Sets and Logic

CSC 1300 – Discrete Structures
Villanova University

Major Themes

• Sets
  – Ways of defining sets
  – Subsets, complements, the universal set
  – Venn diagrams
  – Proofs of set equality via double inclusion

• Logic
  – Propositions
  – Truth tables
  – Venn diagrams
  – Quantifiers
  – Proof techniques: direct, indirect, contradiction

Basic terminology

A set is an unordered collection of distinct objects called elements or members of the set. The cardinality of a finite set S is denoted |S|.

The notation x ∈ S — means "x is an element of S"

Example: S = {2, 4, 6, 8}, |S| = 4
2 ∈ S — "2 is an element of S"
3 ∉ S — "3 is not an element of S"

Example: S = {[2, 4],[6], 8}, |S| = 3
[2, 4] ∈ S — "(2,4) is an element of S"
2 ∉ S — "2 is not an element of S"

A multiset or a bag is an unordered collection of objects that are not necessarily distinct.

Some important sets

• \( \mathbb{N} = \{1, 2, 3, \ldots\} \) - the set of natural numbers
• \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) - the set of integers
• \( \mathbb{W} = \{0, 1, 2, 3, \ldots\} \) - the set of positive integers
• \( \mathbb{Z}_2 = \{0, 1\} \) - the binary digits
• \( \mathbb{R} \) - the set of real numbers
• \( \mathbb{Q} = \{x \mid x = p/q \text{ where } p, q \in \mathbb{Z}, q \neq 0\} \) - the set of rational numbers
• The empty (or null) set, denoted by \( \emptyset \), or \{ \}.
Describing sets

Two ways to describe a set:

1. By listing elements, e.g., \( S = \{2, 4, 6, 8\} \)

2. By a property, e.g.,
   \[ T = \{ x \mid x \text{ is an even positive integer} \} \]
   \( E = \{ x \in \mathbb{Z} \mid \frac{x}{2} \in \mathbb{Z} \} \)

Subsets

\( S \) is a **subset** of \( T \), denoted \( S \subseteq T \), iff every element of \( S \) is also an element of \( T \).

**Examples:**
- \( \{a, b\} \subseteq \{a, b, c\} \)
- \( \{a, b, c\} \subseteq \{a, b, c\} \)
- \( \mathbb{Z} \subseteq \mathbb{Q} \)
- \( \emptyset \subseteq S \) (for every \( S \))
- \( S \subseteq \emptyset \) (for every \( S \))

\( S \) is a **proper subset** of \( T \), denoted \( S \subset T \), iff \( S \) is a subset of \( T \) but not vice versa.

**Examples:**
- \( \{a, b\} \subset \{a, b, c\} \)
- \( \{b\} \subset \{a, b, c\} \)

**Note:**
- What about \( \emptyset \subset S \) ???

Note that \( S \subset T \) iff \( S \subseteq T \) and \( S \neq T \)

The Power Set

The **power set** of a set \( S \) is the set of all subsets of \( S \). The power set of \( S \) is denoted by \( P(S) \).

- \( P(\emptyset) = \{ \emptyset \} \)
- \( P(\{a\}) = \{ \emptyset, \{a\} \} \)
- \( P(\{a, b\}) = \{ \emptyset, \{a\}, \{b\}, \{a, b\} \} \)
- \( P(\{0, 1, 2\}) = \{ \emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\} \} \)
- \( P(\{\}) = \{ \emptyset \} \)

Note that \( |P(S)| = 2^{|S|} \)

Set equality

Two sets \( S \) and \( T \) are **equal**, denoted \( S = T \), iff they have the same elements, i.e., for every \( x \):
- if \( x \in S \) then \( x \in T \)
- if \( x \in T \) then \( x \in S \)

In other words:
- \( S = T \) iff \( S \subseteq T \) and \( T \subseteq S \)

**Proof technique:** double inclusion
Set equality

Examples:

- \{a, b\} = \{b, a\}
- \{1, 2, 3\} = \{x \mid x \text{ is an integer and } 0 < x < 4\}
- \{2, 4, 6\} = \{x \mid x = 2*y, \text{ where } y \in \{1, 2, 3\}\}

The Universal Set

We usually think of sets as subsets of a universal set \(U\).

- Example: \{a, b\} and \{b, d, e\} \(\Rightarrow U = \{a, b, c, d, e\}\)

The complement of \(S\), denoted \(\overline{S}\), is the set of elements of \(U\) that are not in \(S\).

Example: \(\{b, d, e\} = \{a, c\}\)

The set difference, denoted \(S - T\) (or \(S \setminus T\)), is the set of elements of \(S\) that are NOT also in \(T\).

Examples: \(\{a, b, c, d, e\} - \{b, d, e\} = \{a, c\}\) (Note: \(\overline{S} = U - S\))
- \(\{b, c\} - \{a, b\} = \{c\}\)

The Universal Set

Sets \(S\) and \(T\) are equal, denoted \(S = T\), iff they have the same elements, i.e.,

- \(\text{for every } x: \) if \(x \in S\) then \(x \in T\)
- if \(x \in T\) then \(x \in S\)

What does this even mean?????
Set Union and Intersection

\[ S \cup T = \{ x \mid x \in S \text{ or } x \in T \} \]
\[ S \cap T = \{ x \mid x \in S \text{ and } x \in T \} \]

Example: Let \( S = \{1,2,3,4\} \) and \( T = \{2,3,5\} \). Then
\[ S \cup T = \{1,2,3,4,5\} \]
\[ S \cap T = \{2,3\} \]

Set difference and complement

\[ S - T = \{ x \mid x \in S \text{ and } x \notin T \} \]
\[ \overline{S} = U - S \]

Example: Let \( U = \mathbb{N} \)
\( S = \{x \mid x \text{ is an integer greater than 6}\} \)
\( T = \{x \mid x \text{ is an even positive integer}\} \)
Then \( S - T = \{ x \mid x \text{ is an odd integer greater than 6}\} \)
\( \overline{S} = \{x \mid x \text{ is an integer less than or equal to 6}\} \)

Generalized unions and intersections

\[ S_1 \cap S_2 \cap \ldots \cap S_n \text{ denoted by } \bigcap_{i=1}^{n} S_i \]
\[ S_1 \cup S_2 \cup \ldots \cup S_n \text{ denoted by } \bigcup_{i=1}^{n} S_i \]

Example: Let \( S_i = \{ i \} \).
\[ \bigcap_{i=1}^{n} S_i = \text{ and } \bigcup_{i=1}^{n} S_i = \]

Another Example: Let \( A_i = \{ k \mid k = p / i, p \in \mathbb{Z} \} \).
Sets and cardinality

Let \( A = \{a, b, c\}, \quad B = \{1, 2\} \)

**cardinality** of a set = number of members
- \(|A| = 3\)
- \(|B| = 2\)

\( A \cup B = \{a, b, c, 1, 2\} \quad A \cap B = \emptyset \)

**Sum Principle:** If \( A \) and \( B \) are disjoint
- \(|A \cup B| = |A| + |B|\)

Cartesian product

Let \( A = \{a, b, c\}, \quad B = \{1, 2\} \)

The **cartesian product** is the set of ordered pairs \((x, y)\) where \(x \in A\) and \(y \in B\):

\[ A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\} \]

**Product Principle:** \(|A \times B| = |A| \cdot |B|\)

Sets and cardinality

Let \( A = \{a, b, c, d, e\}, \quad B = \{b, d\} \)

- \(|A| = 5\)
- \(|B| = 2\)

\( A \setminus B = \{a, c, e\} \)

**Difference Principle:** If \( A \subseteq B \),
- \(|A \setminus B| = |A| - |B|\)

Ordered pairs and n-tuples

**ordered pairs** \((a_1, a_2)\)

**ordered n-tuples** \((a_1, a_2, ..., a_n)\)
- represent sequences where the order of elements *does* matter and repetitions are allowed.

The **Cartesian product** of the sets \( S_1, S_2, ..., S_n \), denoted by \( S_1 \times S_2 \times ... \times S_n \), is the set of all ordered \( n \)-tuples \((s_1, s_2, ..., s_n)\) where \( s_1 \in S_1, \quad s_2 \in S_2, ..., s_n \in S_n \). In other words,

\[ S_1 \times S_2 \times ... \times S_n = \{ (s_1, s_2, ..., s_n) \mid s_1 \in S_1 \text{ and } s_2 \in S_2 \text{ and } ... \text{ and } s_n \in S_n \} \]
**Set identities**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Identity Laws</th>
<th>Associative Laws</th>
<th>Distributive Laws</th>
<th>Inclusion-Exclusion Laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S \cup \emptyset = S )</td>
<td>( S \cap U = S )</td>
<td>( S \cup (T \cup R) = (S \cup T) \cup R )</td>
<td>( S \cap (T \cap R) = (S \cap T) \cap R )</td>
<td>(</td>
</tr>
<tr>
<td>( S \cap U = S )</td>
<td>( S \cup \emptyset = S )</td>
<td>( S \cup (T \cup R) = (S \cup T) \cup R )</td>
<td>( S \cap (T \cap R) = (S \cap T) \cap R )</td>
<td>(</td>
</tr>
<tr>
<td>( S \cup S = S )</td>
<td>( S \cap S = S )</td>
<td>( S \cup (T \cup R) = (S \cup T) \cup R )</td>
<td>( S \cap (T \cap R) = (S \cap T) \cap R )</td>
<td>(</td>
</tr>
<tr>
<td>( S \cup T )</td>
<td>( S \cap T )</td>
<td>( S \cup (T \cup R) = (S \cup T) \cup R )</td>
<td>( S \cap (T \cap R) = (S \cap T) \cap R )</td>
<td>(</td>
</tr>
</tbody>
</table>

**Proving set identities - example**

Prove that \( S \cap T = S \cup T \) (de Morgan’s Law for sets).

Proof: We proceed by showing that each set is a subset of the other, i.e. \( S \cap T \subseteq S \cup T \) and \( S \cup T \subseteq S \cap T \).

1. Suppose \( x \in S \cap T \). Then \( x \notin S \cup T \). Hence, \( x \notin S \) or \( x \notin T \).
   
   Therefore, \( x \in S \cup T \).
   
   Thus, \( S \cap T \subseteq S \cup T \).

2. Now suppose \( x \in S \cup T \). Then \( x \notin S \cap T \). Hence \( x \notin S \) or \( x \notin T \).
   
   Therefore, \( x \notin S \) or \( x \notin T \). Therefore, \( x \notin S \cap T \).

   Thus, \( S \cup T \subseteq S \cap T \).

**Major Themes**

- **Sets**
  - Ways of defining sets
  - Subsets, complements, the universal set
  - Venn diagrams
  - Proofs of set equality via double inclusion

- **Logic**
  - Propositions
  - Truth tables
  - Venn diagrams
  - Quantifiers

**Why Logic?**

*Logic – a science of reasoning*

- **Basis of mathematical reasoning**
  - gives precise meaning to mathematical statements
  - is used to distinguish between valid and invalid mathematical arguments

- **Applications in CS:**
  - design of hardware
  - programming
  - artificial intelligence
  - databases
A *declarative* statement that is either **true** or **false**.

**Are the following propositions?**
- 1 + 2 = 3
- today is my birthday
- New York is the capital of the USA
- 5 - 3 + 2
- x + y > 5
- Are you a student?
- Don’t talk
- Your feet are ugly
- This sentence is false

---

**Negation**

If $p$ is a proposition, then the statement

“It is not the case that $p$”

is another proposition, called the *negation of $p$*. The negation of $p$, denoted by $\neg p$, and read “not $p$”, is true when $p$ is false, and is false when $p$ is true.

**Example:** What is the negation of “Today is Wednesday”?

The truth table for negation:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

---

**Conjunction**

The proposition “$p$ and $q$”, denoted by $p \land q$, is called the *conjunction of $p$ and $q$*. It is true when both $p$ and $q$ are true, otherwise it is false.

**Examples:**

Today is Wednesday and it is raining.

Today is Wednesday but it is not raining.

The truth table for conjunction:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Disjunction

The proposition “p or q”, denoted by \( p \lor q \), is called the disjunction of \( p \) and \( q \).
It is false when both \( p \) and \( q \) are false, otherwise it is true.

**Example:** Today is Sunday or a holiday.

The truth table for disjunction:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \lor q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Exclusive OR (XOR)

The proposition \( p \oplus q \) is called the exclusive or of \( p \) and \( q \).
It is true when exactly one of \( p \) and \( q \) is true, otherwise it is false.

**Example:** This dish comes with soup or salad.

The truth table for exclusive or:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \oplus q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Implication

The implication or conditional proposition \( p \rightarrow q \) is the proposition that is false only when \( p \) is true and \( q \) is false.

\( p \) is called the hypothesis and \( q \) is called the conclusion.

Readings for \( p \rightarrow q \):
- “if \( p \) then \( q \)”
- “\( p \) only if \( q \)”
- “\( q \) is necessary for \( p \)”
- “\( p \) implies \( q \)”
- “\( q \) if \( p \)”
- “\( q \) whenever \( p \)”

Examples of Implication Wording

If John is in L.A., then he is in California.
To be in California, it is sufficient for John to be in L.A.
To be in LA, it is necessary for John to be in California.

You will get an A if you study hard.
vs.
You will get an A only if you study hard.
More Examples of Implication wording:

If you place your order by 11:59pm December 21st, then we guarantee delivery by Christmas.

Placing your order by 11:59pm December 21st guarantees delivery by Christmas.

We guarantee delivery by Christmas if you place your order by 11:59pm December 21st.

More Examples of Implication wording:

If you place your order by 11:59pm December 21st, then we guarantee delivery by Christmas.

Placing your order by 11:59pm December 21st guarantees delivery by Christmas.

We guarantee delivery by Christmas if you place your order by 11:59pm December 21st.

is this the same too?

We guarantee delivery by Christmas only if you place your order by 11:59pm December 21st.

Biconditional

The **biconditional** \( p \iff q \) is the proposition that is true when \( p \) and \( q \) have the same truth values, and is false otherwise.

The truth table for biconditional:

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \iff q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Readings for \( p \iff q \):

- "\( p \) if and only if \( q \)"
- "\( p \) is necessary and sufficient for \( q \)"
- "If \( p \), then \( q \), and conversely"

Truth tables for more complex propositions

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( r )</th>
<th>( r \land (q \land \lnot p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Tautology
- A (compound) proposition that is always true (irrespective of the values of its components)

\[
\begin{array}{ccc|c}
p & q & r & (\neg p \land (p \lor q)) \rightarrow q \\
T & T & T & T \\
T & T & F & T \\
T & F & T & F \\
T & F & F & T \\
F & T & T & T \\
F & T & F & T \\
F & F & T & F \\
F & F & F & T \\
\end{array}
\]

Logical Equivalence
We say that two propositions are logically equivalent iff they have the same truth table.

\[
\begin{array}{ccc|c}
p & q & \neg p \lor q & p \rightarrow q \\
T & T & T & T \\
T & F & F & T \\
F & T & T & T \\
F & F & T & T \\
\end{array}
\]

* we write: \( \neg p \lor q \equiv p \rightarrow q \)
to indicate that the propositions \( \neg p \lor q \) and \( p \rightarrow q \) are logically equivalent

De Morgan’s Laws for Logic
First De Morgan’s law for logic:
\( \neg (p \lor q) \equiv (\neg p) \land (\neg q) \)

Example: Negate: “Today is Sunday or a holiday”

Second De Morgan’s law for logic:
\( \neg (p \land q) \equiv \\

Example: Negate: “Today is Sunday and a holiday”

Converse, Inverse and Contrapositive
- \( q \rightarrow p \) is called the converse of \( p \rightarrow q \)
- \( \neg p \rightarrow \neg q \) is called the inverse of \( p \rightarrow q \)
- \( \neg q \rightarrow \neg p \) is called the contrapositive of \( p \rightarrow q \)

Which of the above are logically equivalent?
Propositional functions

Interesting statements involve variables.

Definition: A propositional function \( P(x) \) is a function whose values are propositions, i.e., it’s an assignment to each element \( x \) of the function’s domain \( D \) called the domain of discourse a proposition (a true or false statement).

Example

Let \( P(x) \) denote the statement “\( x \) is even”.

Domain of discourse?

\( P(2) \)

\( P(3) \)

\[ \forall x \, P(x) \]

universal quantifier

Examples of universal quantification

\[ \forall x \, (x + 0 = x) \]

\[ \forall x \, (x^2 > x) \]

\[ \forall x \, P(x) \text{ where } P(x) \text{ denotes the statement “} x \text{ loves CS”} \]

Let \( M(x) \) denote “\( x \) is mortal” and \( H(x) \) denote “\( x \) is a human”

Express the proposition: “every human is mortal”

Universal quantifier

Definition: universal quantification of \( P(x) \)

“\( P(x) \) is true for all values of \( x \) in its universe of discourse”

“for all \( x \, P(x) \)”

“for every \( x \, P(x) \)”

\[ \forall x \, P(x) \]

Existential quantifier

Definition: existential quantification of \( P(x) \)

“there exists an element \( x \) in its universe of discourse such that \( P(x) \) is true”

“there is an \( x \) such that \( P(x) \)”

“for some \( x \, P(x) \)”

\[ \exists x \, P(x) \]

existential quantifier.
Examples of existential quantification

True or false?

∃x (x + x = x * x)
∃x (x = x + 1)
∃x P(x) where P(x) denotes the statement “x loves math”

Let Q(x) denote “x is a sophomore”
Express the proposition: “there is a sophomore who loves math”

Generalized De Morgan Laws of Logic

• ¬∀xP(x) ≡ ∃x¬P(x)
  “Not everyone loves CS”
  ≡
  “There is someone who does not love CS”

• ¬∃x¬P(x) ≡ ∀x¬P(x) ≡ ∀xP(x)
  “There is no one who does not love CS”
  ≡
  “Everyone loves CS”

Expressions with several quantifiers

Let the universe of discourse be the set of all students (of VU).
Let

C(x) means “x has a computer”
F(x,y) means “x and y are friends”

Translate the following into English:

• ∀xC(x)
• ∀x[C(x) ∨ ∃y(F(x,y) ∧ C(y))]
• ∃x ¬∃y F(x,y)

Does the order of the quantifiers matter?

— No, if we have several consecutive quantifiers of the same type:

∀x∀yQ(x,y) ≡ ∀y∀xQ(x,y)  ∃x∃yQ(x,y) ≡ ∃y∃xQ(x,y)

— Yes, if we have different quantifiers:

∀x∃yQ(x,y) ∨ ∀y∀xQ(x,y)

Counterexample: Let Q(x,y) mean “x+y=0”, and let the universe of discourse be the set of all real numbers. What is the truth value of:

∀x∃yQ(x,y) ?
∃y∀xQ(x,y) ?
Mathematical System

- Theorems: proved to be true
- Axioms: assumed to be true
- Definitions: used to create terms

Logic is a tool for the analysis of inference.

Rules of Inference

Basic Terminology

- Axiom (postulate): underlying assumption, does not require a proof
- Rules of inference: used to draw conclusions from other assertions
- Proof: a sequence of statements, each of which is:
  - an axiom or
  - follows from one or more earlier statements
  and the last statement in the sequence is $A$
- Informal proof vs. formal: uses rules of inference informally and formally, respectively
- Theorem: a statement that has been proved
- Lemma: a theorem used in the proof of other theorems
- Corollary: a theorem that immediately follows from another theorem

Types of proofs

- Direct
- Indirect (by contrapositive)
- By contradiction
- Proof of equivalence
- Proof by cases
- Proof by mathematical induction

Proving $p \rightarrow q$

- Direct Proof
  
- Indirect Proof / Contrapositive
  
- Proof by Contradiction
  $p \rightarrow q \equiv (p \land \neg q) \rightarrow (r \land \neg r)$
Direct Proof

To prove $p \rightarrow q$:
Suppose $p$ is true; prove that $q$ must also be true

**Example:**
If $n$ is even, then $n^2$ is also even

Indirect Proof

Prove $p \rightarrow q$ by proving contrapositive: $\neg q \rightarrow \neg p$

**Example:**
If $n \cdot m$ is odd, then an $n \times m$ grid cannot be tiled with dominoes.

Contradiction Proof

*Prove $s$ by showing that $\neg s$ is absurd!*

• $\neg s \rightarrow F$  (*Reductio ad absurdum*)

**Example:** $\sqrt{2}$ is irrational

Proofs of equivalence

A *proof of equivalence* of two assertions (i.e., $p \Leftrightarrow q$),
often stated by using “if and only if” or “necessary and sufficient,” requires two separate parts:

$p \rightarrow q$ and $q \rightarrow p$.

• **Example:** An integer $n$ is odd iff $n^2$ is odd.
Proofs by cases

A proof by cases is based on partitioning the theorem’s domain into subdomains and proving the theorem separately for each of these subdomains.

Definition:

\( \lfloor x \rfloor \), called the floor of x, is the largest integer \( \leq x \);

\( \lceil x \rceil \), called the ceiling of x, is the smallest integer \( \geq x \).

Example: \( \forall n \in \mathbb{Z}, \; \lfloor n/2 \rfloor + \lceil n/2 \rceil = n \)

Proofs, examples, and counterexamples: \( \forall x \, P(x) \)

For universal statements:

• Checking validity of a theorem for specific examples does NOT constitute a proof (unless the examples exhaust all the values in the theorem’s domain, which is impossible if the latter is infinite).

• Just a single example suffices to disprove a theorem.
  (Such an example is usually called a counterexample).

Proofs, examples, and counterexamples: \( \exists x \, P(x) \)

For existential statements:

• A single example suffices to prove the theorem (constructive proof).

• Alternatively, using contradiction, prove that it is not possible for such a thing not to exist. (non-constructive proof)
  • Show that a player in a game has a winning strategy without actually saying what it is!
  • Famous proof: There exist irrational \( x, y \) such that \( x^y \) is rational

Which Proof Method?

1. Begin with a direct proof approach
2. If this fails, try either
   – indirect / contrapositive approach
   – proof by contradiction
   – proof by cases
   – a combination...
Major Themes

• Sets
  – Ways of defining sets
  – Subsets, complements, the universal set
  – Venn diagrams
  – Proofs of set equality via double inclusion

• Logic
  – Propositions
  – Truth tables
  – Venn diagrams
  – Quantifiers
  – Proof techniques: direct, indirect, contradiction