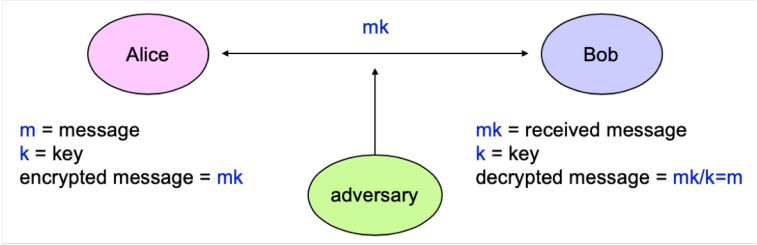
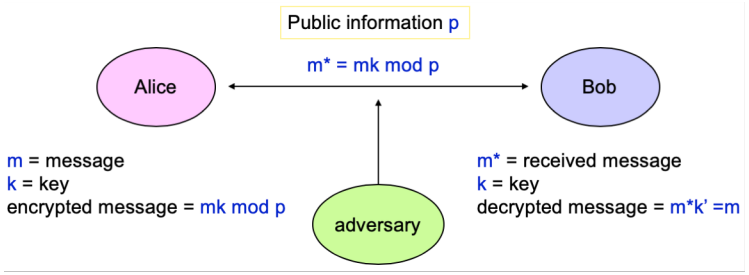
Lecture 21: Mathematic Induction

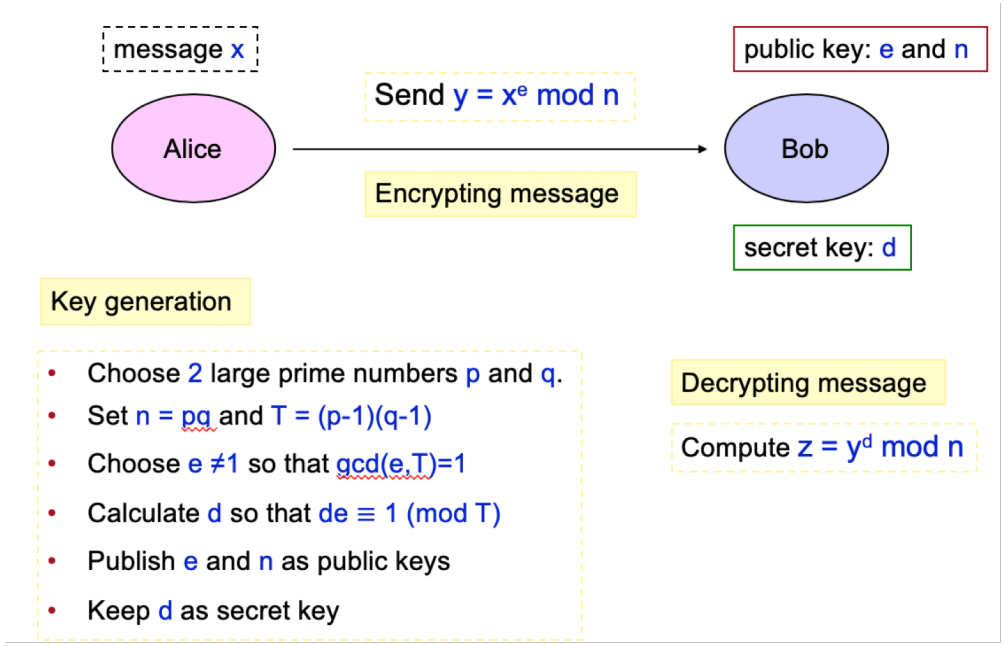
Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: **clong2@albany.edu**

Recap Previous Lecture

- Turing Code Ver 1 & 2.
- RSA Cryptosystem







Outline

- The Ideal of Mathematic Induction
- Basic Induction Proofs
- Applications
- A Paradox

Outline

- **The Ideal of Mathematic Induction**
- Basic Induction Proofs
- Applications
- A Paradox

Odd Power are Odd

Fact: If m is odd and n is odd, then nm is odd.

Proposition: for an odd number m, m^k is odd for all non-negative integer k.

$$\forall k \in N \;\; odd(m^k)$$

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

$$\forall k \in N \;\; P(k)$$

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.

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.

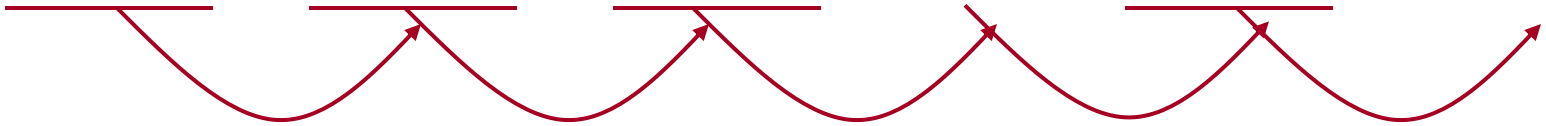
Idea of induction.

Idea of Induction

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

This is to prove

$$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(n) \ldots$$



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…

Idea of Induction

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

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

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

Very easy to prove

$$\frac{P(0),\ P(n) \rightarrow P(n+1)}{\forall m \in \underline{\mathrm{N}}.\ P(m)}$$

For any n>=0

Like domino effect…

Outline

- The Ideal of Mathematic Induction
- **Basic Induction Proofs**
- Applications
- A Paradox

Proof by Induction

Let's prove:

$$\forall r \neq 1.\ 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$$

Statements in green form a template for inductive proofs.

Proof: (by induction on n)

The induction hypothesis, $P(n)$, is:

$$\forall r \neq 1.\ \ 1 + r + r^2 + \cdots + r^{n} = \frac{r^{n+1}-1}{r-1}$$

Proof by Induction

Induction Step: Assume $P(n)$ for some $n \geq 0$ and prove $P(n+1)$:

$$\forall r \neq 1.\ \ 1 + r + r^2 + \cdots + r^{n+1} = \frac{r^{(n+1)+1} - 1}{r - 1}$$

Have $P(n)$ by assumption:

So let r be any number $\neq 1$, then from $P(n)$ we have

$$1 + r + r^2 + \cdots + r^{n} = \frac{r^{n+1} - 1}{r - 1}$$

How do we proceed?

Proof by Induction

adding r^{n+1} to both sides,

$$1+\cdots+r^n+r^{n+1} = \frac{r^{n+1}-1}{r-1}+r^{n+1}$$

$$= \frac{r^{n+1}-1+r^{n+1}(r-1)}{r-1}$$

$$= \frac{r^{(n+1)+1}-1}{r-1}$$

$$\forall r \neq 1.\ 1+r+r^2+\cdots+r^{n+1} = \frac{r^{(n+1)+1}-1}{r-1}$$

which is $P(n+1)$. This completes the induction proof.

Proving an Equality

$$\forall n \geq 1 \qquad 1^3 + 2^3 + \ldots + n^3 = (\frac{n(n+1)}{2})^2$$

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.

$$1^3 + 2^3 + \ldots + n^3 + (n+1)^3$$

$$= (\frac{n(n+1)}{2})^2 + (n+1)^3 \qquad \text{by induction}$$

$$= (n+1)^2(n^2/4 + n + 1)$$

$$= (n+1)^2(\frac{n^2+4n+4}{4}) = (\frac{(n+1)(n+2)}{2})^2$$

Proving a Property

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

Base Case ($n = 1$): $2^{2n} - 1 = 2^2 - 1 = 3$

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.

$$\begin{aligned} 2^{2(i+1)} - 1 &= 2^{2i+2} - 1 \\ &= 4 \cdot 2^{2i} - 1 \\ &= \underbrace{3 \cdot 2^{2i}}_{\text{Divisible by 3}} + \underbrace{2^{2i} - 1}_{\text{Divisible by 3 by induction}} \end{aligned}$$

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.

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) \\ &= \underbrace{(n^3 - n)}_{\text{Divisible by 6 by induction}} + 3\underbrace{(n^2 + n)}_{\text{Divisible by 2 by case analysis}}\end{aligned}$$

Proving an Inequality

$$\forall n \geq 3, \quad 2n + 1 < 2^n$$

Base Case ($n = 3$): $2n + 1 = 7 < 2^n = 2^3 = 8$

Induction Step: Assume $P(i)$ for some $i \geq 3$ and prove $P(i + 1)$:

Assume $2i + 1 < 2^i$, prove $2(i + 1) + 1 < 2^{(i+1)}$

$$\begin{aligned} 2(i+1)+1 &= 2i + 1 + 2 \\ &< 2^i + 2 && \text{by induction} \\ &< 2^i + 2^i && \text{since i >= 3} \\ &= 2^{(i+1)} \end{aligned}$$

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 $P(i + 1)$:

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}}$$

$$> \sqrt{n} + \frac{1}{\sqrt{n+1}} \qquad \text{by induction}$$

$$= \frac{\sqrt{n}\sqrt{n+1} + 1}{\sqrt{n+1}}$$

$$> \frac{\sqrt{n}\sqrt{n} + 1}{\sqrt{n+1}} = \frac{n+1}{\sqrt{n+1}}$$

$$= \sqrt{n+1}$$

Outline

- The Ideal of Mathematic Induction
- Basic Induction Proofs
- **Applications**
- 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 many applications.

How to construct them?

Think inductively! (or recursively!)

2 bit	3 bit
00	000
01	001
11	011
10	010
	110
	111
	101
	100

Can you see the pattern?

How to construct 4-bit gray code?

Gray Code

3 bit	3 bit (reversed)
000	100
001	101
011	111
010	110
110	010
111	011
101	001
100	000

Every 4-bit string appears exactly once.

4 bit

0000
0001
0011 ⟵ differed by 1 bit by induction
0010 ⟵
0110
0111
0101
0100 ⟵ differed by 1 bit by construction
1100 ⟵
1101
1111
1110
1010 ⟵ differed by 1 bit by induction
1011 ⟵
1001
1000

Gray Code

n bit	n bit (reversed)
000…0	100…0
…	…
…	…
…	…
…	…
…	…
…	…
100…0	000…0

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

So, by induction,
Gray code exists for any n.

n+1 bit

0 000…0
0 …
0 … ⟷ differed by 1 bit by induction
0 …
0 …
0 …
0 …
0 100…0 ⟷ differed by 1 bit by construction
1 100…0
1 …
1 …
1 …
1 … ⟷ differed by 1 bit by induction
1 …
1 …
1 …
1 000…0

Hadamard Matrix (Optional)

Can you construct an $n \times n$ matrix with all entries ± 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 many applications.

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

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Hadamard Matrix (Optional)

Then we use the small examples to build larger examples.

Suppose we have an nxn Hadamard matrix H_n.

We can use it to construct an 2nx2n Hadamard matrix as follows.

$$\begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

Check this!

So by induction there is a 2^k x 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
- …

Outline

- The Ideal of Mathematic Induction
- Basic Induction Proofs
- An Interesting Example
- **A Paradox**

Paradox

Theorem: All horses are the same color.

Proof: (by induction on n)

Induction hypothesis:

$P(n)$ ::= any set of n horses have the same color

Base case (n=0):

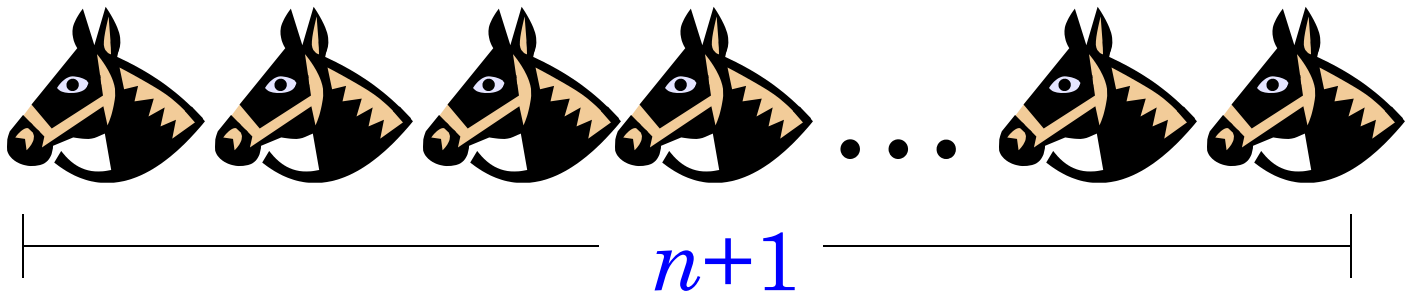
No horses so *obviously* true!

Paradox

(Inductive case)

Assume any n horses have the same color.

Prove that any n+1 horses have the same color.

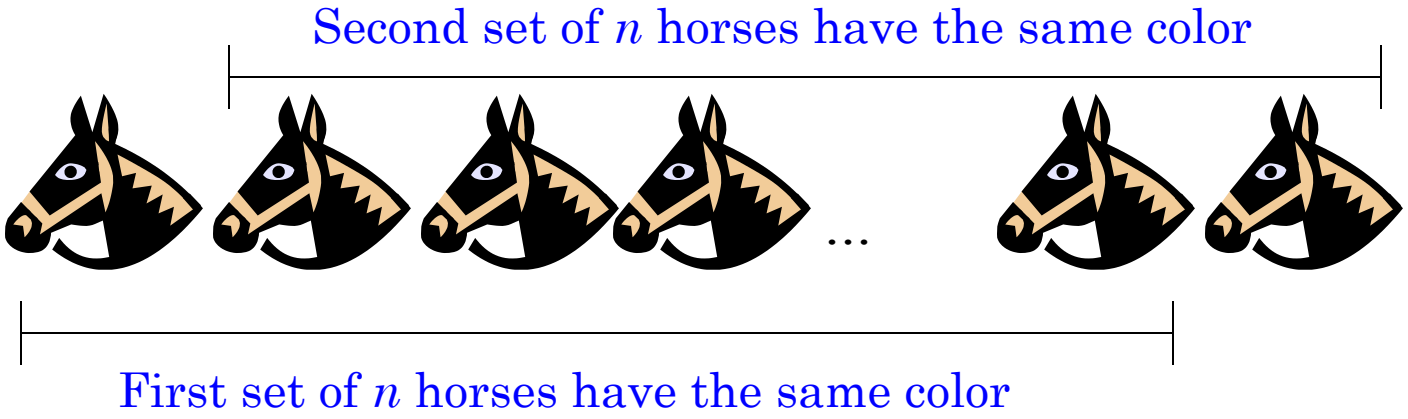


Paradox

(Inductive case)

Assume any n horses have the same color.

Prove that any $n+1$ horses have the same color.

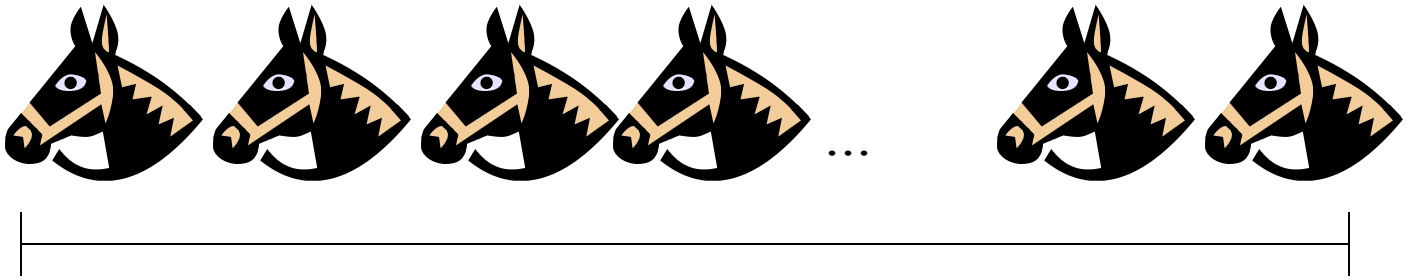


Paradox

(Inductive case)

Assume any n horses have the same color.

Prove that any n+1 horses have the same color.

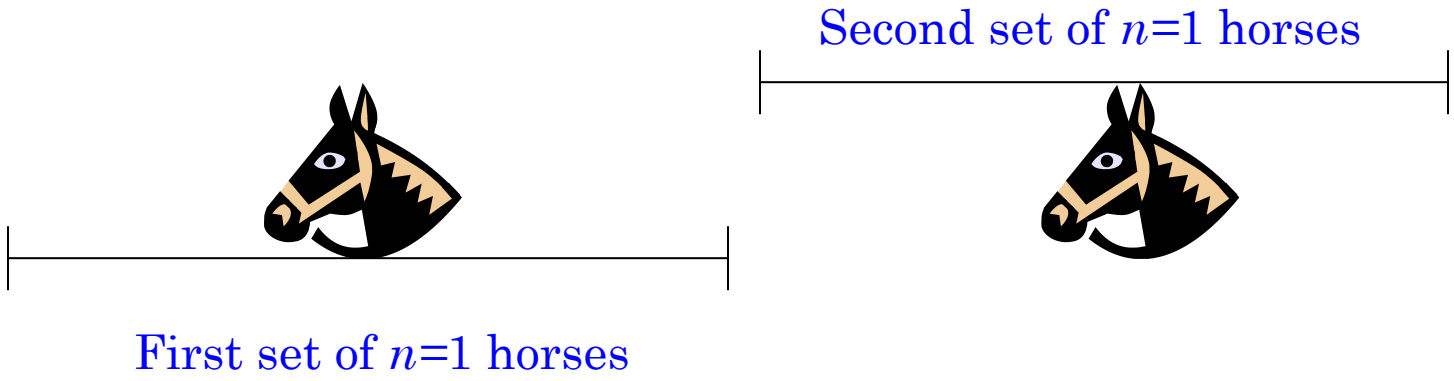


Therefore the set of n+1 have the same color!

Paradox

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 $n \neq 1$)

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.

Next class

- Topic: Strong Induction and Well-Ordering
- Pre-class reading: Chap 5.2