# Lecture 2.8: Set-theoretic proofs

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

# Motivation

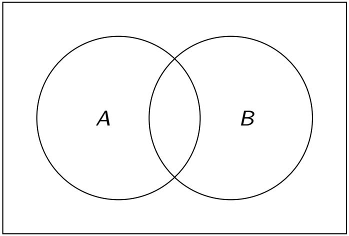
Thus far, we've come across statements like the following:

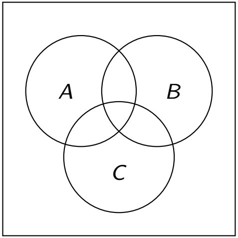
**Theorem**

For any sets $A$, $B$, and $C$,

1. $A \setminus (A \setminus B) \subseteq B$.
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
3. If $A \cup B \subseteq A \cup C$, then $B \subseteq C$.

Thus far, our primary method of "proof" has been by examining a Venn diagram.




Did you catch the "lie" above? Let that be a cautionary tale for "proof by picture"...

# Warm-up

## Basic facts

$$
\begin{array}{rcl}
x \in A \cup B & \Leftrightarrow & x \in A \text{ or } x \in B \\
x \notin A \cup B & \Leftrightarrow & x \notin A \text{ and } x \notin B \\
x \in A \cap B & \Leftrightarrow & x \in A \text{ and } x \in B \\
x \notin A \cap B & \Leftrightarrow & x \notin A \text{ or } x \notin B \\
x \in A \setminus B & \Leftrightarrow & x \in A \text{ and } x \notin B \\
x \notin A \setminus B & \Leftrightarrow & x \notin A \text{ or } x \in B \\
x \in A \times B & \Leftrightarrow & x = (a, b) \text{ for some } a \in A,\ b \in B \\
A \subseteq B & \Leftrightarrow & \text{If } x \in A, \text{ then } x \in B \\
A = B & \Leftrightarrow & A \subseteq B \text{ and } A \supseteq B
\end{array}
$$

In this lecture, we'll see three techniques for proving $A = B$:

(i) Explicitly writing $A = \{x \in U \mid \dots\} = \cdots = \{x \in U \mid \dots\} = B$.

(ii) Showing $A \subseteq B$ and $A \supseteq B$.

(iii) Indirectly, i.e., by contrapositive or contradiction.

# Basic laws of propositional calculus

Recall that we've seen a number of basic laws of propositional calculus.

Moreover, each law has a dual law obtained by exchanging the symbols:

- $\wedge$ with $\vee$
- 0 with 1.

| Basic law | Name | Dual law |
|---|---|---|
| $p \vee q \Leftrightarrow q \vee p$ | Commutativity | $p \wedge q \Leftrightarrow q \wedge p$ |
| $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ | Associativity | $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$ |
| $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ | Distributivity | $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ |
| $p \vee 0 \Leftrightarrow p$ | Identity | $p \wedge 1 \Leftrightarrow p$ |
| $p \wedge \neg p \Leftrightarrow 0$ | Negation | $p \vee \neg p \Leftrightarrow 1$ |
| $p \vee p \Leftrightarrow p$ | Idempotent | $p \wedge p \Leftrightarrow p$ |
| $p \wedge 0 \Leftrightarrow 0$ | Null | $p \vee 1 \Leftrightarrow 1$ |
| $p \wedge (p \vee q) \Leftrightarrow p$ | Absorption | $p \vee (p \wedge q) \Leftrightarrow p$ |
| $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ | DeMorgan's | $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ |

We can turn each of these into an associated law of set theory by replacing:

- $p$ with $A$
- $q$ with $B$
- $\wedge$ with $\cap$
- $\vee$ with $\cup$
- 0 with $\emptyset$
- 1 with $U$
- $\neg$ with ${}^c$
- $\Leftrightarrow$ with $=$

# Basic laws of set theory

The basic laws of propositional calculus all have an associative basic law of set theory.

Moreover, each law has a dual law obtained by exchanging the symbols:

- $\cap$ with $\cup$
- $\emptyset$ with $U$.

| Basic law | Name | Dual law |
|---|---|---|
| $A \cup B = B \cup A$ | Commutativity | $A \cap B = B \cap A$ |
| $(A \cup B) \cup C = A \cup (B \cup C)$ | Associativity | $(A \cap B) \cap C = A \cap (B \cap C)$ |
| $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ | Distributivity | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |
| $A \cup \emptyset = A$ | Identity | $A \cap U = A$ |
| $A \cap A^c = \emptyset$ | Negation | $A \cup A^c = U$ |
| $A \cup A = A$ | Idempotent | $A \cap A = A$ |
| $A \cap \emptyset = \emptyset$ | Null | $A \cup U = U$ |
| $A \cap (A \cup B) = A$ | Absorption | $A \cup (A \cap B) = A$ |
| $(A \cup B)^c = A^c \cap B^c$ | DeMorgan's | $(A \cap B)^c = A^c \cup B^c$ |

Let's start by proving $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ two different ways.

# Method 1: proof using set notation

## Theorem

For any sets $A$, $B$, and $C$,

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

## Proof

$$\begin{aligned}
A \cap (B \cup C) &= \{x \in U \mid (x \in A) \wedge (x \in B \cup C)\} && \text{definition of } \cap \\
&= \{x \in U \mid (x \in A) \wedge [(x \in B) \vee (x \in C)]\} && \text{definition of } \cup \\
&= \{x \in U \mid [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)]\} && \text{distributive law} \\
&= \{x \in U \mid (x \in A \cap B) \vee (x \in A \cap C)\} && \text{definition of } \cap \\
&= \{x \in U \mid x \in [(A \cap B) \cup (A \cap C)]\} && \text{definition of } \cup \\
&= (A \cap B) \cup (A \cap C) && \square
\end{aligned}$$

# Method 2: proof by showing $\subseteq$ and $\supseteq$

## Theorem

For any sets $A$, $B$, and $C$,

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

## Proof

"$\subseteq$"

"$\supseteq$"

# Corollaries

Sometimes, establishing a theorem can lead right away to a follow-up result called a corollary.

## Theorem

For any sets $A$, $B$, and $C$,

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

## Corollary

For any sets $A$, $B$,

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

## Proof

# Which method to use?

In many instances, such as proving $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, either of the two aforementioned methods work equally well.

However, sometimes there is no choice. Consider the following example from linear algebra.

Let $V$ be a vector space over $\mathbb{R}$. Recall that the subspace spanned by $S \subseteq V$ is defined as

$$\text{Span}(S) = \big\{a_1 s_1 + \cdots + a_k s_k \mid a_i \in \mathbb{R},\ s_i \in S\big\}.$$

**Theorem**

For any $S \subseteq V$,

$$\text{Span}(S) = \bigcap_{S \subseteq W_\alpha \leq V} W_\alpha,$$

where the intersection is taken over all subspaces $W$ of $V$ that contain $S$.

# Method 3: Proof by contrapositive or contradiction

If the set equality $A = B$ we wish to prove is the conclusion of an If-Then statement, then we can consider an indirect proof.

Let's recall this concept by considering the following statement that we wish to prove:

$$\forall x \in U, \quad \text{If } P(x), \text{ then } Q(x)$$

An indirect proof can be casted two ways: by proving the contrapositive, or as a proof by contradiction.

| **Method** | **First step** | **Goal** |
|---|---|---|
| Contrapositive | Take $x \in U$ for which $\neg Q(x)$ | $\neg P(x)$ |
| Contradiction | Suppose $\exists x \in U$ for which $P(x)$ and $\neg Q(x)$ | $P(x)$ and $\neg P(x)$ |

Table : Difference between proof by contraposition and contradiction.

# Method 3: Proof by contrapositive or contradiction

To illustrate this method, consider the following theorem.

**Theorem**

Let $A, B, C$ be sets. If $A \subseteq B$ and $B \cap C = \emptyset$, then $A \cap C = \emptyset$.

**Proof**