A proposition is a statement that is either true or false

Non-propositions
- Sky is beautiful!
- Tomorrow will be sunny.

Examples of propositions
- $2 + 3 = 5$
- $n^2 + n + 41$ is always prime
Conjecture: \( a^4 + b^4 + c^4 = d^4 \) has no solutions if \( a, b, c \) and \( d \) are all positive integers \([\text{Euler}]\)

\[1\] “Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.

Conjecture: $a^4 + b^4 + c^4 = d^4$ has no solutions if $a$, $b$, $c$ and $d$ are all positive integers [Euler]

- Shown false after 200+ years for $a = 95800$, $b = 217519$, $c = 414560$ and $d = 422481$. 

---

Conjecture: \( a^4 + b^4 + c^4 = d^4 \) has no solutions if \( a, b, c \) and \( d \) are all positive integers [Euler]
- Shown false after 200+ years for \( a = 95800, b = 217519, c = 414560 \) and \( d = 422481 \).

**Four color theorem**: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.

---

Claims, Conjectures and Theorems (all propositions)

Conjecture: \[ a^4 + b^4 + c^4 = d^4 \] has no solutions if \( a, b, c \) and \( d \) are all positive integers [Euler]
- Shown false after 200+ years for \( a = 95800, b = 217519, c = 414560 \) and \( d = 422481 \).

Four color theorem: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.
- Shown to be true using software\(^1\).

---

\(^1\)“Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.

Claims, Conjectures and Theorems (all propositions)

Conjecture: $a^4 + b^4 + c^4 = d^4$ has no solutions if $a$, $b$, $c$ and $d$ are all positive integers [Euler]
- Shown false after 200+ years for $a = 95800$, $b = 217519$, $c = 414560$ and $d = 422481$.

Four color theorem: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.
- Shown to be true using software\(^1\).

Fermat’s Theorem: $x^n + y^n = z^n$ has no integral solutions for $n > 2$.

\(^1\)“Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.
Claims, Conjectures and Theorems (all propositions)

Conjecture: \(a^4 + b^4 + c^4 = d^4\) has no solutions if \(a, b, c\) and \(d\) are all positive integers [Euler]
- Shown false after 200+ years for \(a = 95800, b = 217519, c = 414560\) and \(d = 422481\).

Four color theorem: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.
- Shown to be true using software\(^1\).

Fermat’s Theorem: \(x^n + y^n = z^n\) has no integral solutions for \(n > 2\).
- Fermat omitted the proof in 1630 because “it did not fit in the margin”
- Remained unproven for 300+ years\(^2\).

---

\(^1\)“Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.
Claims, Conjectures and Theorems (all propositions)

Conjecture: \( a^4 + b^4 + c^4 = d^4 \) has no solutions if \( a, b, c \) and \( d \) are all positive integers [Euler]

- Shown false after 200+ years for \( a = 95800 \), \( b = 217519 \), \( c = 414560 \) and \( d = 422481 \).

Four color theorem: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.

- Shown to be true using software\(^1\).

Fermat’s Theorem: \( x^n + y^n = z^n \) has no integral solutions for \( n > 2 \).

- Fermat omitted the proof in 1630 because “it did not fit in the margin”
- Remained unproven for 300+ years\(^2\).

Goldbach’s Conjecture: Every even integer greater than 2 is the sum of two primes.

---

\(^1\)“Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.

Conjecture: \(a^4 + b^4 + c^4 = d^4\) has no solutions if \(a, b, c\) and \(d\) are all positive integers [Euler]
- Shown false after 200+ years for \(a = 95800\), \(b = 217519\), \(c = 414560\) and \(d = 422481\).

Four color theorem: Every map can be colored with at most 4 colors while ensuring that no two adjacent regions have the same color.
- Shown to be true using software\(^1\).

Fermat’s Theorem: \(x^n + y^n = z^n\) has no integral solutions for \(n > 2\).
- Fermat omitted the proof in 1630 because “it did not fit in the margin”
- Remained unproven for 300+ years\(^2\).

Goldbach’s Conjecture: Every even integer greater than 2 is the sum of two primes.
- Holds for numbers up to \(10^{18}\), but unknown if it is always true

\(^1\)“Four Colors Suffice. How the Map Problem was Solved,” Robin Wilson, Princeton Univ. Press, 2003.
Logical Formulas (Textbook §3.1)

- Obtained by combining propositions using logical connectives (aka logical operators)
  - $\land$ (“and” operation)
  - $\lor$ (“or” operation)
  - $\neg$ (“not” operation)
  - $\rightarrow$ (“implies” operation)
If humans are mortal \textbf{and} Greeks are human \textbf{then} Greeks are mortal
English to Logic Formulas

\[ P ::= \text{“you get an A in the final exam”} \]

\[ Q ::= \text{“you do every problem in the book”} \]

\[ R ::= \text{“you get an A in the course”} \]

- If you do every problem in the book, you will get an A in the final exam
- You got an A in the course but you did not do every problem in the book
- To get an A in the class, it is necessary to get an A on the final.
## Truth Tables

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \rightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$\neg P$</th>
<th>$\neg P \lor Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using Truth Tables to Evaluate Logical Formulas

Does $P \rightarrow Q$ imply $\neg Q \rightarrow \neg P$?

All the two formulas equivalent?
Does $P \rightarrow Q$ imply $\neg P \rightarrow \neg Q$?
Validity, Satisfiability and Equivalence

- A formula $\varphi$ is **valid** iff it is true for all possible values of propositions in them
  - Example: $P \lor \neg P$

- A formula $\varphi$ is **satisfiable** iff it is true for some values of the propositions in them
  - Most formulas are satisfiable
  - Example: $P \rightarrow Q$

- A formula $\varphi$ is **equivalent** to $\psi$ iff they have the exact same value for all possible values of the propositions contained in them
Using Truth Tables to Show Equivalence

What about \( \neg(P \land Q) \) and \( \neg P \lor \neg Q \)?

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( \neg P )</th>
<th>( \neg Q )</th>
<th>( \neg(P \land Q) )</th>
<th>( \neg P \lor \neg Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
<td>( F )</td>
<td>( F )</td>
</tr>
</tbody>
</table>

The truth tables for \( \neg(P \land Q) \) and \( \neg P \lor \neg Q \) match, so we conclude they are equivalent:

\[
\neg(P \land Q) \iff \neg P \lor \neg Q \quad [\text{De Morgan’s Law}]
\]
De Morgan’s Law Examples

\[ \neg(P \vee Q) \]
\[ \neg(P \wedge Q \wedge R) \]
\[ \neg(P \wedge (Q \rightarrow R)) \]
Disjunctive Normal Form (DNF)

- Formulas are of the form
  $\psi_1 \lor \psi_2 \lor \cdots \lor \psi_n$
  where each $\psi$ is a conjunction of (possibly negated) propositions.
- Example: $P_1 \land \neg P_2 \land P_3$
- Any propositional formula can be transformed into a DNF formula that is logically equivalent.
Properties of Boolean Operators

<table>
<thead>
<tr>
<th></th>
<th>Propagation of Logical Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commutativity</strong></td>
<td>$P \lor Q = Q \lor P$</td>
</tr>
<tr>
<td></td>
<td>$P \land Q = Q \land P$</td>
</tr>
<tr>
<td><strong>Associativity</strong></td>
<td>$P \lor (Q \lor R) = (P \lor Q) \lor R$</td>
</tr>
<tr>
<td></td>
<td>$P \land (Q \land R) = (P \land Q) \land R$</td>
</tr>
<tr>
<td><strong>Distributivity</strong></td>
<td>$P \lor (Q \land R) = (P \lor Q) \land (P \lor R)$</td>
</tr>
<tr>
<td></td>
<td>$P \land (Q \lor R) = (P \land Q) \lor (P \land R)$</td>
</tr>
<tr>
<td><strong>De Morgan’s Laws</strong></td>
<td>$\neg (P \lor Q) = \neg P \land \neg Q$</td>
</tr>
<tr>
<td></td>
<td>$\neg (P \land Q) = \neg P \lor \neg Q$</td>
</tr>
</tbody>
</table>

- Compare these laws with those for arithmetic, with ‘+’ for ‘∨’ and ‘∗’ for ‘∧’.

- Which of the properties hold? Which ones don’t?

- Conversion to DNF: Use these laws systematically to convert any boolean formula to DNF.
Conjunctive Normal Form (CNF) and the SAT problem

- Formulas are of the form

\[ \psi_1 \land \psi_2 \land \cdots \land \psi_n \]

where each \( \psi \) is a conjunction of (possibly negated) propositions.

- Example: \( P_1 \land \lnot P_2 \land P_3 \)

- Any propositional formula can be transformed into an equivalent formula in CNF.
  - Use boolean operator properties systematically.

- SAT problem: Given a CNF formula, determine if it is satisfiable.
  - No efficient algorithm known
  - Forms the basis of NP-completeness and the \( P \neq NP \) hypothesis
Axiom: a proposition accepted to be true.

- Usually, no way to prove them; and they seem obviously true.
- Example: there exists a straight line between any two points
Axiom: a proposition accepted to be true.
  - Usually, no way to prove them; and they seem obviously true.
  - Example: there exists a straight line between any two points

Inference rule: an axiom to derive new propositions from existing ones

\[
P, P \rightarrow Q \quad \frac{Q}{Q} \quad \text{(modus ponens)}
\]
Axiom: a proposition accepted to be true.

- Usually, no way to prove them; and they seem obviously true.
- Example: there exists a straight line between any two points

Inference rule: an axiom to derive new propositions from existing ones

$$ P, P \rightarrow Q \quad \Rightarrow \quad Q $$

(modus ponens)

Theorems, Lemmas: Propositions that can be derived from axioms using inference rules
Axioms, Inference Rules, Theorems and Proofs (Textbook §1.3)

Axiom: a proposition accepted to be true.
- Usually, no way to prove them; and they seem obviously true.
- Example: there exists a straight line between any two points

Inference rule: an axiom to derive new propositions from existing ones

\[ P, P \rightarrow Q \quad \Rightarrow \quad Q \]  \hspace{1cm} (modus ponens)

Theorems, Lemmas: Propositions that can be derived from axioms using inference rules

(Formal) Proof: The exact manner in which a theorem was derived from axioms.
Example of a Formal Proof

Use inference rule

\[
\varphi, \varphi \rightarrow \psi \\
\frac{}{\psi}
\]

with no axioms

and given \( P \) and \( P \rightarrow (P \rightarrow R) \)

formally prove \( R \)
Automated Theorem Proving and AI

Problem: Given a set of axioms $A$, inference rules $I$, and a proposition $P$, identify a way to derive $P$ using $A$ and $I$.

Challenge: many possible propositions to which inference rules can be applied at each possible proof step. How to find the "right" application?

Humans rely on intuition and insight.

Computers can rely on brute force (search through all possibilities), or "intelligent heuristics". At one point, the AI community was mostly focused on such heuristics.
Automated Theorem Proving and AI

- Problem: Given a set of axioms $\mathcal{A}$, inference rules $\mathcal{I}$, and a proposition $P$, identify a way to derive $P$ using $\mathcal{A}$ and $\mathcal{I}$

- Challenge: many possible propositions to which inference rules can be applied at each possible proof step. How to find the “right” application?
Automated Theorem Proving and AI

Problem: Given a set of axioms $A$, inference rules $I$, and a proposition $P$, identify a way to derive $P$ using $A$ and $I$

Challenge: many possible propositions to which inference rules can be applied at each possible proof step. How to find the “right” application?

- Humans rely on intuition and insight
- Computers can rely on brute force (search through all possibilities), or “intelligent heuristics”
- At one point, AI community was mostly focused on such heuristics
Example of a Proof Search
Proof Checking or Machine-Checkable Proof

- Identifies the axioms, intermediate lemmas and inference rules used in each step of the proof
- At this point, a machine only needs to check if each step of the proof is correct. No search is needed
- Proof-checking is easy.
  - Machine checkable proofs are increasingly being used in CS research, and to a lesser extent, by practitioners.
Formal proofs are extremely long
- Typically too laborious/tedious for humans to create
- So they are done by machines

So, our proofs will not be quite as formal
- We will rely on numerous “known” results
  - Most things we have learned from high school math
  - When in doubt, make sure that you state your assumptions
Proving an Implication $P \rightarrow Q$

- Strategy 1: Assume $P$, show that $Q$ follows
- Example: If $2 < x < 4$ then $x^2 - 6x + 8 < 0$
Proving an Implication $P \rightarrow Q$

- Strategy 2: Prove the contrapositive $\neg Q \rightarrow \neg P$
- Example: If $r$ is irrational then $\sqrt{r}$ is irrational
Proving $P$ iff $Q$ ("$P$ if and only if $Q$")

- $P \leftrightarrow Q$ is proved by showing $P \rightarrow Q$ and then $Q \rightarrow P$
- Example: $2 < x < 4$ iff $x^2 - 6x + 8 < 0$
Proof by Cases

- To prove $P \rightarrow Q$ when $P$ is complex

- We can simplify the proof by “breaking up” $P$ into cases:
  - Find $P_1, P_2$ such that $P \rightarrow P_1 \lor P_2$
  - Prove $P_1 \rightarrow Q$ and $P_2 \rightarrow Q$
  - Note $P_1$ and $P_2$ can overlap, i.e., they can simultaneously be true.
    - But most proofs consider mutually exclusive cases
  - $P_i$’s must be exhaustive, i.e., cover every possible case when $P$ could be true
Proof by Cases

Example: $max(r, s) + min(r, s) = r + s$
False Hypothesis and Vacuous Truth

What happens to $P \rightarrow Q$ when $P$ is false?

- In this case, $P \rightarrow Q$ holds *vacuously*
- So, $F \rightarrow Q$ for any $Q$!
- If $P$ is false, then $P \rightarrow \neg P$ holds!

- Take the contrapositive of this, you get

- Basis of proof-by-contradiction strategy
Proof by Contradiction

Example: Show that there are infinitely many primes
Unit Summary

- Propositions, claims, conjectures and theorems
- Logical formulas
  - English to logical formulas
  - Truth tables: construction and use
  - Validity, satisfiability and equivalence
  - Equivalences among logical operators
    - DNF, CNF and SAT
- Axioms and inference rules
  - Formal proofs
    - Machine-checkable proofs and automated theorem proving
- Proof techniques
  - Proving an implication
    - Proving the contrapositive, proving equivalence
  - Proof by cases
  - Proof by contradiction