k+1)$, but $\neg\forall x\, P(x)$
- This means that the set $S = \{x \mid \neg P(x)\}$ is nonempty
- By well ordering, S has a least element m with $\neg P(m)$
- Since m is the least element of S, $P(m-1)$ is true
- By $P(k) \rightarrow P(k+1)$, $P(m-1) \rightarrow P(m)$
- Since we have $P(m) \wedge \neg P(m)$ this is a contradiction!

Result: Mathematical induction is a valid proof method

In-class Activities

Activity 1: Prove that $$\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1} \text{ if } r \neq 1$$ [miro]

Activity 2: Prove that $$\sum_{j=1}^{n} (3j - 2) = \frac{n(3n - 1)}{2}$$ [miro]

Hint: Be sure to

1. Define P(x)
2. Prove the base case
3. Make an inductive hypothesis
4. Carry out the inductive step
5. Draw the final conclusion

Steps:

1. Introduce to a classmate
2. Work in pairs on the exercise
3. Submit answers on miro
4. Volunteers to share answers

Prove the formula for the sum of the first n positive squares

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

Base case: P(1): $1^2 = \frac{1(1+1)(2+1)}{6}$ ✔

I.H.: Assume that P(k) holds for an arbitrary positive integer k

Inductive step: We will now show that P(k) → P(k+1)

- $1+4+9+\ldots+k^2 = k(k+1)(2k+1)/6$ by I.H.
- $1+4+9+\ldots+(k+1)^2 = k(k+1)(2k+1)/6 + (k+1)^2$ $(k+1)^2$ to both sides
- $= k(k+1)(2k+1)/6 + 6(k+1)^2/6$ common denom.
- $= (k+1)(2k^2+k+6k+6)/6 = (k+1)(2k^2+7k+6)/6$ factor k+1, mult.
- $= (k+1)(k+2)(2k+3)/6$ factor
- $= (k+1)((k+1)+1)(2(k+1)+1)/6$, ∴P(k+1) proved for k+1

Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{Z}^+ \big(P(n)\big)$ by mathematical induction ❑

Induction can also be used to prove properties other than summations!

$\geq$ $<$

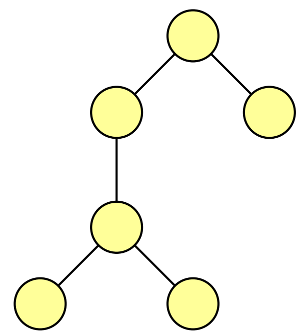
Inequalities

$|$ $\equiv$ $\varphi(p)$

Divisibility and results from number theory

$\subseteq$ $\in$ $\cup$

Set theory



Algorithms and data structures

Prove that $2^n < n!$ for every positive integer $n \geq 4$

Prelude: The expression n! is called the factorial of n.

Definition: $n! = n \times (n-1) \times \ldots \times 3 \times 2 \times 1$

Note how quickly the factorial of n "grows"

Examples:

- $4! = 4 \times 3 \times 2 \times 1 = 24$
- $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$
- $6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$
- $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5{,}040$
- $8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 40{,}320$

Prove that $2^n < n!$ for every positive integer $n \geq 4$

$P(n) \equiv 2^n < n!$

Base case: $P(4)$: $2^4 < 4!$ ✔

I.H.: Assume that $P(k)$ holds for an arbitrary integer $k \geq 4$

Inductive step: We will now show that $P(k) \rightarrow P(k+1)$

$2^k < k!$	by I.H.
$2 \times 2^k < 2 \times k!$	multiply by 2
$2^{k+1} < 2 \times k!$	def'n of exp.
$2^{k+1} < (k+1) \times k!$	since $2 < (k+1)$
$2^{k+1} < (k+1)!$	def'n of factorial

Conclusion: Since we have proved the base case and the inductive case, $\forall n \geq 4\big(P(n)\big)$ by mathematical induction ❑

Prove that $n^3 - n$ is divisible by 3 whenever n is a positive integer

$P(n) \equiv 3 \mid (n^3 - n)$
Base case: $P(1): 3 \mid 0$ ✔
I.H.: Assume that P(k) holds for an arbitrary positive integer k
Inductive step: We will now show that $P(k) \rightarrow P(k+1)$ • $(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - (k+1)$ • $= k^3 + 3k^2 + 2k$ • $= (k^3 - k) + (3k^2 + 3k)$ • $= (k^3 - k) + 3(k^2 + k)$ • Note that $3 \mid (k^3 - k)$ by the I.H. and $3 \mid 3(k^2 + k)$ by definition, so $3 \mid [(k+1)^3 - (k+1)]$
Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{Z}^+ \big(P(n)\big)$ by mathematical induction ❑

In-class Activities

Activity 3: Prove that $n^3 + 2n$ is divisible by 3 for any positive integer n [miro]

Activity 4: Prove that $6^n - 1$ is divisible by 5 for any positive integer n [miro]

Hint: Be sure to

1. Define P(x)
2. Prove the base case
3. Make an inductive hypothesis
4. Carry out the inductive step
5. Draw the final conclusion

Steps:

1. Introduce to a classmate
2. Work in pairs on the exercise
3. Submit answers on miro
4. Volunteers to share answers

Final Thoughts

- Mathematical induction lets us prove universally quantified statements using this inference rule:

$$\begin{array}{l} P(0) \\ \text{For arb. } k,\ P(k) \rightarrow P(k+1) \\ \hline \therefore \forall x \in \mathbf{N}\ P(x) \end{array}$$

- Induction is useful for proving:
  - Summations
  - Inequalities
  - Claims about countable sets
  - Theorems from number theory
  - …

Extra

Prove that if S is a finite set with n elements, then S has 2^n subsets.

$P(n) \equiv$ Set S with cardinality n has 2^n subsets

Base case: P(0): $\emptyset$ has $2^0 = 1$ subsets (i.e., $\emptyset \subseteq \emptyset$) ✔

I.H.: Assume that P(k) holds for an arbitrary natural number k

Inductive step: We will now show that $P(k) \rightarrow P(k+1)$

- Let S be a set of size k
- Assume without loss of generality that $x \notin S$
- Let $T = S \cup \{x\}$, so $|T| = k+1$
- $\forall s \subseteq S\ (s \subseteq T)$ since T is a superset of S
- Furthermore, $\forall s \subseteq S\ (s \cup \{x\} \subseteq T)$ since $x \in T$
- Since S has 2^k subsets by the I.H., T has $2 \times 2^k = 2^{k+1}$ subsets

Conclusion: Since we have proved the base case and the inductive case, $\forall n \in \mathbf{N}(P(n))$ by mathematical induction ❑