This Lecture

Last time we have discussed different proof techniques.

This time we will focus on probably the most important one

- mathematical induction.

This lecture’s plan is to go through the following:

• The idea of mathematical induction
• Basic induction proofs (e.g. equality, inequality, property, etc)
• Inductive constructions
• A paradox
Proving For-All Statements

Objective: Prove $\forall n \geq 0 \ P(n)$

It is very common to prove statements of this form. Some Examples:

For an odd number $m$, $m^i$ is odd for all non-negative integer $i$.

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

(Cauchy-Schwarz inequality) For any $a_1, \ldots, a_n$, and any $b_1, \ldots b_n$

$$a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \leq \sqrt{a_1^2 + a_2^2 + \ldots a_n^2} \sqrt{b_1^2 + b_2^2 + \ldots b_n^2}$$
Universal Generalization

\[
\frac{A \rightarrow R(c)}{A \rightarrow \forall x. R(x)}
\]

valid rule

providing \( c \) is independent of \( A \)

One way to prove a for-all statement is to prove that \( R(c) \) is true for any \( c \), but this is often difficult to prove directly (e.g. consider the statements in the previous slide).

Mathematical induction provides another way to prove a for-all statement. It allows us to prove the statement step-by-step. Let us first see the idea in two examples.
**Odd Powers Are Odd**

**Fact:** If \( m \) is odd and \( n \) is odd, then \( mn \) is odd.

**Proposition:** for an odd number \( m \), \( m^i \) is odd for all non-negative integer \( i \).

\[ \forall i \in \mathbb{Z} \quad odd(m^i) \]

Let \( P(i) \) be the proposition that \( m^i \) is odd.

\[ \forall i \in \mathbb{Z} \quad P(i) \]

**Idea of induction.**

- \( P(1) \) is true by definition.
- \( P(2) \) is true by \( P(1) \) and the fact.
- \( P(3) \) is true by \( P(2) \) and the fact.
- \( P(i+1) \) is true by \( P(i) \) and the fact.
- So \( P(i) \) is true for all \( i \).
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 $n$.

Idea of induction.
Objective: Prove \( \forall n \geq 0 \ P(n) \)

This is to prove

\[ P(0) \land P(1) \land P(2) \land \ldots \land P(n) \ldots \]

The idea of induction is to first prove \( P(0) \) unconditionally,
then use \( P(0) \) to prove \( P(1) \)
then use \( P(1) \) to prove \( P(2) \)
and repeat this to infinity...
The Induction Rule

\[ P(0), \forall n \in \mathbb{Z} \ P(n) \rightarrow P(n+1) \]

\[ \forall m \in \mathbb{Z} \ P(m) \]

0 and (from \( n \) to \( n+1 \)),
proves 0, 1, 2, 3,....

Very easy to prove

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

The point is to use the knowledge on smaller problems to solve bigger problems (i.e. can assume \( P(n) \) to prove \( P(n+1) \)).

Compare it with the universal generalization rule.
This Lecture

• The idea of mathematical induction

• Basic induction proofs (e.g. equality, inequality, property, etc)

• Inductive constructions

• A paradox
Proving an Equality

Let $P(n)$ be the induction hypothesis that the statement is true for $n$.

Base case: $P(1)$ is true because both LHS and RHS equal to 1

Induction step: assume $P(n)$ is true, prove $P(n+1)$ is true.

That is, assuming: $1 + r + \ldots + r^n = \frac{r^{n+1} - 1}{r - 1}$

Want to prove: $1 + r + \ldots + r^n + r^{n+1} = \frac{r^{n+2} - 1}{r - 1}$

This is much easier to prove than proving it directly, because we already know the sum of the first $n$ terms!
Proving an Equality

\[ r \neq 1 \quad \forall n \geq 1 \quad 1 + r + \ldots + r^n = \frac{r^{n+1} - 1}{r - 1} \]

Let \( P(n) \) be the induction hypothesis that the statement is true for \( n \).

Base case: \( P(1) \) is true because both LHS and RHS equal to 1

Induction step: assume \( P(n) \) is true, prove \( P(n+1) \) is true.

\[
1 + r + \ldots + r^n + r^{n+1} = \frac{r^{n+1} - 1}{r - 1} + r^{n+1} = \frac{r^{n+1} - 1 + r^{n+2} - r^{n+1}}{r - 1} = \frac{r^{n+2} - 1}{r - 1}
\]
Proving an Equality

\[ \forall n \geq 1 \quad 1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n + 1)}{2}\right)^2 \]

Let \( P(n) \) be the induction hypothesis that the statement is true for \( n \).

Base case: \( P(1) \) is true

Induction step: assume \( P(n) \) is true, prove \( P(n+1) \) is true.

\[
\begin{align*}
1^3 + 2^3 + \ldots + n^3 + (n + 1)^3 &= \left(\frac{n(n + 1)}{2}\right)^2 + (n + 1)^3 \\
&= (n + 1)^2\left(\frac{n^2 + 4n + 4}{4}\right) \\
&= (n + 1)^2\left(\frac{(n + 2)^2}{4}\right) = \left(\frac{(n + 1)(n + 2)}{2}\right)^2
\end{align*}
\]
Proving a Property

\[ \forall n \geq 1, \quad 2^{2n} - 1 \text{ is divisible by 3} \]

Base Case \((n = 1): \quad 2^{2n} - 1 = 2^2 - 1 = 3 \]

Induction Step: Assume \( P(i) \) for some \( i \geq 1 \) and prove \( P(i + 1): \)

Assume \( 2^{2i} - 1 \) is divisible by 3, prove \( 2^{2(i+1)} - 1 \) is divisible by 3.

\[
2^{2(i+1)} - 1 = 2^{2i+2} - 1 = 4 \cdot 2^{2i} - 1 = 3 \cdot 2^{2i} + 2^{2i} - 1
\]

Divisible by 3 \hspace{1cm} \text{Divisible by 3 by induction}
Proving a Property

\[ \forall n \geq 2, \quad n^3 - n \text{ is divisible by 6} \]

Base Case \((n = 2)\): \[ 2^3 - 2 = 6 \]

Induction Step: Assume \(P(i)\) for some \(i \geq 2\) and prove \(P(i + 1)\):

Assume \( n^3 - n \) is divisible by 6

Prove \((n + 1)^3 - (n + 1)\) is divisible by 6.

\[
(n + 1)^3 - (n + 1) = (n^3 + 3n^2 + 3n + 1) - (n + 1)
\]

\[
= (n^3 - n) + 3(n^2 + n)
\]

Divisible by 6 by induction

Divisible by 2 by case analysis
Proving an Inequality

\[ \forall n \geq 2, \quad \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n} \]

Base Case \((n = 2)\): is true

Induction Step: Assume \(P(i)\) for some \(i \geq 2\) and prove \(P(i+1)\):

\[
\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n + 1}} > \sqrt{n} + \frac{1}{\sqrt{n + 1}} \quad \text{by induction}
\]

\[
= \frac{\sqrt{n} \sqrt{n + 1} + 1}{\sqrt{n + 1}}
\]

\[
> \frac{\sqrt{n} \sqrt{n + 1}}{\sqrt{n + 1}} = \frac{n + 1}{\sqrt{n + 1}}
\]

\[
= \sqrt{n + 1}
\]
Cauchy-Schwarz

(Cauchy-Schwarz inequality) For any $a_1, \ldots, a_n$, and any $b_1, \ldots b_n$

$$a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \leq \sqrt{a_1^2 + a_2^2 + \ldots a_n^2} \sqrt{b_1^2 + b_2^2 + \ldots b_n^2}$$

Proof by induction (on n):

When n=1, LHS <= RHS.

When n=2, want to show

$$a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2} \sqrt{b_1^2 + b_2^2}$$

Consider

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) - (a_1 b_1 + a_2 b_2)^2$$

$$= a_1^2 b_1^2 + a_2^2 b_2^2 + a_2^2 b_1^2 + a_2^2 b_2^2 - a_1^2 b_1^2 - 2a_1 b_1 a_2 b_2 - a_2^2 b_2^2$$

$$= a_1^2 b_2^2 + a_2^2 b_1^2 - 2a_1 b_1 a_2 b_2$$

$$= (a_1 b_2 - a_2 b_1)^2 \geq 0$$
\textbf{Cauchy-Schwarz}

\textit{(Cauchy-Schwarz inequality)} For any \(a_1, \ldots, a_n,\) and any \(b_1, \ldots, b_n\)

\[a_1b_1 + a_2b_2 + \ldots + a_nb_n \leq \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}\sqrt{b_1^2 + b_2^2 + \ldots + b_n^2}\]

Induction step: assume true for \(\leq n,\) prove \(n+1.\)

\[a_1b_1 + a_2b_2 + \ldots + a_nb_n + a_{n+1}b_{n+1}\]
\[\leq \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}\sqrt{b_1^2 + b_2^2 + \ldots + b_n^2} + a_{n+1}b_{n+1}\]

\[
\leq \sqrt{c^2 + a_{n+1}^2}\sqrt{d^2 + b_{n+1}^2}
\]

\[
= \sqrt{\frac{a_1^2 + a_2^2 + \ldots + a_n^2}{d^2 + b_{n+1}^2} + a_{n+1}^2}\sqrt{b_1^2 + b_2^2 + \ldots + b_n^2 + b_{n+1}^2}
\]

\text{by P(2)}
This Lecture

• The idea of mathematical induction
• Basic induction proofs (e.g. equality, inequality, property, etc)
• Inductive constructions
• A paradox
Gray Code

Can you find an ordering of all the n-bit strings in such a way that two consecutive n-bit strings differed by only one bit?

This is called the Gray code and has some applications.

How to construct them? Think inductively!

<table>
<thead>
<tr>
<th>2 bit</th>
<th>3 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>000</td>
</tr>
<tr>
<td>01</td>
<td>001</td>
</tr>
<tr>
<td>11</td>
<td>011</td>
</tr>
<tr>
<td>10</td>
<td>010</td>
</tr>
<tr>
<td>11</td>
<td>011</td>
</tr>
<tr>
<td>10</td>
<td>010</td>
</tr>
<tr>
<td>10</td>
<td>011</td>
</tr>
<tr>
<td>10</td>
<td>010</td>
</tr>
<tr>
<td>00</td>
<td>001</td>
</tr>
</tbody>
</table>

Can you see the pattern?

How to construct 4-bit gray code?
Gray Code

Every 4-bit string appears exactly once.
Gray Code

Every (n+1)-bit string appears exactly once.

So, by induction,
Gray code exists for any n.
Goal: tile the squares, except one in the middle for Bill.
Puzzle

There are only trominos (L-shaped tiles) covering three squares:

For example, for 8 x 8 puzzle might tile for Bill this way:
Puzzle

**Theorem:** For any $2^n \times 2^n$ puzzle, there is a tiling with Bill in the middle.

(Did you remember that we proved $2^{2n} - 1$ is divisible by 3?)

**Proof:** (by induction on $n$)

$\mathcal{P}(n) ::= \text{can tile } 2^n \times 2^n \text{ with Bill in middle.}$

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

(no tiles needed)
Puzzle

Induction step: assume can tile $2^n \times 2^n$, prove can handle $2^{n+1} \times 2^{n+1}$.

Now what??
Idea: It would be nice if we could control the locations of the empty square.
Idea: It would be nice if we could control the locations of the empty square.
The new idea:

Prove that we can always find a tiling with Bill anywhere.

Theorem B: For any $2^n \times 2^n$ plaza, there is a tiling with Bill anywhere.

Clearly Theorem B implies Theorem.

Theorem: For any $2^n \times 2^n$ plaza, there is a tiling with Bill in the middle.
Theorem B: For any $2^n \times 2^n$ plaza, there is a tiling with Bill anywhere.

Proof: (by induction on $n$)

$\mathcal{P}(n) ::= \text{can tile } 2^n \times 2^n \text{ with Bill anywhere.}$

Base case: ($n=0$)  
(no tiles needed)
Induction step:

Assume we can get Bill anywhere in $2^n \times 2^n$.

Prove we can get Bill anywhere in $2^{n+1} \times 2^{n+1}$. 

Puzzle
Induction step:

*Assume* we can get Bill anywhere in $2^n \times 2^n$.

*Prove* we can get Bill anywhere in $2^{n+1} \times 2^{n+1}$.
Method: Now group the squares together, and fill the center with a tile.
Some Remarks

Note 1: It may help to choose a stronger hypothesis than the desired result (e.g. “Bill in anywhere”). We need to prove a stronger statement, but in return we can assume a stronger property in the induction step.

Note 2: The induction proof of “Bill anywhere” implicitly defines a recursive algorithm for finding such a tiling.
Hadamard Matrix

Can you construct an nxn matrix with all entries +1 and -1 and all the rows are orthogonal to each other?

Two rows are orthogonal if their inner product is zero. That is, let \( a = (a_1, \ldots, a_n) \) and \( b = (b_1, \ldots, b_n) \), their inner product \( ab = a_1b_1 + a_2b_2 + \ldots + a_nb_n \)

This matrix is famous and has applications in coding theory.

To think inductively, first we come up with small examples.

\[
\begin{bmatrix}
1 & 1 \\
1 & -1
\end{bmatrix}
\]
Then we use the small examples to build larger examples.

Suppose we have an $n \times n$ Hadamard matrix $H_n$.

We can use it to construct an $2n \times 2n$ Hadamard matrix as follows.

\[
\begin{bmatrix}
H_n & H_n \\
H_n & -H_n
\end{bmatrix}
\]

It is an exercise to check that the rows are orthogonal to each other.

So by induction there is a $2^k \times 2^k$ Hardmard matrix for any $k$. 
Inductive Construction

This technique is very useful.

We can use it to construct:

- codes
- graphs
- matrices
- circuits
- algorithms
- designs
- proofs
- buildings
- ...
This Lecture

- The idea of mathematical induction
- Basic induction proofs (e.g. equality, inequality, property, etc)
- Inductive constructions
- A paradox
Paradox

**Theorem:** All horses have the same color.

**Proof:** (by induction on \( n \))

Induction hypothesis:

\[ P(n) ::= \text{any set of } n \text{ horses have the same color} \]

Base case \((n=0)\):

No horses so *obviously* true!
Paradox

(Inductive case)
Assume any $n$ horses have the same color.
Prove that any $n+1$ horses have the same color.
Paradox

(Inductive case)
Assume any \( n \) horses have the same color.
Prove that any \( n+1 \) horses have the same color.
Paradox

(Inductive case)
Assume any \( n \) horses have the same color.
Prove that any \( n+1 \) horses have the same color.

Therefore the set of \( n+1 \) have the same color!
What is wrong? \( n = 1 \)

Proof that \( P(n) \rightarrow P(n+1) \)
is false if \( n = 1 \), because the two horse groups do not overlap.

(But proof works for all \( n \neq 1 \))
Quick Summary

You should understand the principle of mathematical induction well, and do basic induction proofs like

- proving equality
- proving inequality
- proving property

Mathematical induction has a wide range of applications in computer science.

In the next lecture we will see more applications and more techniques.