CSL 101 DISCRRETE MATHEMATICS

LECTURE 3-4

Dr. Barun Gorain
Department of CSE, IIT Bhilai
Email: barun@iitbhilai.ac.in

SOME MORE FACT ON COUNTABILITY

Theorem 2: Let A be a countably infinite set, and B an infinite subset of A. Then B is countable.

Proof

- let $f : N \rightarrow A$ be a bijection witnessing that A is countable. We want to construct a bijection $g : N \rightarrow B$.
- Let $k1 = \min f\{k \in N : f(k) \in B\}$. That is, k1 is the smallest number that gets mapped into B by f.
- Define $g(1) := f(k1)$. We proceed inductively from here.
- Assume we have defined $g(1), g(2) \ldots\ldots, g(n)$.
- Let $kn+1 = \min \{ k \in N : f(k) \in B \setminus \{g(1); : : : ; g(n)\}\}$

- Prove that $g:N\rightarrow B$ is a bijection

UNCOUNTABLE SETS

The closed interval [0,1] is uncountable

Proof:

Suppose that there exists a bijection from r:N→[0,1]

Then we will be able to list down all the real numbers in [0,1] as follows

$$
\begin{aligned}
r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ \ldots\\
r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ \ldots\\
r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ \ldots\\
r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ \ldots\\
&\ \vdots
\end{aligned}
$$

where $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. (For example, if $r_1 = 0.23794102\ldots$, we have $d_{11} = 2$, $d_{12} = 3$, $d_{13} = 7$, and so on.) Then, form a new real number with decimal expansion

$r = 0.d_1d_2d_3d_4\ldots$, where the decimal digits are determined by the following rule:

$$
\begin{aligned}
d_i &= 1 \text{ if } d_{ii} \neq 1\\
&= 2 \text{ if } d_{ii} = 0
\end{aligned}
$$

Note that r is not same as any of r_i in the above list.

BASIC PROOF TECHNIQUES

This Lecture

We are going to apply the logical rules in proving mathematical theorems.

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Basic Definitions

An integer n is an even number
if there exists an integer k such that $n = 2k$.

An integer n is an odd number
if there exists an integer k such that $n = 2k+1$.

Direct Proofs

Goal: If P, then Q. (P implies Q)

Method 1: Write assume P, then show that Q logically follows.

Claim: If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$

Reasoning: When x=0, it is true.

When x grows, 4x grows faster than x^3 in that range.

Proof: $-x^3 + 4x + 1 = x(2-x)(2+x) + 1$

When $0 \leq x \leq 2$, $x(2-x)(2+x) \geq 0$ $\square$

Direct Proofs

The sum of two even numbers is even.

Proof

$$x = 2m,\ y = 2n$$

$$\begin{aligned} x+y &= 2m+2n \\ &= 2(m+n) \end{aligned}$$

The product of two odd numbers is odd.

Proof

$$x = 2m+1,\ y = 2n+1$$

$$\begin{aligned} xy &= (2m+1)(2n+1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn+m+n) + 1. \end{aligned}$$

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 2: Prove the ***contrapositive***, i.e. prove "not Q implies not P".

Claim: If r is irrational, then $\sqrt{r}$ is irrational.

Proof:

We shall prove the contrapositive –

"*if $\sqrt{r}$ is rational, then r is rational.*"

Since $\sqrt{r}$ is rational, $\sqrt{r} = a/b$ for some integers a,b.

So $r = a^2/b^2$. Since a,b are integers, a^2,b^2 are integers.

Therefore, r is rational. $\square$ Q.E.D.

(Q.E.D.) "which was to be demonstrated", or "quite easily done". ☺

Proving an "if and only if"

Goal: Prove that two statements P and Q are "**logically equivalent**", that is, one holds if and only if the other holds.

Example:

An integer is even if and only if the its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Method 1': Prove P implies Q **and** not P implies not Q.

Method 2: Construct a chain of if and only if statement.

Proof the Contrapositive

An integer is even if and only if its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Statement: If m is even, then m^2 is even

Proof: $m = 2k$

$m^2 = 4k^2$

Statement: If m^2 is even, then m is even

Proof: $m^2 = 2k$

$m = \sqrt{(2k)}$

??

Proof the Contrapositive

An integer is even if and only if its square is even.

Method 1': Prove P implies Q **and** not P implies not Q.

Statement: If m^2 is even, then m is even

Contrapositive: If m is odd, then m^2 is odd.

Proof (the contrapositive):

Since m is an odd number, $m = 2k+1$ for some integer k.

So $m^2 = (2k+1)^2$

$$= (2k)^2 + 2(2k) + 1$$

So m^2 is an odd number.

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof (by contradiction):

- Suppose $\sqrt{2}$ was rational.
- Choose m, n integers without common prime factors (always possible)

  such that $$\sqrt{2} = \frac{m}{n}$$

- Show that m and n are both even, thus having a common factor 2,

  a **contradiction**!

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

Proof (by contradiction):

Want to prove both m and n are even.

$$\sqrt{2} = \frac{m}{n}$$

$$\sqrt{2}n = m$$

$$2n^2 = m^2$$

so m is even.

so can assume $m = 2l$

$$m^2 = 4l^2$$

$$2n^2 = 4l^2$$

$$n^2 = 2l^2$$

so n is even.

Infinitude of the Primes

Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Assume there are only finitely many primes.

Let p_1, p_2, …, p_N be all the primes.

We will construct a number N so that N is not divisible by any p_i.

By our assumption, it means that N is not divisible by any prime number.

On the other hand, we show that any number must be divisible by *some* prime.

It leads to a contradiction, and therefore the assumption must be false.

So there must be infinitely many primes.

Infinitude of the Primes

Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Let $p_1, p_2, \ldots, p_N$ be all the primes.

Consider $p_1 p_2 \ldots p_N + 1$.

Claim: if p divides a, then p does not divide a+1.

Proof (by contradiction):

$a = cp$ for some integer c

$a+1 = dp$ for some integer d

$\Rightarrow 1 = (d-c)p$, contradiction because $p>=2$.

So none of $p_1, p_2, \ldots, p_N$ can divide $p_1 p_2 \ldots p_N + 1$, a contradiction.

This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

The Square of an Odd Integer

$$\forall \text{ odd } n, \exists m, n^2 = 8m + 1?$$

Idea 0: find counterexample.

$3^2 = 9 = 8+1$, $5^2 = 25 = 3x8+1$ …… $131^2 = 17161 = 2145x8 + 1$, ………

Idea 1: prove that $n^2 – 1$ is divisible by 8.

$n^2 – 1 = (n-1)(n+1) =$??…

Idea 2: consider $(2k+1)^2$

$(2k+1)^2 = 4k^2+4k+1$

If k is even, then both k^2 and k are even, and so we are done.

If k is odd, then both k^2 and k are odd, and so k^2+k even, also done.

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)
- An interesting example

Odd Powers 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...

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.

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

For any n>=0

Like domino effect…

This Lecture

- The idea of mathematical induction
- Basic induction proofs (e.g. equality, inequality, property,etc)
- An interesting example
- 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,

$$
\begin{aligned}
1+\cdots+r^n+r^{\boldsymbol{n+1}} &= \frac{r^{n+1}-1}{r-1}+r^{n+1} \\
&= \frac{r^{n+1}-1+r^{n+1}(r-1)}{r-1} \\
&= \frac{r^{(\boldsymbol{n+1})+1}-1}{r-1}
\end{aligned}
$$

But since $r \neq 1$ was arbitrary, we conclude (by UG), that

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

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.

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

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

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.

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

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 $P(i + 1)$:

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

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

by induction

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

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

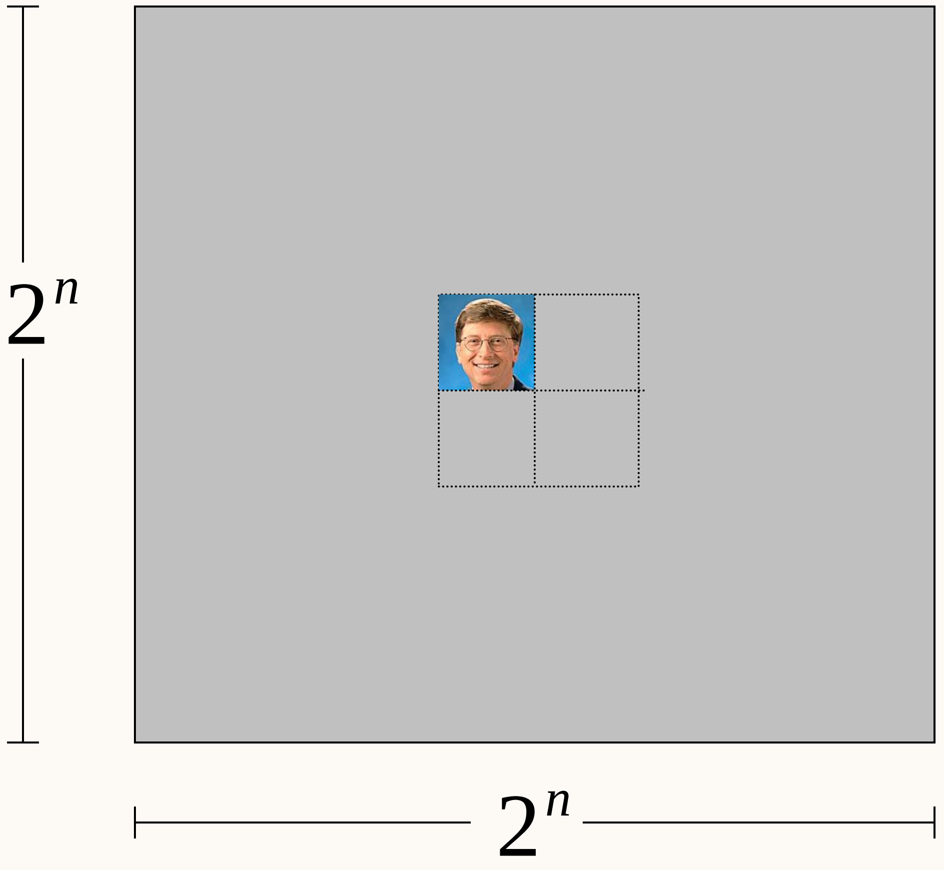
$$= \sqrt{n+1}$$

This Lecture

- The idea of mathematical induction
- Basic induction proofs (e.g. equality, inequality, property,etc)
- An interesting example
- A paradox

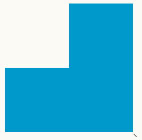
Puzzle

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

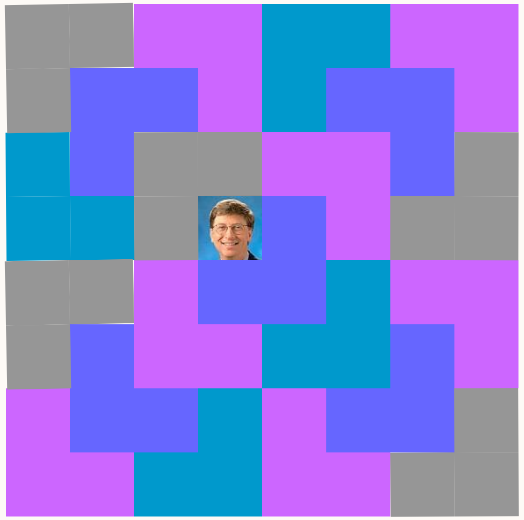


Puzzle

There are only 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 x 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)

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

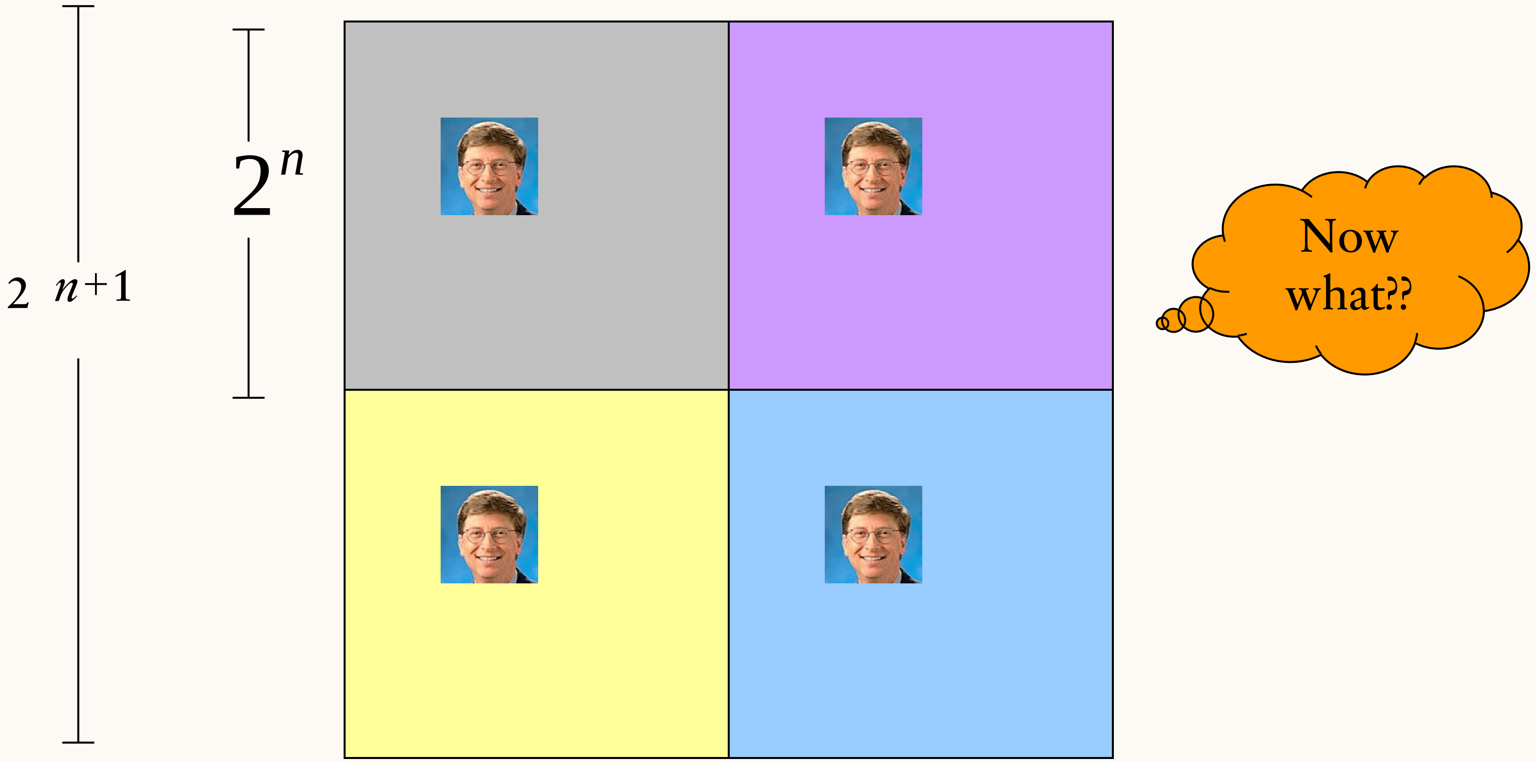
Base case: (n=0)

(no tiles needed)

Puzzle

Induction step: assume can tile 2^n x 2^n,

prove can handle 2^{n+1} x 2^{n+1}.



Puzzle

The new idea:

A stronger property

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

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

Clearly Theorem B implies Theorem.

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

Puzzle

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

Proof: (by induction on n)

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

Base case: (n=0)

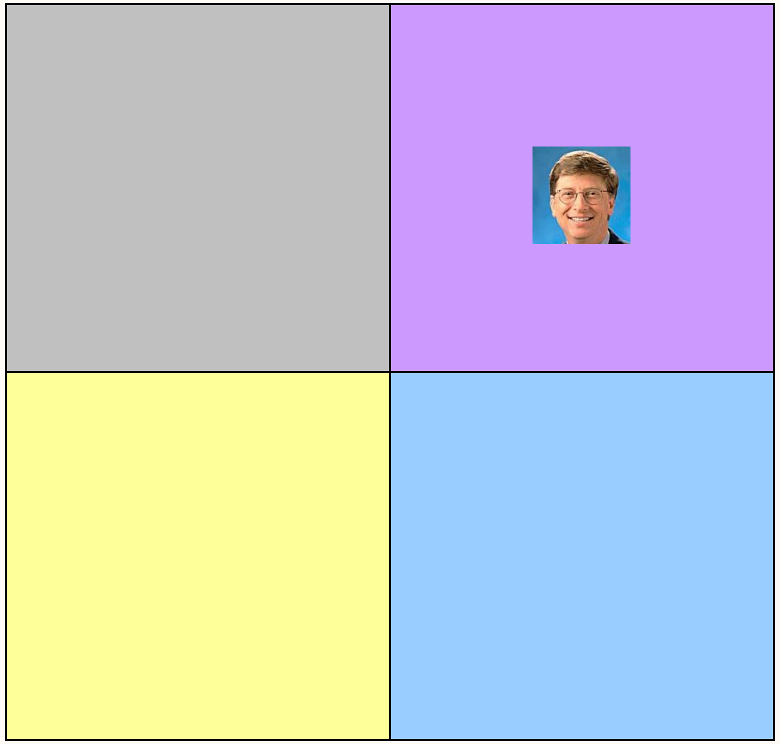
(no tiles needed)

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}.

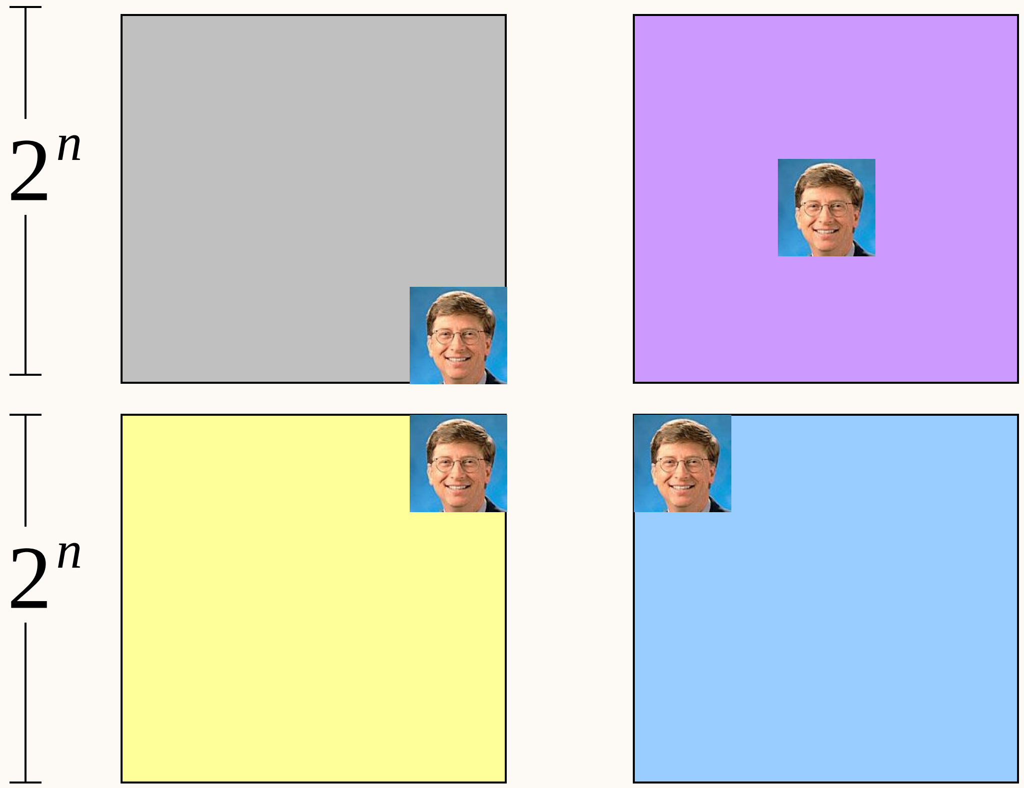


Puzzle

Induction step:

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

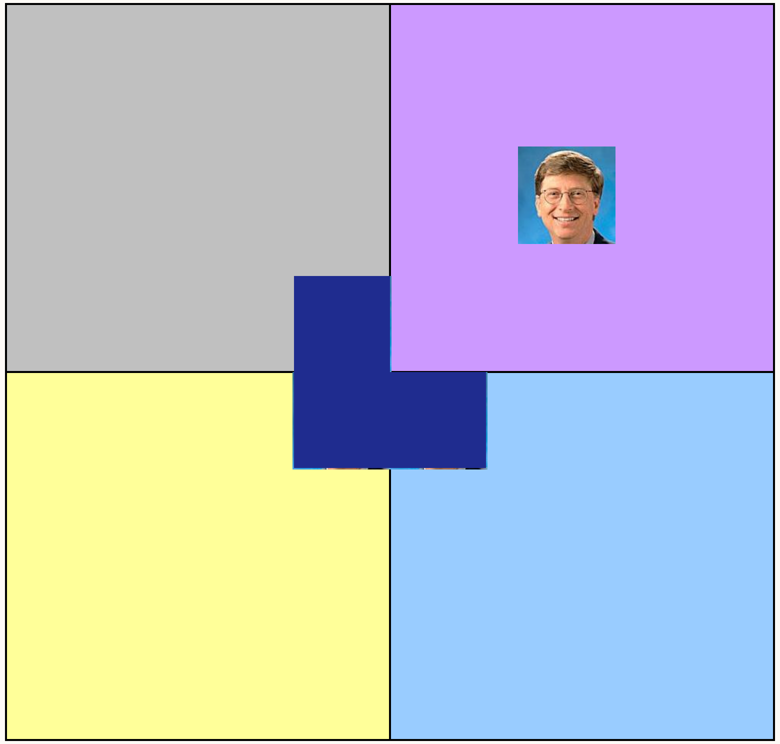
Prove we can get Bill anywhere in 2^{n+1} x 2^{n+1}.



Puzzle

Method: Now group the squares together,

and fill the center with a tile.



Done!