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)

English to Logic Formulas

- If humans are mortal **and** Greeks are human **then** Greeks are mortal

Conditional statement ($P \to Q$)

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

"if P, then Q"	"P implies Q"
"P only if Q"	"if P, Q"
"Q follows from P"	"Q, provided that P"
"not P unless Q"	"Q if/when/whenever Q"
"P is sufficient for Q"	"a sufficient condition for Q is P"
"Q is necessary for P"	"a necessary condition for P is Q"

Understanding Conditionals

- What is the intuitive meaning of $P \to Q$?
  - 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	$P \to Q$
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)

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

Contrapositive, Inverse and Converse

Definitions

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

Identities

- Conditional $\equiv$ Contrapositive $\triangleright$ 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 $P \to Q$
- P is a necessary condition for Q means $\neg P \to \neg Q$
- P only if Q means $P \to Q$
  - Equivalently, if P then Q
- For real x, $x = 1$ is a sufficient condition for $x^2 = 1$
  i.e., If $x = 1$ then $x^2 = 1$ ▷ True
- For real x, $x^2 = 1$ is a necessary condition for $x = 1$
  i.e., If $x^2 \neq 1$ then $x \neq 1$ ▷ True
- For real x, $x = 1$ only if $x^2 = 1$
  i.e., If $x^2 \neq 1$, then $x \neq 1$ ▷ True

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.

Modeling Problems in Propositional Logic

You can't locate your glasses. You know the following statements are true:

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table.

(b) If my glasses are on the kitchen table, then I saw them at breakfast.

(c) I did not see my glasses at breakfast.

(d) I was reading the newspaper in the living room or the kitchen.

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table.

Where are the glasses?

Modeling Problems in Propositional Logic

Let:

- RK = I was reading the newspaper in the kitchen.
- GK = My glasses are on the kitchen table.
- SB = I saw my glasses at breakfast.
- RL = I was reading the newspaper in the living room.
- GC = My glasses are on the coffee table.

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $\mathrm{RK} \rightarrow \mathrm{GK}$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $\mathrm{GK} \rightarrow \mathrm{SB}$

(c) I did not see my glasses at breakfast: $\neg\, \mathrm{SB}$

(d) I was reading the newspaper in the living room or the kitchen: $\mathrm{RL} \lor \mathrm{RK}$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $\mathrm{RL} \rightarrow \mathrm{GC}$

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $RK \rightarrow GK$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $GK \rightarrow SB$

(c) I did not see my glasses at breakfast: $\neg SB$

(d) I was reading the newspaper in the living room or the kitchen: $RL \vee RK$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $RL \rightarrow GC$

- $\neg SB$

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $RK \to GK$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $GK \to SB$

(c) I did not see my glasses at breakfast: $\neg SB$

(d) I was reading the newspaper in the living room or the kitchen: $RL \vee RK$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $RL \to GC$

- $\neg SB$
- From $GK \to SB$, conclude $\neg SB \to \neg GK$

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $RK \rightarrow GK$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $GK \rightarrow SB$

(c) I did not see my glasses at breakfast: $\neg SB$

(d) I was reading the newspaper in the living room or the kitchen: $RL \vee RK$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $RL \rightarrow GC$

- $\neg SB$
- From $GK \rightarrow SB$, conclude $\neg SB \rightarrow \neg GK$
- From the above two, conclude $\neg GK$

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $\mathrm{RK} \rightarrow \mathrm{GK}$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $\mathrm{GK} \rightarrow \mathrm{SB}$

(c) I did not see my glasses at breakfast: $\neg\, \mathrm{SB}$

(d) I was reading the newspaper in the living room or the kitchen: $\mathrm{RL} \vee \mathrm{RK}$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $\mathrm{RL} \rightarrow \mathrm{GC}$

- $\neg\, \mathrm{SB}$
- From $\mathrm{GK} \rightarrow \mathrm{SB}$, conclude $\neg\mathrm{SB} \rightarrow \neg\mathrm{GK}$
- From the above two, conclude $\neg GK$
- Use (a) in a similar manner: from $\neg\, \mathrm{GK}$ and $\mathrm{RG} \rightarrow \mathrm{GK}$, conclude $\neg\, \mathrm{RK}$.

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $RK \rightarrow GK$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $GK \rightarrow SB$

(c) I did not see my glasses at breakfast: $\neg SB$

(d) I was reading the newspaper in the living room or the kitchen: $RL \vee RK$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $RL \rightarrow GC$

- $\neg SB$
- From $GK \rightarrow SB$, conclude $\neg SB \rightarrow \neg GK$
- From the above two, conclude $\neg GK$
- Use (a) in a similar manner: from $\neg GK$ and $RG \rightarrow GK$, conclude $\neg RK$.
- From $RL \vee RK$ and $\neg RK$, conclude RL.

Modeling Problems in Propositional Logic

(a) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table: $RK \rightarrow GK$

(b) If my glasses are on the kitchen table, then I saw them at breakfast: $GK \rightarrow SB$

(c) I did not see my glasses at breakfast: $\neg SB$

(d) I was reading the newspaper in the living room or the kitchen: $RL \vee RK$

(e) If I was reading the newspaper in the living room then my glasses are on the coffee table: $RL \rightarrow GC$

- $\neg SB$
- From $GK \rightarrow SB$, conclude $\neg SB \rightarrow \neg GK$
- From the above two, conclude $\neg GK$
- Use (a) in a similar manner: from $\neg GK$ and $RG \rightarrow GK$, conclude $\neg RK$.
- From $RL \vee RK$ and $\neg RK$, conclude RL.
- From RL and (e), conclude GC. So, look on the coffee table!

Example: Truth tellers and liars

- There is an island that consists of liars and truth tellers:
  - Liars always lie.
  - Truth who always tell the truth
- You visit the island and are approached by two natives A and B:
  - A says: B is a truth teller.
  - B says: A and I are of opposite types.
- What are A and B?

Truth tellers and liars: Logical Reasoning

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

Truth Tables

P	Q	$P \to Q$

P	Q	$\neg P$	$\neg P \vee Q$

Using Truth Tables to Evaluate Logical Formulas

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

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 $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$?

P	Q	$\neg P$	$\neg Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
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 $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ match, so we conclude they are equivalent:

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

De Morgan's Law Examples for Practice

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

Properties of Boolean Operators

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

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

Additional Useful Identities

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

Disjunctive Normal Form (DNF)

- Formulas of the form

$$\psi_1 \vee \psi_2 \vee \cdots \psi_n$$

  where each ψ is a conjunction of (possibly negated) propositions.
  - Example: $P_1 \wedge \neg P_2 \wedge P_3 \;\vee\; \neg P_1 \vee P_3$
- The only operator permitted at the top level is disjunction
  - Only the conjunction operator is permitted at the next level
    - Only propositional variables or their negations at the third level
- Any propositional formula can be transformed into an equivalent formula in DNF.
  - Conversion repeatedly uses the identities from previous slides.

Conjunctive Normal Form (CNF) and the SAT problem

- Formulas are of the form

$$\psi_1 \wedge \psi_2 \wedge \cdots \psi_n$$

  where each ψ is a conjunction of (possibly negated) propositions.
  - Example: $P_1 \wedge \neg P_2 \wedge P_3$
- 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

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

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

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

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

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

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

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

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.

What is a valid argument?

Definition

- An argument is valid if the conclusion follows necessarily from the premises

Valid argument: Examples

- If Socrates is a man, then Socrates is mortal.
  Socrates is a man.
  Therefore, Socrates is mortal. ▷ Valid argument
- If Socrates is a man, then Socrates is mortal.
  Socrates is mortal.
  Therefore, Socrates is a man. ▷ Invalid argument
- If Socrates is a man, then Socrates is mortal.
  Socrates is not mortal.
  Therefore, Socrates is not a man. ▷ Valid argument
- If Socrates is a man, then Socrates is mortal.
  Socrates is not a man.
  Therefore, Socrates is not mortal. ▷ Invalid argument

Valid argument: Examples

- If it is raining, then it is cloudy.
  It is raining.
  Therefore, it is cloudy. ▷ Valid argument
- If it is raining, then it is cloudy.
  It is cloudy.
  Therefore, it is raining. ▷ Invalid argument
- If it is raining, then it is cloudy.
  It is not cloudy.
  Therefore, it is not raining. ▷ Valid argument
- If it is raining, then it is cloudy.
  It is not raining.
  Therefore, it is not cloudy. ▷ Invalid argument

Valid argument: Examples

- If $x > 2$, then $x^2 > 4$.
  $x > 2$.
  Therefore, $x^2 > 4$. ▷ Valid argument
- If $x > 2$, then $x^2 > 4$.
  $x^2 > 4$.
  Therefore, $x > 2$. ▷ Invalid argument
- If $x > 2$, then $x^2 > 4$.
  $x^2 \leq 4$.
  Therefore, $x \leq 2$. ▷ Valid argument
- If $x > 2$, then $x^2 > 4$.
  $x \leq 2$.
  Therefore, $x^2 \leq 4$. ▷ Invalid argument

Valid argument: Examples

- If P, then Q.
  P.
  Therefore, Q. ▷ Valid argument
- If P, then Q.
  Q.
  Therefore, P. ▷ Invalid argument
- If P, then Q.
  $\neg Q$.
  Therefore, $\neg P$. ▷ Valid argument
- If P, then Q.
  $\neg P$.
  Therefore, $\neg Q$. ▷ Invalid argument

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

False Hypothesis and Vacuous Truth

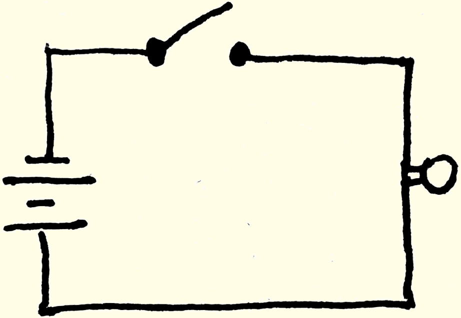
What happens to $P \rightarrow Q$ when P is false?

- In this case, $P \rightarrow Q$ holds *vacuously*
- So, $\boldsymbol{F} \rightarrow Q$ 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

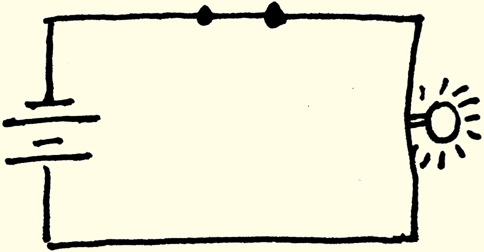
Proof by Contradiction

Example: Show that there are infinitely many primes

Idea: Circuits and logic are related

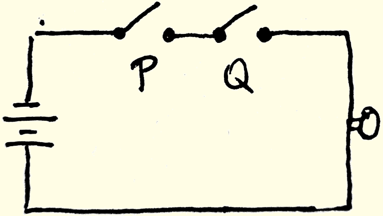


Open or off or false

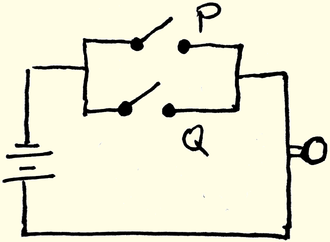


Closed or on or true

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

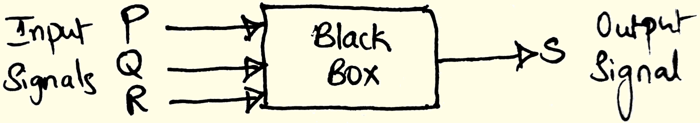
Birth of digital logic circuits

- 1930s: Mechanical switches were used in circuit design
- Late 1930s: Great idea that mathematical logic (or Boolean algebra) can be used to analyze switches
- 1940s and 1950s: Electronic switches for circuit design
  - Led to the development of electronic computers, electronic telephone switching systems, traffic light controls, electronic calculators, and the control mechanisms
- Electronic switches to implement logic is the fundamental concept that underlies all electronic digital computers

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 100 billion transistors, about 10nm!
  - Solid state drives have over 2 trillion transistors

Complicated logic gates as black boxes



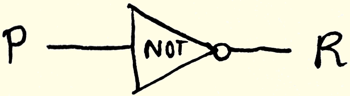
A black box focuses on the functionality and ignores the hardware implementation details

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

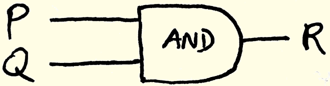
Method

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



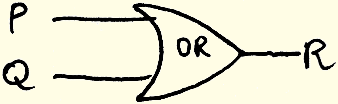
Input	Output
P	R
1	0
0	1

$R \equiv \neg P$



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

$R \equiv P \wedge Q$



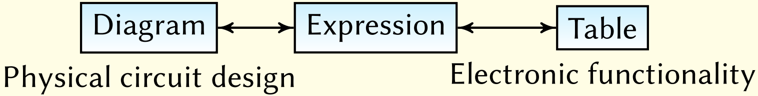
Input		Output
P	Q	R
1	1	1
1	0	1
0	1	1
0	0	0

$R \equiv P \vee Q$

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.
- 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

Problem-solving in digital logic circuits



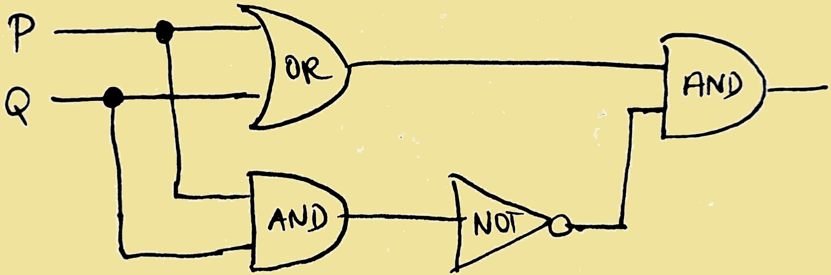
Problem-solving in digital logic circuits

- Circuit → Table
  - Logic circuit → Boolean expression
  - Simplify Boolean expression
  - Boolean expression → Input-output table
- Table → Circuit
  - Input-output table → Boolean expression
  - Simplify Boolean expression
  - Boolean expression → Logic circuit

Circuit → Table

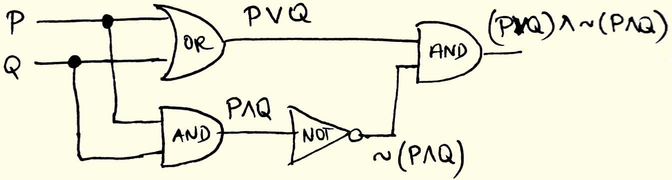
Problem

- Determine the input-output table for the given logic circuit.



Circuit → Table

- Circuit → expression



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

- Expression → table:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge \neg(P \wedge Q)$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	0	1	1
0	0	0	0	1	0

Table → Circuit

Problem

- Determine the logic circuit for the given input-output table.

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

Table → Circuit

1. Table → expression

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

   Disjunctive normal form or sum-of-products form

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	$\neg P \wedge \neg Q \wedge \neg R$

Table → Circuit

2. Expression → circuit

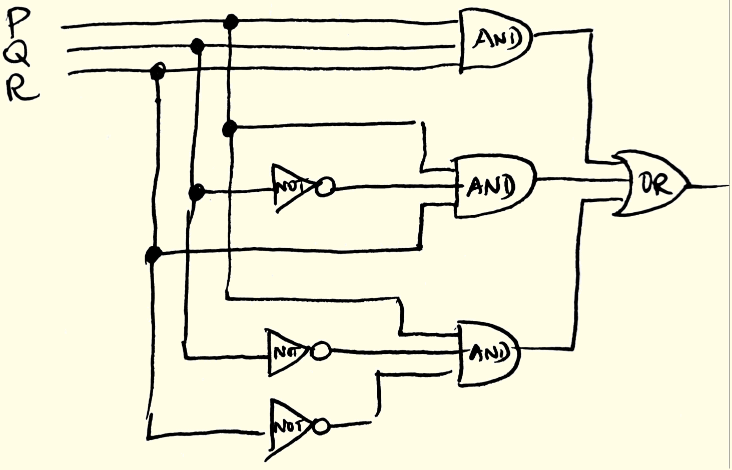
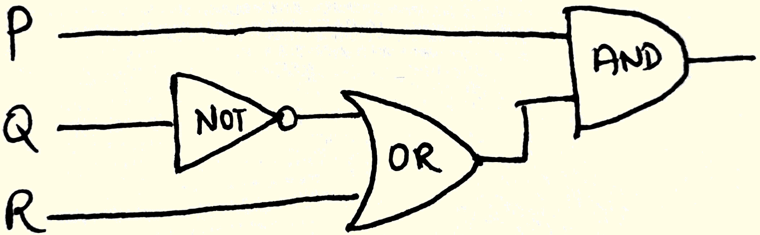


Table → Circuit: Better Version

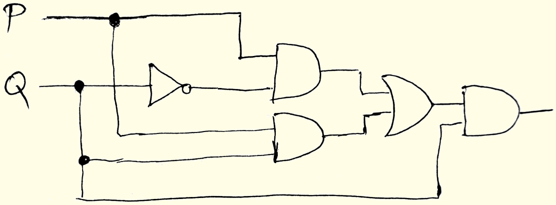
2. Simplify expression
   $(P \land Q \land R) \lor (P \land \neg Q \land R) \lor (P \land \neg Q \land \neg R)$
   $\equiv P \land (\neg Q \lor R)$ ▷ How?

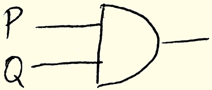
3. Expression → circuit



Equivalence of logic circuits

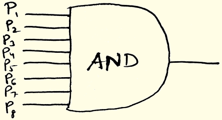
- Two digital logic circuits are called equivalent if and only if their input-output tables are identical
  - We can use boolean simplification as well!
- Show that the following two logic circuits are equivalent.

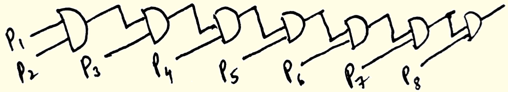


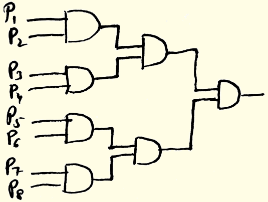


Equivalence of logic circuits

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



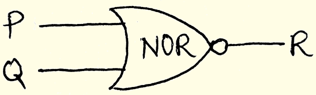




NAND and NOR gates

- 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

Logic and programming

- Is there way to simplify

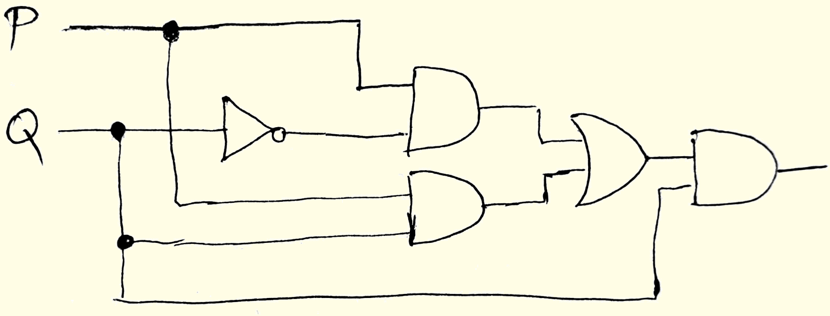
```
if (!((x >= 0) && (x <= 10)) || (x >= 20))
```

- What about

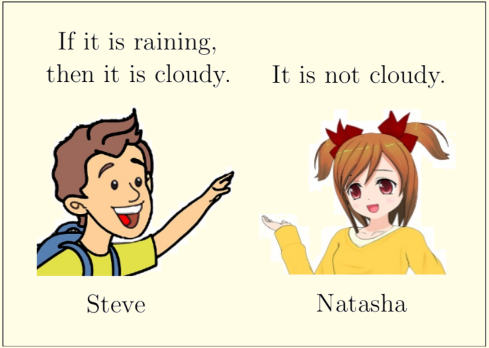
```
if !((x <= 20) || ((x >= 30) && (x <= 39)))
    if ((x >= 20) && (x <= 30)) || (x >= 40))
```

Logic and Computer Hardware

- Can the following circuit be optimized?



Logic and Reasoning



- Is John's conclusion logical?

Logic and proofs

- Proving implications: $\dfrac{P \vdash Q}{\vdash P \to Q}$
- Proving implication by showing the contrapositive: $\dfrac{\neg Q \vdash \neg P}{\vdash P \to Q}$
- Case-splitting: $\dfrac{P \wedge Q \vdash R, \ \ P \wedge \neg Q \vdash R}{\vdash P \to R}$
- Establishing equivalence: $\dfrac{\vdash P \to Q, \ \vdash Q \to P}{\vdash P \leftrightarrow Q}$
- Proof by contradiction: $\dfrac{P \vdash \neg P}{\vdash \neg P}$

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, inference rules and proofs
- Proof techniques
- Digital circuits