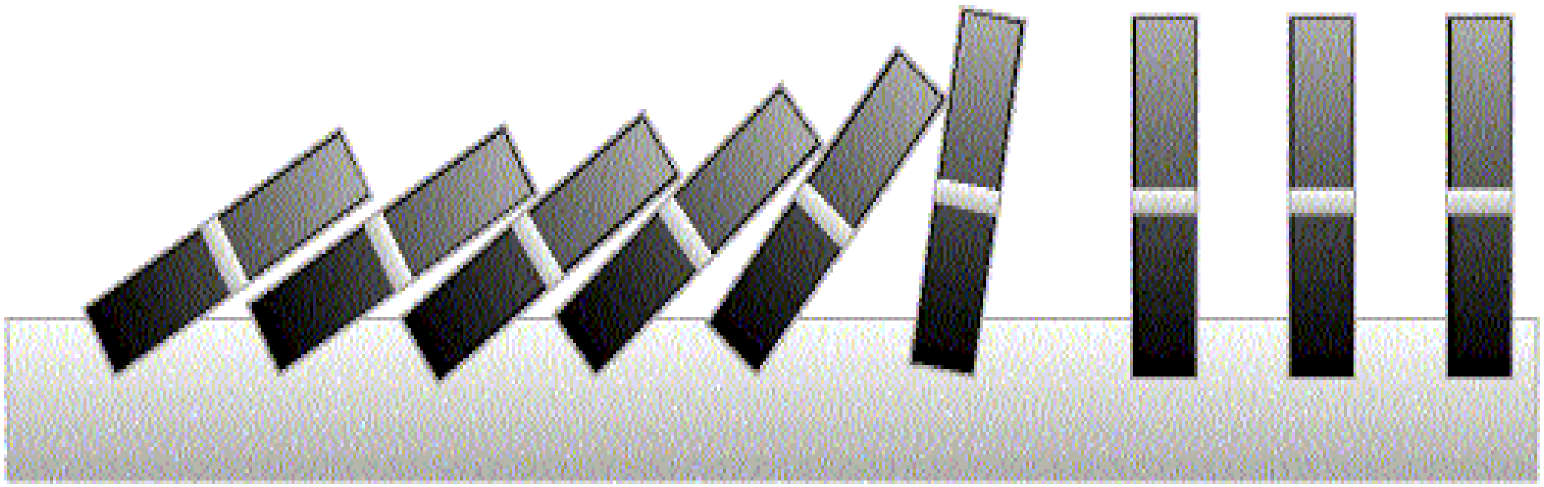
Mathematical Induction I



This Lecture

Last time we discussed different proof techniques.

This time we will focus on probably the most important one

– mathematical induction.

This lecture's plan:

- 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 $b_1,\ldots,b_n$

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

Universal Generalization

valid rule

$$\frac{A \to R(c)}{A \to \forall x.R(x)}$$

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 nm is odd.

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

$$\forall i \in Z \quad odd(m^i)$$

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

$$\forall i \in Z \quad P(i)$$

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.

Idea of Induction

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

This is to prove

$$\underline{P(0)} \wedge \underline{P(1)} \wedge \underline{P(2)} \wedge \ldots \wedge \underline{P(n)} \ldots$$

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

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.

induction rule (an axiom)

$$\frac{P(0),\ \forall n \in Z\ \ P(n) \rightarrow P(n+1)}{\forall m \in Z\ \ P(m)}$$

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, property, inequality, etc)
- Inductive constructions
- A paradox

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.

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

$$= (\frac{n(n+1)}{2})^2 + (n+1)^3$$

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

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

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 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 $P(i + 1)$:

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

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

by induction

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

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

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

Cauchy-Schwarz

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

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

Proof by induction (on n):

Base Case: when n=1, LHS <= RHS.

Induction step: assume true for <=n, prove n+1.

$$a_1b_1+a_2b_2+\ldots+a_nb_n+a_{n+1}b_{n+1}$$

$$\leq \sqrt{a_1^2+a_2^2+\ldots a_n^2}\sqrt{b_1^2+b_2^2+\ldots b_n^2}+a_{n+1}b_{n+1}$$

How to get to this step?

$$\leq \sqrt{a_1^2+a_2^2+\ldots+a_n^2+a_{n+1}^2}\sqrt{b_1^2+b_2^2+\ldots+b_n^2+b_{n+1}^2}$$

Cauchy-Schwarz

(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 <=n, prove n+1.

$$a_1b_1+a_2b_2+\ldots+a_nb_n+a_{n+1}b_{n+1}$$

$$\leq \underbrace{\sqrt{a_1^2+a_2^2+\ldots a_n^2}}_{c}\underbrace{\sqrt{b_1^2+b_2^2+\ldots b_n^2}}_{d}+a_{n+1}b_{n+1}$$

induction

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

This is exactly P(2)!

$$= \sqrt{a_1^2+a_2^2+\ldots+a_n^2+a_{n+1}^2}\sqrt{b_1^2+b_2^2+\ldots+b_n^2+b_{n+1}^2}$$

Cauchy-Schwarz

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

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

Proof by induction (on n): When n=1, LHS <= RHS.

When n=2, want to show $a_1b_1+a_2b_2 \leq \sqrt{a_1^2+a_2^2}\sqrt{b_1^2+b_2^2}$

Consider $(a_1^2+a_2^2)(b_1^2+b_2^2)-(a_1b_1+a_2b_2)^2$

$$=a_1^2b_1^2+a_1^2b_2^2+a_2^2b_1^2+a_2^2b_2^2-a_1^2b_1^2-2a_1b_1a_2b_2-a_2^2b_2^2$$

$$=a_1^2b_2^2+a_2^2b_1^2-2a_1b_1a_2b_2$$

$$=(a_1b_2-a_2b_1)^2 \geq 0$$

Inductive step: use P(2) and the assumption P(n) to prove P(n+1).

Some Remarks

There are three important steps in mathematical induction:

- First step: write down clearly the inductive hypothesis P(n).
  (This is sometimes super IMPORTANT!!! You will see this soon.)

- Second step: prove the base case P(1), P(2), etc.
  (You may need to prove more than one base cases sometimes. E.g. Cauchy-Schwarz inequality.)

- Inductive step: prove the inductive case, that is,
  show P(n) => P(n+1)
  (You need to make sure you have used the assumption P(n).)

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 a way such 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!

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

4 bit

0000
0001
0011
0010
0110
0111
0101
0100
1100
1101
1111
1110
1010
1011
1001
1000

differed by 1 bit by induction

differed by 1 bit by construction

differed by 1 bit by induction

Every 4-bit string appears exactly once.

Gray Code

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

n+1 bit

0000…0
0…
0…
0…
0…
0…
0…
0100…0
1 100…0
1 …
1 …
1 …
1 …
1 …
1 …
1 000…0

differed by 1 bit
by induction

differed by 1 bit
by construction

differed by 1 bit
by induction

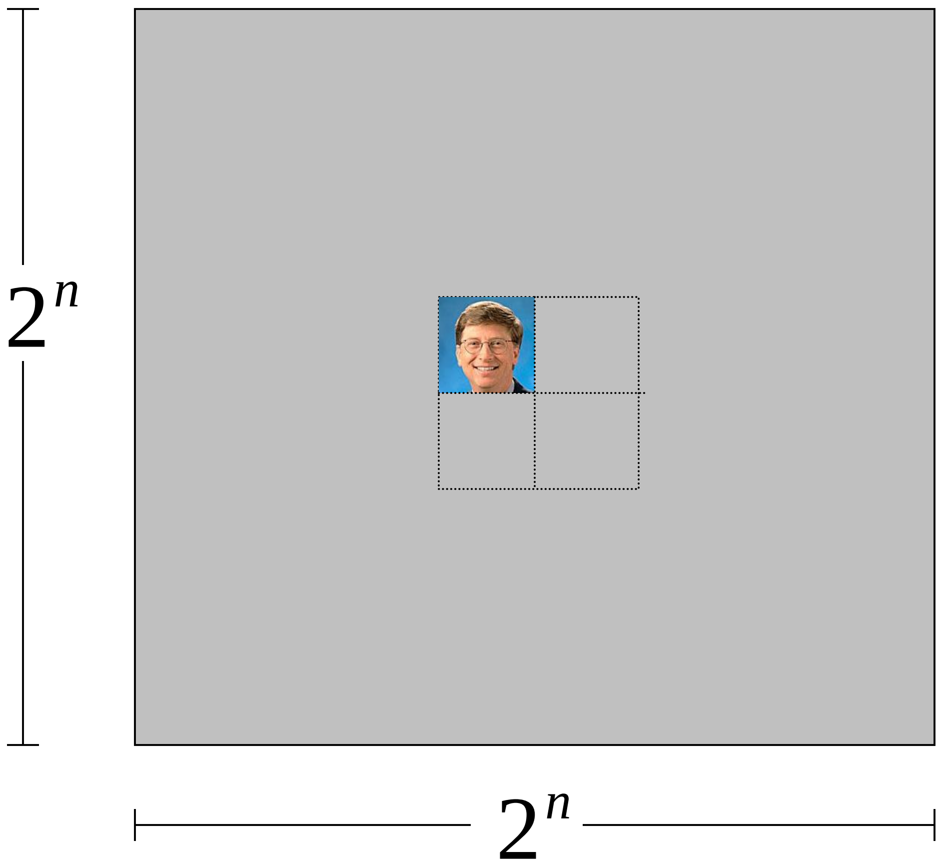
Every (n+1)-bit string appears exactly once.

So, by induction,

Gray code exists for any n.

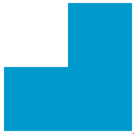
Puzzle

Goal: tile the squares, except one in the middle for Bill.

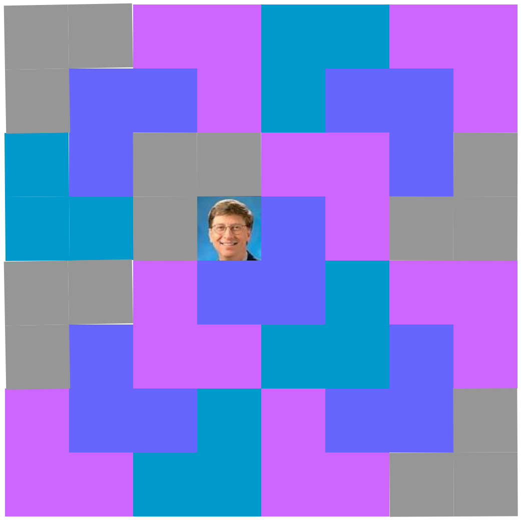


Puzzle

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



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



Puzzle

Theorem: For any 2^n x 2^n puzzle, there is a tiling with Bill in the middle.

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

Proof: (by induction on n)

$P(n)$ ::= can tile 2^n x 2^n with Bill in middle.

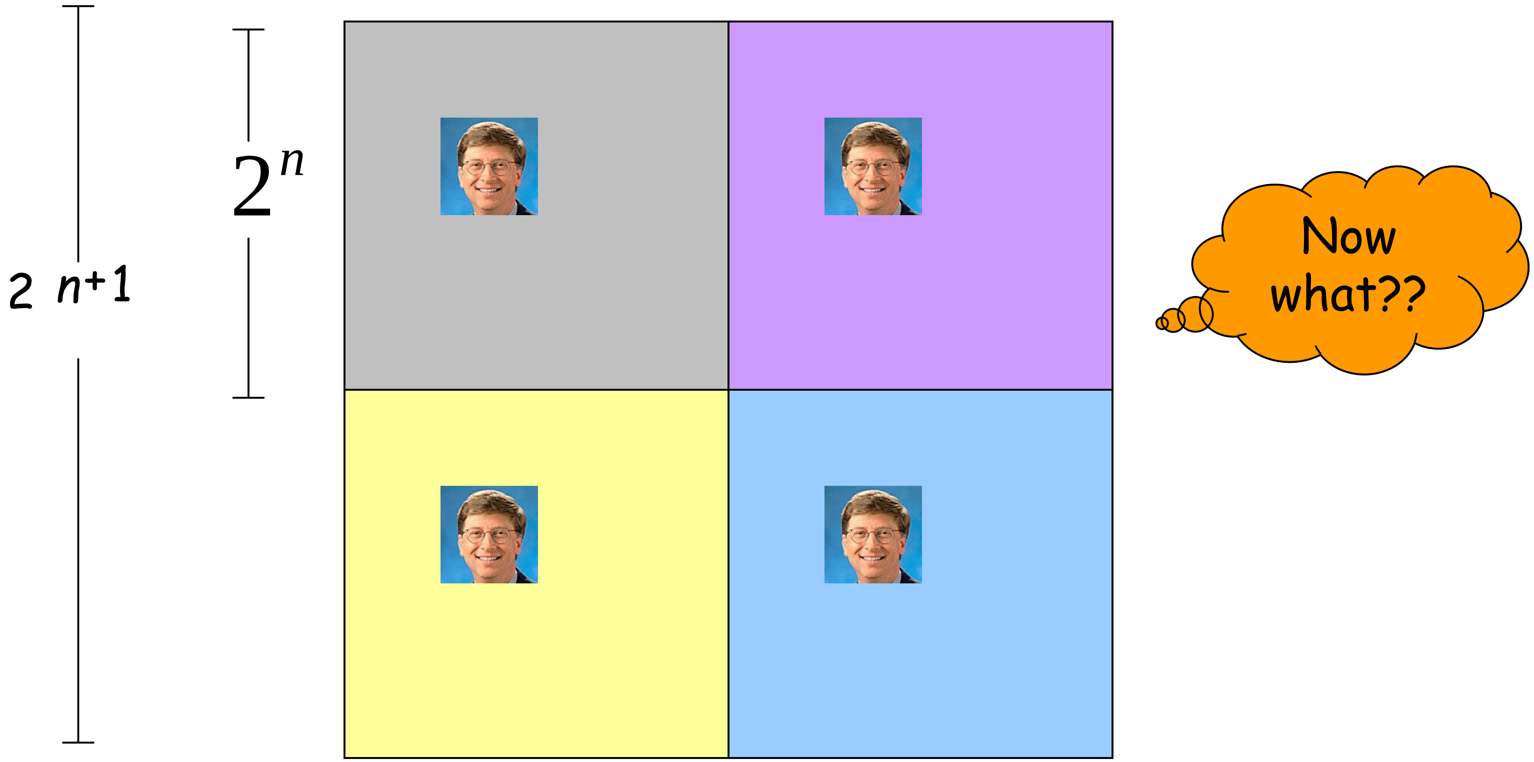
Base case: (n=0)

(no tiles needed)

Puzzle

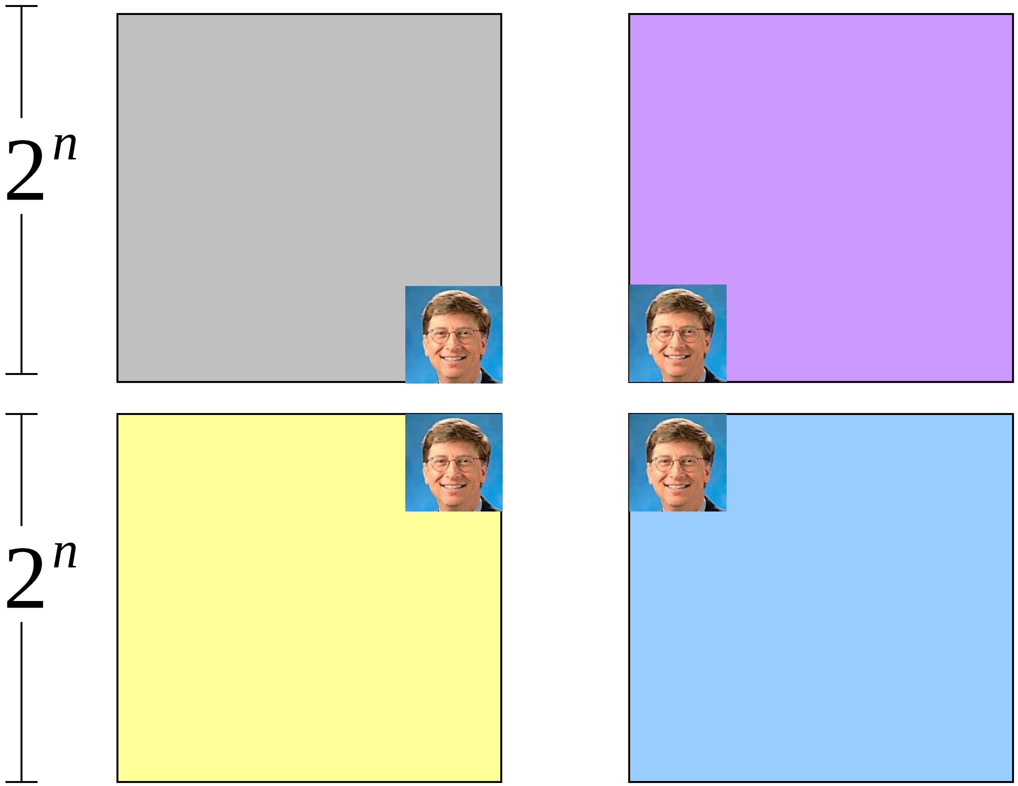
Induction step: assume can tile $2^n \times 2^n$,

prove can handle $2^{n+1} \times 2^{n+1}$.



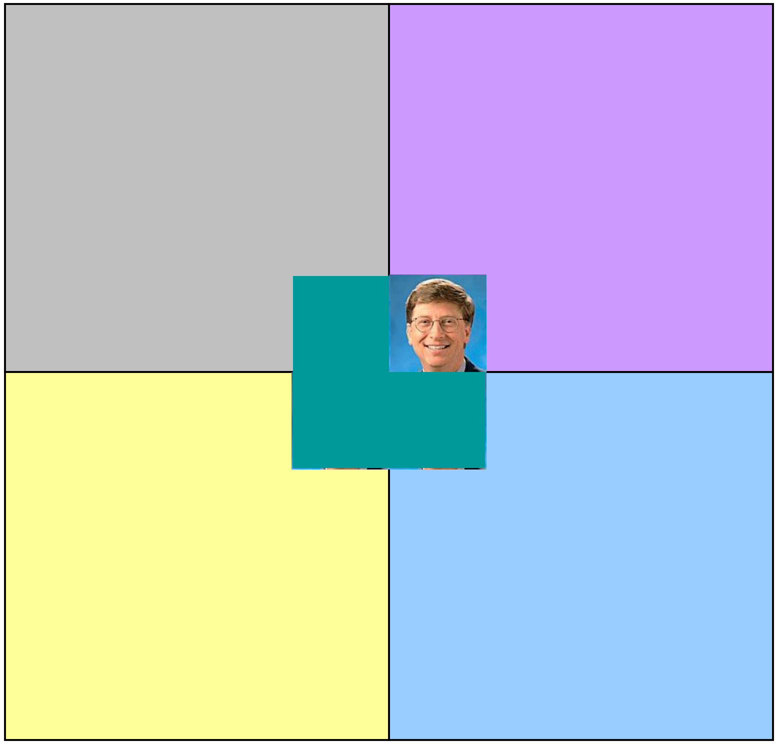
Puzzle

Idea: It would be nice if we could control the locations of Bill.



Puzzle

Idea: It would be nice if we could control the locations of the empty square.



Done!

Puzzle

A stronger property

The new idea:

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

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

Clearly Theorem B implies the original Theorem.

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

Puzzle

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

Proof: (by induction on n)

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

Base case: (n=0)

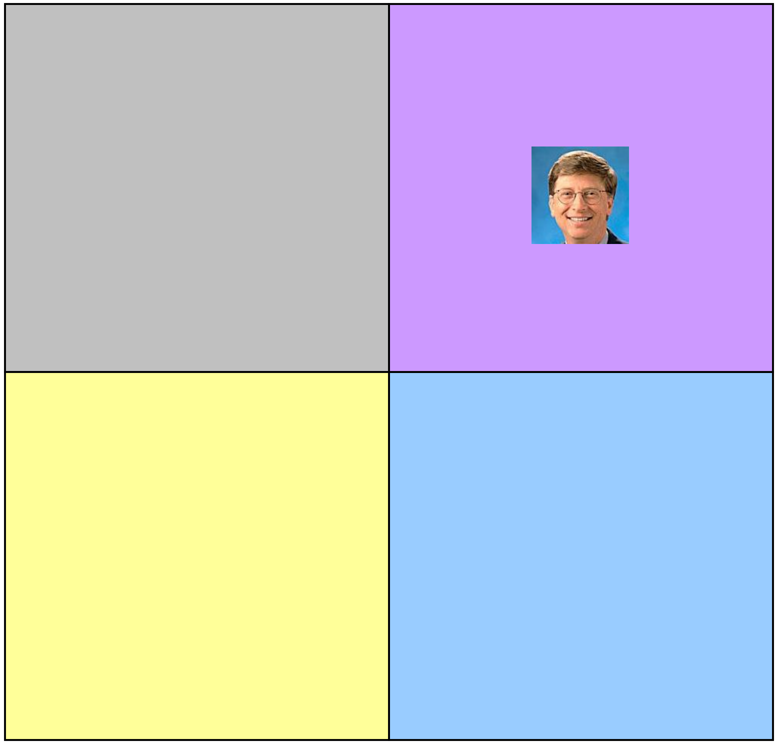
(no tiles needed)

Puzzle

Induction step:

Assume we can get Bill anywhere in 2^n x 2^n.

Prove we can get Bill anywhere in 2^{n+1} x 2^{n+1}.

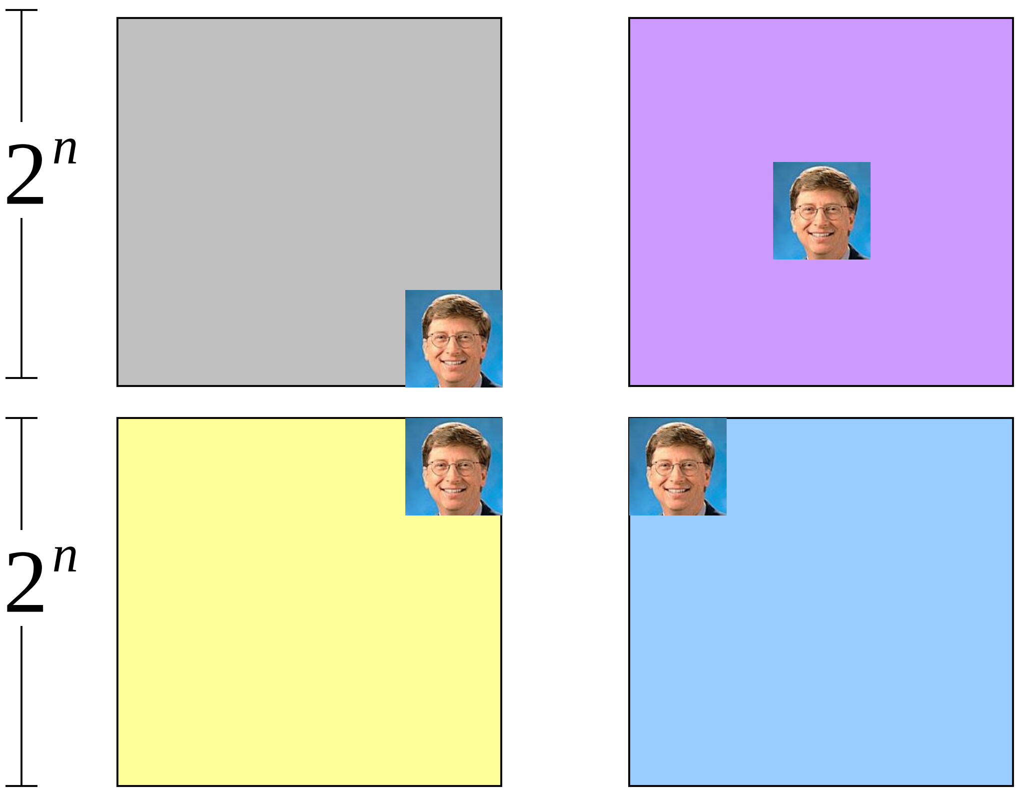


Puzzle

Induction step:

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

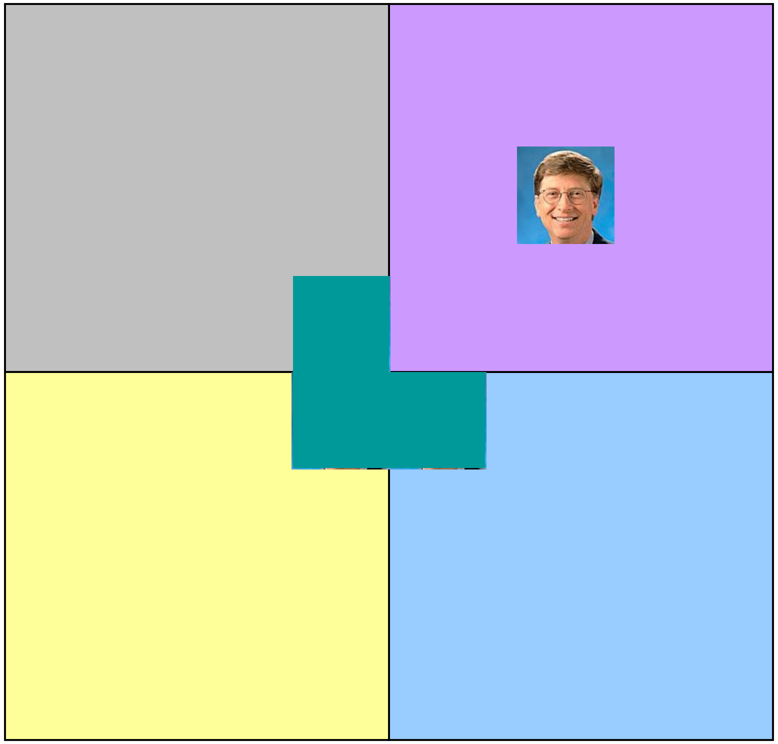
Prove we can get Bill anywhere in $2^{n+1} \times 2^{n+1}$.



Puzzle

Method: Now group the squares together,

and fill the center with a tromino.



Done!

Some Remarks

Note 1: It may help to choose a *stronger statement* (i.e., *P(n)*) 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 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.

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

Hadamard Matrix

Then we use an nxn Hadamard matrix H_n to construct a 2nx2n matrix as follows.

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \quad R_1, R_2$$

We can check that H_{2n} is a Hadamard matrix:

Take rows $R_1=(a,b)$, $R_2=(c,d)$ from H_{2n}.

- If R_1, R_2 are from the first n rows, then $R_1 \cdot R_2 = a \cdot c + b \cdot d = 0+0 = 0$
- Similarly, if R_1, R_2 are from the last n rows, then they are orthogonal.
- If R_1 from the first n rows, R_2 from the last n rows.
  1. If $a \neq c$, $b \neq -d$, then $R_1 \cdot R_2 = a \cdot c + b \cdot d = 0+0 = 0$
  2. If $a=b=c=-d$, then $R_1 \cdot R_2 = a \cdot c + b \cdot d = a \cdot a + a \cdot (-a) = 0$

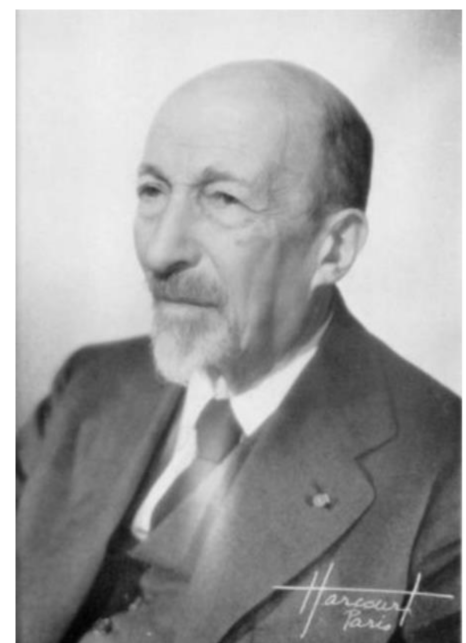
Hadamard Matrix

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

Does there exist an n x n Hardmard matrix for odd n? NO!

Does there exist an n x n Hardmard matrix for even n? Not sure…

This yields the long term "Hadamard conjecture".



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:

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

Base case (n=0):

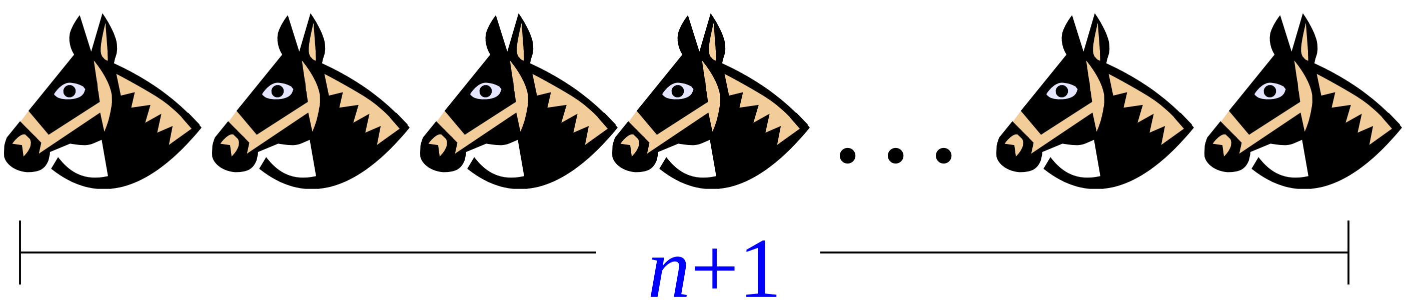
No horses, so *obviously* true!

Paradox

(Inductive case)

Assume any n horses have the same color.

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

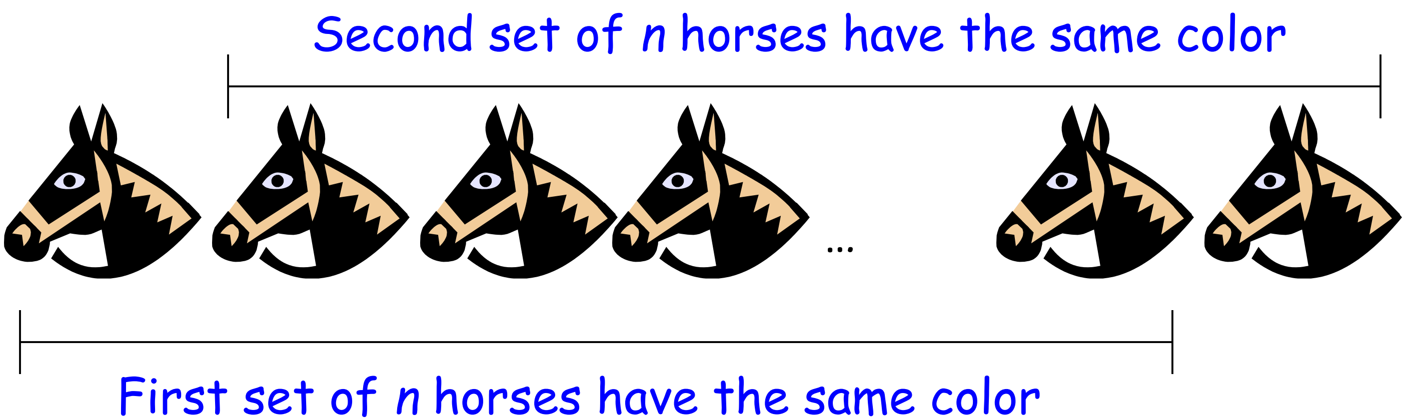


Paradox

(Inductive case)

Assume any n horses have the same color.

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

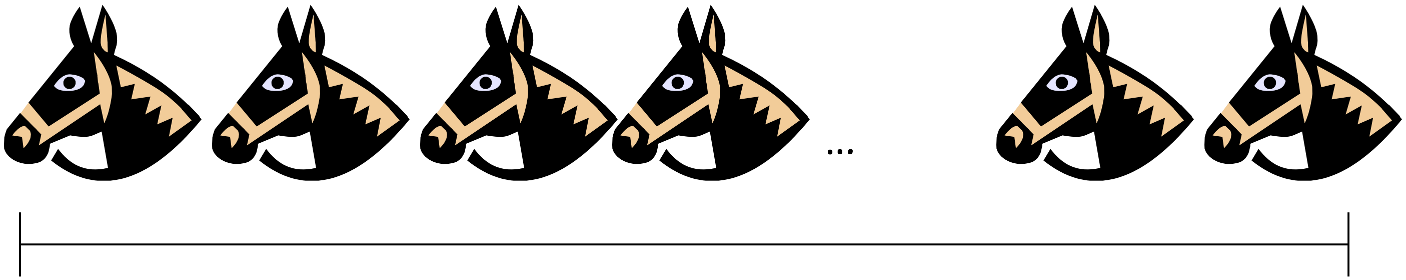


Paradox

(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

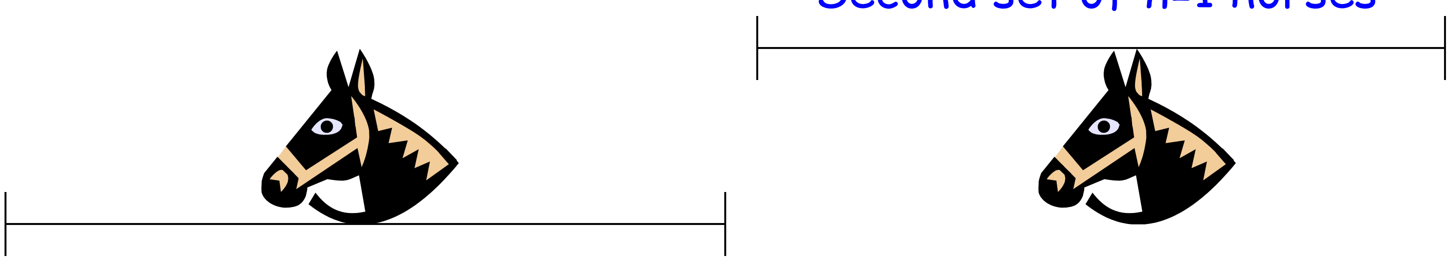
What is wrong? $n = 1$

Proof of $P(n) \rightarrow P(n+1)$

is false when $n = 1$, because the two

horse groups *do not overlap*.

Second set of n=1 horses



First set of n=1 horses

(But the 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.