Proof by exhaustion (aka proof by cases)

- Tautology

  $[(p_1 \vee p_2 \vee \ldots p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

- **Crucial first step:** Identify a **complete list** of possible cases (in principle, they need not be mutually exclusive, but in practice they usually are).

- **Exercises**

  1. Prove that if $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.
  2. Prove that if n is an integer, then $n^2 \geq n$
  3. Let n be an integer. If 3 does not divide n, then 3 divides $n^2 - 1$.

  Solutions on blackboard

Without loss of generality (wlog)

- Example: If three objects are each painted either red or blue, then there must be at least two objects of the same color.

  Proof: Assume without loss of generality that the first object is red. If either of the other two objects is red, we are finished; if not, the other two objects must both be blue and we are still finished.
- Remarks
  1. The *wlog* allows us to cover the symmetric case where the first object is blue.
  2. We will see this again later in class (pigeonhole principle)

Vacuous and Trivial proofs

- Suppose we wish to prove that $p \to q$
    1. If p is always false, then the statement is always true (vacuous proof)
    2. If q is always true, then the statement is again always true (trivial proof)
- Examples
    1. Prove that if n is an integer with $10 \leq n \leq 11$ which is a perfect square, then n is also a perfect cube.
    2. Let $P(n)$ be " if a,b are positive integers with $a \geq b$ then $a^n \geq b^n$, where the domain consists of all nonnegative integers. Show that $P(0)$ is true.
- Proofs on blackboard (see also [Rosen p.88,89])

Uniqueness proofs

- $\exists! x P(x)$
- A uniqueness proof consists typically of two parts
  1. Prove existence of x that has the desired property
  2. Prove that if y has the desired property, then $y = x$
- **Example:** There is a unique function $f : \mathbb{R} \to \mathbb{R}$ such that $f'(x) = 2x$ and $f(0) = 3$.

Proof.

1. Existence: $f(x) = x^2 + 3$ (why?)

2. Uniqueness: If $f_0(x)$ and $f_1(x)$ both satisfy these conditions, then $f_0'(x) = 2x = f_1'(x)$, so they differ by a constant, i.e., there is a C such that $f_0(x) = f_1(x) + C$. Hence, $3 = f_0(0) = f_1(0) + C = 3 + C$. This gives $C = 0$ and so $f_0(x) = f_1(x)$

□

Forward/backward reasoning

- **AM-GM:** Let x, y be two non-negative real numbers. Prove that $\frac{x+y}{2} \geq \sqrt{xy}$.

Backward reasoning.

$$\frac{x+y}{2} \geq \sqrt{xy} \leftrightarrow (\frac{x+y}{2})^2 \geq (\sqrt{xy})^2 \leftrightarrow (x+y)^2 \geq 4xy \leftrightarrow$$
$$(x^2+2xy+y^2) \geq 4xy \leftrightarrow (x^2-2xy+y^2) \geq 0 \leftrightarrow (x-y)^2 \geq 0.$$

- **Remark:** We can use backward reasoning to produce forward reasoning since we used *equivalent* inequalities.
- Details on the blackboard.

Lecture 8 (9/26)
Outline

- Finish off lecture 7 [Rosen 1.7, 1.8]
- Sets and set operations [Rosen 2.1, 2.2]

Sets

- $\{0, 3, 1\}$ is a set
- $\{0, 1, 3\}$ is a set and it is the same as $\{0, 3, 1\}$
- $(0, 1, 3)$ is not a set
- $\{a, b, c, d, ..., z\}$ is a set
- $\{\{a, b\}, \{b, c\}\}$ is a set
- $\{a, b, b, c\}$ is not a set
- $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of naturals
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integers
- $\mathbb{Z}^+ = \{1, 2, \ldots\}$ is the set of positive integers
- $\mathbb{R}$ is the set of reals

Question: Can you define what a set is?

Sets

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

- Some remarks.
  1. These objects are called elements or members of the set.
  2. The elements could be sets themselves, or sets containing other sets etc.!
  3. We write $a \in S$ to denote that a is a member of the set S.
  4. We write $a \notin S$ to denote that a is not a member of the set S.
  5. It may be impractical to define a set by listing all its elements.
     - $P = \{2, 3, 5, 7, \ldots\}$
     - Using dots is a common practice but requires the pattern to be clear.
     - A better practice: $P = \{x | \text{x is a prime number}\}$ (set builder)

Exercise: Rewrite the following sets using the set builder notation.

- $E = \{2, 4, 6, 8, 10, \ldots\}$
- $A = \{\text{Brad Pitt, Matt Damon, Meryl Streep}, \ldots\}$

Sets

Exercise: Rewrite the following sets using the set builder notation.

- $E = \{2, 4, 6, 8, 10, \ldots\}$
  $E = \{n | n \text{ is a positive even integer}\}$

- $A = \{\text{Brad Pitt, Matt Damon, Meryl Streep}, \ldots\}$
  $A = \{z | z \text{ is a Holywood actor}\}$

- The set of rationals
  $\mathbb{Q} = \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$

Sets

Three definitions and a question.

1. Subset/superset: The set A is a subset of B (and B a superset of A) if and only if every element of A is an element of B, i.e.,

$$\forall(x \in A \to x \in B).$$

   To denote this, we write $A \subseteq B$.

2. We say that A is a proper subset of B (we write $A \subset B$) if

$$\forall x(x \in A \to x \in B) \land \exists x(x \in B \land x \notin A).$$

3. Equal sets: Two sets A, B are equal if and only

$$\forall x(x \in A \leftrightarrow x \in B).$$

   We write $A = B$. Equivalently, this means A is a subset of B and B is a subset of A

Sets

- **Exercise:** Prove that for any subset S, $\emptyset \subseteq S$. (blackboard)
- Continuing with definitions...
- **Size/cardinality of a set:** If there are exactly n distinct elements, we say that the set is finite and the cardinality is n. We write $|S| = n$ to denote the size. When a set is not finite, it is infinite.
- Can two sets be equal if they have different cardinalities? (blackboard)
- **Power set:** Given a set S, the power set $\mathcal{P}(S)$ is the set of all possible subsets of S.

  Example: What is the power set of $\{0, 1, 2\}$? (blackboard)

Truth set

- A truth set is a special type of a set.

- **Definition:** The truth set of a statement $P(x)$ is the set of all values of x that make the statement $P(x)$ true, i.e.,

$$\text{Truth set of } P(x) := \{x | P(x)\}.$$

- **Example 1:** $P(n) := n$ is an even prime number

  The truth set is $\{2\}$, since 2 is the only even prime number
- **Example 2:** Let $Q(x)$ be $x + 1 = 0$
  - If the domain of x is the set of naturals, the truth set is the empty set $\{\}$ denoted as $\emptyset$.
  - If the domain is the set of integers, the truth set is $\{-1\}$.

Operations on sets

- The intersection of two sets A, B is denoted $A \cap B$ and is defined as follows:

$$A \cap B := \{x | x \in A \text{ and } x \in B\}.$$

- The union of A, B is the set of $A \cup B$ and is defined as follows:

$$A \cup B := \{x | x \in A \text{ or } x \in B\}.$$

- The difference of A, B is the set $A \backslash B$ (also denoted as $A - B$) defined as follows:

$$A \backslash B := \{x | x \in A \text{ and } x \notin B\}.$$

- The complement $\bar{A}$ of a set A is defined as $\bar{A} := \text{Domain} \backslash A$. We refer to the domain frequently as *universe* and we denote it as U.

Venn diagrams

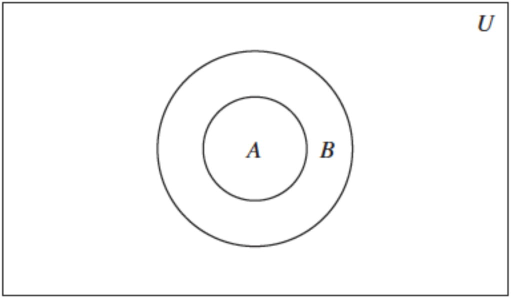
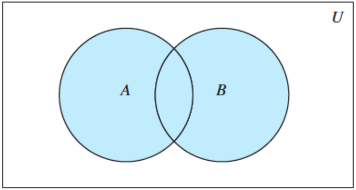


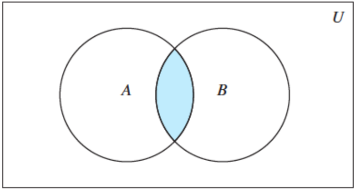
FIGURE 2 **Venn diagram showing that A is a subset of B.**

Venn diagrams



$A \cup B$ is shaded.

FIGURE 1 **Venn diagram of the union of A and B.**



$A \cap B$ is shaded.

FIGURE 2 **Venn diagram of the intersection of A and B.**

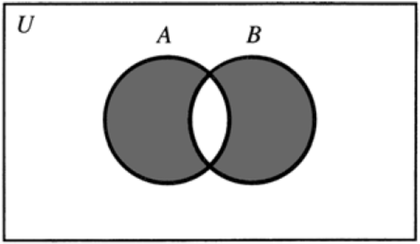
Problems on sets – Exercise

- Suppose $A = \{1, 2, 3, 4, 5\}, B = \{2, 4, 6, 8, 10\}$.
  - Visualize the sets using Venn diagrams
  - List the elements of the following sets
    1. $A \cap B$
    2. $A \cup B$
    3. $A \backslash B$
    4. $(A \backslash B) \cup (B \backslash A)$
    5. $(A \backslash B) \cap (B \backslash A)$
  - Prove that $|A \cup B| = |A| + |B| - |A \cap B|$. Generalize.

[Proof on blackboard]

Symmetric difference

- The set $(A \backslash B) \cap (B \backslash A)$ is an important set.
- The corresponding operation is also known as the symmetric difference of A, B and is denoted as $A \triangle B$



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

Problems on sets – Exercise

- Let A, B be sets such that $A \cap B = A$. Prove that $A \subseteq B$.

  To prove this, we follow the steps we have seen in class

  1. Read carefully. What is given to you, and what is asked? **Understand the problem**!
  2. Design a proof strategy.
  3. Complete the proof.

- Ideas?

Problems on sets – Exercise

Let's identify what is given, and what we are being asked to prove.

- Givens: $A \cap B = A$
- Goal: $\forall x(x \in A \rightarrow x \in B)$

Therefore, we may design a direct proof, where we consider an arbitrary $x \in A$, and prove $x \in B$.

- Givens: $A \cap B = A$, arbitrary $x \in A$
- Goal: $x \in B$

Problems on sets – Exercise

Therefore a direct proof outline would like this:

- Suppose $A \cap B = A$.
- Choose an arbitrary x
- Prove that if $x \in A$ then $x \in B$
- Since x was arbitrary we can conclude that $A \subseteq B$.

- Now that we have designed the proof, and filled all the details, we write it down nicely.

Proof: Suppose $A \cap B = A$, and $x \in A$. Since $A = A \cap B = A$, $x \in A \cap B$ and therefore $x \in B$ as well. Therefore, $A \subseteq B$. **QED**

Problems on sets – Exercise

- Prove that $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ (first De Morgan law for sets.)

$$
\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union} \\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}
$$

Set identities

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws