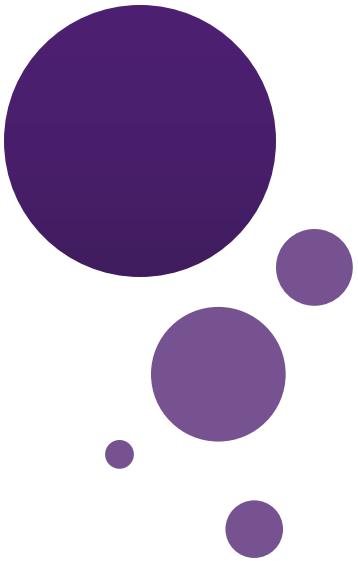
UNIVERSITY AT ALBANY

State University of New York



Lecture 22: Strong Induction and Well-Ordering

Dr. Chengjiang Long

Computer Vision Researcher at Kitware Inc.

Adjunct Professor at SUNY at Albany.

Email: **clong2@albany.edu**

Recap Previous Lecture

0 and (from n to $n+1$),

proves 0, 1, 2, 3,....

Much easier to prove with P(n) as an assumption.

$$P(0),\ P(n) \rightarrow P(n+1)$$

$$\forall m \in \underline{\mathrm{N}}.\ P(m)$$

For any n>=0

Like domino effect…

Outline

- Strong Induction
- Well-Ordering Principle

Outline

- **Strong Induction**
- Well-Ordering Principle

Proofs

- **Basic proof methods**:
  - Direct, Indirect, Contradiction, By Cases,
- **Equivalences Proof of quantified statements**:
  - **There exists x with some property P(x).**

    – It is sufficient to find one element for which the property holds.
  - **For all x some property P(x) holds**.

    – Proofs of 'For all x some property P(x) holds' must cover all x and can be harder.
  - **Mathematical induction** is a technique that can be applied to prove the universal statements for sets of positive integers or their associated sequences.

Mathematical induction

- Used to prove statements of the form ∀ x P(x) where $x \in Z^+$

- **Mathematical induction proofs** consists of two steps:

  1) **Basis**: The proposition P(1) is true.

  2) **Inductive Step**: The implication P(n) → P(n+1), is true for all positive n.

  Therefore we conclude ∀ x P(x).

- Based on the **well-ordering property**: Every nonempty set of nonnegative integers has a least element

Correctness of Mathematical Induction

- Suppose **P(1) is true** and **P(n) → P(n+1)** is true for all positive integers n. Want to show **∀ x P(x).**
- Assume there is at least one n such that P(n) is false. Let S be the set of nonnegative integers where P(n) is false. Thus S≠ ∅.
- **Well-Ordering Property**: Every nonempty set of nonnegative integers has a least element.
- **By the Well-Ordering Property**, S has a least member, say k. k > 1, since P(1) is true. This implies k - 1 > 0 and P(k-1) is true (since k is the smallest integer where P(k) is false).
- **Now**: P(k-1) → P(k) is true thus, P(k) must be true (a contradiction).
- **Therefore ∀ x P(x).**

Strong induction

- The **regular induction**:
  - uses the basic step P(1) and
  - inductive step P(n-1) → P(n)

- **Strong induction**:
  - Uses the basis step P(1) and
  - inductive step P(1) and P(2) … P(n-1) → P(n)

Fundamental Theorem of Arithmetic

- **Problem**: Prove that if *n* is an integer greater than 1, then *n* can be written as $\prod_{i=1}^{l} p_i$ where p_i is a prime number.

- **Solution:**

I. Let *P*(*n*) be the predicate that *n* can be written as "a product of primes."

II. Base Case: *P*(2) is true since 2 itself is a prime.

III. Inductive Step: The inductive hypothesis is *P*(*j*) is true for all integers *j* with $2 \leq j \leq k$.
Show that *P*(*k* + 1) must be true.

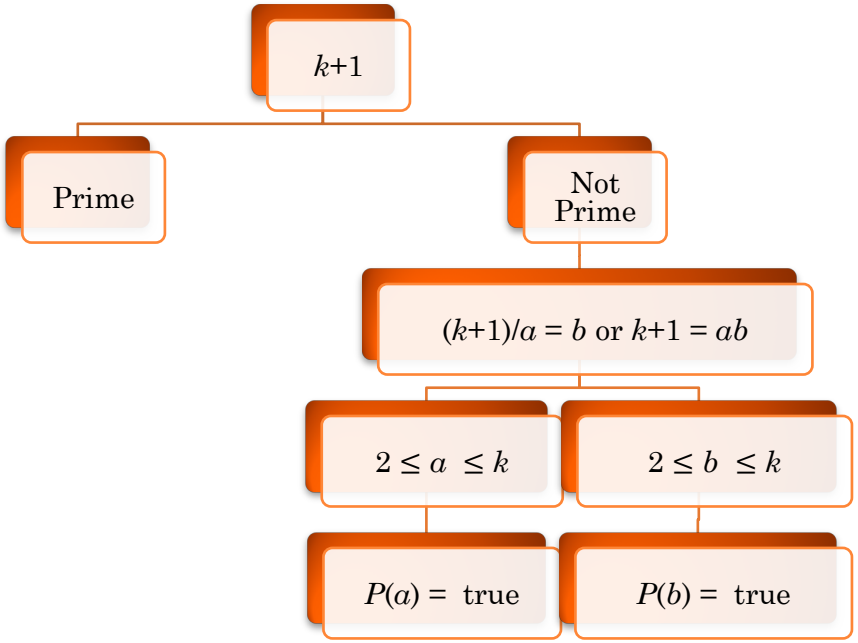
Fundamental Theorem of Arithmetic, cont'd

Consider $P(k + 1)$:

- If $k + 1$ is prime, then $P(k + 1)$ is true.

- Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$. By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes.

Hence, it has been shown that every integer greater than 1 can be written as the product of primes.



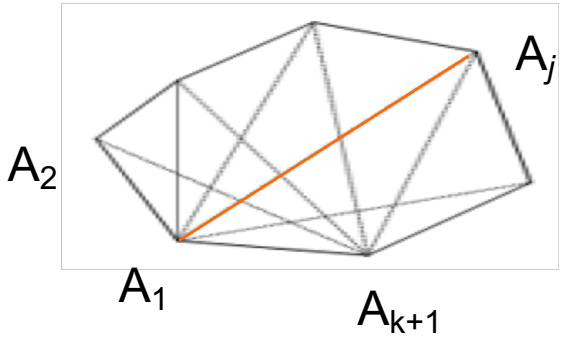
Polygon of *n* Sides – Strong Induction

- **Problem:** Prove that any polygon of *n* sides could be triangulated into *n*-2 triangles.
- **Solution:**
  - Base Case: $P(3)$ is true as 3-2 = 1
  - Inductive hypothesis: $P(k)$ is true for all j where $3 \le j \le k$.
  - Proof: Consider (k+1)-gon. A diagonal A_1A_j splits $(k+1)$-gon into two polygons:
    - j-gon
    - $((k + 1) – j + 2)$-gon.

Both polygons are of sides less than k and not less than 3, so the numbers of triangles are

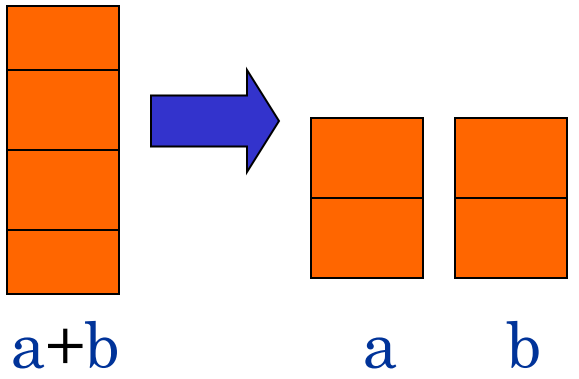
- $j – 2$
- $((k + 1) – j + 2) – 2 = k + 1 – j$.

The total number of triangles for $(k + 1)$-gon is $j – 2 + k + 1 – j = k + 1 – 2$.



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



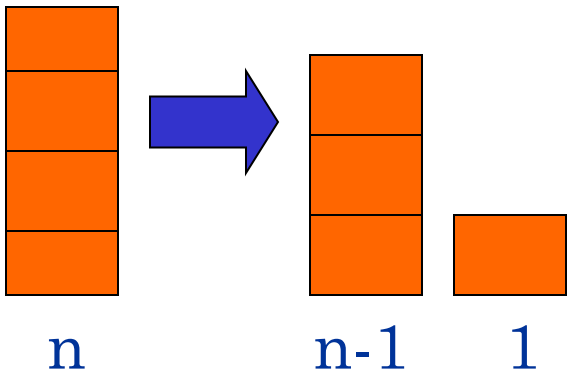
Unstacking Game

What is the best way to play this game?

Suppose there are n boxes.

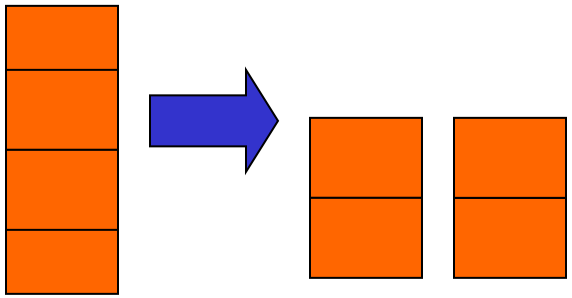
What is the score if we just take the box one at a time?

$$\sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$$



Unstacking Game

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 1x4x4 + 2x2x2 + 4x1 = 28

first round second third

Not better than the first strategy!

$$\frac{n(n-1)}{2}$$

Say n=16, then the score is 8x8 + 2x28 = 120

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 $n = 0$:

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

Claim(0) is okay.

Unstacking Game

Inductive step. assume for n-stack,

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

$(n+1)$-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 $a + b = n + 1$.

$(a + b)$-stack score = ab + a-stack score + b-stack score

by induction:

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

b-stack score = $\dfrac{b(b-1)}{2}$

Unstacking Game

(a + b)-stack score = ab + a-stack score + b-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 $C(n+1)$ is okay. We're done!

Outline

- Strong Induction
- **Well-Ordering Principle**

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.* NO!

Every nonempty set of *negative integers* has a *least element.* NO!

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*, ∃ 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 $\left|m_0 / c\right| < \left|m_0\right|$ 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*

$$C ::= \{n \in \mathbb{N} \mid \neg P(n)\}$$

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

$$a^3 + b^3 = c^3$$

Fermat's theorem

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

$$4a^3 + 2b^3 = c^3$$

Non-Fermat's theorem

Hint: Prove by contradiction using well ordering principle…

Non-Fermat Theorem

$$4a^3 + 2b^3 = c^3$$

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.

Non-Fermat Theorem

$$4a^3 + 2b^3 = c^3$$

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 (*)

Next class

- Topic: Recursive Definitions and Structural Induction
- Pre-class reading: Chap 5.3