37181 DISCRETE MATHEMATICS

Lecture 7: induction

PLAN

- principle of mathematical induction

HOW TO PROVE

incl 0

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

?

$n = 0$ $\quad 11^0 - 4^0 = 1 - 1 = 0$

$7 \mid 0 \quad 0 = 7 \cdot 0$

$n = 1$

$11 - 4 = 7$

Lemma

If A is a set of size $n \in \mathbb{N}$, then $\mathscr{P}(A)$ has size 2^n.

? $\quad n = 0 \quad A = \emptyset \quad \mathscr{P}(\emptyset) = \{\emptyset\}$

$n = 1$

$A = \{a\}$

$\mathscr{P}(A) = \{\emptyset, \{a\}\}$ $\quad |\mathscr{P}(\emptyset)| = 1$

$|\mathscr{P}(A)| = 2^1$

PMI

Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

If

1. $P(s)$ is true
2. $P(k) \to P(k+1)$ is true

$P(1)$

$P(1) \to P(2)$

$P(2) \to P(3)$

Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

If

1. $P(s)$ is true
2. $P(k) \to P(k+1)$ is true

then $P(n)$ is true for all $n \geqslant s$.

$n \in \mathbb{N}$

(domino picture)

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$\underbrace{1 + 2 + 3 + \cdots + n}_{} = \frac{n(n+1)}{2}$$

Proof Let $P(n)$ be the statement:

" $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ ".

$P(1)$: LHS $= 1$

RHS $= \frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1$

LHS = RHS so $P(1)$ is true

Assume $p(k)$ is true for some $k \geqslant 1$.

$\rightarrow \left(1 + \ldots + k = \frac{k(k+1)}{2}\right)$ ⊛

To show: $p(k+1)$:

$$LHS = \underbrace{1 + 2 + 3 + 4 - - - - - - k}_{} + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1)$$

by Inductive Assumption ⊛

$$= (k+1)\left(\frac{k}{2} + 1\right)$$

$$= (k+1)\left(\frac{k}{2} + \frac{2}{2}\right)$$

$$= \frac{(k+1)(k+2)}{2} . = RHS.$$

thus $p(k) \rightarrow p(k+1)$.

Thus by P.M.I., $p(n)$ is true for all $n \geqslant 1$.

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

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

Proof.

$\boxed{\text{Let } P(n) \text{ be the statement that } 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.}$

Don't write

$\cancel{P(n) =}$

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

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

Proof.

Let $P(n)$ be the statement that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Thus by PMI $P(n)$ is true for all $n \geqslant 1$. $\square$

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Let $P(n)$ be statement "$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$"

$P(1)$: LHS $= 1^2 = 1$

RHS $= \frac{1(1+1)(2+1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1$

so $P(1)$ true

Assume $P(k)$ * is true for some $k \geq 1$

To show: $P(k+1)$

$$\text{LHS} = \underbrace{1^2 + 2^2 + \cdots + k^2}_{} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

by Ind assumption *

$$= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right)$$

$$= (k+1)\left(\frac{2k^2 + k + 6k + 6}{6}\right)$$

$$= (k+1)\frac{(k+2)(2k+3)}{6}$$

$$= \text{RHS}$$

So $P(k) \rightarrow P(k+1)$

So by PMI, $P(n)$ is true for all $n \geq 1$.

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof.

Let $P(n)$ be the statement that

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof.

Let $P(n)$ be the statement that

Thus by PMI $P(n)$ is true for all $n \geqslant 1$. $\square$

incl 0.

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Let $P(n)$: " $7 \mid (11^n - 4^n)$ ".

$P(0)$: $n = 0$, $11^n - 4^n = 11^0 - 4^0 = 1 - 1$

$= 0$

and $7 \mid 0$ since $0 = 7 \cdot 0$

Assume $P(k)$ true. $\exists s \in \mathbb{Z}$ so that $11^k - 4^k = 7 \cdot s$

To show: $P(k+1)$:

$$11^{k+1} - 4^{k+1}$$

$$= 11 \cdot 11^{k} - 4 \cdot 4^{k}$$

$$= (7+4)\,11^{k} - 4 \cdot 4^{k}$$

$$= 7 \cdot 11^{k} + 4\underbrace{(11^{k} - 4^{k})}_{\text{divisible by } 7}$$

$$= 7 \cdot 11^{k} + 4 \cdot 7s$$

$$= 7(11^{k} + 4s)$$

so $7 \mid 11^{k+1} + 4^{k+1}$

so $P(k+1)$ is true

so $P(k) \to P(k+1)$

so by PMI $P(n)$ true $n \geq 0$.

EG

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Proof.

Let $P(n)$ be the statement that

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Proof.

Let $P(n)$ be the statement that

Thus by PMI $P(n)$ is true for all $n \geqslant 0$. $\square$

Lemma

If A is a set of size $n \in \mathbb{N}$, then $\mathscr{P}(A)$ has size 2^n.

Proof.

Let $P(n)$ be the statement that if $|A| = n$ then $|\mathcal{P}(A)| = 2^n$.

$P(0)$: The only set of size 0 is $\emptyset$, and $\mathcal{P}(\emptyset) = \{\emptyset\}$, so $|\mathcal{P}(\emptyset)| = 1 = 2^0$ so $P(0)$ is true

~~Thus by PMI $P(n)$ is true for all $n \geq 0$.~~ □

Assume $P(k)$ is true.

To show: $P(k+1)$:

Let A be some set with $|A| = k+1$.

$A = \{a_1, a_2, a_3, \ldots, a_{k+1}\}$

Consider all the subsets:

Put all the subsets that don't contain a_1

$\emptyset$

$\{a_2\}$

$\{a_2, a_3\}$

$\vdots$

$\{a_2 a_3 \ldots a_{k+1}\}$

2^k

same number

Put all subsets do contain a_1

$\{a_1\}$

$\{a_1, a_2\}$

2^k

A

$\{\boxed{a_1}, a_2 a_3 \ldots a_{k+1}\}$

Either a subset of A contains a_1 or not all subsets of $\{\underbrace{a_2, a_3, \ldots, a_{k+1}}_{\text{only } k \text{ elements}}\}$

by Inductive assumption, there are 2^k subsets on the left side,

and 2^k on right side.

$$2^k + 2^k = 2 \cdot 2^k$$
$$= 2^{k+1}.$$

 — Please use

0, 1, ~~2~~

Lemma

For all $n \in \mathbb{N}$, if $n \geqslant \square$ then (some statement).

Proof.

Let $P(n)$ be the statement $\boxed{}$

Then $P(\square)$ is true since $\boxed{}$

Assume $P(k)$ for $k \geqslant \square$. Then

$\boxed{}$

∴ $p(k+1)$ is true

$P(k)$:

Thus by PMI $P(n)$ is true for all $n \geqslant \square$. $\square$

STRONGER VERSION (OR IS IT?)

PMI is equivalent to the following: Let $s \in \mathbb{N}$.

If

- $P(s)$ is true and
- if *for all* $s \leqslant i \leqslant n$ $P(i)$ is true, then $P(n+1)$ is true,

STRONGER VERSION (OR IS IT?)

PMI is equivalent to the following: Let $s \in \mathbb{N}$.

If

- $P(s)$ is true and
- if *for all* $s \leqslant i \leqslant n$ $P(i)$ is true, then $P(n+1)$ is true,

then $P(n)$ is true for all $n \in \mathbb{Z}, n \geqslant s$.

Lemma

For all $n \in \mathbb{N}, n > 1$ if n is not prime then some prime number p divides n.

Proof.

(Strong PMI)

Let $P(n)$ statement that if n not prime then $\exists p$ prime so that $p \mid n$.

$P(2)$: 2 is a prime so $P(2)$ is true

Assume $P(2), P(3), \ldots, P(n)$ is true.
$n \geq 2$

To show: $P(n+1)$.

If $n+1$ is prime, $P(n+1)$ is true

Else, $n+1$ is not prime, so $\exists\, a, b \in \mathbb{N}$

so that $(n+1) = a \cdot b$ $\boxed{a, b \neq 1.}$

$a, b \geq 2$

$$2 \leq a \leq n$$

So by Inductive assumption,
$P(a)$ is true

so $\exists\, p$ prime so that $p \mid a$
$a = p \cdot s$, $s \in \mathbb{N}$

$$n+1 = a \cdot b$$
$$= p \cdot s \cdot b$$

So $p \mid n+1$. So $P(n+1)$ is true.

So by SPMI

...true for all $n \geqslant 2$.

EG

Lemma

For all $n \in \mathbb{N}, n > 1$ if n is not prime then some prime number p divides n.

Proof.

Let $P(n)$ be the statement that either n is prime or some prime divides n.

$\square$

EG

$n = 0$ LHS $= 0! = 1$

RHS $= 2^{-1} = \frac{1}{2}$

Lemma

For all $n \in \mathbb{N}$, $n! \geqslant 2^{n-1}$

Proof.

Let $P(n)$ be the statement that $n! \geqslant 2^{n-1}$

~~$P(0)$ is true since $0! = 1$ and $2^{-1} = \frac{1}{2}$~~

$P(1)$ is true $1! \geqslant 2^{1-1} = 1$

Assume $P(k)$ $*$ is true, $k \geqslant 1$

To show $P(k+1)$:

$$(k+1)! = (k+1)\,k!$$

$$\geqslant (k+1)\,2^{k-1}$$

□

(start at 0)

by Inductive Assumption ⊛

$$\geq (1+1)\,2^{k-1}$$ since $k \geq 1$

$$= 2 \cdot 2^{k-1} = 2^{k}$$

$$= 2^{(k+1)-1}$$

So $p(k+1)$ is true.

So by PMI, $p(n)$ is true for all $n \geq 1$

and we also showed it is true for $n = 0$,

So $p(n)$ is true for $n \geq 0$.

EG

Consider the statement: For all $n \in \mathbb{N}$, $n! \geqslant 3^{n-1}$.

Is this true? Is it true for all $n \geqslant ??$

$n=0$ ✓

$n=1$: $1! = 1$, $3^{0} = 1$ ✓

$n=2$: $2! = 2$, $3^{2-1} = 3$

$n=3$: $3! = 6$, $3^{3-1} = 9$

$4! = 24$, $3^3 = 27$

Proof.

Let $P(n)$ be the statement that

$n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$

$3 \cdot 3 \cdot 3 \cdots 3 \cdot 3 \cdot 1$

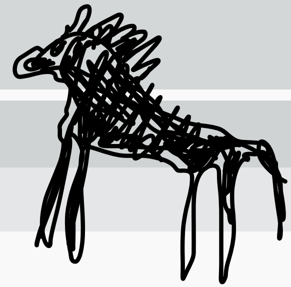
□

(start at ??)

EG

Lemma

All horses are black.



Proof:

If I have $n \in \mathbb{N}$ horses, then they are all black.

$n = 0$

I have no horses

Which is true:

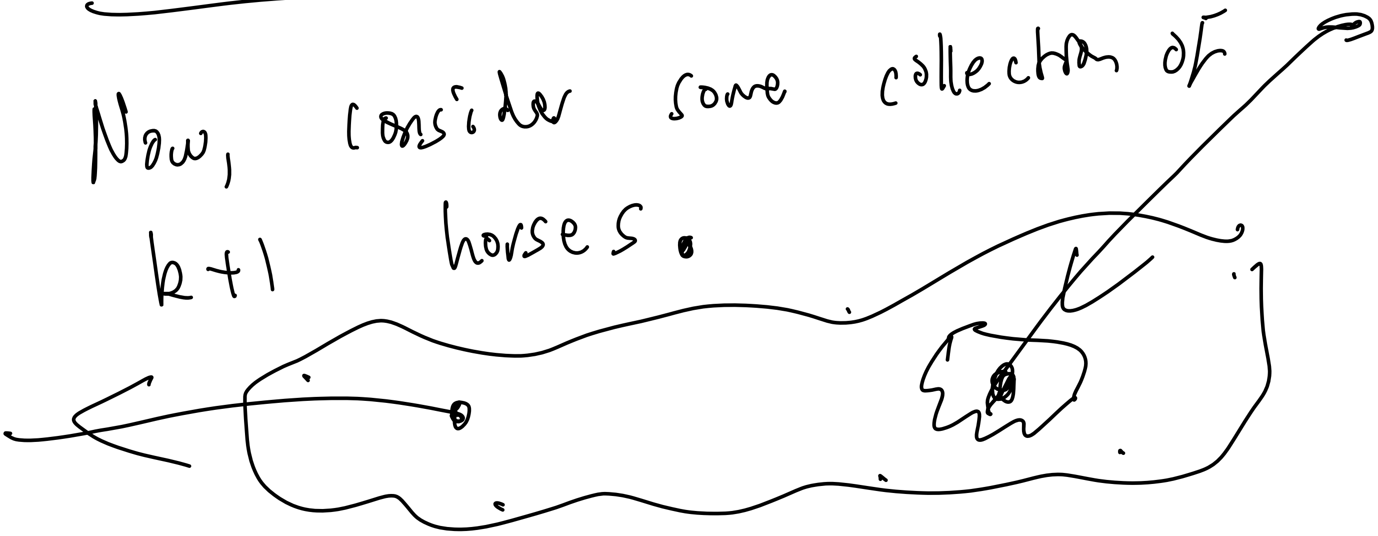
They are all black

NOT $\exists$ one horse that is not black.

So $P(0)$ is true.

Assume (for induction) that for any collection of $k \geq 0$ horses, $k \in \mathbb{N}$, they are all black.

Now, consider some collection of $k+1$ horses.



Remove one horse

→ you get k horses left.

By Ind. Assumption, these horses are all black.

Put that horse back
and remove another horse

leaves k horses

→ ~~new~~ that horse must be black horse.

by PMI, all horses are black.

EG

Lemma

All horses are black.

Proof.

Let $P(n)$ be the statement that

$\square$

NEXT

Next lecture:

- application of induction: correctness of computer code/algorithms
- WOP and PMI

Important to gets lots of practice doing proofs by induction.