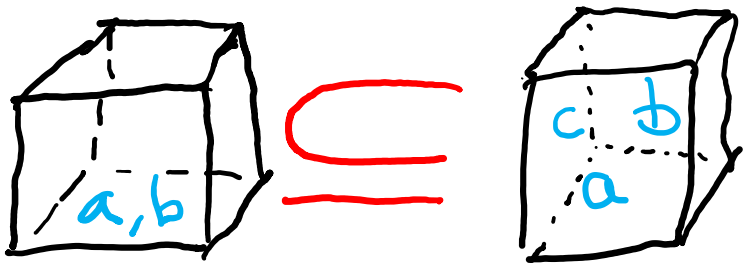
Announcements:

- Email later today w/return to in-person plans & questions for you.
- We reorganized/added a few links on the resources tab of the webpage.
- HW3 due tonight, HW4 out tonight.



Sets

CSE 311 Winter 22
Lecture 10

Today

Is a laundry list day – everything you ever wanted to know about sets.

By the end, we'll get to do two proofs.

No breakout rooms today ☹

Sets

A set is an **unordered** group of **distinct** elements.

We'll always write a set as a list of its elements inside {curly, brackets}.

Variable names are capital letters, with lower-case letters for elements.

$|A| = 2$. "The size of A is 2." or "A has cardinality 2."

$A = \{\text{curly, brackets}\}$

$B = \{0,5,8,10\} = \{5,0,8,10\} = \{0,0,5,8,10\}$

$C = \{0,1,2,3,4,\ldots\}$

$|B| = 4$

Sets

Some more symbols:

$a \in A$ ("a is in A" or "a is an element of A") means a is one of the members of the set.

For $B = \{0,5,8,10\}$, $0 \in B$.

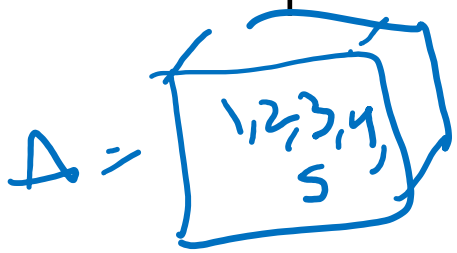
$A \subseteq B$ (A is a subset of B) means every element of A is also in B.

For $A = \{1,2\}$, $B = \{1,2,3\}$ $A \subseteq B$

Sets

Be careful about these two operations:

If $A = \{1,2,3,4,5\}$



$\{1\} \subseteq A$, but $\{1\} \notin A$

$\in$ asks: is this item in that box?

$\subseteq$ asks: is everything in this box also in that box?

Try it!

Let $A = \{1,2,3,4,5\}$

$B = \{1,2,5\}$

Is $A \subseteq A$? Yes!

Is $B \subseteq A$? Yes

Is $A \subseteq B$? No

Is $\{1\} \in A$? No

Is $1 \in A$? Yes

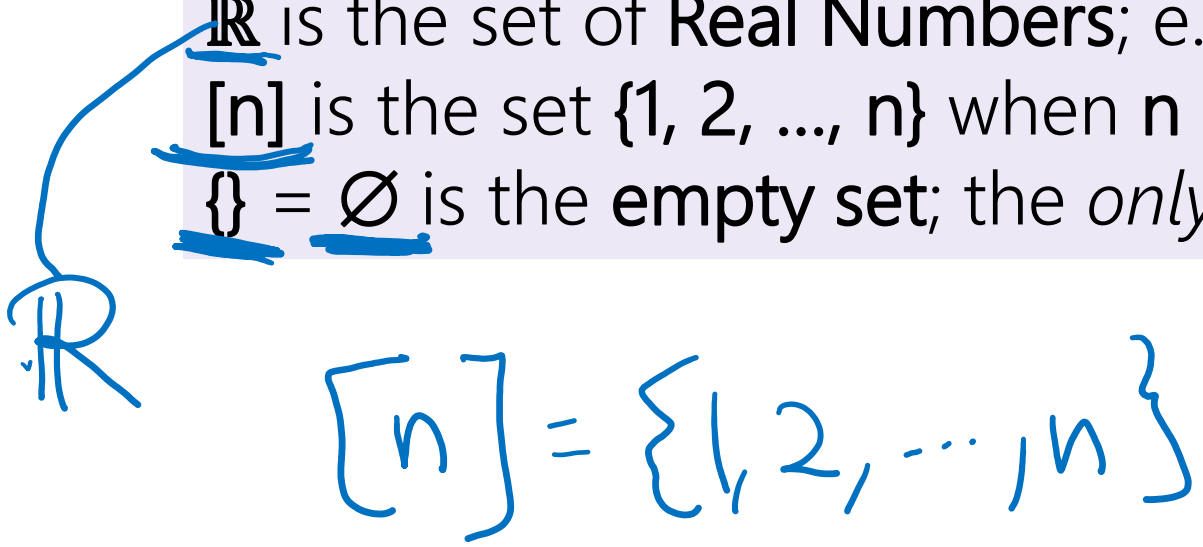
$\{1\} \in \{\{1\}, 2, 3\}$

$S = \{\text{"abc"}, 1, \pi, \{1\}\}$

$\{1\} \subseteq A$

Some old friends (and some new ones)

$\mathbb{N}$ is the set of **Natural Numbers**; $\mathbb{N}$ = {0, 1, 2, …}
$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z}$ = {…, -2, -1, 0, 1, 2, …}
$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48
$\mathbb{R}$ is the set of **Real Numbers**; e.g. 1, -17, 32/48, π, $\sqrt{2}$
[n] is the set **{1, 2, …, n}** when **n** is a positive integer
{} = ∅ is the **empty set**; the *only* set with no elements



Definitions

$A \subseteq B$ ("A is a subset of B") iff every element of A is also in B.

$$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$$

$A = B$ ("A equals B") iff A and B have identical elements.

$$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$$

Set Builder Notation

Sometimes we want to give a property and say "everything with that property is in the set (and nothing else is in the set)."

$A = \{x : \texttt{Even}(x)\}$

"The set of all x such that x is even."

In general $\{variable : Condition(variable)\}$

Sometimes the colon is replaced with |

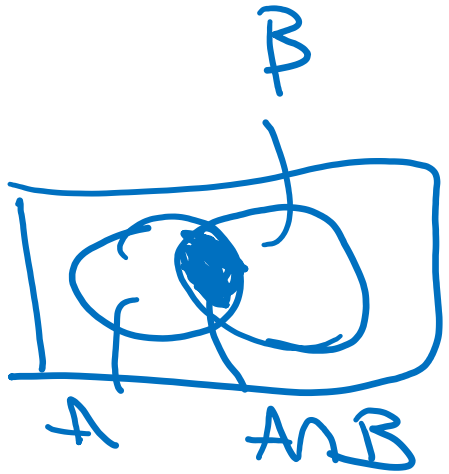
What do we do with sets?

We combined propositions with $\vee, \wedge, \neg$.

We combine sets with $\cap$ [intersection], $\cup$, [union] $\bar{}$ [complement]

$$A \cup B = \{x : x \in A \vee x \in B\}$$

$$A \cap B = \{x : x \in A \wedge x \in B\}$$



$$\bar{A} = \{x : x \notin A\}$$

$A^c = \{x : x \notin A\}$

That's a lot of elements…if we take the complement, we'll have some "universe" $\mathcal{U}$, and $\bar{A} = \{x : x \in U \wedge x \notin A\}$
It's a lot like the domain of discourse.

A proof!

What's the analogue of DeMorgan's Laws...

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

A proof!

What's the analogue of DeMorgan's Laws...

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

Let x be an arbitrary element of $\bar{A} \cap \bar{B}$.

By definition of $\cap$ and complement, $x \notin A \wedge x \notin B$.

Applying DeMorgan's Law, we get that it is not the case that $x \in A \vee x \in B$.

That is, x is in the complement of $A \cup B$, as required.

$\neg(x \in A \vee x \in B)$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Let x be an arbitrary element of $\overline{A \cup B}$.

By definition, x is not an element of $A \cup B$. That is, $\neg(x \in A \vee x \in B)$

Applying DeMorgan's Law, we get: $x \notin A \wedge x \notin B$

By definition of $\cap$ and complement, we get $x \in \bar{A} \cap \bar{B}$

Proof-writing advice

When you're writing a set equality proof, often the two directions are nearly identical, just reversed.

It's very tempting to use that $x \in A \leftrightarrow x \in B$ definition.

Be VERY VERY careful. It's easy to mess that up, at every step you need to be saying "if and only if."

More connectors!

$A \setminus B$ "A minus B"

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

$A \oplus B$ "XOR" (also called "symmetric difference")

$$A \oplus B = \{x : x \in A \oplus x \in B\}$$

Two claims, two proof techniques

Suppose I claim that for all sets A, B, C: $A \cap B \subseteq C$

That…doesn't look right.

How do you prove me wrong?

Want to show: $\exists A, B, C: A \cap B \nsubseteq C$

Consider $A = \{1,2,3\}$, $B = \{1,2\}$, $C = \{2,3\}$, then $A \cap B = \{1,2\}$, which is not a subset of C.

Proof By [Counter]Example

To prove an existential statement (or disprove a universal statement), provide an example, and demonstrate that it is the needed example.

You don't have to explain where it came from! (In fact, you **shouldn't)**

Computer scientists and mathematicians like to keep an air of mystery around our proofs.

(or more charitably, we want to focus on just enough to believe the claim)

Proof By Cases

Let $A = \{x : \texttt{Prime}(x)\}$, $B = \{x: \texttt{Odd}(x) \vee \texttt{PowerOfTwo}(x)\}$

Where $\texttt{PowerOfTwo}(x) \coloneqq \exists c(\texttt{Integer}(c) \wedge x = 2\hat{}c)$

Prove $A \subseteq B$

We need two different arguments – one for 2 and one for all the other primes…

Proof By Cases

$\forall x (x \in A \rightarrow x \in B)$

Let x be an arbitrary element of A.

We divide into two cases.

Case 1: x is even

If x is even and an element of A (i.e. both even and prime) it must be 2.

So it equals 2^c for $c = 1$, and thus is in B by definition of B.

Case 2: x is odd

Then $x \in B$ by satisfying the first requirement in the definition of B.

In either case, $x \in B$. Since an arbitrary element of A is also in B, we have $A \subseteq B$.

Proof By Cases

Make it clear how you decide which case your in.

It should be obvious your cases are “exhaustive”

Reach the same conclusion in each of the cases, and you can say you’ve got that conclusion no matter what (outside the cases).

Advanced version: sometimes you end up arguing a certain case “can’t happen”

Two More Set Operations

Given a set, let's talk about it's powerset.

$\mathcal{P}(A) = \{\text{X: X is a subset of } A\}$

The powerset of A is the **set** of all subsets of A.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

$\subseteq \{1,2\}$

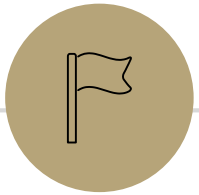
Two More Set Operations

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Called "the Cartesian product" of A and B.

$\mathbb{R} \times \mathbb{R}$ is the "real plane" ordered pairs of real numbers.

$$\{1,2\} \times \{1,2,3\} = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$$



Number Theory

Divides

For integers $\mathbf{x, y}$ **we say** $x|y$ ("x divides y") iff there is an integer z such that $zx = y$.

"x is a divisor of y" or "x is a factor of y" means the same thing as x divides y.

"The small number goes first"

Divides

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Which of these are true?

$2|4$ $\quad$ $4|2$ $\quad$ $2|-2$

$5|0$ $\quad$ $0|5$ $\quad$ $1|5$

Why Number Theory?

Applicable in Computer Science

"hash functions" (you'll see them in 332) commonly use modular arithmetic
Much of classical cryptography is based on prime numbers.

More importantly, a great playground for writing English proofs.

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

Remember when non integers were still secret, you did division like this?

q is the "quotient"
r is the "remainder"

Unique

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

"unique" means "only one"....but be careful with how this word is used.

r is unique, **given** a, d. – it still depends on a, d but once you've chosen a and d

"unique" is not saying $\exists r \forall a, d \quad P(a, d, r)$
It's saying $\forall a, d \exists r [P(a, d, r) \wedge [P(a, d, x) \rightarrow x = r]]$

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

The q is the result of `a/d` (integer division) in Java

The r is the result of `a%d` in Java

That's slightly a lie, r is always non-negative, Java's % operator sometimes gives a negative number.

Terminology

You might have called the % operator in Java “mod”

We’re going to use the word “mod” to mean a closely related, but different thing.

Java’s % is an operator (like + or ·) you give it two numbers, it produces a number.

The word “mod” in this class, refers to a set of rules