More on Mathematical Induction

COMPSCI 230 — Discrete Math

March 9, 2017
More on Mathematical Induction

1. Solomon Golomb’s Tromino Problem
2. Induction Pitfalls
3. Mathematical Induction and Recursion
4. Strong Mathematical Induction
Mathematical Induction

• Used to prove predicates of the form

\[ \forall n \in \mathbb{Z} : n \geq a \rightarrow P(n) \]

• Inference rule: Let \( b \) be an integer with \( b \geq a \).

<table>
<thead>
<tr>
<th>Base case(s)</th>
<th>( P(a) \land \ldots \land P(b) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inductive step</td>
<td>( \forall k \in \mathbb{Z} : ((k \geq b) \land P(k)) \rightarrow P(k + 1) )</td>
</tr>
<tr>
<td>Conclusion</td>
<td>( \forall n \in \mathbb{Z} : n \geq a \rightarrow P(n) )</td>
</tr>
</tbody>
</table>
Solomon Golomb’s Tromino Problem

- Remove a single cell (black or white) from a regular $2^n \times 2^n$ chessboard

- We can always tile it with trominos

- Proof by induction

- Base case $n = 1$: Check four possibilities, depending on location of missing cell
Solomon Golomb’s Tromino Problem

• Inductive step: Consider a $2^{k+1} \times 2^{k+1}$ board

• Assume w.l.o.g. that missing tile is in upper left quarter

• Inductive assumption: A $2^k \times 2^k$ board with one cell missing can be tiled

• Big idea: Place one tromino as shown

• Each quarter is $2^{k-1} \times 2^{k-1}$ and misses one cell so it can be tiled (by the inductive assumption)

• Done!
All Horses are the Same Color

- \( P(n) \): The horses in any group of \( n \) horses are all the same color
- Prove by induction that \( \forall n : n \geq 1 \rightarrow P(n) \)
- Base case \( P(1) \): A horse is the same color as itself, so \( P(1) \) is true
- Inductive step \( P(k) \rightarrow P(k + 1) \):
  - Make the inductive hypothesis that \( P(k) \) is true so all horses in any group of \( k \) are the same color
  - Number the horses in a new group of \( k + 1 \) horses from 1 to \( k + 1 \)
  - Because of \( P(k) \), horses 1 through \( k \) are the same color
  - For the same reason, horses 2 through \( k + 1 \) are the same color
  - The middle horses, between 2 and \( k \), do not change color if they are in different groups
  - By transitivity, horse 1 and horse \( k + 1 \) are the same color: Horse 1 color = any middle horse color = horse \( k + 1 \) color
- Are all horses the same color? If not, where is the flaw?
Observations

• The inductive step works for all $k > 1$ but not for $k = 1$
• Set of horses for $k + 1 = 2$ is $\{1, 2\}$
• There are no “middle horses” (between 2 and $k$, that is, between 2 and 1)
• Make sure that the inductive step proof is general
• It must hold for every $k \geq b$, not just for most of them
Mathematical Induction and Recursion

- There is an intimate connection between
  - recursively defined objects
  - and proving properties about them by induction
- Example: Prove that Russian Peasant Multiplication (RPM) computes the product of any integer $i$ with a nonnegative integer $j$
- FDM 3.7.1 does it based on iteration
- Iteration complicates the analysis
- Recursive thinking elucidates the connection best
- A recursive variant on FDM 3.7.1
- FDM 3.7.1 is not required reading. These slides are
### Sample Run of RPM

<table>
<thead>
<tr>
<th>$i$</th>
<th>$j$</th>
<th>$p$</th>
<th>$i{2}$</th>
<th>$j{2}$</th>
<th>$p{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>5</td>
<td>0</td>
<td>1100</td>
<td>101</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>12</td>
<td>11000</td>
<td>10</td>
<td>1100</td>
</tr>
<tr>
<td>48</td>
<td>1</td>
<td>12</td>
<td>110000</td>
<td>1</td>
<td>1100</td>
</tr>
<tr>
<td>96</td>
<td>0</td>
<td>60</td>
<td>11000000</td>
<td>0</td>
<td>1111000</td>
</tr>
</tbody>
</table>

Observation: In each row, $ij + p = 60$
A Recursive Description of RPM

- We work with $i \in \mathbb{Z}$ and $j \in \mathbb{N}$ while keeping a running value for the product, initially zero
- $j$ is repeatedly divided by 2 to reveal its bits one at a time
- For each new bit in $j$, the value of $i$ is multiplied by 2
- Code structure:
  - If $j = 0$, we are done
  - Otherwise
    - If $j$ is odd, we add $i$ to the product, otherwise we leave the product as is
    - Either way, we apply RPM to twice $i$ and the integer division of $j$ by 2
Recursive Implementation of RPM

# RPM multiplies integer i by nonnegative integer j
# by keeping a running product, initially 0
def rpm(i, j, p = 0):
    assert type(i) is int and type(j) is int and j >= 0
    # If j = 0, we are done and return the product.
    if j == 0: return p
    # Otherwise, we return the result of calling rpm on
    else: return rpm(
        # twice i,
        2 * i,
        # the integer division of j by 2,
        j // 2,
        # and the product plus i if j is odd
        p + i if j % 2 \
        # or the product itself otherwise
        else p)
Remove the Comments

def rpm(i, j, p=0):
    assert type(i) is int and type(j) is int and j>=0
    if j==0: return p
    else: return rpm(2*i, j//2, p+i if j%2 else p)

Even more succinctly, and removing the assert statement just while we reason about the code:

def rpm(i, j, p=0):
    return p if j==0 else rpm(2*i, j//2, p+i if j%2 else p)
What we Prove

def rpm(i, j, p=0):
    return p if j==0 else rpm(2*i, j//2, p+i if j%2 else p)

• Suppose calling \( \text{rpm}(i_0, j_0) \).
• **Termination:** The argument \( j \) keeps shrinking and will hit 0
• **Correctness:** Prove that

\[
\forall n \geq 1 : I(n)
\]

where the predicate \( I(n) \) (an *invariant*) means

\[
i j + p = i_0 j_0 \quad \text{in the } n\text{-th recursive call}
\]

• Since \( \text{rpm} \) returns when \( j = 0 \), it returns \( p = i_0 j_0 \)
def rpm(i, j, p=0):
    return p if j==0 else rpm(2*i, j//2, p+i if j%2 else p)

• Suppose calling \( \text{rpm}(i_0, j_0) \). Prove that

\[ \forall n \geq 1 : I(n) \]

where \( I(n) \) means that \( ij + p = i_0j_0 \) in the \( n \)-th recursive call

• Base case \( I(1) \): Initially, \( i = i_0, j = j_0, \) and \( p = 0 \), so

\[ ij + p = i_0j_0 + 0 = i_0j_0 \]

(notice that we do not know what \( i_0j_0 \) is!)
Inductive Step

```python
def rpm(i, j, p=0):
    return p if j==0 else rpm(2*i, j//2, p+i if j%2 else p)
```

- $I(n)$ means that $ij + p = i_0j_0$ in the $n$-th recursive call
- **Inductive step:** $I(k) \rightarrow I(k+1)$
- **Inductive assumption:** $I(k)$ holds: $ij + p = i_0j_0$ in the $k$-th call
- What are the values $i', j', p'$ of $i, j, p$ in the $k + 1$st call?

\[
\begin{align*}
i' & = 2i \\
j' & = \begin{cases} 
\frac{j-1}{2} & \text{if } j \text{ is odd} \\
\frac{j}{2} & \text{otherwise}
\end{cases} \\
p' & = \begin{cases} 
p + i & \text{if } j \text{ is odd} \\
p & \text{otherwise}
\end{cases}
\end{align*}
\]

- So

\[
\begin{align*}
i'j' + p' & = \begin{cases} 
2i \frac{j-1}{2} + p + i & \text{if } j \text{ is odd} \\
2i \frac{j}{2} + p & \text{otherwise}
\end{cases} \\
& = ij + p = i_0j_0
\end{align*}
\]

(last equality by the inductive assumption)

- So $I(k + 1)$ holds: $ij + p = i_0j_0$ in the $k + 1$-st call
- **Done!** $rpm$ is correct
Strong Mathematical Induction

• Still prove $\forall n \geq a \ P(n)$

• Same base case: $P(a) \land \ldots \land P(b)$

• Inductive step of weak mathematical induction: $P(k) \rightarrow P(k + 1)$

• Inductive step of strong mathematical induction: $[P(a) \land \ldots \land P(k)] \rightarrow P(k + 1)$

• Used when the inductive assumption needs to be stronger in order to conclude $P(k + 1)$

• Proof of validity:
  • Let $Q(n)$ be the predicate $P(a) \land \ldots \land P(n)$
  • Use weak induction to prove $\forall n \geq a \ Q(n)$
  • (Weak) Inductive step $Q(k) \rightarrow Q(k + 1)$ now means $P(a) \land \ldots \land P(k) \rightarrow P(a) \land \ldots \land P(k + 1)$
  • ... and so in particular $P(a) \land \ldots \land P(k) \rightarrow P(k + 1)$
Strong Mathematical Induction

Multiple dominos contribute to toppling the next one
Football Example

• Assume that a football team can only score either 3 points (field goal) or 7 points (touchdown)
• Prove that (ignoring time constraints) it is mathematically possible for a team to score any number of points from 12 on up
Football

A football team can only score either 3 points (field goal) or 7 points (touchdown) in one possession.

“It is mathematically possible for a team to score any number of points from 12 on up.”

We want to formalize this statement as $\forall n \geq 12 : P(n)$

What is $P(n)$?

A: $\exists n : 3f + 7t = 12n$

B: $\forall n : 3f + 7t = 12n$

C: $\forall f \forall t : 3f + 7t = n$

D: $\exists f \exists t : 3f + 7t = n$

E: $\forall n \exists f \exists t : 3f + 7t = n$
Football Example

• Assume that a football team can only score either 3 points (field goal) or 7 points (touchdown)
• Prove that (ignoring time constraints) it is mathematically possible for a team to score any number of points from 12 on up
• \( \forall n \geq 12 \ \exists f \in \mathbb{N} \ \exists t \in \mathbb{N} : 3f + 7t = n \)
• Observation: cannot score 1, 2, 4, 5, 8, or 11 points
• Base cases: \( P(12) \land P(13) \land P(14) \)
• \( P(12) \): score four field goals (12)
• \( P(13) \): score two field goals (6) and a touchdown (7)
• \( P(14) \): score two touchdowns (14)
Strong Inductive Step

- Inductive assumption: $k \geq 14$ and $P(12) \land \ldots \land P(k)$
- Can the team then score $k + 1$ points with field goals and touchdowns?
- If we can score $k + 1 - 3$, then just add a field goal
- $k + 1 - 3 = k - 2$ is between 12 (because $k \geq 14$) and $k$
- So $P(k + 1 - 3)$ holds by the inductive assumption
- Add a field goal to score $k + 1$ points: $P(k + 1)$ holds
- Done!
Observations

• We had to reach back *three* values of $k$, not just one
• If $k + 1 - 3$ hadn’t worked, we could have tried $k + 1 - 7$
• Needed three base cases because we reach three values back:
  $P(12) \rightarrow P(15)$
  $P(13) \rightarrow P(16)$
  $P(14) \rightarrow P(17)$
  $P(15) \rightarrow P(18)$
  $\vdots$
Number Theory Example

• Every integer greater than 1 has a prime divisor
• \( \forall n \geq 2 \ \exists p \in \mathbb{N} : p \text{ is prime and } p|n \)
• Base case \( P(2) \): 2 is prime and 2|2
• **Strong** inductive assumption: \( k \geq 2 \) and every integer \( i \) with \( 2 \leq i \leq k \) has a prime divisor
• Inductive step: Does \( k + 1 \) then have a prime divisor?
  • Case 1: \( k + 1 \) is prime. \( P(k + 1) \) same reasoning as \( P(2) \)
  • Case 2: \( k + 1 = ab \) with \( a, b \in \mathbb{N} \) and \( 2 \leq a, b \leq k \)
  • So in particular \( P(a) \) holds: \( \exists \text{ prime } u \in \mathbb{N} : u|a \)
  • That is, \( a = uv \) for some prime \( u \) and integer \( v \)
  • So \( k + 1 = ab = uvb \) and \( u \) is a prime divisor of \( k + 1 \)
• Done!
Number Theory

\[
\binom{4 \mod 7}{7 \mod 4} = \ldots
\]

Pick one (Not Graded)

A: 0  
B: 3  
C: 4  
D: 12  
E: 24
Sets and Functions

Is $2^n$ a surjection from $\mathbb{N}$ to $\{k \in \mathbb{N} : 2|k\}$?

Pick one (Not Graded)

A: No
B: Yes
C: Depends on $k$
D: Not enough information
Combinatorics

When does the following equality hold?

\[(n)_k = n!\]

When...

<table>
<thead>
<tr>
<th></th>
<th>(Not Graded)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>never</td>
</tr>
<tr>
<td>B</td>
<td>( n &lt; k )</td>
</tr>
<tr>
<td>C</td>
<td>( n = k )</td>
</tr>
<tr>
<td>D</td>
<td>( (n)_k = \binom{n}{k} )</td>
</tr>
<tr>
<td>E</td>
<td>always</td>
</tr>
</tbody>
</table>
Combinatorics

How many anagrams are there for the word BANANA (I think all of them are meaningless)?

Pick one

<table>
<thead>
<tr>
<th>Option</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>$3 \binom{6}{3}$</td>
</tr>
<tr>
<td>B</td>
<td>$\binom{6}{1} \binom{6}{2} \binom{6}{3}$</td>
</tr>
<tr>
<td>C</td>
<td>$\binom{6}{1} \binom{6}{2} \binom{6}{3}$</td>
</tr>
<tr>
<td>D</td>
<td>$1! \cdot 2! \cdot 3!$</td>
</tr>
<tr>
<td>E</td>
<td>$\binom{6}{3} \cdot \binom{3}{2}$</td>
</tr>
</tbody>
</table>