Lecture Notes: Week 4

Set Theory & Induction

These notes will differ somewhat from the last week's notes in that we are gravitating to the more standard mathematical style of "definition, theorem, proof, repeat." There will be a minor detour away from this when we come across the need for induction. So without further ado ...

NOTATION (Recall)

Often, capital letters denote sets and small letters denote elements.

$x \in A$ means, "x is an element of the set A."

(new) $x \notin A$ means, "x is not an element of A."

$A = \{x_1, x_2, \ldots\}$ means A consists of $x_1, x_2, \ldots$

$A = \{x \mid x \text{ has property } P\}$ means A consists of all x having property P.

interchangeable

(new) $A = \{x : x \text{ has property } P\}$ means A consists of all x having property P.

EXAMPLES (recall)

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all examples of set.

(see last week for definitions)

DEF For sets A and B,

(1) A is <u>equal</u> to B means A and B consist of the same elements, i.e. $x \in A$ if and only if $x \in B$.

We write $A = B$.

(2) A is a <u>subset</u> of B means that if $x \in A$, then $x \in B$.

We write $\underbrace{A \subset B}$, or $\underbrace{B \supset A}$.

$$\begin{array}{cc} \downarrow & \downarrow \\ \text{"A is a subset of B"} & \text{"B contains A"} \\ \downarrow & \downarrow \\ x \in A \Rightarrow x \in B & x \in B \Leftarrow x \in A \end{array}$$

EXAMPLES The set $\{1, 2\}$ is a subset of $\mathbb{Z}$.

The set $\{1, \sqrt{2}\}$ is <u>not</u> a subset of $\mathbb{Q}$.

THM 1 Let A and B be sets. $A = B$ if and only if $A \subset B$ and $B \subset A$.

proof: We first show that if $A = B$, then $A \subset B$ and $B \subset A$. Assume $A = B$. Then $x \in A$ if and only if $x \in B$, by definition. If $x \in A$, then $x \in B$ means $A \subset B$, and conversely, if $x \in B$, then $x \in A$ means $B \subset A$. Thus, $A = B$ implies $A \subset B$ and $B \subset A$.

Now, we show the converse: if $A \subset B$ and $B \subset A$, then $A = B$. Assume $A \subset B$ and $B \subset A$. By definition, this means if $x \in A$, then $x \in B$ and if $x \in B$, then $x \in A$. Thus, $x \in A$ if and only if $x \in B$, so we can conclude $A = B$. $\blacksquare$

REMARK In a set, neither order nor repitition matter. In other words, $\{x, y\} = \{y, x\} = \{x, y, y\}$.

RECALL The empty set, i.e. the set with no elements, is denoted $\emptyset$.

Homework Question 1

Show that $\emptyset$ is a subset of any set X.

THM 2 If $A \subset B$ and $B \subset C$, then $A \subset C$.

proof: Assume $A \subset B$ and $B \subset C$. Then by definition $x \in A$ implies $x \in B$, which in turn implies $x \in C$. Thus, any $x \in A$ is an $x \in C$, so $A \subset C$. $\boxtimes$

Homework Question 2

Prove that if $A \subset B \subset C$ and $A = C$, then $A = B = C$.

DEF Let A and B be sets. We say A is a proper subset of B if $A \subset B$ but $A \neq B$. We denote this $A \subsetneq B$.

EXAMPLES ϕ is a proper subset of any non-empty! set. More interestingly,

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

Why?
- $0 \in \mathbb{Z}$, but $0 \notin \mathbb{N}$.
- $\frac{1}{2} \in \mathbb{Q}$, but $\frac{1}{2} \notin \mathbb{Z}$
- $\sqrt{2} \in \mathbb{R}$, but $\sqrt{2} \notin \mathbb{Q}$
- $i \in \mathbb{C}$, but $i \notin \mathbb{R}$

DEF For any two sets A and B,

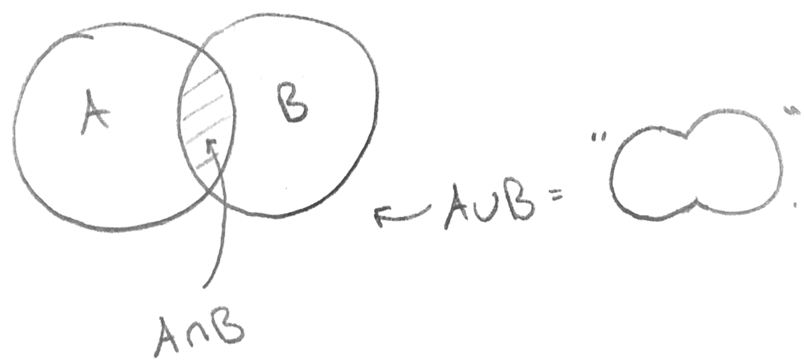
1) the <u>union</u> of A and B, denoted $A \cup B$, is the set

$$\{x \mid x \in A \text{ or } x \in B\},$$

2) the <u>intersection</u> of A and B, denoted $A \cap B$, is the set

$$\{x \mid x \in A \text{ and } x \in B\}.$$

PICTURE



THM 3 For any three sets A, B, C

(1) $A \cup B = B \cup A$ and $A \cap B = B \cap A$ (commutative)

(2) $A \cup (B \cup C) = (A \cup B) \cup C$

and $A \cap (B \cap C) = (A \cap B) \cap C$ (associative)

(3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

and $A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$

(distributive)

proof: The proof of (1) and (2) are left to ~~the~~ the reader. (annoying, right??! When this happens, sketch the ideas and make sure you believe the statement really is true!)

For (3), assume $x \in A \cap (B \cup C)$.

- $x \in A \cap (B \cup C)$ if and only if $x \in A$ and $x \in B \cup C$, by definition of the intersection.

  $\left(x \in A \cap (B \cup C) \iff x \in A \text{ and } x \in B \cup C \right)$

- $x \in A$ and $x \in B \cup C$ if and only if $[x \in A]$ and $[x \in B \text{ or } x \in C]$, by definition of the union.

  $\left(x \in A \text{ and } x \in B \cup C \iff x \in A \text{ and } [x \in B \text{ or } x \in C] \right)$

- $x \in A$ and $[x \in B \text{ or } x \in C]$ if and only if $[x \in A \text{ and } x \in B]$ or $[x \in A \text{ and } x \in C]$, by properties of "and" and "or" from week 1.

  $\left(x \in A \text{ and } [x \in B \text{ or } x \in C] \iff [x \in A \text{ and } x \in B] \text{ or } [x \in A \text{ and } x \in C] \right)$

- $[x \in A \text{ and } x \in B]$ or $[x \in A \text{ and } x \in C]$ if and only if $x \in A \cap B$ or $x \in A \cap C$, by definition of the intersection.

  $\left([x \in A \text{ and } x \in B] \text{ or } [x \in A \text{ and } x \in C] \iff x \in A \cap B \text{ or } x \in A \cap C. \right)$

- Finally, $x \in A \cap B$ or $x \in A \cap C$ if and only if $x \in (A \cap B) \cup (A \cap C)$.

  $(x \in A \cap B \text{ or } x \in A \cap C \iff x \in (A \cap B) \cup (A \cap C))$.

  Since each statement is an if and only if statement, we have proven equality of sets.

A similar argument works for the right equation in (3).

$\boxtimes$

Here is a sketch of the ideas in the proof:

$$
\begin{aligned}
x \in A \cap (B \cup C) &\iff x \in A \text{ and } x \in B \cup C \\
&\iff x \in A \text{ and } (x \in B \text{ or } x \in C) \\
&\iff (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\
&\iff x \in A \cap B \text{ or } x \in A \cap C \\
&\iff x \in (A \cap B) \cup (A \cup C).
\end{aligned}
$$

this is okay for set theory proofs, provided you justify each line!

DEF For any collection $\mathcal{A}$ of sets (finite or otherwise!),

$$\bigcup_{A\in\mathcal{A}} A := \{x : x\in A \text{ for some } A\in\mathcal{A}\}$$

$$\bigcap_{A\in\mathcal{A}} A := \{x : x\in A \text{ for all } A\in\mathcal{A}\}$$

THM 4 Let $\mathcal{A}$ be a collection of sets and let B be any set. We can generalize (3) from THM 3 as follows.

$$(1) \quad \left(\bigcup_{A\in\mathcal{A}} A\right)\cap B = \bigcup_{A\in\mathcal{A}} (A\cap B)$$

$$(2) \quad \left(\bigcap_{A\in\mathcal{A}} A\right)\cup B = \bigcap_{A\in\mathcal{A}} (A\cup B)$$

Sketch of proof: $x\in \left(\bigcup_{A\in\mathcal{A}} A\right)\cap B \Leftrightarrow x\in\left(\bigcup_{A\in\mathcal{A}} A\right)$ and $x\in B$

$\Leftrightarrow x\in\{y : y\in A \text{ for some } A\in\mathcal{A}\}$ and $x\in B$

$\Leftrightarrow x\in\{y : y\in A \text{ for some } A\in\mathcal{A} \text{ and } y\in B\}$

$\Leftrightarrow x\in\{y : y\in A \text{ and } y\in B \text{ for}$

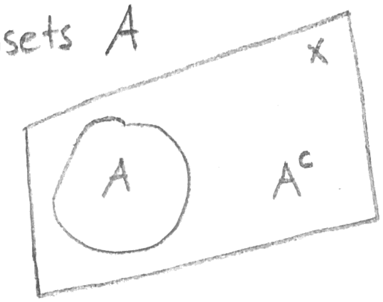
some $A \in \mathcal{A}\}$

$$\iff x \in \{y : y \in A \cap B \text{ for some } A \in \mathcal{A}\}$$

$$\iff x \in \bigcup_{A \in \mathcal{A}} (A \cap B).$$

Similar for (2). $\blacksquare$

DEF For a while, we will consider only subsets A of some fixed container set X.



For $A \subset X$, the complement of A relative to X, denoted $X \setminus A$ or $\underbrace{A^c \text{ or } A'}$, is

$$X \setminus A = \{x \in X : x \notin A\}$$

(*) only use these if X is clear from the context! (*)

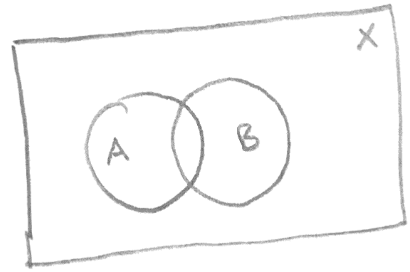
THM 5 (DeMorgan's Rules)

For $A, B \subset X$,

(1) $(A \cup B)^c = A^c \cap B^c$

(2) $(A \cap B)^c = A^c \cup B^c$

(3) $(A^c)^c = A$



Sketch of proof: (1) Assume $A, B \subset X$, let

$x \in (A \cup B)^c$, by which we mean

$x \in X \setminus (A \cup B)$.

(Let $x \in X$)

$x \in (A \cup B)^c \iff x \notin A \cup B$, by definition of the complement

$\iff x \notin A$ and $x \notin B$, by negation of or.

$\iff x \in A^c$ and $x \in B^c$, by def. of complement.

$\iff x \in A^c \cap B^c$, by definition of intersection.

Homework Question 3

Prove (2) similarly.

---

(3) Let $x \in (A^c)^c$

$x \in (A^c)^c \iff x \notin A^c$, by definition of complement

$\iff x$ is not not in A, by def. of complement

$\iff x \in A$, since "not not" is a double negation.

$\boxtimes$

We can also prove (2) by using (1) and (3), once we have proven them.

Notice: $\left(A^c \cup B^c\right)^c \underset{\text{by (1)}}{=} (A^c)^c \cap (B^c)^c \underset{\text{by (3)}}{=} A \cap B$

Thus, $(A \cap B)^c = \left(\left(A^c \cup B^c\right)^c\right)^c \underset{\text{by (3)}}{=} A^c \cup B^c$.

Homework Question 4

Prove the right-most equation in THM3 (3) by starting with the left-most equation in THM3 (3), applied to A^c, B^c, C^c (assume $A \subset X$, $B \subset X$, $C \subset X$), then use DeMorgan's Rules.

(We can do this because we did not need THM3 to prove DeMorgan's Rules!)

Homework Question 5

Prove that for each collection $\mathcal{a}$ of subsets of a set X,

(1) $\left(\bigcup_{A \in \mathcal{a}} A\right)^c = \bigcap_{A \in \mathcal{a}} (A^c)$ $\quad$ (i.e. $X \setminus \left(\bigcup_{A \in \mathcal{a}} A\right) = \bigcap_{A \in \mathcal{a}} (X \setminus A)$)

and

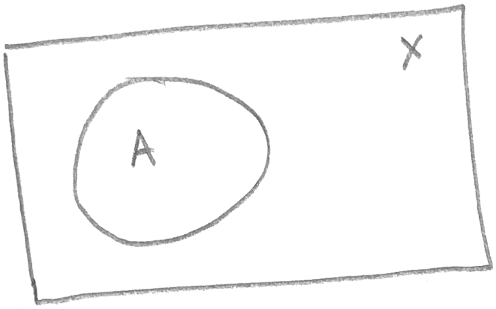
(2) $\left(\bigcap_{A \in \mathcal{a}} A\right)^c = \bigcup_{A \in \mathcal{a}} (A^c)$ $\quad$ (i.e. $X \setminus \bigcap_{A \in \mathcal{a}} A = \bigcup_{A \in \mathcal{a}} (X \setminus A)$)

THM 6 For each subset $A \subset X$,

(1) $\emptyset \cup A = A$ and $\emptyset \cap A = \emptyset$

(2) $X \cup A = X$ and $X \cap A = A$

(3) $\emptyset^c = X$ and $X^c = \emptyset$



Sketch of proof:

(1) $x \in \emptyset \cup A \iff x \in \emptyset$ or $x \in A$

$\iff x \in A$, since $x \notin \emptyset$

and

$x \in \emptyset \cap A \iff x \in \emptyset$ and $x \in A$, which is false since $x \notin \emptyset$.

Thus, there is no $x \in \emptyset \cap A$, so we can conclude by definition of the empty set that

$$\emptyset \cap A = \emptyset.$$

(2) $x \in X \cup A \iff x \in X$ or $x \in A$

$\iff x \in X$, since $x \in A \Rightarrow x \in X$. $(A \subset X)$

and

$x \in X \cap A \iff x \in X$ and $x \in A$

$\iff x \in A$, since $x \in A \Rightarrow x \in X$ $(A \subset X)$

$(x \notin X \Rightarrow x \notin A)$.

(3) $x \in \emptyset^c = X \setminus \emptyset \iff x \in X$ and $x \notin \emptyset$

$\iff x \in X$, since it is alway true that $x \notin \emptyset$ by definition of the empty set.

and

$x \in X^c = X \setminus X \iff x \in X$ and $x \notin X$,

which is always false, so there is no $x \in X^c$. Thus, by definition, $X^c = \emptyset$.

$\boxtimes$

DEF Sets A and B are disjoint if $A \cap B = \emptyset$. In this case, we write $A \cup B = A \sqcup B$, or sometimes as $A + B$.

NOTATION If A is a finite set, $|A|$ denotes the number of elements in A. For example, $|\{1,2\}| = 2$.

DEF For any set X, $\mathcal{P}(X)$ denotes the set of all subsets.

EXAMPLE For $X = \{1,2\}$, $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Questions ① How many elements does $\emptyset$ have?

None! so $|\emptyset| = 0$

② How many subsets does $\emptyset$ have?

Only one! $\emptyset$ itself, so $|\mathcal{P}(\emptyset)| = 1$.

③ How many elements does $\{x\}$ have? Subsets?

One element : x

two subsets : $\emptyset, \{x\}$

so, $\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}$ and $|\mathcal{P}(\{x\})| = 2$.

THM 7 Let X be a finite set. If $|X| = n$, then $|\mathcal{P}(X)| = 2^n$.

proof: ... oof. We need a new proof technique.

- - - - - - - - - - - - - - - -

For a moment, we will depart from the classical "definition, theorem, proof" style to talk a bit about a new proof technique.

Induction

Notice that in the Theorem above (THM 7), we need to prove that something is true for all non-negative integers. In other words, we need to prove the statement for the empty set, a one-element set, a two-element set, etc.

Sometimes, it is very difficult to prove such a statement directly starting with an arbitrary n.

Fortunately, there is an idea that can help us out. These integers above come in a sequence (0, 1, 2, 3, ...

or 1, 2, 3, ...). In other words, give an integer n, it will have a successor $(n+1)$. In reference to the previous theorem, just notice that we need to prove the statement for a two-element set <u>and</u> a $(2+1)$-element set (its successor). We can use this structure to prove it: if we show it is true for the empty set (first element in the sequence), then we show that *if* the statement is true for an n-element set, then it must be true of the $(n+1)$-element set, we would be done! Why? Because if it is true of the first element, then the implication

"If true of an n-element set,
then true of an $(n+1)$-element set,"

means it is true of the $(0+1)$-element set. Applying the implication again, we see it is true of the $(1+1)$-element set, then $(2+1)$-element set, etc.

In other words, it would be true of any finite element set! This procedure is known as induction.

$\boxed{\text{The Induction Principle}}$

Suppose that $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers $1, 2, 3, \ldots$ if

We call this our base case

(i) $P(1)$ is true, and

(ii) $P(k)$ true implies $P(k+1)$ is true for all positive integers k.

We call this the inductive hypothesis!

(You get to assume it!)

<u>REMARK</u> It can be helpful to think of induction as toppling dominoes. Once you know a statement is true for the first thing in a sequence, and you know (ii) holds, it is like using the first domino to knock down an entire sequence of dominoes.

REMARK It doesn't really matter where we start the sequence. However, once we apply the induction principle, only things coming after your starting point will be true.

Let's work an example.

EXAMPLE

looks true!

n	1, 2, 3, ...
2^n	2, 4, 8, ...

For all positive integers n, $n \le 2^n$.

proof: We use induction.

we are showing (i) in the induction principle

Base Case: For our $\boxed{\text{base case}}$, let $n=1$. Notice that $1 \le 2^1$, so the statement holds for $n=1$.

We are showing (ii).

Inductive Step: Now we want to use the $\boxed{\text{inductive hypothesis}}$. We assume the statement is true for k, in other words, $k \le 2^k$. (This is the inductive hypothesis!) We want to show that this implies $k+1 \le 2^{k+1}$.

Let's start with $k+1$.

(*) Must point out where you use this!

$$\underbrace{k}+1 \leq \underbrace{2^k}+1 \text{, by the inductive hypothesis!}$$

$$\leq 2^k + \underbrace{k} \text{, since } k \geq 1$$

$$\leq 2^k + 2^k \text{, by the inductive hypothesis again!}$$

$$= 2 \cdot 2^k$$

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

Thus, we see that $k+1 \leq 2^{k+1}$, as desired.

This completes the inductive step, so we are done!

☑

Let's try one more.

<u>EXAMPLE</u>

The sum of the first n positive integers, $\sum_{i=1}^{n} i$, is equal to $\frac{1}{2}n(n+1)$.

<u>proof</u>: We use induction.

Base Case: Let $n=1$. Then $\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1$.

Notice: $\frac{1}{2}n(n+1) = \frac{1}{2}\cdot 1(1+1) = 1$

So we see that $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$ for $n=1$, which completes the base case.

Inductive Step: Assume the statement is true for the first k positive integers (inductive hypothesis). Then we will show that it is true for the first $k+1$.

The sum of the first $k+1$ integers is

remember $\sum_{i=1}^{5} i = 1+2+3+4+5$

just sum over each i

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

we pull the last integer out of the sum

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

by the inductive hypothesis.

Now, notice

$$\underbrace{\frac{1}{2}k(k+1) + (k+1)}_{\text{factor out } k+1} = (k+1)\underbrace{\left(\frac{1}{2}k + 1\right)}_{\text{factor out } \frac{1}{2}}$$

We showed that the sum of the first $\underset{\sim}{k+1}$ positive integers is $\frac{1}{2}(k+1)(k+2)$

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

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

which is the desired formula. This completes the inductive step, so the proof is complete.

REMARK (Question?)

Is it clear how induction is like toppling dominoes?

Before we return to set theory, we need to cover one more idea. That is the strong induction principle:

Strong Induction Principle

Suppose that $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers n if

(i) $P(1)$ is true (Base Case!)

(ii) [$P(m)$ holds true for all $m \leq k$] implies $P(k+1)$ is true. (Inductive step)

It turns out that this is equivalent to regular induction, but you may use this instead if you need. The only real difference is that instead of assuming the statement is true for k and showing the statement is true for $k+1$, we can assume the statement is true for $1, 2, 3, \ldots,$ and k, then show the statement is true for $k+1$.

Here is an example. If we assume that every integer $n \geq 2$ has a smallest prime divisor, we can use strong induction to prove the Fundamental Theorem of Arithmetic:

EXAMPLE For all integers $n \geq 2$, n can be expressed as the product of prime numbers.

Sketch: We use induction.

Base Case: Let $n=2$. 2 is a prime, so n is expressible as a product of primes.

Inductive step: Assume the statement is true of all integers $n = 2, 3, \ldots, k$.

If $k+1$ is prime, we are done. Otherwise $k+1$ has a smallest prime divisor p so we can write

$$(k+1) = pN$$

for some integer N. Since $N < K$ (because $p \geq 2$), we can apply the inductive hypothesis: N is expressible as a product of primes. We can write $N = p_1 p_2 p_3 \cdots p_\ell$ for some primes $p_1, p_2, \ldots, p_\ell$ (where some might repeat!). Thus,

$$(k+1) = p \cdot p_1 p_2 p_3 \cdots p_\ell,$$

and we see $k+1$ is expressible as a product of primes, as desired. ∎

Great! So ... now we will return to Set Theory.

Homework Question 6

Prove THM 7. Hint: You can express an $n+1$-element A set as a disjoint union of an n-element B and a 1-element set $\{a\}$ (where a is the one element). In other words $A = B \sqcup \{a\}$. Now, let $X \subset A$ be an arbitrary subset of A. We have two cases:

(1) $a \notin X$, in which case $X \subset B$.

or

(2) $a \in X$, in which case $X = C \sqcup \{a\}$, where $C \subset B$.

For your inductive step, count the number of subsets in Case 1 and Case 2 separately, and sum them up.