Propositions (Textbook Chapter 1)

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

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]

[1]"Four Colors Suffice. How the Map Problem was Solved," Robin Wilson, Princeton Univ. Press, 2003.
[2]"Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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 $d = 422481$.

[1]"Four Colors Suffice. How the Map Problem was Solved," Robin Wilson, Princeton Univ. Press, 2003.
[2]"Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.

---

[1]"Four Colors Suffice. How the Map Problem was Solved," Robin Wilson, Princeton Univ. Press, 2003.
[2]"Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.
[2] "Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.
[2] "Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.
[2] "Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.
[2] "Fermat's Enigma," Simon Singh, Walker & Company, 1997.

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.

- 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.

[2] "Fermat's Enigma," Simon Singh, Walker & Company, 1997.

Logical Formulas (Textbook Chapter 3)

- Obtained by combining propositions using logical connectives (aka logical operators)

  $\wedge$ (“and” operation)
  $\vee$ (“or” operation)
  $\neg$ (“not” operation)
  $\rightarrow$ (“implies” operation)

Properties of $\vee$, $\wedge$ and $\neg$

Commutativity	$P \vee Q \leftrightarrow Q \vee P$	$P \wedge Q \leftrightarrow Q \wedge P$

Properties of $\vee$, $\wedge$ and $\neg$

Commutativity	$P \vee Q \leftrightarrow Q \vee P$	$P \wedge Q \leftrightarrow Q \wedge P$
Associativity	$P \vee (Q \vee R) \leftrightarrow (P \vee Q) \vee R$	$P \wedge (Q \wedge R) \leftrightarrow (P \wedge Q) \wedge R$

Properties of $\vee$, $\wedge$ and $\neg$

Commutativity	$P \vee Q \leftrightarrow Q \vee P$	$P \wedge Q \leftrightarrow Q \wedge P$
Associativity	$P \vee (Q \vee R) \leftrightarrow (P \vee Q) \vee R$	$P \wedge (Q \wedge R) \leftrightarrow (P \wedge Q) \wedge R$
Distributivity	$P \vee (Q \wedge R) \leftrightarrow (P \vee Q) \wedge (P \vee R)$	$P \wedge (Q \vee R) \leftrightarrow (P \wedge Q) \vee (P \wedge R)$

Properties of $\vee$, $\wedge$ and $\neg$

Commutativity	$P \vee Q \leftrightarrow Q \vee P$	$P \wedge Q \leftrightarrow Q \wedge P$
Associativity	$P \vee (Q \vee R) \leftrightarrow (P \vee Q) \vee R$	$P \wedge (Q \wedge R) \leftrightarrow (P \wedge Q) \wedge R$
Distributivity	$P \vee (Q \wedge R) \leftrightarrow (P \vee Q) \wedge (P \vee R)$	$P \wedge (Q \vee R) \leftrightarrow (P \wedge Q) \vee (P \wedge R)$
De Morgan's Laws	$\neg(P \vee Q) \leftrightarrow \neg P \wedge \neg Q$	$\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$

Properties of ∨, ∧ and ¬

Commutativity	$P \vee Q \leftrightarrow Q \vee P$	$P \wedge Q \leftrightarrow Q \wedge P$
Associativity	$P \vee (Q \vee R) \leftrightarrow (P \vee Q) \vee R$	$P \wedge (Q \wedge R) \leftrightarrow (P \wedge Q) \wedge R$
Distributivity	$P \vee (Q \wedge R) \leftrightarrow (P \vee Q) \wedge (P \vee R)$	$P \wedge (Q \vee R) \leftrightarrow (P \wedge Q) \vee (P \wedge R)$
De Morgan's Laws	$\neg(P \vee Q) \leftrightarrow \neg P \wedge \neg Q$	$\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$

- Compare these laws with those for arithmetic, with '$+$' for '$\vee$' and '$*$' for '$\wedge$'.
- Which of the properties hold? Which ones don't?

De Morgan's Law Examples for Practice

- $\neg(P \vee Q)$
- $\neg(P \wedge Q \wedge R)$
- $\neg(P \wedge (Q \rightarrow R))$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$\neg\neg P \quad \leftrightarrow \quad P$$

Additional Useful Identities on ∨, ∧ and ¬

$$\neg\neg P \quad \leftrightarrow \quad P$$

$$P \lor \neg P \quad \leftrightarrow \quad \mathit{true}$$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$
\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \vee \neg P &\leftrightarrow \mathit{true} \\
P \wedge \neg P &\leftrightarrow \mathit{false}
\end{aligned}
$$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$\begin{aligned} \neg\neg P &\leftrightarrow P \\ P \vee \neg P &\leftrightarrow \mathit{true} \\ P \wedge \neg P &\leftrightarrow \mathit{false} \\ P \vee P &\leftrightarrow P \end{aligned}$$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \vee \neg P &\leftrightarrow \mathit{true} \\
P \wedge \neg P &\leftrightarrow \mathit{false} \\
P \vee P &\leftrightarrow P \\
P \wedge P &\leftrightarrow P
\end{aligned}$$

Additional Useful Identities on ∨, ∧ and ¬

$$
\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \vee \neg P &\leftrightarrow \mathit{true} \\
P \wedge \neg P &\leftrightarrow \mathit{false} \\
P \vee P &\leftrightarrow P \\
P \wedge P &\leftrightarrow P \\
\mathit{true} \vee P &\leftrightarrow \mathit{true}
\end{aligned}
$$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$
\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \vee \neg P &\leftrightarrow \mathit{true} \\
P \wedge \neg P &\leftrightarrow \mathit{false} \\
P \vee P &\leftrightarrow P \\
P \wedge P &\leftrightarrow P \\
\mathit{true} \vee P &\leftrightarrow \mathit{true} \\
\mathit{false} \vee P &\leftrightarrow P
\end{aligned}
$$

Additional Useful Identities on $\vee$, $\wedge$ and $\neg$

$$\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \vee \neg P &\leftrightarrow \mathit{true} \\
P \wedge \neg P &\leftrightarrow \mathit{false} \\
P \vee P &\leftrightarrow P \\
P \wedge P &\leftrightarrow P \\
\mathit{true} \vee P &\leftrightarrow \mathit{true} \\
\mathit{false} \vee P &\leftrightarrow P \\
\mathit{true} \wedge P &\leftrightarrow P
\end{aligned}$$

Additional Useful Identities on ∨, ∧ and ¬

$$
\begin{aligned}
\neg\neg P &\leftrightarrow P \\
P \lor \neg P &\leftrightarrow \mathit{true} \\
P \land \neg P &\leftrightarrow \mathit{false} \\
P \lor P &\leftrightarrow P \\
P \land P &\leftrightarrow P \\
\mathit{true} \lor P &\leftrightarrow \mathit{true} \\
\mathit{false} \lor P &\leftrightarrow P \\
\mathit{true} \land P &\leftrightarrow P \\
\mathit{false} \land P &\leftrightarrow \mathit{false}
\end{aligned}
$$

Propositional formula simplifications and programming

- Is there way to simplify

```
if (!((x >= 0) && (x <= 10)) || (x >= 20))
```

- What about

```
if !((x <= 20) || ((x >= 30) && (x <= 39)))
    if ((x >= 20) && (x <= 30)) || (x >= 40))
```

Conditional statement ($P \rightarrow Q$)

- P is the hypothesis/premise/antecendent, Q is the conclusion/consequence
- $P \rightarrow Q$ is also called:

"if P, then Q"	"P implies Q"
"Q follows from P"	"Q, provided that P"
...	...

Understanding Conditionals

- What is the intuitive meaning of $P \rightarrow Q$?
  - Conditional statement is like a promise
  - Under what circumstances is the promise kept/broken?
  - Example: "If tomorrow is sunny, I will take you to the beach."

P	Q	$P \rightarrow Q$
Tomorrow is sunny	Go to the beach	Promise is kept (T)
Tomorrow is sunny	Did not go to the beach	Promise is broken (F)
Tomorrow is not sunny	Go to the beach	Promise is not broken (T)
Tomorrow is not sunny	Did not go to the beach	Promise is not broken (T)

- $P \rightarrow Q$ being true because P is false is called vacuously true or true by default

English to Logic Formulas

P ::= "you get an A in the final exam"

Q ::= "you do every problem in the book"

R ::= "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.

Contrapositive, Inverse and Converse

Definitions

- Contrapositive of $P \to Q$ is $\neg q \to \neg p$
- Converse of $P \to Q$ is $q \to p$
- Inverse of $P \to Q$ is $\neg p \to \neg q$

Contrapositive, Inverse and Converse

Definitions

- Contrapositive of $P \to Q$ is $\neg q \to \neg p$
- Converse of $P \to Q$ is $q \to p$
- Inverse of $P \to Q$ is $\neg p \to \neg q$

Identities

- Conditional $\equiv$ Contrapositive ▷ Useful for proofs
- Conditional $\not\equiv$ Converse
- Conditional $\not\equiv$ Inverse
- Converse $\equiv$ Inverse

Examples of Contrapositive, Inverse and Converse

- Conditional $\equiv$ Contrapositive.
  "If tomorrow is sunny, we will go to the beach."
  "If we don't go to the beach tomorrow, then it is not sunny."

- Converse $\equiv$ Inverse.
  "If we go to the beach tomorrow, then it is sunny."
  "If tomorrow is not sunny, then we will not go to the beach."

- Conditional $\equiv$ Contrapositive.
  "If $x > 2$, then $x^2 > 4$." $\triangleright$ True
  "If $x^2 \leq 4$, then $x \leq 2$." $\triangleright$ True

- Converse $\equiv$ Inverse.
  "If $x^2 > 4$, then $x > 2$." $\triangleright$ False
  "If $x \leq 2$, then $x^2 \leq 4$." $\triangleright$ False

Necessary and Sufficient Conditions

- P is a sufficient condition for Q means $P \to Q$

Necessary and Sufficient Conditions

- P is a sufficient condition for Q means $P \rightarrow Q$
- P is a necessary condition for Q means $\neg P \rightarrow \neg Q$
  - Equivalently, $Q \rightarrow P$

Necessary and Sufficient Conditions

- P is a sufficient condition for Q means $P \rightarrow Q$
- P is a necessary condition for Q means $\neg P \rightarrow \neg Q$
  - Equivalently, $Q \rightarrow P$
- P only if Q means $P \rightarrow Q$
  - Equivalently, if P then Q

Truth Tables

P	Q	$P \to Q$

P	Q	$\neg P$	$\neg P \lor Q$

Using Truth Tables to Evaluate Logical Formulas

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

All the two formulas equivalent?

Using Truth Tables to Evaluate Logical Formulas

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

Using Truth Tables to Show Equivalence

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

P	Q	$\neg P$	$\neg Q$	$\neg(P \land Q)$	$\neg P \lor \neg Q$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	T	T
T	T	F	F	F	F

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

$$\neg(\boldsymbol{P} \land \boldsymbol{Q}) \;\leftrightarrow\; \neg \boldsymbol{P} \lor \neg \boldsymbol{Q} \qquad \text{[De Morgan's Law]}$$

Validity, Satisfiability and Equivalence

- A formula φ is *valid* iff it is true for **all** possible values of propositions in them
  - Example: $P \vee \neg P$
- A formula φ is *satisfiable* iff it is true for **some** values of the propositions in them
  - Most formulas are satisfiable
  - Example: $P \rightarrow Q$
- A formula φ is *equivalent* to ψ iff they have the exact same value for all possible values of the propositions contained in them
  - In other words, the truth tables for φ and ψ match fully
  - We saw several examples in the previous slides

Disjunctive Normal Form (DNF)

- Example: $(P \wedge \neg Q \wedge R) \;\vee\; \neg P \vee (\neg P \wedge R)$

Disjunctive Normal Form (DNF)

- Example: $(P \wedge \neg Q \wedge R) \;\vee\; \neg P \vee (\neg P \wedge R)$
- The only operator permitted at the top level is disjunction ($\vee$)
  - Only the conjunction ($\wedge$) operator is permitted at the next level
    - Only propositional variables or their negations at the third level
    - no variable is repeated within a conjunction

Disjunctive Normal Form (DNF)

- Example: $(P \wedge \neg Q \wedge R) \ \vee \ \neg P \vee (\neg P \wedge R)$
- The only operator permitted at the top level is disjunction ($\vee$)
  - Only the conjunction ($\wedge$) operator is permitted at the next level
    - Only propositional variables or their negations at the third level
    - no variable is repeated within a conjunction
- Any propositional formula can be transformed into an equivalent formula in DNF.
  - Conversion repeatedly uses the identities from previous slides.
  - But this may take time exponential in formula size
- All DNF formulas are satisfiable.

Conjunctive Normal Form (CNF) and the SAT problem

- Example: $(P \vee \neg Q \vee R) \ \wedge \ \neg P \wedge (\neg P \vee R)$

Conjunctive Normal Form (CNF) and the SAT problem

- Example: $(P \vee \neg Q \vee R) \;\wedge\; \neg P \wedge (\neg P \vee R)$
- The only operator permitted at the top level is conjunction ($\wedge$)
  - Only the disjunction ($\vee$) operator is permitted at the next level
    - Only propositional variables or their negations at the third level
    - no variable is repeated within a conjunction

Conjunctive Normal Form (CNF) and the SAT problem

- Example: $(P \vee \neg Q \vee R) \ \wedge \ \neg P \wedge (\neg P \vee R)$
- The only operator permitted at the top level is conjunction ($\wedge$)
  - Only the disjunction ($\vee$) operator is permitted at the next level
    - Only propositional variables or their negations at the third level
    - no variable is repeated within a conjunction
- **SAT** problem: Given a CNF formula, determine if it is satisfiable.
  - No efficient algorithm known
  - Forms the basis of NP-completeness, used to prove that a problem is hard
    - Any efficient algorithm for solving one NP-complete problem can be used to solve all other NP-complete problems!

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

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

$$\frac{\vdash P, \ \vdash P \to Q}{\vdash Q} \qquad (\textit{modus ponens})$$

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

$$\frac{\vdash P,\ \vdash P \rightarrow Q}{\vdash Q} \qquad (\textit{modus ponens})$$

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

$$\frac{\vdash P, \ \vdash P \to Q}{\vdash Q} \qquad (\textit{modus ponens})$$

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.

Common Proof Techniques

- (Boolean formula simplification)
- Proof by cases
- For an implication $P \to Q$, assume P and then prove Q
- Proof by contradiction
- Proof by induction

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 $P \rightarrow P_1 \vee P_2$
  - Prove $P_1 \rightarrow Q$ and $P_2 \rightarrow Q$

Proof by Cases

- To prove $P \to Q$ when P is complex
- We can simplify the proof by "breaking up" P into cases:
  - Find P_1, P_2 such that $P \to P_1 \vee P_2$
  - Prove $P_1 \to Q$ and $P_2 \to Q$
  - Note P_1 and P_2 can overlap, i.e., they can simultaneously be true.
    - But most proofs consider mutually exclusive cases

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 $P \rightarrow P_1 \vee P_2$
  - 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: $max(r, s) + min(r, s) = r + s$

Proving an Implication $P \to Q$

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

Proving an Implication $P \to Q$

- Strategy 2: Prove the contrapositive $\neg Q \to \neg P$
- Example:If r is irrational then $\sqrt{r}$ is irrational

Proving Equivalence ("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 Contradiction

- If P is false, then $P \to \neg P$ holds (vacuously).

Proof by Contradiction

- If P is false, then $P \to \neg P$ holds (vacuously).

$$\text{i.e., } \neg P \to (P \to \neg P)$$

Proof by Contradiction

- If P is false, then $P \rightarrow \neg P$ holds (vacuously).

$$\text{i.e., } \neg P \rightarrow (P \rightarrow \neg P)$$

- Take the contrapositive of this, you get

$$\text{i.e., } (P \rightarrow \neg P) \rightarrow \neg P$$

Proof by Contradiction

- If P is false, then $P \to \neg P$ holds (vacuously).

$$\text{i.e., } \neg P \to (P \to \neg P)$$

- Take the contrapositive of this, you get

$$\text{i.e., } (P \to \neg P) \to \neg P$$

- Basis of proof-by-contradiction strategy:
  - Assume P, prove $\neg P$
    - Thus, we have proved $P \to \neg P$

Proof by Contradiction

- If P is false, then $P \rightarrow \neg P$ holds (vacuously).

$$\text{i.e., } \neg P \rightarrow (P \rightarrow \neg P)$$

- Take the contrapositive of this, you get

$$\text{i.e., } (P \rightarrow \neg P) \rightarrow \neg P$$

- Basis of proof-by-contradiction strategy:
  - Assume P, prove $\neg P$
    - Thus, we have proved $P \rightarrow \neg P$
  - From this and the fact that $(P \rightarrow \neg P) \rightarrow \neg P$ we conclude $\neg P$.
    - i.e., we have proved P is false.

Knights (truth tellers) and knaves (liars)

- There is an island that consists of knights and knaves:
  - Knights always tell the truth.
  - Knaves always lie.

Knights (truth tellers) and knaves (liars)

- There is an island that consists of knights and knaves:
  - Knights always tell the truth.
  - Knaves always lie.
- You visit the island and are approached by two natives A and B:
  - A says: B is a knight.
  - B says: A and I are of opposite types.

Knights (truth tellers) and knaves (liars)

- There is an island that consists of knights and knaves:
  - Knights always tell the truth.
  - Knaves always lie.
- You visit the island and are approached by two natives A and B:
  - A says: B is a knight.
  - B says: A and I are of opposite types.
- What are A and B?

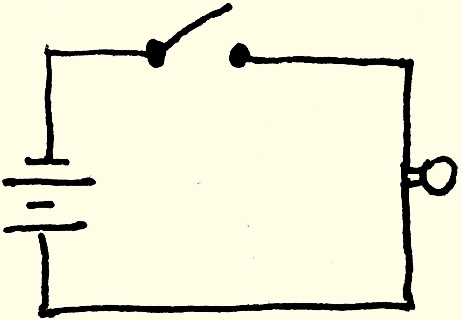
Solution: Case-splitting + Proof by contradiction

- Suppose *A* is a knight.
  - What *A* says is true. ▷ by definition of knight
  - So *B* is also a knight. ▷ That's what *A* said.
  - So, what *B* says is true. ▷ by definition of knight
  - So, *A* and *B* are of opposite types. ▷ That's what *B* said.
  - Contradiction: *A* and *B* are both knights and *A* and *B* are of opposite type.
- So, initial assumption is false. ▷ by the contradiction rule
  - So *A* is not a knight. ▷ negation of assumption
  - So *A* is a knave. ▷ by elimination: All inhabitants are knights or knaves, so since *A* is not a knight, *A* is a knave.
  - So What *A* says is false.
  - So *B* is not a knight.
  - So *B* is also a knave. ▷ by elimination
- Final answer: *A* and *B* are both knaves

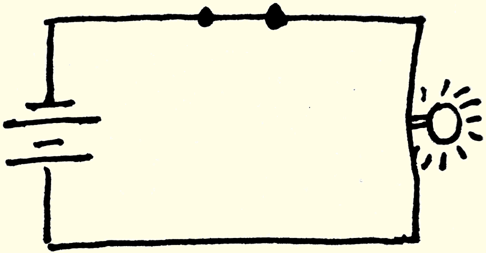
Another proof by Contradiction

Example: Show that there are infinitely many primes

Idea: Circuits and logic are related

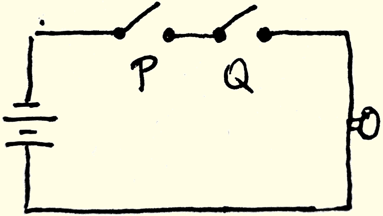


Open or off or false

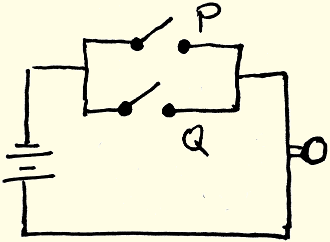


Closed or on or true

Idea: Circuits and logic are related



Switches		Light bulb
P	Q	State
closed	closed	on
closed	open	off
open	closed	off
open	open	off

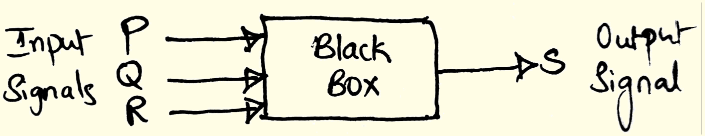


Switches		Light bulb
P	Q	State
closed	closed	on
closed	open	on
open	closed	on
open	open	off

Evolution of electronic computers

- Vacuum tube switches (1940s on)
- Semiconductor switches (transistors) from 1950s ...
- Integrated circuits from 1960s
- The number of transistors have increased by 2x every two years
  - Predicted by Gordon Moore (Moore's Law) (1965)
  - Intel 4004 processor had 2250 gates in 1971, about 10μm
  - Today's microprocessors have more than 10 to 100 billion transistors, about 10nm in size!
  - Solid state drives have several *trillion* transistors

Complicated logic gates as black boxes

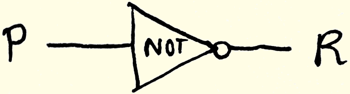


A black box focuses on the functionality and ignores the hardware implementation details

Input			Output
P	Q	R	S
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

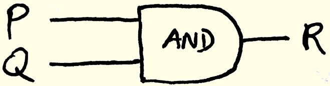
Simple logic gates

Complicated logic gates can be built using a collection of simple logic gates such as NOT-gate, AND-gate, and OR-gate



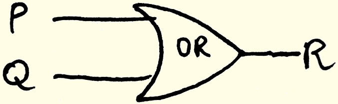
Input	Output
P	R
1	0
0	1

$$R \equiv \neg P$$



Input		Output
P	Q	R
1	1	1
1	0	0
0	1	0
0	0	0

$$R \equiv P \wedge Q$$



Input		Output
P	Q	R
1	1	1
1	0	1
0	1	1
0	0	0

$$R \equiv P \vee Q$$

Combinational Vs Sequential Logic

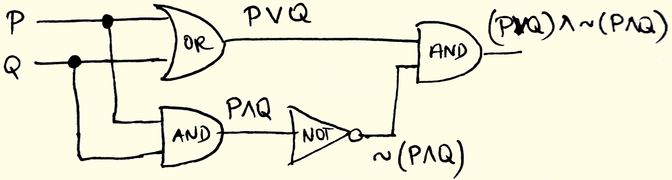
- Combinational circuit: output is purely a function of current inputs
  - Combines inputs using a series of gates
  - No output of a gate can eventually feed back into that gate.

Combinational Vs Sequential Logic

- Combinational circuit: output is purely a function of current inputs
  - Combines inputs using a series of gates
  - No output of a gate can eventually feed back into that gate.
- Sequential circuits: output feeds back into input, so it depends on current *and* previous inputs.
  - Basis of memory and sequential instruction processing
    - Basic unit is called a flip-flop, which in turn is realized using gates
  - Divides computation into steps
  - Progress from one step to next is governed by a clock

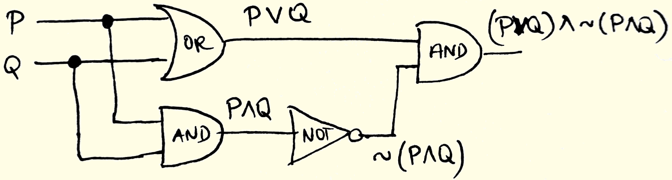
Given a circuit, compute its input/output function

- Circuit → expression



Given a circuit, compute its input/output function

- Circuit $\rightarrow$ expression



- Simplify expression: $(P \vee Q) \wedge \neg(P \wedge Q) \equiv P \oplus Q$ $\triangleright$ Exclusive or

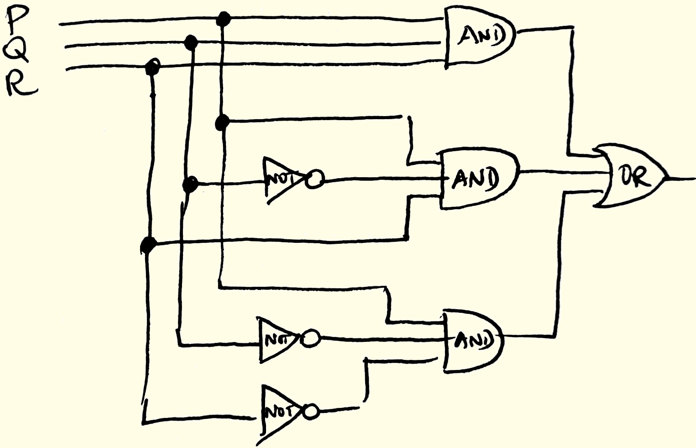
Design a circuit for realizing a given truth table

Input			Output	Expression
P	Q	R	S	S
1	1	1	1	$P \wedge Q \wedge R$
1	1	0	0	$P \wedge Q \wedge \neg R$
1	0	1	1	$P \wedge \neg Q \wedge R$
1	0	0	1	$P \wedge \neg Q \wedge \neg R$
0	1	1	0	$\neg P \wedge Q \wedge R$
0	1	0	0	$\neg P \wedge Q \wedge \neg R$
0	0	1	0	$\neg P \wedge \neg Q \wedge R$
0	0	0	0	$\neg P \wedge \neg Q \wedge \neg R$

Equivalent expression in DNF: $(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$

Design a circuit for realizing a given truth table

Input			Output	Expression
P	Q	R	S	S
1	1	1	1	$P \wedge Q \wedge R$
1	1	0	0	$P \wedge Q \wedge \neg R$
1	0	1	1	$P \wedge \neg Q \wedge R$
1	0	0	1	$P \wedge \neg Q \wedge \neg R$
0	1	1	0	$\neg P \wedge Q \wedge R$
0	1	0	0	$\neg P \wedge Q \wedge \neg R$
0	0	1	0	$\neg P \wedge \neg Q \wedge R$
0	0	0	0	$\neg P \wedge \neg Q \wedge \neg R$



Equivalent expression in DNF: $(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$

Better Version

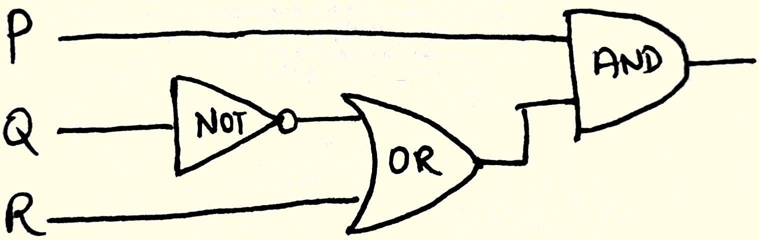
Simplify expression

$$(P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$$

to

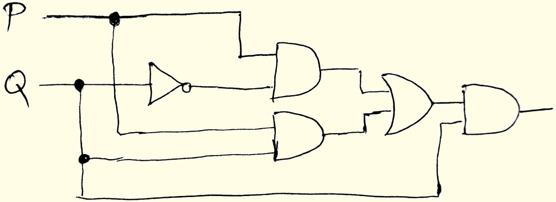
$$P \wedge (\neg Q \vee R)$$

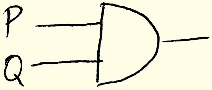
Leads to the circuit:



Equivalence of logic circuits

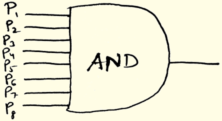
- Two digital logic circuits are called equivalent if and only if their input-output tables are identical
  - We can use boolean simplification as well!
- Show that the following two logic circuits are equivalent.

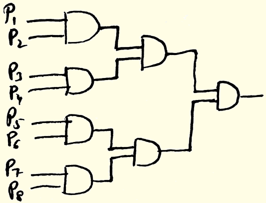




Equivalence of logic circuits

- Write this 8-input AND gate using 2-input AND gates only.

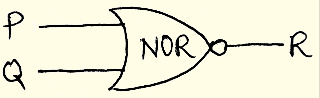




NAND and NOR gates

- NAND: $\neg(P \wedge Q)$ NOR: $\neg(P \vee Q)$
- *Note:* Every boolean function can be realized entirely using NAND gates
  - Same holds for NOR as well

Input		Output
P	Q	$R = P \mid Q$
1	1	0
1	0	1
0	1	1
0	0	1



Input		Output
P	Q	$R = P \downarrow Q$
1	1	0
1	0	0
0	1	0
0	0	1

Unit Summary

- Propositions, claims, conjectures and theorems
- Logical formulas
  - English to logical formulas
- Truth tables: construction and use
- Validity, satisfiability and equivalence
- Proof methods
- Digital circuits