COSC 290 Discrete Structures

Lecture 14: Proof by induction

Prof. Michael Hay
Friday, Sep. 29, 2017
Colgate University

Plan for today

1. Proof by induction
2. Example: exact change theorem
3. Example application: analyzing algorithms

Proof by induction

Proof by induction

Suppose you want to prove that predicate $P(n)$ holds for all $n \in \mathbb{Z}^{\geq 0}$.

$P(n)$ is some statement that is "parameterized" by an integer n.

Examples: n could represent...

- the size of an array
- the n^{th} iteration through a loop
- the height of a binary tree
- the number of variables in a proposition
- etc.

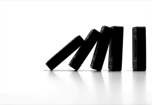
Procedure for proof by induction

Claim: $\forall n \in \mathbb{Z}^{\geq 0} : P(n)$

Process:

1. Base case: show that $P(0)$ is true.
2. Inductive case: show that $\forall n \in \mathbb{Z}^{\geq 1} : P(n-1) \implies P(n)$
   - Typically shown using direct proof by *assuming the antecedent*.
   - **Assume**: $P(n-1)$ is true.
   - **Show**: $P(n)$ must also be true.

Intuition



(a) Base case: show first one falls

(b) Inductive case: show this can't happen

Show that the first domino falls and if the $(n-1)^{th}$ domino falls, the n^{th} domino falls too.

Starting point

You don't always have to start at zero.

Suppose $P(n)$ only holds for $n \geq 3$.

- Base case: show $P(3)$ is true.
- Inductive case: Show $\forall n \geq 4 : P(n-1) \implies P(n)$ is true.

Proof by Induction Template

- **Claim**: [State claim: "$\forall n \in \mathbb{Z}^{\geq 0} : P(n)$ is true."]
- **Proof by induction**:
  - **Base case** ($n = 0$)**:** [Prove that $P(0)$]
    - Usually the base case is easy.
  - **Inductive case** ($n \geq 1$)**:** [Show that $P(n-1) \implies P(n)$]
    - **Assume:** $P(n-1)$ is true. [Write out what $P(n-1)$ is in full!]
    - **Want to show:** $P(n)$ is true.
    - Prove the inductive case: "Suppose that [$P(n-1)$ is true]... "
    - *... body of proof for inductive case...*
    - "... therefore the inductive step holds."
  - **Conclusion:** "By induction, the claim has been shown."

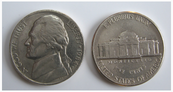
Proof by Induction (Alternative) Template

- **Claim**: [State claim: "$\forall n \in \mathbb{Z}^{\geq 0} : P(n)$ is true."]
- **Proof by induction**:
  - **Base case** ($n = 0$): [Prove that $P(0)$]
    - Usually the base case is easy.
  - **Inductive case** ($n \geq 0$): [Show that $P(n) \implies P(n+1)$]
    - **Assume:** $P(n)$ is true. [Write out what $P(n)$ is in full!]
    - **Want to show:** $P(n+1)$ is true.
    - Prove the inductive case: "Suppose that [$P(n)$ is true]... "
    - ... *body of proof for inductive case...*
    - "... therefore the inductive step holds."
  - **Conclusion:** "By induction, the claim has been shown."

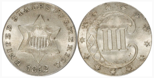
Example: exact change theorem

Exact Change Theorem

- **Claim**: For any price $n \geq 8$, the price n can be paid using only 5-cent coins and 3-cent coins.



(a) A five cent piece (nickel)



(b) A three cent piece (circa 1865-1873)

Poll: base case

- **Claim**: For any price $n \geq 8$, the price n can be paid using only 5-cent coins and 3-cent coins.
- **Proof by induction**:
  - **Base case:** Show the claim holds for $n = ??$

A) 0 cents
B) 1 cent
C) 2 cents
D) 3 cents
E) None of the above / More than one

Poll: inductive case

- **Claim**: For any price $n \geq 8$, the price n can be paid using only 5-cent coins and 3-cent coins.
- **Proof by induction**:
  - **Base case:** Show the claim holds for $n = 8$
  - **Inductive case:**
    - **Assume:** Assume that ... what goes here?
    - **Want to show:** We will show that ... and here?

A) ...the claim is true for $n = 8$... the claim holds for $n = 9$.

B) ...the claim is true for all $n \geq 8$... the claim holds for n.

C) ...the claim is true for all $n > 8$... the claim holds for $n + 1$.

D) ...the claim is true for n where $n \geq 8$... the claim holds for $n + 1$.

E) ...the claim is true for n where $n > 8$... the claim holds for $n + 1$.

Inductive step

Assume that when price is n, we can make change using only three-cent and five-cent coins.

Show that this implies you can make change for price $n + 1$.

Poll: making change

Suppose you used $k = 10$ five-cent coins and $\ell = 10$ three-cent coins to pay the price of $n = \$0.80$. What is the *smallest* amount by which we must change k and ℓ to pay the price $n + 1 = \$0.81$?

A) $k = 0$ five-cent coins and $\ell = 27$ three-cent coins.

B) $k = 9$ five-cent coins and $\ell = 12$ three-cent coins.

C) $m = 12$ five-cent coins and $\ell = 7$ three-cent coins.

D) None of the above / More than one

Poll: a generic algorithm

Suppose you used k five-cent coins and ℓ three-cent coins to pay the price of $n = 5k + 3\ell$. How can we modify the number of coins so that we can pay the price $n + 1$?

You ask a student who took 290 last spring, they suggest the following approach: use $k - 1$ five-cent coins and $\ell + 2$ three-cent coins. Will this work?

A) Yes, I think this always works.

B) Hmm... I'm not convinced it always works but I don't see a specific problem.

C) It won't always work and I know why.

Poll: without a nickel to your name

Suppose you used $k = 0$ five-cent coins and ℓ three-cent coins to pay the price of $n = 5k + 3\ell = 0 + 3\ell$. How can we modify the number of coins so that we can pay the price $n + 1$?

You ask a student who took 290 last spring, and they say you can't.

A) The student is right. [Explain why during discussion.]
B) Hmm... I'm not convinced either way.
C) The student is wrong. [Explain why during discussion.]

Poll: three is the magic number

If you used $k = 0$ five-cent coins and ℓ three-cent coins to pay the price of $n = 5k + 3\ell$, you can pay price $n + 1$ provided that $\ell \geq 3$.

Student A asks: "What if we don't have that many three-cent coins?"

Student B says: "Don't worry about it, just pay with your 'Gate Card."

Choose the best answer:

A) Darn... student A just ruined our proof.
B) Student B is kinda right: we don't need to worry because this situation can never happen.
C) Student A raises a good point, we need to add this case to our proof.
D) None of the above / More than one

Final proof

Proof by induction:

- **Base case:** Show the claim holds for $n = 8$
  - One five-cent coin and one three-cent coin does it.
- **Inductive case:**
  - **Assume:** Assume that the claim holds for some $n \geq 8$. That is, there is some k and ℓ such that $n = 5k + 3\ell$.
  - **Want to show:** We will show that the claim holds for $n + 1$.
  - Cases:
    - $k > 0$: Then $n + 1 = 5(k - 1)$ and $3(\ell + 2)$
    - $k = 0$ and $\ell \geq 3$: Then $n + 1 = 5(k + 2)$ and $3(\ell - 3)$
    - $k = 0$ and $\ell < 3$: Then $n = 3\ell < 8$, which contradictions our assumption that $n \geq 8$.
  - Therefore, the inductive step holds.

Example application: analyzing algorithms

An algorithm for making change

Input: An integer $n \geq 8$
Output: Integers k, ℓ such that $m = 5k + 3\ell$

Let $m = 8$ and $k = 1$ and $\ell = 1$ ▷ Thus, $m = 5k + 3\ell$
while $m < n$ **do**
  ▷ Invariant: before loop body $m = 5k + 3\ell$
  $m = m + 1$
  if $k \geq 1$ **then**
    $k = k - 1$ and $\ell = \ell + 2$
  else
    $k = k + 2$ and $\ell = \ell - 3$
  ▷ Invariant: after loop body $m = 5k + 3\ell$
return k, ℓ

Our proof implies that $k \geq 0$ and $\ell \geq 0$ throughout this algorithm. This is not obvious looking at the code.

Exercise: work in small groups

Prove that the algorithm uses at most two nickels. In other words, for any input n, the algorithm never sets $k > 2$ at any point during the execution of the algorithm. (Hint: do induction on the number of times thru the loop.)

Input: An integer $n \geq 8$
Output: Integers k, ℓ such that $n = 5k + 3\ell$

Let $m = 8$ and $k = 1$ and $\ell = 1$ ▷ Thus, $m = 5k + 3\ell$
while $m < n$ **do**
  $m = m + 1$
  if $k \geq 1$ **then**
    $k = k - 1$ and $\ell = \ell + 2$
  else
    $k = k + 2$ and $\ell = \ell - 3$
return k, ℓ

Proof of claim that $k \leq 2$

Proof by induction: We will use proof by induction on the number of times through the loop.

- **Base case (0 iterations):**
  - Before the loop, $k = 1 \leq 2$.
- **Inductive case (t iterations):**
  - **Assume:** We will assume that after t times through the loop, the claim holds. Thus, $k \leq 2$ at the start of the $(t+1)^{th}$ iteration.
  - **Want to show:** We will show $k \leq 2$ at the end of the $(t+1)^{th}$ iteration.
  - Cases:
    1. $k \in \{1, 2\}$, then $k = k - 1$, so now $k \in \{0, 1\}$.
    2. $k = 0$, then $k = k + 2$, so k is now 2.
  - Therefore at the end of the $(t+1)^{th}$ iteration, $k \leq 2$.
- **Conclusion:** By induction, the claim has been shown.