The Logic of Compound Statements

CSE 215: Foundations of Computer Science

Stony Brook University

http://www.cs.stonybrook.edu/~liu/cse215

Mathematical Formalization

- Why formalize?
  - to remove ambiguity
  - to represent facts on a computer and use it for proving, proof-checking, etc.
  - to detect unsound reasoning in arguments

$$\left.\begin{array}{l}\text{All people are mortal.}\\ \text{Socrates is a person.}\end{array}\right] \longrightarrow \text{Socrates is mortal.}$$

$$\left.\begin{array}{l}\forall x\ P(x) \to M(x)\\ P(S)\end{array}\right] \longrightarrow \left.\begin{array}{l}P(S) \to M(S)\\ P(S)\end{array}\right] \longrightarrow M(S)$$

Logic

- Mathematical logic is a tool for dealing with formal reasoning
  - formalization of natural language and reasoning methods
- Logic does:
  - Assess if an argument is valid or invalid
- Logic does not directly:
  - Assess the truth of atomic statements

Propositional Logic

- Propositional logic is the study of:
  - the structure/form (syntax) and
  - the meaning (semantics) of (simple and complex) propositions.
- The key questions are:
  - How is the truth value of a complex proposition obtained from the truth value of its simpler components?
  - Which propositions represent correct reasoning arguments?

Proposition

- A **proposition** is a sentence that is either true or false, but not both. and no quantified variables
- Examples of simple propositions:
  - John is a student
  - 5+1 = 6
  - 426 > 1721
  - It is 52 degrees outside right now.
- Example of a complex proposition:
  - Tom is five and Mary is six
- Sentences that are not propositions:
  - Did Steve get an A on the 215 exam?
  - Go away!

Proposition formula

- In studying properties of propositions, we represent them by expressions called **proposition forms** or **formulas** built from propositional variables (atoms), which represent simple propositions and symbols representing logical connectives.
  - **Proposition** or **propositional variables**: $p, q, \ldots$

    each can be true or false

    Examples: p=*"Socrates is mortal"*

    q=*"Plato is mortal"*
  - **Connectives**: $\wedge, \ \vee, \ \rightarrow, \ \leftrightarrow, \ \sim$

    Connect propositions: $p \vee q$
- Example: "I passed the exam or I did not pass it." $p \vee \sim p$
  - The formula expresses the logical structure of the proposition, where p is an abbreviation for the simple proposition "I passed the exam."

Connectives

- $\sim$ not
- $\wedge$ and
- $\vee$ or (non-exclusive!)
- $\rightarrow$ implies (if … then …)
- $\leftrightarrow$ if and only if

next two are not in propositional logic

- $\forall$ for all
- $\exists$ there exists

Formulas

- Atomic: $p, q, x, y, \ldots$
- Unit Formula: $p, \sim p$, (formula), $\ldots$
- Conjunctive: $p \wedge q, p \wedge \sim q, \ldots$
- Disjunctive: $p \vee q, p \vee (q \wedge x), \ldots$
- Conditional: $p \longrightarrow q$
- Biconditional: $p \leftrightarrow q$

Negation ($\sim$ or $\neg$ or !)

- We use symbol $\sim$ to denote negation (same as the textbook)
- Form (syntax): If p is a formula, then $\sim p$ is also a formula.

  We say that the second formula is the *negation* of the first.
  - Examples: p, $\sim p$, and $\sim\sim p$ are all formulas.
- Meaning (semantics):

  If a proposition is true, then its negation is false;

  if it is false, then its negation is true.
  - The structure of a formula and its negation reflects a relationship between the meaning of propositions.

Negation (~ or ¬ or !)

- Examples:
  - John went to the store yesterday (p).
  - John did not go to the store yesterday ($\sim p$).
- At the formula level we express the connection via what is called a **truth table**:
  - If p is true, then $\sim p$ is false
  - If p is false, then $\sim p$ is true

Truth Table for $\sim p$

p	$\sim p$
T	F
F	T

Negation (~ or ¬ or !)

- Note: $\sim\sim p \equiv p$

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

p and ~(~*p*) always have the same truth values, so they are logically equivalent

Conjunction (∧ or & or •)

- We use symbol ∧ to denote conjunction (same as the textbook)
- Syntax: If p and q are formulas, then $p \wedge q$ is also a formula.
- Semantics: If p is true and q is true, then $p \wedge q$ is true; in all other cases, $p \wedge q$ is false.

Truth Table for $p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Conjunction ($\wedge$ or & or •)

- Example:
  1. Bill went to the store.
  2. Mary ate cantaloupe.
  3. Bill went to the store and Mary ate cantaloupe.
- If p and q abbreviate the first and second sentence, then the third is represented by the conjunction $p \wedge q$.

Disjunction (∨ or | or +)

- We use symbol ∨ to denote (inclusive) disjunction.
- Syntax: If p and q are formulas, then $p \vee q$ is also a formula.
- Semantics: If p is true or q is true or both are true, then $p \vee q$ is true; if p and q are both false, then $p \vee q$ is false.

Truth Table for $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Disjunction (∨ or | or +)

- Example:
  - John works hard (p).
  - Mary is happy (q).
  - John works hard or Mary is happy ($p \lor q$).

Exclusive Or ($\oplus$, XOR)

- We use symbol $\oplus$ to denote exclusive or.
- Syntax: If p and q are formulas, then $p \oplus q$ is also a formula.
- Semantics: An exclusive or $p \oplus q$ is true if, and only if, one of p or q is true, but not both.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

- Example:
  - Either John works hard or Mary is happy ($p \oplus q$)

Implication, conditional

- Example proposition:

  If I do not pass the exam I will fail the course.

- Corresponding formula: $\sim p \rightarrow q$

Determining Truth of a Formula

- Atomic formulae: given
- Compound formulae: via meaning of the connectives
  - The semantics of logical connectives determines how propositional formulas are evaluated using the truth values assigned to propositional variables.
  - Each possible truth assignment or valuation for the propositional variables of a formula yields a truth value of the formula.

    The different possibilities can be summarized in a truth table.

Determining Truth of a Formula

- Example 1: $p \wedge \sim q$ (read "p and not q")

p	q	$\sim q$	$p \wedge \sim q$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	T	F

Determining Truth of a Formula

- Example 2: $p \land (q \lor r)$ (read "p and, in addition, q or r")

p	q	r	$q \lor r$	$p \land (q \lor r)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

- Note: It is usually necessary to evaluate all subformulas.

Evaluation of formulas - Truth tables

- A truth table for a formula lists all possible "situations" of truth or falsity, depending on the values assigned to the propositional variables of the formula.

Truth Tables

- Example: If p, q, and r are the propositions "Peter [Quincy, Richard] will lend Sam money," then Sam can deduce logically correctly, that he will be able to borrow money whenever one of his three friends is willing to lend him some ($p \vee q \vee r$)

p	q	r	$p \vee q \vee r$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	F

- Each row in the truth table corresponds to one possible situation of assigning truth values to p, q, and r

Truth Tables

- How many rows are there in a truth table with n propositional variables?
  - For n = 1, there are two rows,
  - for n = 2, there are four rows,
  - for n = 3, there are eight rows, and so on.
- Do you see a pattern?

Truth Table for $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Constructing Truth Tables

- There are two choices (true or false) for each of n variables, so in general there are 2x2x2x…x2 = 2^n rows for n variables.
- A systematic procedure (an algorithm) is necessary to make sure you construct all rows without duplicates.
  - construct the rows systematically:
    - count in binary: 000, 001, 010, 011,100, . . .
    - the rightmost column must be computed as a function of all the truth values in the row.

Truth Table for $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Constructing Truth Tables

- Because it is clumsy and time-consuming to build large explicit truth tables, we will be interested in more efficient logical evaluation procedures.

Syntax of Formulas

- The **formal language** of propositional logic can be specified by **grammar rules**
- The **syntactic structure** of a complex logical expression (i.e., its parse tree) must be **unambiguous**

$$
\begin{aligned}
\langle\text{proposition}\rangle ::= \quad & \langle\text{variable}\rangle \\
& \mid (\sim\langle\text{proposition}\rangle) \\
& \mid (\langle\text{proposition}\rangle \land \langle\text{proposition}\rangle) \\
& \mid (\langle\text{proposition}\rangle \lor \langle\text{proposition}\rangle) \\
& \ldots
\end{aligned}
$$

$$\langle\text{variable}\rangle ::= p \mid q \mid r \mid \ldots$$

Ambiguities in Syntax of Formulas

- For example, the expression $p \land q \lor r$ can be interpreted in two different ways:

p	q	r	$p \land q$	$(p \land q) \lor r$	$q \lor r$	$p \land (q \lor r)$
F	F	T	F	**T**	T	**F**

- Parentheses are needed to avoid ambiguities.
  - Without parentheses the meaning of the formula is not clear!
- The same problem arises in arithmetic: does 5+2 x 4 mean (5+2) x 4 or 5+(2 x 4)?
  - order/precedence of operators

Simplified Syntax

- In arithmetic, one often species a precedence among operators (say, times ahead of plus) to eliminate the need for some parentheses; same in certain programming languages.
- The same can be done for the logical connectives, though deleting parentheses may cause confusion.
- Example: If $\wedge$ is ahead of $\vee$ in the precedence, there is no ambiguity in $p \wedge q \vee r$

Precedence

- $\sim$ *highest*
- $\wedge$
- $\vee$
- $\rightarrow$, $\leftrightarrow$ *lowest*

- Note, the textbook gives $\wedge$ and $\vee$ the same precedence.
- Avoid confusion - use '(' and ')':
  - $(p \wedge q) \vee x$

- In general, don't want too few levels, or too many levels.

Simplified Syntax

- The properties of logical connectives can also be exploited to simplify the notation.
  - Example: Disjunction is commutative

p	q	$p \lor q$	$q \lor p$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Simplified Syntax

- Disjunction is also associative

p	q	r	$(p \vee q) \vee r$	$p \vee (q \vee r)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	F

- We will therefore ambiguously write $p \vee q \vee r$ to denote either $(p \vee q) \vee r$ or $p \vee (q \vee r)$. The ambiguity is usually of no consequence, as both formulas have the same meaning.

Logical Equivalence

- If two formulas evaluate to the same truth value in all situations, so that their truth tables are the same, they are said to be logically equivalent.
- We write $p \equiv q$ to indicate that two formulas p and q are logically equivalent.
- If two formulas are logically equivalent, their syntax may be different, but their semantics is the same. The logical equivalence of two formulas can be established by inspecting the associated truth tables.
- Substituting logically inequivalent formulas is the source of most real-world reasoning errors.

Logical Equivalence

- Example 1:
  - Is $\sim(p \wedge q)$ logically equivalent to $\sim p \wedge \sim q$?

p	q	$p \wedge q$	$\sim(p \wedge q)$	$\sim p$	$\sim q$	$\sim p \wedge \sim q$
T	T	T	F	F	F	F
T	**F**	**F**	**T**	**F**	**T**	**F**
F	**T**	**F**	**T**	**T**	**F**	**F**
F	F	F	T	T	T	T

  - Lines 2 and 3 prove that this is not the case.

Logical Equivalence

- Example 2:
  - Is $\sim(p \wedge q)$ logically equivalent to $\sim p \vee \sim q$?

p	q	$p \wedge q$	$\sim(p \wedge q)$	$\sim p$	$\sim q$	$\sim p \vee \sim q$
T	T	T	**F**	F	F	**F**
T	F	F	**T**	F	T	**T**
F	T	F	**T**	T	F	**T**
F	F	F	**T**	T	T	**T**

  - Yes.

De Morgan's Laws

- There are a number of important equivalences, including the following De Morgan's Laws:
  - $\sim(p \wedge q) \equiv \sim p \vee \sim q$
  - $\sim(p \vee q) \equiv \sim p \wedge \sim q$
  - These equivalences can be used to transform a formula into a logically equivalent one of a certain syntactic form, called a "normal form“
- Another useful logical equivalence is double negation:
  - $\sim\sim p \equiv p$

De Morgan's Laws

- Example:
  - $\sim(\sim p \wedge \sim q) \equiv \sim\sim(p \vee q) \equiv p \vee q$
  - The first equivalence is by De Morgan's Law, the second by double negation.
  - We have just derived a new equivalence: $p \vee q \equiv \sim(\sim p \wedge \sim q)$ (as equivalence can be used in both directions) which shows that disjunction can be expressed in terms of conjunction and negation!

Some Logical Equivalences

- You should be able to convince yourself of (i.e., prove) each of these:
  - Commutativity of $\wedge$: $p \wedge q \equiv q \wedge p$
  - Commutativity of $\vee$: $p \vee q \equiv q \vee p$
  - Associativity of $\wedge$: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
  - Associativity of $\vee$: $p \vee (q \vee r) \equiv (p \vee q) \vee r$
  - Idempotence: $p \equiv p \wedge p \equiv p \vee p$
  - Absorption: $p \equiv p \wedge (p \vee q) \equiv p \vee (p \wedge q)$

Some Logical Equivalences

- You should be able to convince yourself of (i.e., prove) each of these:
  - Distributivity of $\wedge$: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - Distributivity of $\vee$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  - Contradictions: $p \wedge \mathrm{F} \equiv \mathrm{F} \equiv p \wedge \sim p$
  - Identities: $p \wedge \mathrm{T} \equiv p \equiv p \vee \mathrm{F}$
  - Tautologies: $p \vee \mathrm{T} \equiv \mathrm{T} \equiv p \vee \sim p$

Tautologies

- A tautology is a formula that is always true, no matter which truth values we assign to its variables.
- Consider the proposition "I passed the exam or I did not pass the exam," the logical form of which is represented by the formula $p \vee \sim p$

p	$\sim p$	$p \vee \sim p$
T	F	**T**
F	T	**T**

  - This is a tautology, as we get T in every row of its truth table.

Contradictions

- A contradiction is a formula that is always false.
- The logical form of the proposition "I passed the exam and I did not pass the exam" is represented by $p \land \sim p$

p	$\sim p$	$p \land \sim p$
T	F	**F**
F	T	**F**

- This is a contradiction, as we get F in every row of its truth table.

Tautologies and contradictions

- Tautologies and contradictions are related

Theorem: If p is a tautology (contradiction) then $\sim p$ is a contradiction (tautology).

$$\sim(p \vee \sim p) \equiv \sim p \wedge \sim\sim p \equiv \sim p \wedge p \equiv p \wedge \sim p$$

Implication ($\rightarrow$), condl stmt

- Syntax: If p and q are formulas, then $p \rightarrow q$ (read "p implies q") is also a formula.
- We call p the hypothesis and q the conclusion of the implication.
- Semantics: If p is true and q is false, then $p \rightarrow q$ is false. In all other cases, $p \rightarrow q$ is true.
- Truth table:

Truth Table for $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Implication ($\rightarrow$)

- Example:
  - p: You get A's on all exams.
  - q: You get an A in this course.
  - $p \rightarrow q$: If you get A's on all exams, then you get an A in this course.

Implication ($\rightarrow$)

- The semantics of implication is trickier than for the other connectives
  - if p and q are both true, clearly the implication $p \rightarrow q$ is true
  - if p is true but q is false, clearly the implication $p \rightarrow q$ is false
  - If hypothesis p is false, no conclusion can be drawn, but both q being true and being false are consistent, so that the implication $p \rightarrow q$ is true in both cases
- Implication can also be expressed by other connectives, for example, $p \rightarrow q$ is logically equivalent to $\sim(p \wedge \sim q)$, or $\sim p \vee q$.

Example: Bad Defense Attorney

- Prosecutor:
  - *"If the defendant is guilty, then he had an accomplice."*
- Defense Attorney:
  - *"That's not true!!"*
- What did the defense attorney just claim??
  - $\sim(p \to q) \equiv \sim\sim(p \wedge \sim q) \equiv p \wedge \sim q$

Biconditional

- Syntax: If p and q are formulas, then $p \leftrightarrow q$ (read "p if and only if (iff) q") is also a formula.
- Semantics: If p and q are either both true or both false, then $p \leftrightarrow q$ is true. Otherwise, $p \leftrightarrow q$ is false.
- Truth table:

Truth Table for $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Biconditional

- Example:
  - p: Bill will get an A.
  - q: Bill studies hard.
  - $p \leftrightarrow q$: Bill will get an A if and only if Bill studies hard.
- The biconditional may be viewed as a shorthand for a conjunction of two implications, as $p \leftrightarrow q$ is logically equivalent to $(p \rightarrow q) \land (q \rightarrow p)$

Necessary and Sufficient Conditions

- The phrase "necessary and sufficient conditions" appears often in mathematics.
- A proposition p is ***necessary*** for q means: q cannot be true without p, that is, $\sim p \rightarrow \sim q$ (equivalent to $q \rightarrow p$).
  - Example: It is necessary for a student to have a 3.0 GPA in the core courses to be admitted to become a CSE major.
- A proposition p is ***sufficient*** for q means: $p \rightarrow q$.
  - Example: It is sufficient for a student to get A's in CSE114, CSE215, CSE214, and CSE220 in order to be admitted to become a CSE major.

Only if

- It p and q are statements,

  p **only if** q means "if not q then not p,"

  or, equivalently,

  "if p then q."

- John will break the world's record for the mile run ***only if*** he will run the mile in under four minutes.
  - Solution *Version 1:* If John will not run the mile in under four minutes, then he will not break the world's record.
  - Solution *Version 2:* If John will break the world's record, then he will have run the mile in under four minutes.

Necessary and Sufficient Conditions

Theorem: If a proposition p is both necessary and sufficient for q, then p and q are logically equivalent (and vice versa).

Tautologies and Logical Equivalence

Theorem: A propositional formula p is logically equivalent to q if and only if $p \leftrightarrow q$ is a tautology.

- Proof:
  - (a) If $p \leftrightarrow q$ is a tautology, then p is logically equivalent to q

  Why? If $p \leftrightarrow q$ is a tautology, then it is true for all truth assignments. By the semantics of the biconditional, this means that p and q agree on every row of the truth table. Hence the two formulas are logically equivalent.

  - (b) If p is logically equivalent to q, then $p \leftrightarrow q$ is a tautology

  Why? If p and q logically equivalent, then they evaluate to the same truth value for each truth assignment. By the semantics of the biconditional, the formula $p \leftrightarrow q$ is true in all situations. ■

Related Implications

- **Implication:** $p \rightarrow q$
  - If you got A's on all exams, you got an A in the course.
- **Contrapositive:** $\sim q \rightarrow \sim p$
  - If you didn't get an A in the course, then you didn't get A's on all exams.
- Implication is logically equivalent to the contrapositive.

p	q	$p \rightarrow q$	$\sim q$	$\sim p$	$\sim q \rightarrow \sim p$
T	T	**T**	F	F	**T**
T	F	**F**	T	F	**F**
F	T	**T**	F	T	**T**
F	F	**T**	T	T	**T**

Related Implications

- **Converse:** $q \rightarrow p$
  - If you got an A in the course, then you got A's on all exams.
- **Inverse:** $\sim p \rightarrow \sim q$
  - If you didn't get A's on all exams, then you didn't get an A in the course.
- Converse is logically equivalent to the inverse.

p	q	$q \rightarrow p$	$\sim p$	$\sim q$	$\sim p \rightarrow \sim q$
T	T	**T**	F	F	**T**
T	F	**T**	F	T	**T**
F	T	**F**	T	F	**F**
F	F	**T**	T	T	**T**

Deriving Logical Equivalences

- We can establish logical equivalence either via truth tables OR symbolically
- Example: $p \leftrightarrow q$ is logically equivalent to $(p \rightarrow q) \land (q \rightarrow p)$

p	q	$q \leftrightarrow p$		$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \land (q \rightarrow p)$
T	T	**T**		T	T	**T**
T	F	**F**		F	T	**F**
F	T	**F**		T	F	**F**
F	F	**T**		T	T	**T**

- Symbolic proofs are much like the simplifications you did in high school algebra: trial-and-error leads to experience and finally cunning

Symbolic proofs

- Example: $p \land q \equiv (p \lor \sim q) \land q$
  - Proof:

$$
\begin{aligned}
(p \lor \sim q) \land q &\equiv q \land (p \lor \sim q) && (1)\\
&\equiv (q \land p) \lor (q \land \sim q) && (2)\\
&\equiv (q \land p) \lor \mathrm{F} && (3)\\
&\equiv (q \land p) && (4)\\
&\equiv p \land q && (5)
\end{aligned}
$$

Symbolic proofs

- Example: $p \land q \equiv (p \lor \sim q) \land q$
  - Proof: which laws are used at each step?

$$
\begin{aligned}
(p \lor \sim q) \land q &\equiv q \land (p \lor \sim q) && (1)\\
&\equiv (q \land p) \lor (q \land \sim q) && (2)\\
&\equiv (q \land p) \lor \mathrm{F} && (3)\\
&\equiv (q \land p) && (4)\\
&\equiv p \land q && (5)
\end{aligned}
$$

Symbolic proofs

- Example: $p \land q \equiv (p \lor \sim q) \land q$
  - Proof: which laws are used at each step?

$$
\begin{aligned}
(p \lor \sim q) \land q &\equiv q \land (p \lor \sim q) && \text{(1) Commutativity of } \land \\
&\equiv (q \land p) \lor (q \land \sim q) && \text{(2)} \\
&\equiv (q \land p) \lor \mathrm{F} && \text{(3)} \\
&\equiv (q \land p) && \text{(4)} \\
&\equiv p \land q && \text{(5)}
\end{aligned}
$$

Symbolic proofs

- Example: $p \land q \equiv (p \lor \sim q) \land q$
  - Proof: which laws are used at each step?

$(p \lor \sim q) \land q$	$\equiv q \land (p \lor \sim q)$	(1) Commutativity of $\land$
	$\equiv (q \land p) \lor (q \land \sim q)$	(2) Distributivity of $\land$
	$\equiv (q \land p) \lor \mathrm{F}$	(3)
	$\equiv (q \land p)$	(4)
	$\equiv p \land q$	(5)

Symbolic proofs

- Example: $p \wedge q \equiv (p \vee \sim q) \wedge q$
  - Proof: which laws are used at each step?

$(p \vee \sim q) \wedge q$	$\equiv q \wedge (p \vee \sim q)$	(1) Commutativity of $\wedge$
	$\equiv (q \wedge p) \vee (q \wedge \sim q)$	(2) Distributivity of $\wedge$
	$\equiv (q \wedge p) \vee \mathrm{F}$	(3) Contradiction
	$\equiv (q \wedge p)$	(4)
	$\equiv p \wedge q$	(5)

Symbolic proofs

- Example: $p \wedge q \wedge r \equiv (p \vee \sim q) \wedge q$
  - Proof: which laws are used at each step?

$(p \vee \sim q) \wedge q$	$\equiv q \wedge (p \vee \sim q)$	(1) Commutativity of $\wedge$
	$\equiv (q \wedge p) \vee (q \wedge \sim q)$	(2) Distributivity of $\wedge$
	$\equiv (q \wedge p) \vee \mathrm{F}$	(3) Contradiction
	$\equiv (q \wedge p)$	(4) Identity
	$\equiv p \wedge q$	(5)

Symbolic proofs

- Example: $p \wedge q \equiv (p \vee \sim q) \wedge q$
  - Proof: which laws are used at each step?

$(p \vee \sim q) \wedge q$	$\equiv q \wedge (p \vee \sim q)$	(1) Commutativity of $\wedge$
	$\equiv (q \wedge p) \vee (q \wedge \sim q)$	(2) Distributivity of $\wedge$
	$\equiv (q \wedge p) \vee \mathrm{F}$	(3) Contradiction
	$\equiv (q \wedge p)$	(4) Identity
	$\equiv p \wedge q$	(5) Commutativity of $\wedge$

Logical Consequence

- We say that p logically implies q, or that q is a logical consequence of p, if q is true whenever p is true.
- Example: p logically implies $p \vee q$

p	q	$p \vee q$
T	T	**T**
T	F	**T**
F	T	T
F	F	F

- Logical consequence is a weaker condition than logical equivalence.

Logical Consequence

Theorem: A formula p logically implies q if and only if $p \rightarrow q$ is a tautology.

- This gives us a tool to infer truths!
- A rule of inference is a rule of the form:

  "From hypotheses $p_1, p_2, \ldots, p_n$ infer conclusion q"

  - A rule of inference is **sound** or **valid** if the conclusion q is a logical consequence of the conjunction $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ of all hypotheses
  - A rule of inference is **unsound** or **bogus** if it isn't!

Logical Arguments

- An argument (form) is a (finite) sequence of statements (forms), usually written as follows:

$$p_1$$
$$\ldots$$
$$p_n$$
$$\therefore q$$

- We call $p_1, \ldots, p_n$ the premises (or assumptions or hypotheses) and q the conclusion, of the argument.

- We read: "p_1, p_2, …, p_n, therefore q"

Logical Arguments

- Argument forms are also called *inference rules.*
- An inference rule is said to be *valid*, or (*logically*) *sound*, if it is the case that, for each truth valuation, if all the premises true, then the conclusion is also true!

Theorem: An inference rule is valid if, and only if, the conditional $p_1 \wedge p_2 \wedge \ldots \wedge p_n \rightarrow q$ is a tautology.

- An argument form consisting of two premises and a conclusion is called a *syllogism*.

Determining Validity or Invalidity

- **Testing an Argument Form for Validity**
  1. Identify the premises and conclusion of the argument form.
  2. Construct a truth table showing the truth values of all the premises and the conclusion.
  3. A row of the truth table in which **all the premises are true** is called a **critical row.** If there is a critical row in which the conclusion is false, then the argument form is invalid. If the conclusion in every critical row is true, then the argument form is valid.

Determining Validity or Invalidity

$$p \rightarrow q \vee \sim r$$
$$q \rightarrow p \wedge r$$
$$\therefore p \rightarrow r$$

						premises		conclusion
p	q	r	$\sim r$	$q \vee \sim r$	$p \wedge r$	$p \rightarrow q \vee \sim r$	$q \rightarrow p \wedge r$	$p \rightarrow r$
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	F
T	F	T	F	F	T	F	T	F
T	F	F	T	T	F	T	T	F
F	T	T	F	T	F	T	F	F
F	T	F	T	T	F	T	F	F
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

This row shows it is possible for an argument of this form to have true premises and a false conclusion. Hence this form of argument is invalid.

Modus Ponens

- Modus Ponens: $p \rightarrow q$

"method of affirming" p

Latin $\therefore q$

		premises		conclusion	
p	q	$p \rightarrow q$	p	q	
T	T	T	T	T	← critical row
T	F	F	T	F	
F	T	T	F	T	
F	F	T	F	F	

Modus Ponens

- The following argument is valid**:**

  If Socrates is a man, then Socrates is mortal.

  Socrates is a man.

  ∴ Socrates is mortal.

Modus Ponens

- **Example:**

  If the sum of the digits of 371,487 is divisible by 3,
  then 371,487 is divisible by 3.
  The sum of the digits of 371,487 is divisible by 3.
  ∴ 371,487 is divisible by 3.

Modus Tollens

- Modus Tonens: $p \rightarrow q$

"method of denying" $\sim q$

Latin $\therefore \sim p$

- Modus Tollens is valid because :
  - modus ponens is valid and the fact that a conditional statement is logically equivalent to its contrapositive, OR
  - it can be established formally by using a truth table.

Modus Tollens

- Example:

  (1) If Zeus is human, then Zeus is mortal.

  (2) Zeus is not mortal.

  ∴ Zeus is not human.

- An intuitive proof is proof by contradiction
  - if Zeus were human, then by (1) he would be mortal.
  - But by (2) he is not mortal.
  - Hence, Zeus cannot be human.

Recognizing Modus Ponens and Modus Tollens

If there are more pigeons than there are pigeonholes, then at least two pigeons roost in the same hole.

There are more pigeons than there are pigeonholes.

∴ ?

Recognizing Modus Ponens and Modus Tollens

If there are more pigeons than there are pigeonholes, then at least two pigeons roost in the same hole.

There are more pigeons than there are pigeonholes.

∴ At least two pigeons roost in the same hole.

by modus ponens

Recognizing Modus Ponens and Modus Tollens

If 870,232 is divisible by 6, then it is divisible by 3.

870,232 is **not** divisible by 3.

∴ ?

Recognizing Modus Ponens and Modus Tollens

If 870,232 is divisible by 6, then it is divisible by 3.

870,232 is **not** divisible by 3.

∴ 870,232 is not divisible by 6.   by modus tollens

Other Rules of Inference

- **Generalization:**

$$p \qquad\qquad \textbf{and} \qquad\qquad q$$

$$\therefore p \lor q \qquad\qquad\qquad \therefore p \lor q$$

- Example:

Anton is a junior.

∴ (more generally) Anton is a junior or Anton is a senior.

Other Rules of Inference

- **Specialization:**

$p \wedge q$ **and** $p \wedge q$

$\therefore p$ $\therefore q$

- Example:

Ana knows numerical analysis and Ana knows graph algorithms.

∴ (in particular) Ana knows graph algorithms.

Other Rules of Inference

- **Elimination :**

$$p \vee q \qquad\qquad \textbf{and} \qquad\qquad p \vee q$$
$$\sim q \qquad\qquad\qquad\qquad\qquad \sim p$$
$$\therefore p \qquad\qquad\qquad\qquad\qquad \therefore q$$

  - If we have only two possibilities and we can rule one out, the other one must be the case

- Example:

$x - 3 = 0$ or $x + 2 = 0$

$x + 2 \neq 0.$

$\therefore x - 3 = 0.$

Other Rules of Inference

- **Transitivity :**

$$p \longrightarrow q$$
$$q \longrightarrow r$$
$$\therefore p \longrightarrow r$$

- Example:

If 18,486 is divisible by 18, then 18,486 is divisible by 9.

If 18,486 is divisible by 9, then the sum of the digits of 18,486 is divisible by 9.

$\therefore$ If 18,486 is divisible by 18, then the sum of the digits of 18,486 is divisible by 9.

Proof Techniques

- **Proof by Contradiction:**

$$\sim p \longrightarrow c, \textit{ where } c \textit{ is a contradiction}$$
$$\therefore p$$

  - The usual way to derive a conditional $\sim p \longrightarrow c$ is to assume $\sim p$ and then derive c (i.e., a contradiction).
  - Thus, if one can derive a contradiction from $\sim p$, then one may conclude that p is true.

Knights and Knaves: knights always tell the truth and knaves always lie

A says: B is a knight.

B says: A and I are of opposite type.

Suppose A is a knight.

∴ What A says is true.	**by definition of knight**
∴ B is also a knight.	**That's what A said.**
∴ What B says is true.	**by definition of knight**
∴ A and B are of opposite types.	**That's what B said.**

∴ We have arrived at the following contradiction: A and B are both knights and A and B are of opposite type.

∴ The supposition is false.	**by the contradiction rule**
∴ A is not a knight.	**negation of supposition**
∴ A is a knave.	**since A is not a knight, A is a knave.**
∴ What A says is false.	**by definition of knave**
∴ B is not a knight.	**~(what A said) by definition of knave**
∴ B is also a knave.	**by elimination**

Proof Techniques

- **Proof by Division into Cases:**

$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\therefore r$$

  - If a disjunction $p \vee q$ has been derived and the goal is to prove r, then according to this inference rule it would be sufficient to derive $p \rightarrow r$ and $q \rightarrow r$.

- Example: x is positive or x is negative.

  If x is positive, then $x^2 > 0$.

  If x is negative, then $x^2 > 0$.

  $\therefore x^2 > 0$.

Quine's Method

- The following method can be used to determine whether a given propositional formula is a tautology, a contradiction, or a contingency.

Let p be a propositional formula.

- If p contains no variables, it can be simplified to T or F, and hence is either a tautology or a contradiction.
- If p contains a variable, then
  1. select a variable, say q,
  2. simplify both $p[q := \mathrm{T}]$ and $p[q := \mathrm{F}]$, denoting the simplified formulas by p_1 and p_2, respectively, and
  3. apply the method recursively to p_1 and p_2.
- If p_1 and p_2 are both tautologies, so is p.
- If p_1 and p_2 are both contradictions, so is p.
- In all other cases, p is a contingency.

Quine's Method Example

$(p \land \sim q \rightarrow r) \land (r \rightarrow p \lor q) \land (p \rightarrow \sim r) \land (p \lor q \lor r) \rightarrow q$

We first select a variable, say q, and then consider the two cases, $q := \mathrm{T}$ and $q := \mathrm{F}$.

1. For $q := \mathrm{T}$, the formula $\ldots \rightarrow \mathrm{T}$ can be simplified to T.
2. For $q := \mathrm{F}$,

$(p \land \sim \mathrm{F} \rightarrow r) \land (r \rightarrow p \lor \mathrm{F}) \land (p \rightarrow \sim r) \land (p \lor \mathrm{F} \lor r) \rightarrow \mathrm{F}$

$\equiv (p \land \mathrm{T} \rightarrow r) \land (r \rightarrow p) \land (p \rightarrow \sim r) \land (p \lor r) \rightarrow \mathrm{F}$

$\equiv (p \rightarrow r) \land (r \rightarrow p) \land (p \rightarrow \sim r) \land (p \lor r) \rightarrow \mathrm{F}$

$\equiv \sim[(p \rightarrow r) \land (r \rightarrow p) \land (p \rightarrow \sim r) \land (p \lor r)]$

Quine's Method Example cont.

$\sim[(p \rightarrow r) \wedge (r \rightarrow p) \wedge (p \rightarrow \sim r) \wedge (p \vee r)]$

We select the variable p

1. For $p := \mathrm{T}$

$\sim[(\mathrm{T} \rightarrow r) \wedge (r \rightarrow \mathrm{T}) \wedge (\mathrm{T} \rightarrow \sim r) \wedge (\mathrm{T} \vee r)]$

$\equiv \sim[r \wedge \mathrm{T} \wedge \sim r \wedge \mathrm{T}] \equiv \sim[r \wedge \sim r] \equiv \sim\mathrm{F} \equiv \mathrm{T}$

2. For $p := \mathrm{F}$

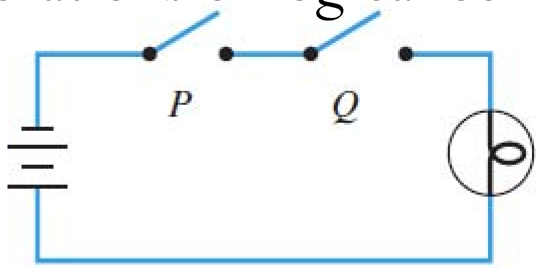
$\sim[(\mathrm{F} \rightarrow r) \wedge (r \rightarrow \mathrm{F}) \wedge (\mathrm{F} \rightarrow \sim r) \wedge (\mathrm{F} \vee r)]$

$\equiv \sim[\mathrm{T} \wedge \sim r \wedge \mathrm{T} \wedge r] \equiv \sim[\sim r \wedge r] \equiv \sim\mathrm{F} \equiv \mathrm{T}$

- This completes the process. All formulas considered, including the original formula, are tautologies.

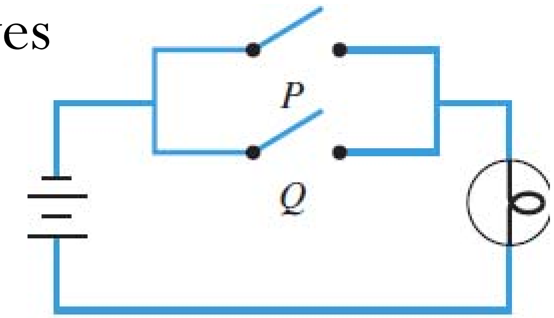
Application: Digital Logic Circuits

- Analogy between the operations of switching devices and the operations of logical connectives



Switches "in series"

Switches		Light Bulb
P	***Q***	**State**
closed	closed	on
closed	open	off
open	closed	off
open	open	off



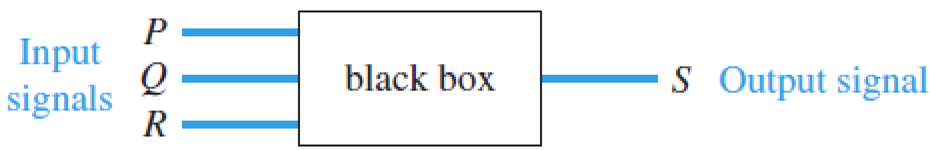
Switches "in parallel"

Switches		Light Bulb
P	***Q***	**State**
closed	closed	on
closed	open	on
open	closed	on
open	open	off

Binary digits (bits): we will use the symbols 1 and 0 instead of "on" ("closed" or True) and "off" ("open" or False)

Black Boxes and Gates

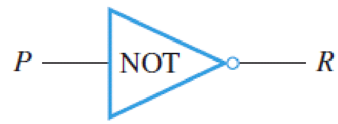
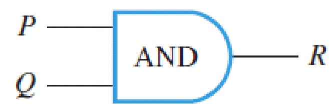
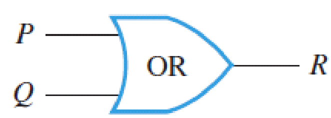
- Combinations of signal bits (1's and 0's) can be transformed into other combinations of signal bits (1's and 0's) by means of various circuits



An Input/Output Table

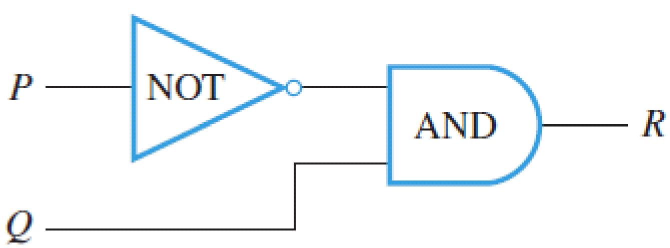
Input			Output
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

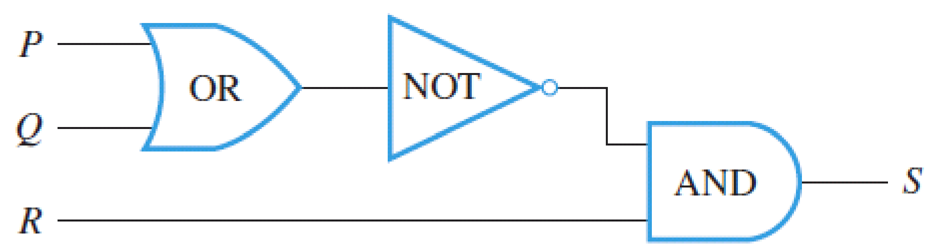
- An efficient method for designing complicated circuits is to build them by connecting less complicated black box circuits: NOT-,AND-, and OR-gates.

<table>
<tr><th>Type of Gate</th><th>Symbolic Representation</th><th>Action</th></tr>
<tr><td>NOT</td><td>
</td><td>
<table>
<tr><th>Input</th><th>Output</th></tr>
<tr><th>P</th><th>R</th></tr>
<tr><td>1</td><td>0</td></tr>
<tr><td>0</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>AND</td><td>
</td><td>
<table>
<tr><th colspan="2">Input</th><th>Output</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>OR</td><td>
</td><td>
<table>
<tr><th colspan="2">Input</th><th>Output</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
</table>

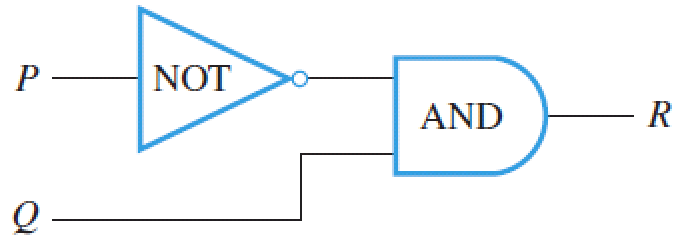
Combinational Circuits

- Rules for a Combinational Circuit:
  - Never combine two input wires.
  - A single input wire can be split partway and used as input for two separate gates.
  - An output wire can be used as input.
  - No output of a gate can eventually feed back into that gate.
- Examples:

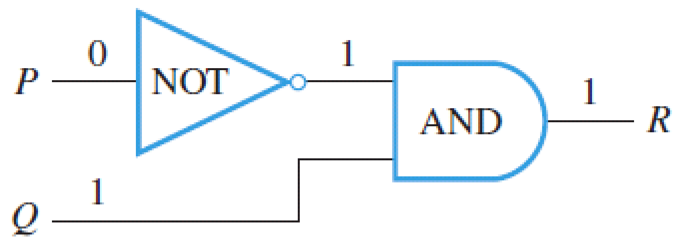




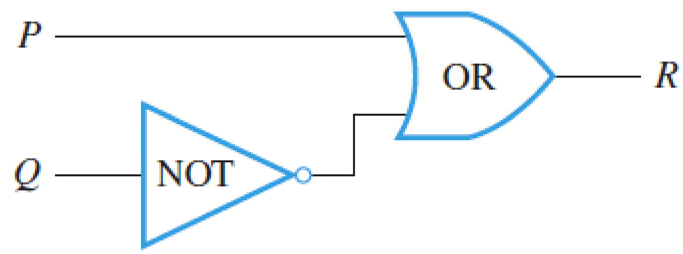
Determining Output for a Given Input



- Inputs: P = 0 and Q = 1



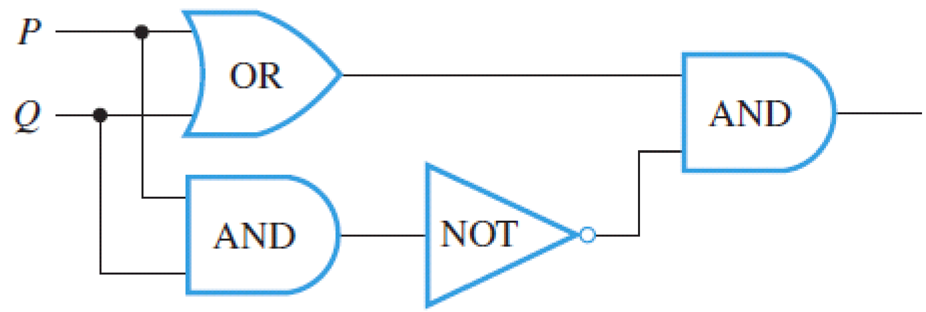
Constructing the Input/Output Table for a Circuit



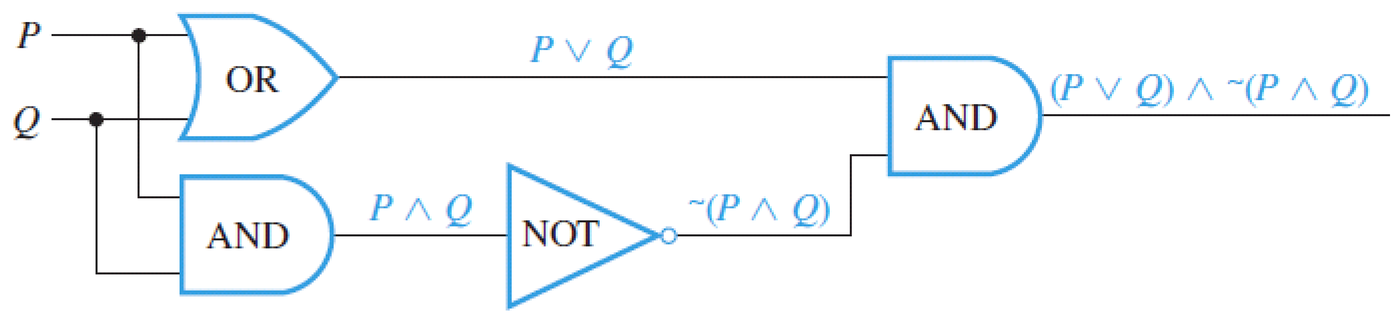
- List the four possible combinations of input signals, and find the output for each by tracing through the circuit.

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

The Boolean Expression Corresponding to a Circuit

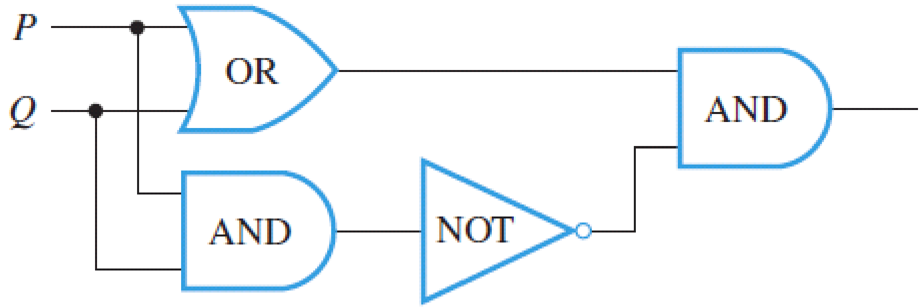


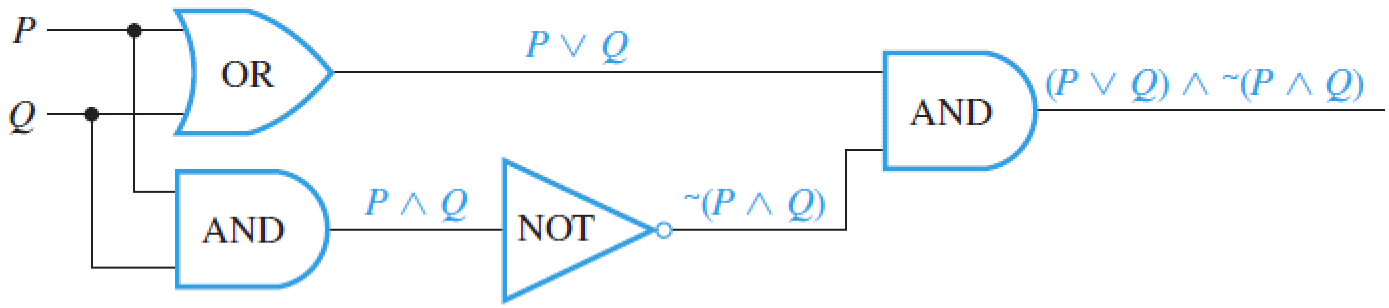
- Trace through the circuit from left to right:



- What is the result?

The Boolean Expression Corresponding to a Circuit

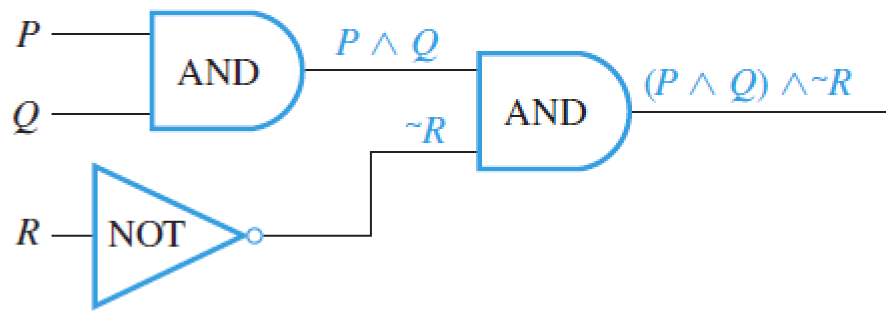




The result is: exclusive OR

Recognizer

- A **recognizer** is a circuit that outputs a 1 for exactly one particular combination of input signals and outputs 0's for all other combinations.
- Example:



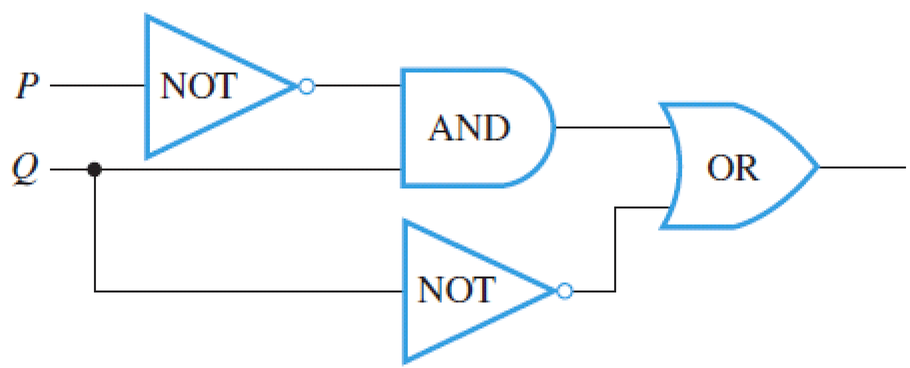
Input/Output Table for a Recognizer

P	Q	R	$(P \wedge Q) \wedge \sim R$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

The Circuit Corresponding to a Boolean Expression

1. Write the input variables in a column on the left side of the diagram
2. Go from the right side of the diagram to the left, working from the outermost part of the expression to the innermost part

- Example: $(\sim P \land Q) \lor \sim Q$



Find a Circuit That Corresponds to an Input/Output Table

1. Construct a Boolean expression with the same truth table

- identify each row for which the output is 1 and construct an and expression that produces a 1 for the exact combination of input values for that row

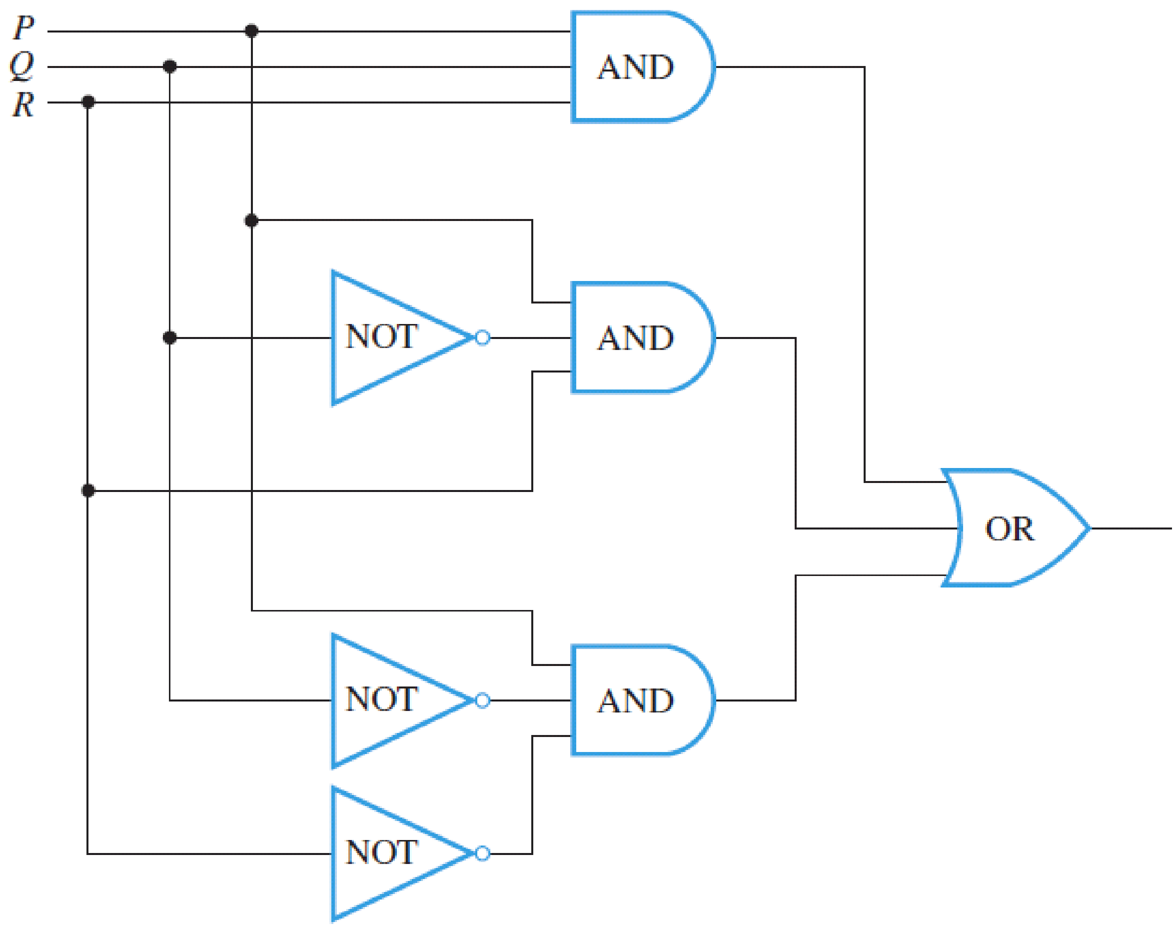
Input			Output	
P	*Q*	*R*	*S*	
1	1	1	1	$P \wedge Q \wedge R$
1	1	0	0	
1	0	1	1	$P \wedge \sim Q \wedge R$
1	0	0	1	$P \wedge \sim Q \wedge \sim R$
0	1	1	0	
0	1	0	0	
0	0	1	0	
0	0	0	0	

Result: $(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R)$

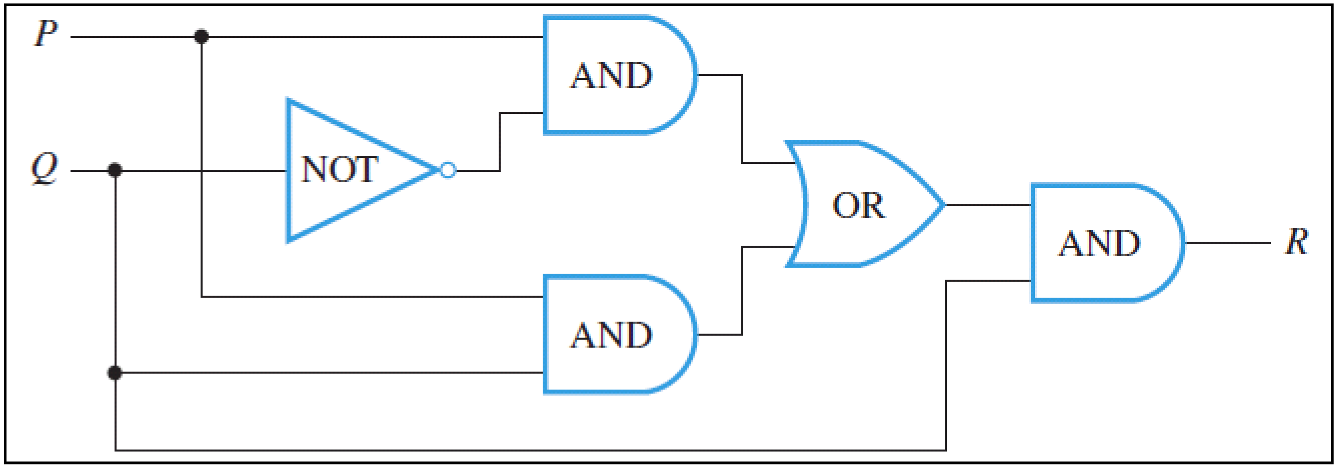
disjunctive normal form

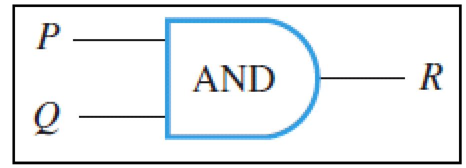
Find a Circuit That Corresponds to an Input/Output Table

2. Construct the circuit for: (P ∧ Q ∧ R) ∨ (P∧ ~Q ∧ R) ∨ (P∧ ~Q∧ ~R)



Equivalent Combinational Circuits

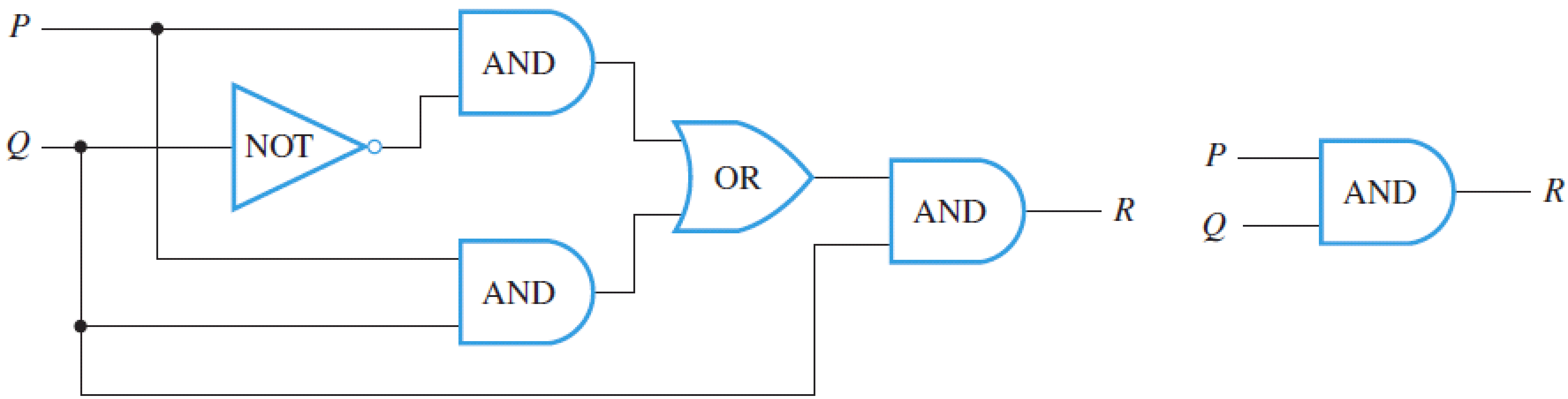




- Two digital logic circuits are **equivalent if, and only if, their input/output tables are** identical.

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

Simplifying Combinational Circuits



1. Find the Boolean expressions for each circuit.
2. Show that these expressions are logically equivalent.

$$((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q$$

$\equiv (P \wedge (\sim Q \vee Q)) \wedge Q$ by the distributive law

$\equiv (P \wedge (Q \vee \sim Q)) \wedge Q$ by the commutative law for $\vee$

$\equiv (P \wedge T) \wedge Q$ by the negation law

$\equiv P \wedge Q$ by the identity law.

NAND and NOR Gates

- A NAND-gate is a single gate that acts like an AND-gate followed by a NOT-gate
  - it has the logical symbol: |

  (called **Sheffer stroke**)

  $$P \mid Q \equiv \sim(P \wedge Q)$$

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

- A NOR-gate is a single gate that acts like an OR-gate followed by a NOT-gate
  - it has the logical symbol:

  (called **Peirce arrow**)

  $$P \downarrow Q \equiv \sim(P \vee Q)$$

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

Rewriting Expressions Using the Sheffer Stroke

- Any Boolean expression is equivalent to one written entirely with Sheffer strokes or entirely with Peirce arrows

$$\begin{aligned} \sim P &\equiv \sim(P \wedge P) && \text{by the idempotent law for } \wedge \\ &\equiv P \mid P && \text{by definition of } \mid . \end{aligned}$$

$$\begin{aligned} P \vee Q &\equiv \sim(\sim(P \vee Q)) && \text{by the double negative law} \\ &\equiv \sim(\sim P \wedge \sim Q) && \text{by De Morgan's laws} \\ &\equiv \sim((P \mid P) \wedge (Q \mid Q)) && \text{by the above } \sim P \equiv P \mid P \\ &\equiv (P \mid P) \mid (Q \mid Q) && \text{by definition of } \mid \end{aligned}$$