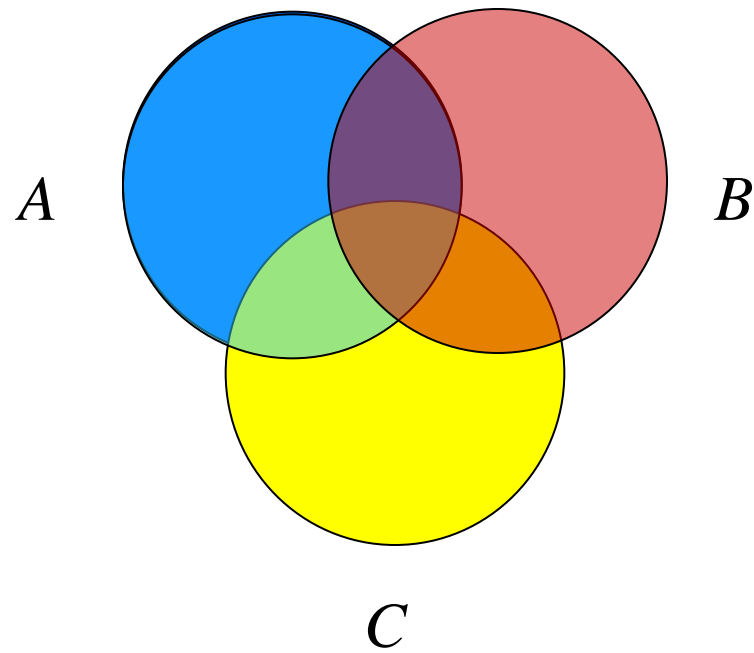


Sets



Lecture 1: Sep 10

This Lecture

We will first introduce some basic set theory before we do counting.

- Basic Definitions
- Operations on Sets
- Set Identities
- Russell's Paradox

Defining Sets

Definition: A **set** is an unordered collection of objects.

The objects in a set are called the **elements** or **members** of the set S , and we say S **contains** its elements.

We can define a set by directly listing all its elements.

e.g. $S = \{2, 3, 5, 7, 11, 13, 17, 19\}$,

$S = \{\text{CSC1130}, \text{CSC2110}, \text{ERG2020}, \text{MAT2510}\}$

After we define a set, the set is a single mathematical object, and it can be an element of another set.

e.g. $S = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

Defining Sets by Properties

It is inconvenient, and sometimes impossible, to define a set by listing all its elements.

Alternatively, we can define by a set by describing the *properties* that its elements should satisfy.

We use the notation $\{x \in A \mid P(x)\}$

to define the set as the *set of elements*, x , in A *such that* x satisfies property P .

e.g. $\{x \mid x \text{ is a prime number and } x < 1000\}$

$\{x \mid x \text{ is a real number and } -2 < x < 5\}$


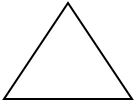
Examples of Sets

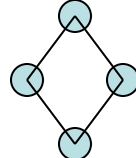
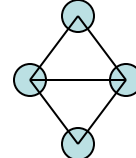
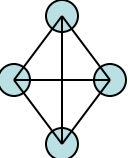
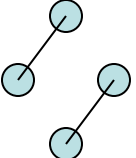
- Well known sets:
- the set of all real numbers, \mathbb{R}
 - the set of all complex numbers, \mathbb{C}
 - the set of all integers, \mathbb{Z}
 - the set of all positive integers \mathbb{Z}^+
 - **empty set**, $\emptyset = \{\}$, the set with no elements.

Other examples:

The set of all polynomials with degree at most three: $\{1, x, x^2, x^3, 2x+3x^2, \dots\}$.

The set of all n-bit strings: $\{000\dots 0, 000\dots 1, \dots, 111\dots 1\}$

The set of all triangles without an obtuse angle: {  ,  , ... }

The set of all graphs with four nodes: {  ,  ,  ,  , ... }

Membership

Order, number of occurrence are not important.

$$\text{e.g. } \{a,b,c\} = \{c,b,a\} = \{a,a,b,c,b\}$$

The most basic question in set theory is whether an element is in a set.

$x \in A$ x is an element of A x is in A	$x \notin A$ x is not an element of A x is not in A
---	--

e.g. Recall that Z is the set of all integers. So $7 \in Z$ and $2/3 \notin Z$.

Let P be the set of all prime numbers. Then $97 \in P$ and $321 \notin P$

Let Q be the set of all rational numbers. Then $0.5 \in Q$ and $\sqrt{2} \notin Q$
↑
(will prove later)

Size of a Set

In this course we mostly focus on finite sets.

Definition: The **size** of a set S , denoted by $|S|$, is defined as the number of elements contained in S .

e.g. if $S = \{2, 3, 5, 7, 11, 13, 17, 19\}$, then $|S|=8$.

if $S = \{\text{CSC1130}, \text{CSC2110}, \text{ERG2020}, \text{MAT2510}\}$, then $|S|=4$.

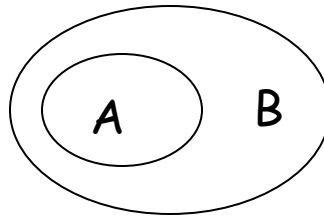
if $S = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$, then $|S|=6$.

Later we will study how to determine the size of the following sets:

- the set of poker hands which are "full house".
- the set of n -bit strings without three consecutive ones.
- the set of valid ways to add n pairs of parentheses

Subset

Definition: Given two sets A and B , we say A is a **subset** of B , denoted by $A \subseteq B$, if every element of A is also an element of B .



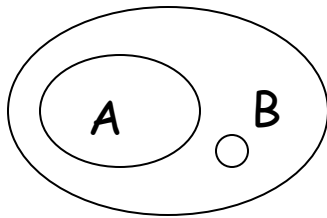
not a subset

- If $A = \{4, 8, 12, 16\}$ and $B = \{2, 4, 6, 8, 10, 12, 14, 16\}$, then $A \subseteq B$ but $B \not\subseteq A$
- $A \subseteq A$ because every element in A is an element of A .
- $\emptyset \subseteq A$ for any A because the empty set has no elements.
- If A is the set of prime numbers and B is the set of odd numbers, then $A \not\subseteq B$

Fact: If $A \subseteq B$, then $|A| \leq |B|$.

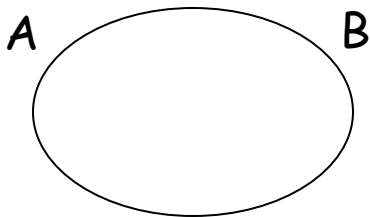
Proper Subset, Equality

Definition: Given two sets A and B , we say A is a **proper subset** of B , denoted by $A \subset B$, if every element of A is an element of B , But there is an element in B that is not contained in A .



Fact: If $A \subset B$, then $|A| < |B|$.

Definition: Given two sets A and B , we say $A = B$ if $A \subseteq B$ and $B \subseteq A$.



Fact: If $A = B$, then $|A| = |B|$.

Exercises

1. $\mathbb{Z} \subset \mathbb{R}$?
2. $\{3\} \in \{5,7,3\}$?
3. $\emptyset \in$ every set?
4. $\{1,2\} \subseteq \{\{1,2\}, \{2,3\}, \{3,1\}\}$?
5. $\{a\} = \{\{a\}\}$?
6. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$?
7. If $A \subset B$ and $B \subseteq C$, then $A \subset C$?

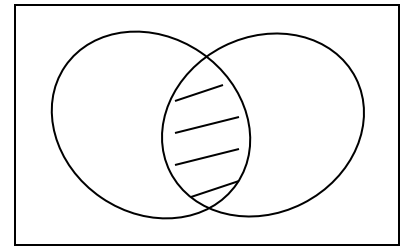
This Lecture

- Basic Definitions
- Operations on Sets
- Set Identities
- Russell's Paradox

Basic Operations on Sets

Let A, B be two subsets of a *universal* set U
(depending on the context U could be \mathbb{R} , \mathbb{Z} , or other sets).

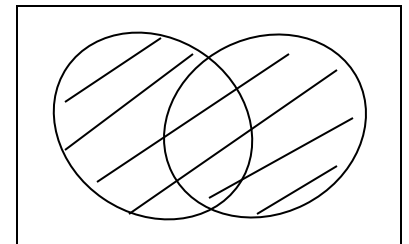
intersection: $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$



Defintion: Two sets are said to be **disjoint** if their intersection is an empty set.

e.g. Let A be the set of odd numbers, and B be the set of even numbers.
Then A and B are disjoint.

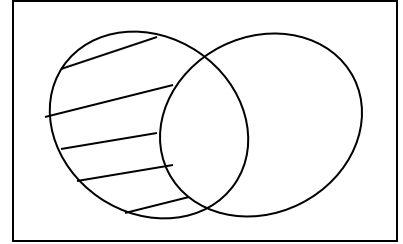
union: $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$



Fact: $|A \cup B| = |A| + |B| - |A \cap B|$

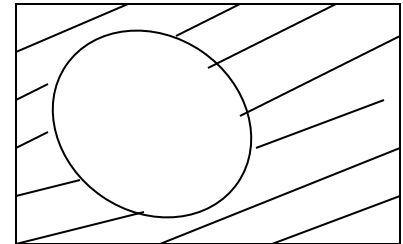
Basic Operations on Sets

difference: $A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}$



Fact: $|A - B| = |A| - |A \cap B|$

complement: $\overline{A} = A^c = \{x \in U \mid x \notin A\}$



e.g. Let $U = \mathbb{Z}$ and A be the set of odd numbers.

Then \overline{A} is the set of even numbers.

Fact: If $A \subseteq B$, then $\overline{B} \subseteq \overline{A}$

Examples

$$A = \{1, 3, 6, 8, 10\} \quad B = \{2, 4, 6, 7, 10\}$$

$$A \cap B = \{6, 10\}, \quad A \cup B = \{1, 2, 3, 4, 6, 7, 8, 10\} \quad A - B = \{1, 3, 8\}$$

$$\text{Let } U = \{x \in \mathbb{Z} \mid 1 \leq x \leq 100\}.$$

$$A = \{x \in U \mid x \text{ is divisible by } 3\}, \quad B = \{x \in U \mid x \text{ is divisible by } 5\}$$

$$A \cap B = \{x \in U \mid x \text{ is divisible by } 15\}$$

$$A \cup B = \{x \in U \mid x \text{ is divisible by } 3 \text{ or is divisible by } 5 \text{ (or both)}\}$$

$$A - B = \{x \in U \mid x \text{ is divisible by } 3 \text{ but is not divisible by } 5\}$$

Exercise: compute $|A|$, $|B|$, $|A \cap B|$, $|A \cup B|$, $|A - B|$.

Partitions of Sets

Two sets are **disjoint** if their intersection is empty.

A collection of nonempty sets $\{A_1, A_2, \dots, A_n\}$ is a **partition** of a set A if and only if

$$A = A_1 \cup A_2 \cup \dots \cup A_n$$

A_1, A_2, \dots, A_n are **mutually disjoint (or pairwise disjoint)**.

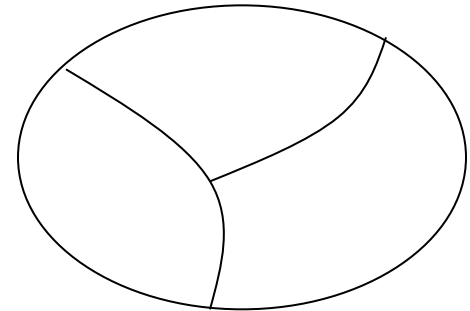
e.g. Let A be the set of integers.

$$A_1 = \{x \in A \mid x = 3k+1 \text{ for some integer } k\}$$

$$A_2 = \{x \in A \mid x = 3k+2 \text{ for some integer } k\}$$

$$A_3 = \{x \in A \mid x = 3k \text{ for some integer } k\}$$

Then $\{A_1, A_2, A_3\}$ is a partition of A



Partitions of Sets

e.g. Let A be the set of integers divisible by 6.

A_1 be the set of integers divisible by 2.

A_2 be the set of integers divisible by 3.

Then $\{A_1, A_2\}$ is not a partition of A , because A_1 and A_2 are not disjoint,
and also $A \subset A_1 \cup A_2$ (so both conditions are not satisfied).

e.g. Let A be the set of integers.

Let A_1 be the set of negative integers.

Let A_2 be the set of positive integers.

Then $\{A_1, A_2\}$ is not a partition of A , because $A \neq A_1 \cup A_2$
as 0 is contained in A but not contained in $A_1 \cup A_2$

Power Sets

power set: $\text{pow}(A) ::= \{S \mid S \subseteq A\}$

In words, the power set $\text{pow}(A)$ of a set A contains all the subsets of A as members.

$$\text{pow}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$$

$$\text{pow}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

$$\begin{aligned} \text{pow}(\{a,b,c,d\}) = & \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \\ & \{a,b\}, \{a,c\}, \{b,c\}, \{a,d\}, \{b,d\}, \{c,d\}, \\ & \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}\} \end{aligned}$$

Fact (to be explained later): If A has n elements, then $\text{pow}(A)$ has 2^n elements.

Cartesian Products

Definition: Given two sets A and B , the **Cartesian product** $A \times B$ is the set of all **ordered** pairs (a,b) , where a is in A and b is in B . Formally,

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Ordered pairs means the ordering is important, e.g. $(1,2) \neq (2,1)$

e.g. Let A be the set of letters, i.e. $\{a,b,c,\dots,x,y,z\}$.

Let B be the set of digits, i.e. $\{0,1,\dots,9\}$.

$A \times A$ is just the set of strings with two letters.

$B \times B$ is just the set of strings with two digits.

$A \times B$ is the set of strings where the first character is a letter and the second character is a digit.

Cartesian Products

The definition can be generalized to any number of sets, e.g.

$$A \times B \times C = \{(a, b, c) \mid a \in A \text{ and } b \in B \text{ and } c \in C\}$$

Using the above examples, $A \times A \times A$ is the set of strings with three letters.

Our ID card number has one letter and then six digits,
so the set of ID card numbers is the set $A \times B \times B \times B \times B \times B$.

Fact: If $|A| = n$ and $|B| = m$, then $|A \times B| = nm$.

Fact: If $|A| = n$ and $|B| = m$ and $|C| = l$, then $|A \times B \times C| = nml$.

Fact: $|A_1 \times A_2 \times \dots \times A_k| = |A_1| \times |A_2| \times \dots \times |A_k|$.

Exercises

1. Let A be the set of prime numbers, and let B be the set of even numbers. What is $A \cap B$ and $|A \cap B|$?
2. Is $|A \cup B| > |A| > |A \cap B|$ always true?
3. Let A be the set of all n -bit binary strings, A_i be the set of all n -bit binary strings with i ones. Is $(A_1, A_2, \dots, A_i, \dots, A_n)$ a partition of A ?
4. Why the name Cartesian product?
5. Let $A = \{x, y\}$. What is $\text{pow}(A) \times \text{pow}(A)$ and $|\text{pow}(A) \times \text{pow}(A)|$?

This Lecture

- Basic Definitions
- Operations on Sets
- Set Identities
- Russell's Paradox

Set Identities

Some basic properties of sets, which are true for all sets.

$$A \cap B \subseteq A$$

$$A \subseteq A \cup B$$

$$\text{if } A \subseteq B \text{ and } B \subseteq C, \text{ then } A \subseteq C$$

$$A \cap \overline{A} = \emptyset$$

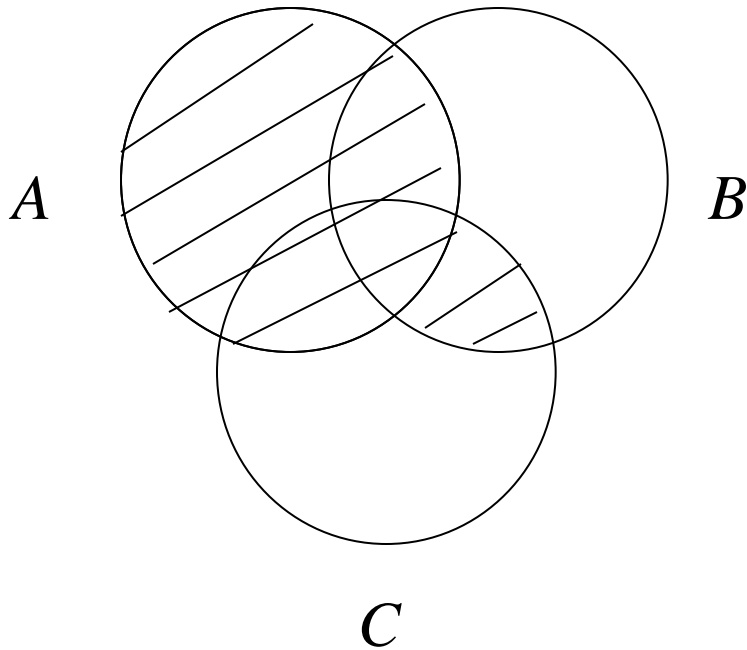
$$\overline{\overline{A}} = A$$

$$A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$$

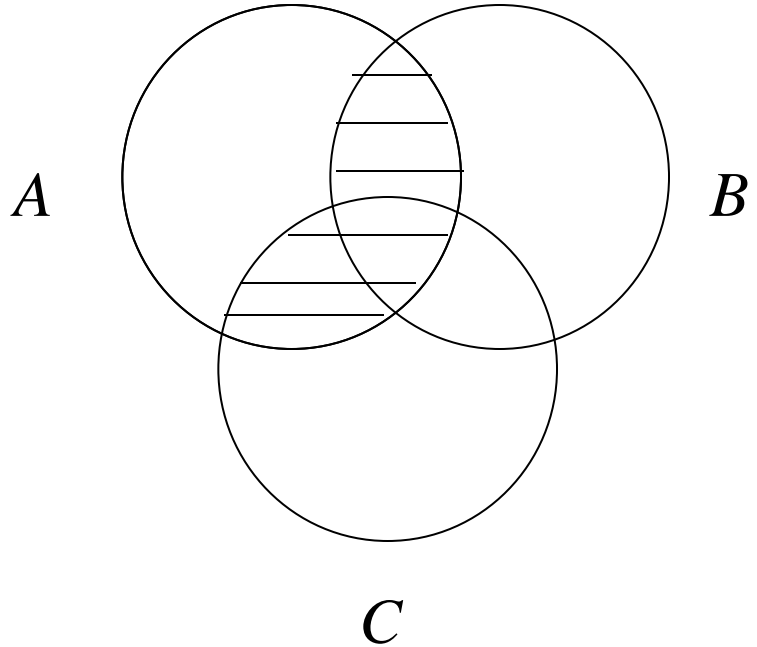
Set Identities

Distributive Law: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (1)

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



(1)

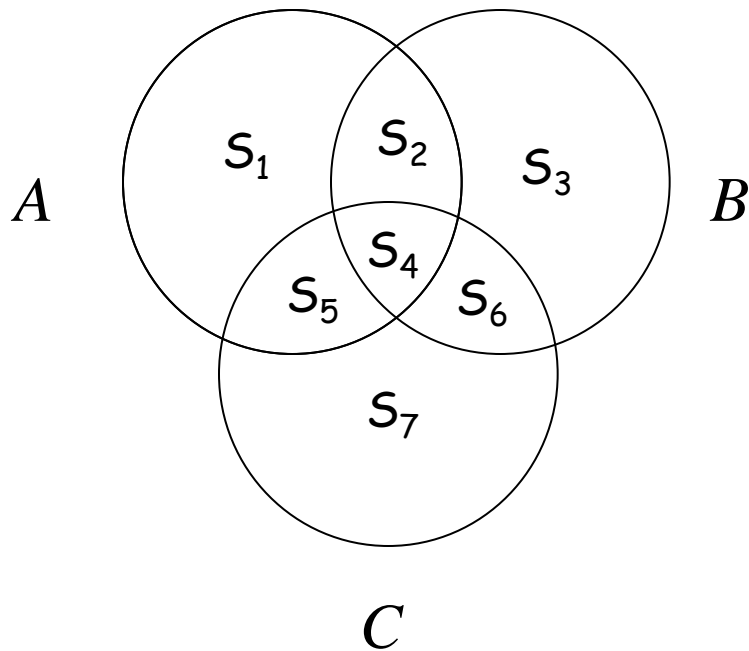


(2)

Set Identities

Distributive Law: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

We can also verify this law more carefully



L.H.S.

$$A = S_1 \cup S_2 \cup S_4 \cup S_5$$

$$B \cap C = S_4 \cup S_6$$

$$A \cup (B \cap C) = S_1 \cup S_2 \cup S_4 \cup S_5 \cup S_6$$

R.H.S.

$$(A \cup B) = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6$$

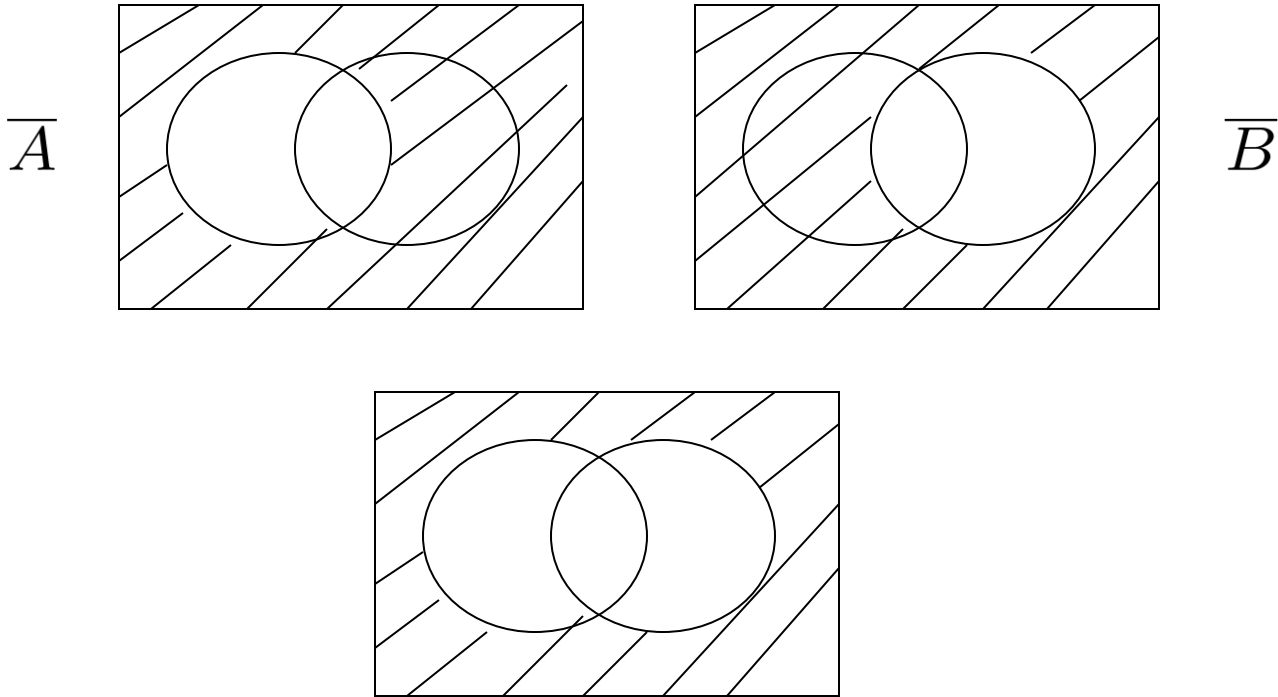
$$(A \cup C) = S_1 \cup S_2 \cup S_4 \cup S_5 \cup S_6 \cup S_7$$

$$(A \cup B) \cap (A \cup C) = S_1 \cup S_2 \cup S_4 \cup S_5 \cup S_6$$

There are formal proofs in the textbook, but we don't do that.

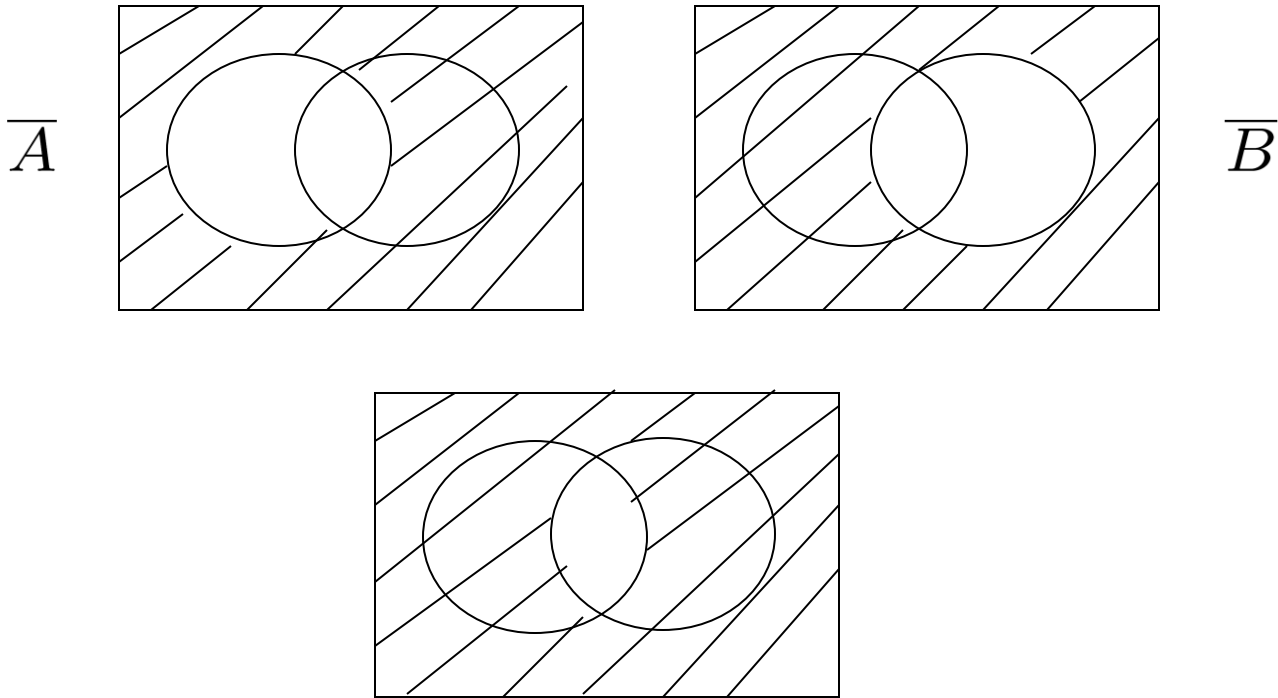
Set Identities

De Morgan's Law: $\overline{A \cup B} = \overline{A} \cap \overline{B}$



Set Identities

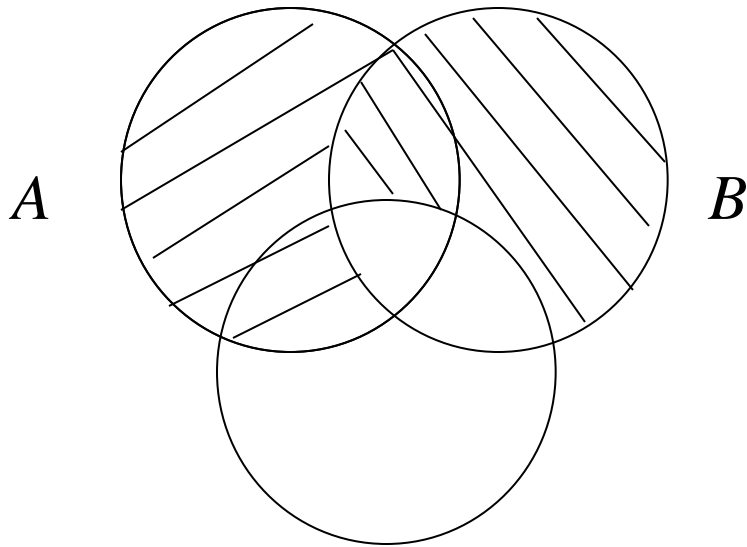
De Morgan's Law: $\overline{A \cap B} = \overline{A} \cup \overline{B}$



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

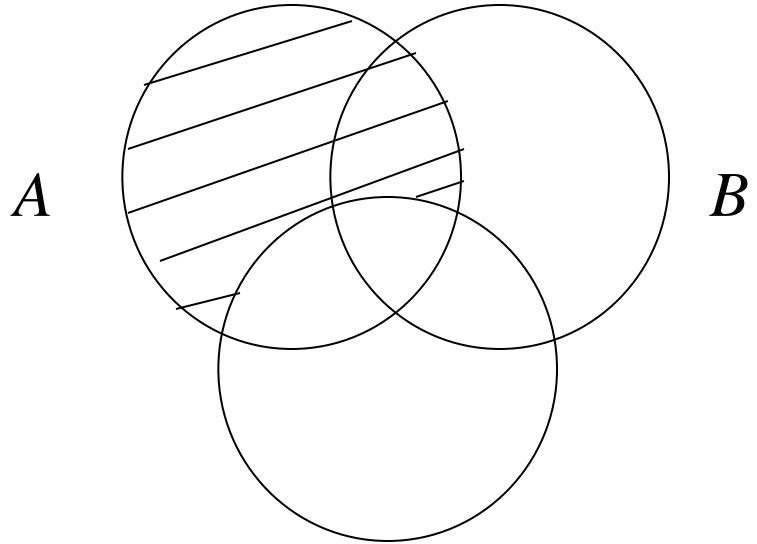
Disproof

$$(A - B) \cup (B - C) = A - C?$$



C

L.H.S

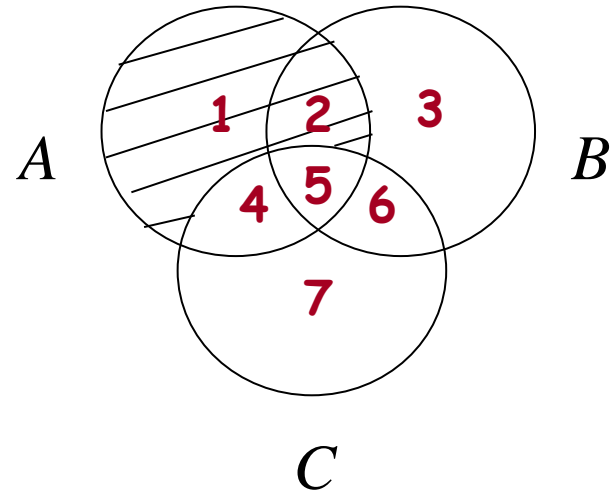
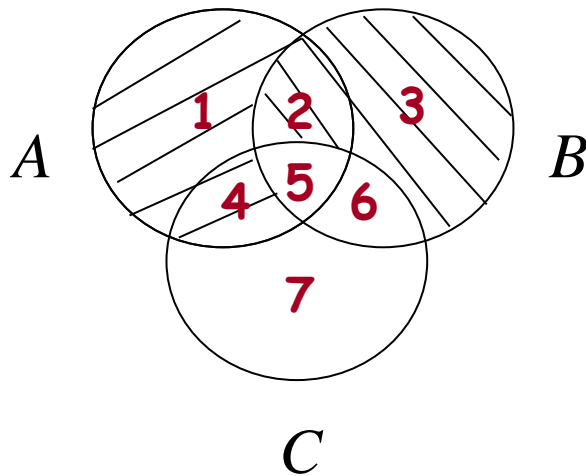


C

R.H.S

Disproof

$$(A - B) \cup (B - C) = A - C?$$



We can easily construct a **counterexample** to the equality, by putting a number in each region in the figure.

Let $A = \{1, 2, 4, 5\}$, $B = \{2, 3, 5, 6\}$, $C = \{4, 5, 6, 7\}$.

Then we see that L.H.S = $\{1, 2, 3, 4\}$ and R.H.S = $\{1, 2\}$.

Algebraic Proof

Sometimes when we know some rules, we can use them to prove new rules without drawing figures.

e.g. we can prove $\overline{(\overline{A} \cap \overline{B})} = A \cup B$ without drawing figures.

$$\begin{aligned}\overline{(\overline{A} \cap \overline{B})} &= \overline{\overline{A}} \cup \overline{\overline{B}} && \text{by using DeMorgan's rule on } \overline{A} \text{ and } \overline{B} \\ &= A \cup B\end{aligned}$$

Algebraic Proof

$$\overline{((A \cup C) \cap (B \cup C))} = (\overline{A} \cup \overline{B}) \cup \overline{C}?$$

$$\overline{((A \cup C) \cap (B \cup C))}$$

$$= \overline{(A \cup C)} \cup \overline{(B \cup C)} \quad \text{by DeMorgan's law on } A \cup C \text{ and } B \cup C$$

$$= (\overline{A} \cap \overline{C}) \cup \overline{(B \cup C)} \quad \text{by DeMorgan's law on the first half}$$

$$= (\overline{A} \cap \overline{C}) \cup (\overline{B} \cap \overline{C}) \quad \text{by DeMorgan's law on the second half}$$

$$= (\overline{A} \cup \overline{B}) \cap \overline{C} \quad \text{by distributive law}$$

$$\neq (\overline{A} \cup \overline{B}) \cup \overline{C}$$

Exercises

$$A - (A \cap B) = A - B?$$

$$(A \cup B) - C = (A - C) \cup (B - C)?$$

$$\overline{(A \cup B \cup C)} = \overline{A} \cap \overline{B} \cap \overline{C}?$$

This Lecture

- Basic Definitions
- Operations on Sets
- Set Identities
- Russell's Paradox

Russell's Paradox (Optional)

$$\text{Let } W ::= \{S \in \text{Sets} \mid S \notin S\}$$

In words, W is the set that contains all the sets that don't contain themselves.

Is W in W ?

If W is in W , then W contains itself.

But W contains only those sets that don't contain themselves.

So W is not in W .

If W is not in W , then W does not contain itself.

But W contains those sets that don't contain themselves.

So W is in W .

What's wrong???

Barber's Paradox (Optional)

There is a male barber who shaves all those men,
and only those men, who do not shave themselves.

Does the barber shave himself?

Suppose the barber shaves himself.

But the barber only shaves those men who don't shave themselves.

Since the barber shaves himself, he does not shave himself.

Suppose the barber does not shave himself.

But the barber shaves those men who don't shave themselves.

Since the barber does not shave himself, he shaves himself.

What's wrong???

Solution to Russell's Paradox (Optional)

A man either shaves himself or not shaves himself.

A barber neither shaves himself nor not shaves himself.

Perhaps such a barber does not exist?

Actually that's the way out of this paradox.

Going back to the barber's paradox,

we conclude that W cannot be a set,

because every set is either contains itself or not,

but either case cannot happen for W .

This paradox tells us that not everything we define is a set.

Later on mathematicians define sets more carefully,

e.g. using sets that we already know.

Halting Problem (Optional)

Now we mention one of the most famous problems in computer science.

The halting problem: Can we write a program which detects infinite loop?

We want a program H that given any program P and input I :

$H(P,I)$ returns "halt" if P will terminate given input I ;

$H(P,I)$ returns "loop forever" if P will not terminate given input I .

And H itself must terminate in finite time.

The halting problem: Does such a program H exist?

NO!

The reasoning used in solving the halting problem is very similar to that of Russell's paradox, if you're interested please see Chapter 5.4 of the textbook.

Summary

Recall what we have covered so far.

- Basic Definitions (defining sets, membership, subsets, size)
- Operations on Sets (intersection, union, difference, complement, partition, power set, Cartesian product)
- Set Identities (distributive law, DeMorgan's law, checking set identities - proof & disproof, algebraic)

We won't ask difficult questions about sets,
but later on sets will be in our language in this course,
so make sure that you remember the basic definitions and notation.