37181 DISCRETE MATHEMATICS

Lecture 5: set theory

PLAN

- introduction to set theory notation
- set theory proofs
- definition of “set” again
- power set

SET THEORY

A *set* is a well-defined collection of objects.

(Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory)

The objects are called *elements* of the set, or *members* of the set.

A *set* is a well-defined collection of objects.

(Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory)

The objects are called *elements* of the set, or *members* of the set.

We can represent a set using brackets, for example
$A = \{1, 2, a, 5, c, 3\}$.

A *set* is a well-defined collection of objects.

(Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory)

The objects are called *elements* of the set, or *members* of the set.

We can represent a set using brackets, for example
$A = \{1, 2, a, 5, c, 3\}$.

The elements are the six symbols you see listed inside the brackets.
We could also describe a set using variables satisfying some conditions, for example:

$$B = \{x \mid ((x \in \mathbb{N}) \wedge (1 \leqslant x \leqslant 5) \wedge (x \neq 4)) \vee (x = a) \vee (x = c)\}.$$

A *set* is a well-defined collection of objects.

(Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory)

The objects are called *elements* of the set, or *members* of the set.

We can represent a set using brackets, for example
$A = \{1, 2, a, 5, c, 3\}$.

The elements are the six symbols you see listed inside the brackets.
We could also describe a set using variables satisfying some conditions, for example:

$$B = \{x \mid ((x \in \mathbb{N}) \wedge (1 \leqslant x \leqslant 5) \wedge (x \neq 4)) \vee (x = a) \vee (x = c)\}.$$

The set B is the same as the set A, since a set is defined only by the elements it contains, no matter how they are listed or displayed.

The notation $x \in A$ means x *is an element of* A

and $x \notin A$ means $\neg(x \in A)$.

The notation $x \in A$ means x *is an element of* A

and $x \notin A$ means $\neg(x \in A)$.

Formally, if A, B are sets we define $A = B$ if

$$\forall x[x \in A \leftrightarrow x \in B]$$

Eg: We sometimes use "comma" instead of $\wedge$

- $A = \{x \mid x \in \mathbb{Q}, x < 0\}$
- $B = \{y \mid y \in \mathbb{R}, y^2 = 2\}$

Test: where does the real number $-\sqrt{2}$ live?

Eg: We sometimes use "comma" instead of $\wedge$

- $A = \{x \mid x \in \mathbb{Q}, x < 0\}$
- $B = \{y \mid y \in \mathbb{R}, y^2 = 2\}$

Test: where does the real number $-\sqrt{2}$ live?

Definition

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (intersection)
- $A \cup B = \{x \mid x \in A \vee x \in B\}$ (union)

Eg: We sometimes use "comma" instead of $\wedge$

- $A = \{x \mid x \in \mathbb{Q}, x < 0\}$
- $B = \{y \mid y \in \mathbb{R}, y^2 = 2\}$

Test: where does the real number $-\sqrt{2}$ live?

Definition

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (intersection)
- $A \cup B = \{x \mid x \in A \vee x \in B\}$ (union)

Note the similarity of notation for $\cap$ and $\wedge$, and $\cup$ and $\vee$. same but different

Eg: We sometimes use "comma" instead of $\wedge$

- $A = \{x \mid x \in \mathbb{Q}, x < 0\}$
- $B = \{y \mid y \in \mathbb{R}, y^2 = 2\}$

Test: where does the real number $-\sqrt{2}$ live?

Definition

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (intersection)
- $A \cup B = \{x \mid x \in A \vee x \in B\}$ (union)

Note the similarity of notation for $\cap$ and $\wedge$, and $\cup$ and $\vee$. same but different

In our Eg: $A \cap B =$

YOUR TURN

Let $A = \{a, b, c, d, e\}, B = \{b, d, e\}, C = \{f, g, a\}$. Find

1. $(A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C)$
3. $A \cup (B \cap C)$

YOUR TURN

Let $A = \{a, b, c, d, e\}, B = \{b, d, e\}, C = \{f, g, a\}$. Find

1. $(A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C)$
3. $A \cup (B \cap C)$

A pictorial way to do this exercise is to draw a *Venn diagram*.

If A, B are sets then $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

Eg: $A = \{a, b, c, d, e\}, B = \{b, d, e\}, C = \{f, g, a\}$. Find

1. $A \setminus B$
2. $A \setminus C$

MORE NOTATION

If A, B are sets we say A is a *subset* of B if $\forall x \in A, x \in B$, or $(x \in A) \rightarrow (x \in B)$. Notation $A \subseteq B$.

If A, B are sets we say A is a *subset* of B if $\forall x \in A, x \in B$, or $(x \in A) \to (x \in B)$. Notation $A \subseteq B$.

The notation $A \subsetneq B$ means *strictly contains*:

$$((x \in A) \to (x \in B)) \wedge (\exists y[y \in B \wedge y \notin A]).$$

If A, B are sets we say A is a *subset* of B if $\forall x \in A, x \in B$, or $(x \in A) \rightarrow (x \in B)$. Notation $A \subseteq B$.

The notation $A \subsetneq B$ means *strictly contains*:

$$((x \in A) \rightarrow (x \in B)) \wedge (\exists y[y \in B \wedge y \notin A]).$$

So $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. who is the "$y$" in each case?

MORE NOTATION

If A, B are sets we say A is a *subset* of B if $\forall x \in A, x \in B$, or $(x \in A) \to (x \in B)$. Notation $A \subseteq B$.

The notation $A \subsetneq B$ means *strictly contains*:

$$((x \in A) \to (x \in B)) \wedge (\exists y[y \in B \wedge y \notin A]).$$

So $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. who is the "$y$" in each case?

Let $\mathscr{U}$ be some large "universal" set, so we assume all sets we speak about are subsets of $\mathscr{U}$. Then $\overline{A} = \{x \mid x \notin A\} = \mathscr{U} \setminus A$ means the set of elements in $\mathscr{U}$ that are not in A.

There is a strong connection to the propositional logic we covered in Week 1. We have three operations on sets: $\cap, \cup, ^{-}$ which we can use to build new sets from old ones, and in logic we have three connectives $\wedge, \vee, \neg$. actually you only need two

LOGIC VS. SET THEORY

There is a strong connection to the propositional logic we covered in Week 1. We have three operations on sets: $\cap, \cup, ^{-}$ which we can use to build new sets from old ones, and in logic we have three connectives $\wedge, \vee, \neg$. actually you only need two

Recall the tautologies in logic such as

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$

In set theory we could consider sets

$$\overline{A \cap B} \text{ and } \overline{A} \cup \overline{B}.$$

There is a strong connection to the propositional logic we covered in Week 1. We have three operations on sets: $\cap, \cup, ^{-}$ which we can use to build new sets from old ones, and in logic we have three connectives $\wedge, \vee, \neg$. actually you only need two

Recall the tautologies in logic such as

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$

In set theory we could consider sets

$$\overline{A \cap B} \text{ and } \overline{A} \cup \overline{B}.$$

How do we show two sets are the same? We show they contain exactly the same elements.

LOGIC VS. SET THEORY

There is a strong connection to the propositional logic we covered in Week 1. We have three operations on sets: $\cap, \cup, ^{-}$ which we can use to build new sets from old ones, and in logic we have three connectives $\wedge, \vee, \neg$. actually you only need two

Recall the tautologies in logic such as

$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$

In set theory we could consider sets

$$\overline{A \cap B} \text{ and } \overline{A} \cup \overline{B}.$$

How do we show two sets are the same? We show they contain exactly the same elements.

Formally, if A, B are sets we define $A = B$ if

$$\forall x[x \in A \leftrightarrow x \in B]$$

DE MORGAN (SET VERSION)

Lemma

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

DE MORGAN (SET VERSION)

Lemma

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

The proof goes: pick some arbitrary element of the LHS.

DE MORGAN (SET VERSION)

Lemma

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

The proof goes: pick some arbitrary element of the LHS.

Show it belongs to the RHS.

Lemma

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

The proof goes: pick some arbitrary element of the LHS.

Show it belongs to the RHS.

Since we picked an arbitrary thing, this shows everything in the LHS is also in the RHS, so LHS$\subseteq$RHS.

DE MORGAN (SET VERSION)

Lemma

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

The proof goes: pick some arbitrary element of the LHS.

Show it belongs to the RHS.

Since we picked an arbitrary thing, this shows everything in the LHS is also in the RHS, so LHS$\subseteq$RHS.

Repeat to get RHS$\subseteq$LHS, then LHS$=$RHS.

DE MORGAN (SET VERSION)

Lemma

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

Proof. Suppose $x \in \overline{A \cap B}$.

DE MORGAN (SET VERSION)

Lemma

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

Proof. Suppose $x \in \overline{A \cap B}$.

Then x is not in $A \cap B$.

DE MORGAN (SET VERSION)

Lemma

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

Proof. Suppose $x \in \overline{A \cap B}$.

Then x is not in $A \cap B$.

Now either $x \in A$ or not. If $x \in A$ then since $x \notin A \cap B$ we must have x is not in B.

DE MORGAN (SET VERSION)

Lemma

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

Proof. Suppose $x \in \overline{A \cap B}$.

Then x is not in $A \cap B$.

Now either $x \in A$ or not. If $x \in A$ then since $x \notin A \cap B$ we must have x is not in B.

So either $x \in \overline{A}$ or $x \in \overline{B}$, so $x \in \overline{A} \cup \overline{B}$.

Lemma

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

Proof. Suppose $x \in \overline{A \cap B}$.

Then x is not in $A \cap B$.

Now either $x \in A$ or not. If $x \in A$ then since $x \notin A \cap B$ we must have x is not in B.

So either $x \in \overline{A}$ or $x \in \overline{B}$, so $x \in \overline{A} \cup \overline{B}$.

Thus

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

Next, start over and suppose $x \in \overline{A} \cup \overline{B}$.

Thus

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

Since each set is contained in the other, they are equal. $\square$

YOUR TURN

Show that for any sets $A, B, C \subseteq \mathscr{U}$

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

VENN DIAGRAMS ARE NOT PROOFS

Note: a *Venn diagram* can be useful to check if a statement about sets looks correct, or to find a counterexample.

But **drawing a picture of a Venn diagram does not constitute a proof – you must do the LHS, RHS proof.**

VENN DIAGRAMS ARE NOT PROOFS

Note: a *Venn diagram* can be useful to check if a statement about sets looks correct, or to find a counterexample.

But **drawing a picture of a Venn diagram does not constitute a proof – you must do the LHS, RHS proof.**

Eg: check if you think $A \cup (B \cap C) = (A \cup B) \cap C$ is true or not.

BACK TO THE DEFINITION OF “SET”

The next exercise explains why *well-defined collection of objects* is not quite good enough.

BACK TO THE DEFINITION OF "SET"

The next exercise explains why *well-defined collection of objects* is not quite good enough.

Let $P(S)$ be the property (of sets) that S does not contain itself.

BACK TO THE DEFINITION OF “SET”

The next exercise explains why *well-defined collection of objects* is not quite good enough.

Let $P(S)$ be the property (of sets) that S does not contain itself.

For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

The next exercise explains why *well-defined collection of objects* is not quite good enough.

Let $P(S)$ be the property (of sets) that S does not contain itself.

For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

Another example: the *empty set* $\emptyset$ is the set that has no elements, $\emptyset = \{\}$. So it contains nothing so cannot contain itself.

The next exercise explains why *well-defined collection of objects* is not quite good enough.

Let $P(S)$ be the property (of sets) that S does not contain itself.

For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

Another example: the *empty set* $\emptyset$ is the set that has no elements, $\emptyset = \{\}$. So it contains nothing so cannot contain itself.

(a) Give some more examples.

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

BACK TO THE DEFINITION OF “SET”

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

(c) Which is true: $\mathscr{S} \in \mathscr{S}$ or $\mathscr{S} \notin \mathscr{S}$?

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, imaginary numbers.

(b) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

(c) Which is true: $\mathscr{S} \in \mathscr{S}$ or $\mathscr{S} \notin \mathscr{S}$?

The moral of this story: you cannot define a set using a condition, in general. *i.e.* $\{x \mid P(x)\}$ may not actually be a well-defined collection of objects.

BACK TO THE DEFINITION OF "SET"

The moral of this story: you cannot define a set using a condition, in general. *i.e.* $\{x \mid P(x)\}$ may not actually be a well-defined collection of objects.

This fact is called Russell's paradox, and it lead to the development of axiomatic set theory.

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Another axiom: $\emptyset$ is a set.

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Another axiom: $\emptyset$ is a set.

What can you build with just these two axioms?

YOUR TURN

- Given $A = \{1, 2, 3\}$ is a set, what is $\mathscr{P}(A)$?

YOUR TURN

- Given $A = \{1, 2, 3\}$ is a set, what is $\mathscr{P}(A)$?

- Prove that if A is a set then $A \subsetneq \mathscr{P}(A)$

Next lecture:

- Division and remainder lemma
- Euclidean algorithm