Mathematical Induction II

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>15</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

Lecture 5: Sep 19
This Lecture

We will continue our discussions on mathematical induction.

The new elements in this lecture are some variants of induction:

• Strong induction
• Well Ordering Principle
• Invariant Method
Unstacking Game

- Start: a stack of boxes
- Move: split any stack into two stacks of sizes $a, b > 0$
- Scoring: $ab$ points
- Keep moving: until stuck
- Overall score: sum of move scores
What is the best way to play this game?

Suppose there are \( n \) boxes.

What is the score if we just take the box one at a time?

\[
\sum_{i=0}^{n-1} i = \frac{n(n - 1)}{2}
\]
What is the best way to play this game?

Suppose there are $n$ boxes.

What is the score if we cut the stack into half each time?

Say $n=8$, then the score is $1 \times 4 \times 4 + 2 \times 2 \times 2 + 4 \times 1 = 28$

Say $n=16$, then the score is $8 \times 8 + 2 \times 28 = 120$

Not better than the first strategy! $\frac{n(n - 1)}{2}$
**Unstacking Game**

*Claim:* Every way of unstacking gives the same score.

*Claim:* Starting with size $n$ stack, final score will be $\frac{n(n-1)}{2}$

*Proof:* by Induction with *Claim*($n$) as hypothesis

**Base case** $n = 0$: 

score $= 0 = \frac{0(0-1)}{2}$

*Claim*(0) is okay.
Unstacking Game

Inductive step. assume for $n$-stack,

and then prove $C(n+1)$:

$\text{(n+1)-stack score} = \frac{(n + 1)n}{2}$

Case $n+1 = 1$. verify for 1-stack:

score = 0 = $\frac{1(1 - 1)}{2}$

$C(1)$ is okay.
Unstacking Game

Case $n+1 > 1$. So split into an $a$-stack and $b$-stack, where $a + b = n + 1$.

$$(a + b)\text{-stack score} = ab + a\text{-stack score} + b\text{-stack score}$$

by induction:

$a$-stack score $= \frac{a(a - 1)}{2}$

$b$-stack score $= \frac{b(b - 1)}{2}$
Unstacking Game

\[(a + b)\text{-stack score} = ab + a\text{-stack score} + b\text{-stack score}\]

\[
ab + \frac{a(a - 1)}{2} + \frac{b(b - 1)}{2} = \]

\[
\frac{2ab + a^2 - a + b^2 - b}{2} = \frac{(a + b)^2 - (a + b)}{2} = \]

\[
\frac{(a + b)((a + b) - 1)}{2} = \frac{(n + 1)n}{2}
\]

so \(\mathcal{C}(n+1)\) is okay. We're done!
Induction Hypothesis

Wait: we assumed \( \mathcal{A}(a) \) and \( \mathcal{A}(b) \) where \( 1 \leq a, b \leq n \).

But by induction can only assume \( \mathcal{A}(n) \)

the fix: revise the induction hypothesis to

\[
\mathcal{Q}(n) := \forall m \leq n. \mathcal{C}(m)
\]

In words, it says that we assume the claim is true for all numbers up to \( n \).

Proof goes through fine using \( \mathcal{Q}(n) \) instead of \( \mathcal{A}(n) \).

So it's OK to assume \( \mathcal{A}(m) \) for all \( m \leq n \) to prove \( \mathcal{A}(n+1) \).
Proof by Strong Induction:

1. Prove $P(0)$.
2. Then prove $P(n+1)$ assuming all of $P(0), P(1), ..., P(n)$ (instead of just $P(n)$).
3. Conclude $\forall n. P(n)$.

Strong induction is equivalent to ordinary induction:

0 $\rightarrow$ 1, 1 $\rightarrow$ 2, 2 $\rightarrow$ 3, ..., $n-1$ $\rightarrow$ $n$.

So by the time we get to $n+1$, already know all of $P(0), P(1), ..., P(n)$.

The point is: assuming $P(0)$, $P(1)$, up to $P(n)$, it is often easier to prove $P(n+1)$. 
Divisibility by a Prime

**Theorem.** Any integer $n > 1$ is divisible by a prime number.

- Let $n$ be an integer.
- If $n$ is a prime number, then we are done.
- Otherwise, $n = ab$, both are smaller than $n$.
- If $a$ or $b$ is a prime number, then we are done.
- Otherwise, $a = cd$, both are smaller than $a$.
- If $c$ or $d$ is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we have found a prime factor of $n$. 

Remember this slide? Now we can prove it by strong induction very easily. In fact we can prove a stronger theorem very easily.
Theorem. Any integer $n > 1$ is divisible by a prime number.

**Theorem:** Every integer $> 1$ is a product of primes.

**Proof:** (by strong induction)

- Base case is easy.
- Suppose the claim is true for all $2 \leq i < n$.
- Consider an integer $n$.
- If $n$ is prime, then we are done.
- So $n = k \cdot m$ for integers $k, m$ where $n > k, m > 1$.
- Since $k, m$ smaller than $n$,
- _By the induction hypothesis, both $k$ and $m$ are product of primes_

\[
k = p_1 \cdot p_2 \cdot \ldots \cdot p_{94}
\]
\[
m = q_1 \cdot q_2 \cdot \ldots \cdot q_{214}
\]
Prime Products

*Theorem:* Every integer > 1 is a product of primes.

...So

\[ n = k \cdot m = p_1 \cdot p_2 \cdot \ldots \cdot p_{94} \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_{214} \]

is a prime product.

∴ This completes the proof of the induction step.
Postage by Strong Induction

Available stamps:

- 5¢
- 3¢

What amount can you form?

Theorem: Can form any amount \( \geq 8¢ \)

Prove by strong induction on \( n \).

\( P(n) ::= \text{can form } n¢. \)
Postage by Strong Induction

Base case \((n = 8)\):

\(8¢:\)

Inductive Step: assume \(m¢\) for \(8 \leq m < n\),
then prove \(n¢\)

cases:

\(n=9:\)

\(n=10:\)
Postage by Strong Induction

\textbf{case } n \geq 11: \text{ let } m = n - 3. \\\n
now \( n \geq m \geq 8 \), so by induction hypothesis have:

\[ n - 3 + 3 = n \]

\begin{itemize}
  \item We're done!
\end{itemize}

\begin{itemize}
  \item In fact, use at most two 5-cent stamps!
\end{itemize}
Postage by Strong Induction

Given an unlimited supply of 5 cent and 7 cent stamps, what postages are possible?

**Theorem:** For all $n \geq 24$,

it is possible to produce $n$ cents of postage from 5¢ and 7¢ stamps.
This Lecture

- Strong induction
- Well Ordering Principle
- Invariant Method
Well Ordering Principle

Axiom

Every nonempty set of nonnegative integers has a least element.

This is an axiom equivalent to the principle of mathematical induction.

Note that some similar looking statements are not true:

Every nonempty set of nonnegative rationals has a least element.  

Every nonempty set of nonnegative integers has a least element.
Well Ordering Principle

Thm: $\sqrt{2}$ is irrational

Proof: suppose $\sqrt{2} = \frac{m}{n}$

...can always find such $m, n$ without common factors...

why always?

By WOP, $\exists$ minimum $|m|$ s.t. $\sqrt{2} = \frac{m}{n}$.

so $\sqrt{2} = \frac{m_0}{n_0}$ where $|m_0|$ is minimum.
Well Ordering Principle

but if $m_0$, $n_0$ had common factor $c > 1$, then

$$\sqrt{2} = \frac{m_0 / c}{n_0 / c}$$

and $|m_0 / c| < |m_0|$ contradicting minimality of $|m_0|$

The well ordering principle is usually used in “proof by contradiction”.

• Assume the statement is not true, so there is a counterexample.

• *Choose the “smallest” counterexample, and find a even smaller counterexample.*

• Conclude that a counterexample does not exist.
Well Ordering Principle in Proofs

To prove \[ \forall n \in \mathbb{N}. P(n) \] using WOP:

1. Define the set of counterexamples
   \[ C ::= \{ n \in \mathbb{N} | \neg P(n) \} \]

2. Assume \( C \) is not empty.

3. By WOP, have minimum element \( m_0 \in C \).

4. Reach a contradiction (somehow) –
   usually by finding a member of \( C \) that is < \( m_0 \).

5. Conclude no counterexamples exist. QED
Non-Fermat Theorem

It is difficult to prove there is no positive integer solutions for

$$a^3 + b^3 = c^3$$  \hspace{1cm} \text{Fermat's theorem}

But it is easy to prove there is no positive integer solutions for

$$4a^3 + 2b^3 = c^3$$  \hspace{1cm} \text{Non-Fermat's theorem}

\textbf{Hint:} Prove by contradiction using well ordering principle...
Suppose, by contradiction, there are integer solutions to this equation.

By the well ordering principle, there is a solution with $|a|$ smallest.

In this solution, $a, b, c$ do not have a common factor.

Otherwise, if $a = a'k$, $b = b'k$, $c = c'k$,

then $a', b', c'$ is another solution with $|a'| < |a|$, contradicting the choice of $a, b, c$.

(*) There is a solution in which $a, b, c$ do not have a common factor.
On the other hand, we prove that every solution must have $a, b, c$ even. This will contradict (*), and complete the proof.

First, since $c^3$ is even, $c$ must be even. (because odd power is odd).

Let $c = 2c'$, then

$$4a^3 + 2b^3 = (2c')^3$$
$$4a^3 + 2b^3 = 8c'^3$$

$$b^3 = 4c'^3 - 2a^3$$
Non-Fermat Theorem

\[ b^3 = 4c'^3 - 2a^3 \]

Since \( b^3 \) is even, \( b \) must be even. (because odd power is odd).

Let \( b = 2b' \), then

\[ (2b')^3 = 4c'^3 - 2a^3 \]

\[ 8b'^3 = 4c'^3 - 2a^3 \]

\[ a^3 = 2c'^3 - 4b'^3 \]

Since \( a^3 \) is even, \( a \) must be even. (because odd power is odd).

There \( a, b, c \) are all even, contradicting (*)
This Lecture

- Strong induction
- Well Ordering Principle
- Invariant Method
A Chessboard Problem

A rook \( \text{.Insert rook image here} \) can only move along a diagonal.

Can a rook move from its current position to the question mark?
A Chessboard Problem

A rook \( \text{pawn} \) can only move along a diagonal

Can a rook move from its current position to the question mark?

Impossible!

Why?
A Chessboard Problem

1. The rook is in a red position.
2. A red position can only move to a red position by diagonal moves.
3. The question mark is in a white position.
4. So it is impossible for the rook to go there.

This is a simple example of the invariant method.
Domino Puzzle

An 8x8 chessboard, 32 pieces of dominos

Can we fill the chessboard?
Domino Puzzle

An 8x8 chessboard, 32 pieces of dominos

Easy!
Domino Puzzle

An 8x8 chessboard with two holes, 31 pieces of dominos

Can we fill the chessboard?

Easy??
Domino Puzzle

An 4x4 chessboard with two holes, 7 pieces of dominos

Can we fill the chessboard?

Impossible!
Domino Puzzle

An 8x8 chessboard with **two holes**, 31 pieces of dominos

*Can we fill the chessboard?*

Then what??
Domino Puzzle

An 8x8 chessboard with two holes, 31 pieces of dominos

Can we fill the chessboard?
Domino Puzzle

1. Each domino will occupy one white square and one red square.

2. There are 32 red squares but only 30 white squares.

3. So it is impossible to fill the chessboard using only 31 dominos.

This is another example of the invariant method.
Invariant Method

1. Find properties (the invariants) that are satisfied throughout the whole process (by induction).
2. Show that the target do not satisfy the properties.
3. Conclude that the target is not achievable.

In the rook example, the invariant is the colour of the position of the rook.

In the domino example, the invariant is that any placement of dominos will occupy the same number of red positions and white positions.

Very useful in analysis of algorithms.
Challenge (Optional)

Show that we can not move from the left state to the right state.

See the answer in L6 in 2009.
Quick Summary

Induction is perhaps the most important proof technique in computer science. For example it is very important in proving the correctness of an algorithm (by invariant method) and also analyzing the running time of an algorithm.

There is no particular example that you should remember.

The point here is to understand the principle of mathematical induction (the way that you “reduce” a large problem to smaller problems), and apply it to the new problems that you will encounter in future.

Possibly the only way to learn this is to do more exercises.