CISC 1100: Structures of Computer Science

Chapter 3
Logic

Arthur G. Werschulz

Fordham University Department of Computer and Information Sciences

Summer, 2015

Logical (or illogical?) reasoning

- Is this a valid argument?
  - All men are mortal.
  - Socrates is a man.
  - Therefore,

- Is this a valid argument?
  - All men are mortal.
  - Socrates is a man.
  - Therefore, Socrates is mortal.

  Valid or not?

Logical (or illogical?) reasoning

- Is this a valid argument?
  - All men are mortal.
  - Socrates is a man.
  - Therefore, Socrates is mortal.

  Valid or not? Yes!
- Is this a valid argument?
  - If we finish our homework, then we will go out for ice cream.
  - We are going out for ice cream.
  - Therefore we finished our homework.

  Valid or not?

Logical (or illogical?) reasoning

- Is this a valid argument?
  - All men are mortal.
  - Socrates is a man.
  - Therefore, Socrates is mortal.

  Valid or not? Yes!
- Is this a valid argument?
  - If we finish our homework, then we will go out for ice cream.
  - We are going out for ice cream.
  - Therefore we finished our homework.

  Valid or not? No!

Logical (or illogical?) reasoning

- Is this a valid argument?
    - All men are mortal.
    - Socrates is a man.
    - Therefore, Socrates is mortal.

  Valid or not? Yes!
- Is this a valid argument?
    - If we finish our homework, then we will go out for ice cream.
    - We are going out for ice cream.
    - Therefore we finished our homework.

  Valid or not? No!
- How to recognize the difference?

Outline

- Propositional logic
  - Logical operations
  - Propositional forms
  - From English to propositions
  - Propositional equivalence
- Predicate logic
  - Quantifiers
  - Some rules for using predicates

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.
- It rained yesterday in Manhattan.

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.
- It rained yesterday in Manhattan.
- It will rain tomorrow in Manhattan.

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.
- It rained yesterday in Manhattan.
- It will rain tomorrow in Manhattan.

These are *not* propositions:

- $x + 2 = 4$.

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.
- It rained yesterday in Manhattan.
- It will rain tomorrow in Manhattan.

These are *not* propositions:

- $x + 2 = 4$.
- Will it rain today in Manhattan?

Propositional logic

Proposition: A statement that is either true or false:

- $2 + 2 = 4$.
- $2 + 2 = 5$.
- It rained yesterday in Manhattan.
- It will rain tomorrow in Manhattan.

These are *not* propositions:

- $x + 2 = 4$.
- Will it rain today in Manhattan?
- Colorless green ideas sleep furiously.

Propositional logic (cont'd)

- *Truth value* of a proposition (T, F)

Propositional logic (cont'd)

- *Truth value* of a proposition (T, F)
- Propositional variables: lower case letters (p, q, ...)

Propositional logic (cont'd)

- *Truth value* of a proposition (T, F)
- Propositional variables: lower case letters (p, q, ...)
  (Analogous to variables in algebra.)
  - $p=$"A New York City subway fare is \$2.50."
  - $q=$"It will rain today in Manhattan."
  - $r=$"All multiples of four are even numbers."

Logical operations: negation

- *Negation*, the NOT operation: reverses a truth value.
- Negation is a *unary operation*: only depends on one variable.
- Negation of p is denoted p'.
  (Some books use other notations, such as $\overline{p}$, $\sim p$, or $\neg p$.)
- Can display via a *truth table*

p	p'
T	F
F	T

Logical operations: conjunction, disjunction

- The remaining operations we discuss are *binary operations*: they depend on two variables (also called *connectives*).

Logical operations: conjunction, disjunction

- The remaining operations we discuss are *binary operations*: they depend on two variables (also called *connectives*).
- *Conjunction*, the AND operation: true if *both* operands are true. Denote by $\wedge$.

Logical operations: conjunction, disjunction

- The remaining operations we discuss are *binary operations*: they depend on two variables (also called *connectives*).
- *Conjunction*, the AND operation: true if *both* operands are true. Denote by $\wedge$.
- *Disjunction*, the (inclusive) OR operation: true if *either* operand is true (including both). Denote by $\vee$.

Logical operations: conjunction, disjunction

- The remaining operations we discuss are *binary operations*: they depend on two variables (also called *connectives*).
- *Conjunction*, the AND operation: true if *both* operands are true. Denote by $\wedge$.
- *Disjunction*, the (inclusive) OR operation: true if *either* operand is true (including both). Denote by $\vee$.
- Truth tables:

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

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

Logical operations: exclusive or

- The inclusive or $\vee$ is not the "or" of common language.
- That role is played by *exclusive or* (XOR), denoted $\oplus$.
- Truth table:

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

Logical operations: exclusive or

- The inclusive or $\vee$ is not the "or" of common language.
- That role is played by *exclusive or* ($\textsc{xor}$), denoted $\oplus$.
- Truth table:

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

- Be careful to distinguish between $\textsc{or}$ and $\textsc{xor}$!

Logical operations: conditional

- Denoted $p \Rightarrow q$.

Logical operations: conditional

- Denoted $p \Rightarrow q$.
- Captures the meaning of
  - If p, then q.
  - p implies q.
  - p only if q.
  - p is sufficient for q.
  - q is necessary for p.

Logical operations: conditional

- Denoted $p \Rightarrow q$.
- Captures the meaning of
  - If p, then q.
  - p implies q.
  - p only if q.
  - p is sufficient for q.
  - q is necessary for p.
- Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Logical operations: conditional

- Denoted $p \Rightarrow q$.
- Captures the meaning of
  - If p, then q.
  - p implies q.
  - p only if q.
  - p is sufficient for q.
  - q is necessary for p.
- Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

- First two rows are "obvious".

Logical operations: conditional

- Denoted $p \Rightarrow q$.
- Captures the meaning of
  - If p, then q.
  - p implies q.
  - p only if q.
  - p is sufficient for q.
  - q is necessary for p.
- Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

- First two rows are "obvious".
- Last two rows are not so obvious:

Logical operations: conditional

- Denoted $p \Rightarrow q$.
- Captures the meaning of
  - If p, then q.
  - p implies q.
  - p only if q.
  - p is sufficient for q.
  - q is necessary for p.
- Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

- First two rows are "obvious".
- Last two rows are not so obvious:
  "One can derive anything from a false hypothesis."

Logical operations: biconditional

- Denoted $p \Leftrightarrow q$

Logical operations: biconditional

- Denoted $p \Leftrightarrow q$
- Captures the meaning of
  - p if and only if q.
  - p is necessary and sufficient for q.
  - p is logically equivalent to q.

Logical operations: biconditional

- Denoted $p \Leftrightarrow q$
- Captures the meaning of
  - p if and only if q.
  - p is necessary and sufficient for q.
  - p is logically equivalent to q.
- Truth table:

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

In arithmetic and algebra, you learned how to build up complicated arithmetic expressions, such as

- $1 + 2$

Propositional Forms

In arithmetic and algebra, you learned how to build up complicated arithmetic expressions, such as

- $1 + 2$
- $-(1 + 2)$

Propositional Forms

In arithmetic and algebra, you learned how to build up complicated arithmetic expressions, such as

- $1 + 2$
- $-(1 + 2)$
- 3×4

Propositional Forms

In arithmetic and algebra, you learned how to build up complicated arithmetic expressions, such as

- $1 + 2$
- $-(1 + 2)$
- 3×4
- $-(1 + 2)/(3 \times 4)$

Propositional Forms

In arithmetic and algebra, you learned how to build up complicated arithmetic expressions, such as

- $1 + 2$
- $-(1 + 2)$
- 3×4
- $-(1 + 2)/(3 \times 4)$
- $-(1 + 2)/(3 \times 4) + (5 + 6 \times 7)/(8 + 9) - 10$

Propositional Forms (cont'd)

- Use connectives to build complicated expressions from simpler ones, *or*
- break down complicated expressions as being simpler subexpressions, connected by connectives.

Propositional Forms (cont'd)

- Use connectives to build complicated expressions from simpler ones, *or*
- break down complicated expressions as being simpler subexpressions, connected by connectives.
- **Example:** $-(1+2)/(3\times 4)+(5+6\times 7)/(8+9)-10$ consists of

$$-(1+2)/(3\times 4) \qquad \text{and} \qquad (5+6\times 7)/(8+9)-10,$$

connected by $+$.

  - Now break down these two subexpressions.

Propositional Forms (cont'd)

- Use connectives to build complicated expressions from simpler ones, *or*
- break down complicated expressions as being simpler subexpressions, connected by connectives.
- **Example:** $-(1+2)/(3\times 4)+(5+6\times 7)/(8+9)-10$ consists of

$$-(1+2)/(3\times 4) \qquad \text{and} \qquad (5+6\times 7)/(8+9)-10,$$

  connected by $+$.
  - Now break down these two subexpressions.
  - Now break down the four sub-subexpressions.

Propositional Forms (cont'd)

- Use connectives to build complicated expressions from simpler ones, *or*
- break down complicated expressions as being simpler subexpressions, connected by connectives.
- **Example:** $-(1+2)/(3\times 4)+(5+6\times 7)/(8+9)-10$ consists of

$$-(1+2)/(3\times 4) \qquad \text{and} \qquad (5+6\times 7)/(8+9)-10,$$

  connected by $+$.
  - Now break down these two subexpressions.
  - Now break down the four sub-subexpressions.
  - And so forth.

Propositional Forms (cont'd)

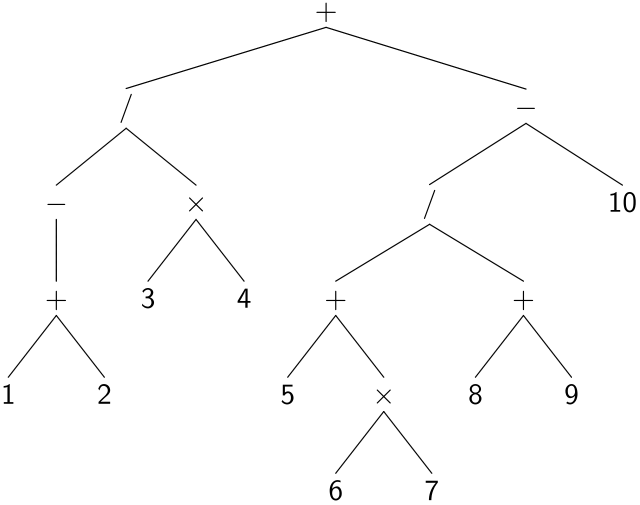
Systematize the process via a *parse tree*.

Parse tree for $-(1+2)/(3 \times 4) + (5 + 6 \times 7)/(8+9) - 10$:

Propositional Forms (cont'd)

Systematize the process via a *parse tree*.

Parse tree for $-(1+2)/(3\times 4)+(5+6\times 7)/(8+9)-10$:



Propositional Forms (cont'd)

We're inherently using the following rules:

1. Parenthesized subexpressions are evaluated first.
2. Operations have a *precedence hierarchy*:
   1. Unary operations (for example, -1) are done first.
   2. Multiplicative operations ($\times$ and $/$) are done next.
   3. Additive operations ($+$ and $-$) are done last.
3. In case of a tie (two additive operations or two multiplicative operations), the remaining operations are done from left to right.

Propositional Forms (cont'd)

We're inherently using the following rules:

1. Parenthesized subexpressions are evaluated first.
2. Operations have a *precedence hierarchy*:
   1. Unary operations (for example, -1) are done first.
   2. Multiplicative operations ($\times$ and $/$) are done next.
   3. Additive operations ($+$ and $-$) are done last.
3. In case of a tie (two additive operations or two multiplicative operations), the remaining operations are done from left to right.

These guarantee that (e.g.) $2 + 3 \times 4$ is 14, rather than 20.

Propositional Forms (cont'd)

- Now jump from numerical algebra to propositional algebra.

Propositional Forms (cont'd)

- Now jump from numerical algebra to propositional algebra.
- We can build new (complicated) propositions out of old (simpler) ones.

Propositional Forms (cont'd)

- Now jump from numerical algebra to propositional algebra.
- We can build new (complicated) propositions out of old (simpler) ones.
- **Example:** $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$ consists of

$$(p \vee q) \wedge ((p') \vee r) \qquad \text{and} \qquad (p \Leftrightarrow q) \vee (p \wedge r),$$

connected by $\Rightarrow$.

- Now jump from numerical algebra to propositional algebra.
- We can build new (complicated) propositions out of old (simpler) ones.
- **Example:** $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$ consists of

$$(p \vee q) \wedge ((p') \vee r) \qquad \text{and} \qquad (p \Leftrightarrow q) \vee (p \wedge r),$$

  connected by $\Rightarrow$.
  - Now break down these two subexpressions.

Propositional Forms (cont'd)

- Now jump from numerical algebra to propositional algebra.
- We can build new (complicated) propositions out of old (simpler) ones.
- **Example:** $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$ consists of

$$(p \vee q) \wedge ((p') \vee r) \qquad \text{and} \qquad (p \Leftrightarrow q) \vee (p \wedge r),$$

  connected by $\Rightarrow$.
  - Now break down these two subexpressions.
  - Now break down the four sub-subexpressions.

Propositional Forms (cont'd)

- Now jump from numerical algebra to propositional algebra.
- We can build new (complicated) propositions out of old (simpler) ones.
- **Example:** $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$ consists of

$$(p \vee q) \wedge ((p') \vee r) \qquad \text{and} \qquad (p \Leftrightarrow q) \vee (p \wedge r),$$

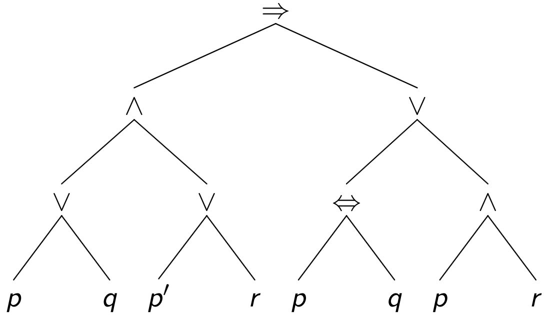
  connected by $\Rightarrow$.
  - Now break down these two subexpressions.
  - Now break down the four sub-subexpressions.
  - And so forth.

Propositional Forms (cont'd)

Parse tree for $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$:

Propositional Forms (cont'd)

Parse tree for $[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$:



Propositional Forms (cont'd)

- The expression

$$[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$$

  is completely parenthesized (and hard to read).
- If we agree upon (standard) precedence rules, can get rid of extraneous parentheses.

Propositional Forms (cont'd)

- The expression

$$[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$$

  is completely parenthesized (and hard to read).
- If we agree upon (standard) precedence rules, can get rid of extraneous parentheses.
  1. Parenthesized subexpressions are evaluated first.
  2. Operations have a *precedence hierarchy*:
     1. Unary negations ($'$) are done first.
     2. Multiplicative operations ($\wedge$) are done next.
     3. Additive operations ($\vee$, $\oplus$) are done next.
     4. The conditional-type operations ($\Rightarrow$ and $\Leftrightarrow$) are done last.
  3. In case of a tie (two operations at the same level in the hierarchy), operations are done in a left-to-right order, *except* for the conditional operator $\Rightarrow$, which is done in a right-to-left order. That is, $p \Rightarrow q \Rightarrow r$ is interpreted as $p \Rightarrow (q \Rightarrow r)$.

Propositional Forms (cont'd)

So can replace

$$[(p \vee q) \wedge ((p') \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee (p \wedge r)]$$

by

$$[(p \vee q) \wedge (p' \vee r)] \Rightarrow [(p \Leftrightarrow q) \vee p \wedge r]$$

or even

$$(p \vee q) \wedge (p' \vee r) \Rightarrow (p \Leftrightarrow q) \vee p \wedge r.$$

Propositional Forms (cont'd)

- Precedence rules are too hard to remember!
- Let's simplify!

Propositional Forms (cont'd)

- Precedence rules are too hard to remember!
- Let's simplify!
  1. Parenthesized subexpressions come first.
  2. Next comes the only unary operation ($'$).
  3. Next comes the only multiplicative operation ($\wedge$).
  4. Next comes the additive operations ($\vee$, $\oplus$).
  5. Use parentheses if you have *any* doubt.
     Always use parentheses if you have multiple conditionals.
  6. Evaluate ties left-to-right.

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach.

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach. Let

$$a = \text{“Alice will have coffee”}$$
$$b = \text{“Bob will go to the beach”}$$

Solution?

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach. Let

$$a = \text{“Alice will have coffee”}$$
$$b = \text{“Bob will go to the beach”}$$

Solution? $a \vee b$.

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach. Let

$$a = \text{"Alice will have coffee"}$$
$$b = \text{"Bob will go to the beach"}$$

  Solution? $a \vee b$.
- **Example:** If I make peanut butter sandwiches for lunch, then Carol will be disappointed.

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach. Let

$$\begin{aligned} a &= \text{“Alice will have coffee”} \\ b &= \text{“Bob will go to the beach”} \end{aligned}$$

  Solution? $a \vee b$.
- **Example:** If I make peanut butter sandwiches for lunch, then Carol will be disappointed. Let

$$\begin{aligned} p &= \text{“I will make peanut butter sandwiches”} \\ c &= \text{“Carol will be disappointed”} \end{aligned}$$

  Solution?

From English to Propositions

- Can use propositional forms to capture logical arguments in English.
- Help to expose logical fallacies.
- **Example:** Alice will have coffee or Bob will go to the beach. Let

$$a = \text{"Alice will have coffee"}$$
$$b = \text{"Bob will go to the beach"}$$

  Solution? $a \vee b$.
- **Example:** If I make peanut butter sandwiches for lunch, then Carol will be disappointed. Let

$$p = \text{"I will make peanut butter sandwiches"}$$
$$c = \text{"Carol will be disappointed"}$$

  Solution? $p \Rightarrow c$.

- **Example:** If Alice will have coffee and Bob will go to the beach, then either Carol will be disappointed or I will make peanut butter sandwiches.
  Solution?

From English to Propositions (cont'd)

- **Example:** If Alice will have coffee and Bob will go to the beach, then either Carol will be disappointed or I will make peanut butter sandwiches.
  Solution? $a \wedge b \Rightarrow c \vee p$

From English to Propositions (cont'd)

- **Example:** If Alice will have coffee and Bob will go to the beach, then either Carol will be disappointed or I will make peanut butter sandwiches.
  Solution? $a \wedge b \Rightarrow c \vee p$
- **Example:**

  Alice will have coffee and
  Bob will not go to the beach

  if and only if

  Carol will be disappointed and
  I will not make peanut butter sandwiches.

  Solution?

- **Example:** If Alice will have coffee and Bob will go to the beach, then either Carol will be disappointed or I will make peanut butter sandwiches.
  Solution? $a \wedge b \Rightarrow c \vee p$
- **Example:**

  Alice will have coffee and
  Bob will not go to the beach

  if and only if

  Carol will be disappointed and
  I will not make peanut butter sandwiches.

  Solution? $(a \wedge b') \Leftrightarrow (c \wedge p')$

Propositional Equivalence

High school algebra: establishes many useful rules, such as

$$\begin{aligned} a + b &= b + a, \\ a \times (b + c) &= a \times b + a \times c, \\ -(a + b) &= (-a) + (-b), \end{aligned}$$

Anything analogous for propositions?

Propositional Equivalence

High school algebra: establishes many useful rules, such as

$$a + b = b + a,$$
$$a \times (b + c) = a \times b + a \times c,$$
$$-(a + b) = (-a) + (-b),$$

Anything analogous for propositions?

- How to state them? (No equal sign.)
- How to prove correct rules?
- How to disprove incorrect "rules"?

Propositional Equivalence (cont'd)

- **Logical equivalence:** $p \equiv q$ means

  p is true if and only if q is true

Propositional Equivalence (cont'd)

- **Logical equivalence:** $p \equiv q$ means

  p is true if and only if q is true

- Beware!
  - $p \equiv q$ is *not* a proposition; it's a statement *about* propositions.
  - $p \equiv q$ is a statement in a *metalanguage* about propositions.
  - $\equiv$ is a *metasymbol* in this language.

- **Logical equivalence:** $p \equiv q$ means

$$p \text{ is true if and only if } q \text{ is true}$$

- Beware!
    - $p \equiv q$ is *not* a proposition; it's a statement *about* propositions.
    - $p \equiv q$ is a statement in a *metalanguage* about propositions.
    - $\equiv$ is a *metasymbol* in this language.
- Analogous to

$$\begin{aligned} a + b &= b + a, \\ a \times (b + c) &= a \times b + a \times c, \\ -(a + b) &= (-a) + (-b), \end{aligned}$$

we might *conjecture* that

Propositional Equivalence (cont'd)

- **Logical equivalence:** $p \equiv q$ means
$$p \text{ is true if and only if } q \text{ is true}$$
- Beware! 
    - $p \equiv q$ is *not* a proposition; it's a statement *about* propositions.
    - $p \equiv q$ is a statement in a *metalanguage* about propositions.
    - $\equiv$ is a *metasymbol* in this language.
- Analogous to
$$\begin{aligned} a + b &= b + a, \\ a \times (b + c) &= a \times b + a \times c, \\ -(a + b) &= (-a) + (-b), \end{aligned}$$
we might *conjecture* that
$$\begin{aligned} p \vee q &\equiv q \vee p, \\ p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r), \\ (p \vee q)' &\equiv p' \vee q'. \end{aligned}$$

- Want to prove (or disprove) conjectured identities such as

$$
\begin{aligned}
p \vee q &\equiv q \vee p, \\
p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r), \\
(p \vee q)' &\equiv p' \vee q'.
\end{aligned}
$$

- Want to prove (or disprove) conjectured identities such as

$$
\begin{aligned}
p \vee q &\equiv q \vee p, \\
p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r), \\
(p \vee q)' &\equiv p' \vee q'.
\end{aligned}
$$

- How? Use a truth table.

Propositional Equivalence (cont'd)

- Want to prove (or disprove) conjectured identities such as

$$
\begin{gathered}
p \vee q \equiv q \vee p, \\
p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r), \\
(p \vee q)' \equiv p' \vee q'.
\end{gathered}
$$

- How? Use a truth table.
- Suppose that p and q are propositional formulas.
  The equivalence $p \equiv q$ is true iff the truth tables for p and q are identical.

Propositional Equivalence (cont'd)

Example: Is it true that $p \vee q \equiv q \vee p$?

Propositional Equivalence (cont'd)

Example: Is it true that $p \vee q \equiv q \vee p$?

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

Example: Is it true that $p \vee q \equiv q \vee p$?

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

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

Propositional Equivalence (cont'd)

Example: Is it true that $p \lor q \equiv q \lor p$?

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

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

They match! So $p \lor q \equiv q \lor p$.
More compact form:

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

Example: Is it true that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$?

Propositional Equivalence (cont'd)

Example: Is it true that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$?

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

Propositional Equivalence (cont'd)

Example: Is it true that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$?

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

So $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

Propositional Equivalence (cont'd)

- How to organize the table?
  - Two variables: TT, TF, FT, FF
  - Three variables: TTT, TTF, TFT, TFF, FTT, FTF, FFT, FFF.
  - General pattern?
    - Rightmost variable alternates: TFTFTFTF ...
    - Next alternates in pairs: TTFFTTFF ...
    - Next alternates in quadruples: TTTTFFFFTTTTFFFF ...

Propositional Equivalence (cont'd)

- How to organize the table?
  - Two variables: TT, TF, FT, FF
  - Three variables: TTT, TTF, TFT, TFF, FTT, FTF, FFT, FFF.
  - General pattern?
    - Rightmost variable alternates: TFTFTFTF ...
    - Next alternates in pairs: TTFFTTFF ...
    - Next alternates in quadruples: TTTTFFFFTTTTFFFF ...
- Size of table?
  - Two variables? 4 rows.
  - Three variables? 8 rows.
  - n variables?

Propositional Equivalence (cont'd)

- How to organize the table?
  - Two variables: TT, TF, FT, FF
  - Three variables: TTT, TTF, TFT, TFF, FTT, FTF, FFT, FFF.
  - General pattern?
    - Rightmost variable alternates: TFTFTFTF ...
    - Next alternates in pairs: TTFFTTFF ...
    - Next alternates in quadruples: TTTTFFFFTTTTFFFF ...
- Size of table?
  - Two variables? 4 rows.
  - Three variables? 8 rows.
  - n variables? 2^n rows.
  - Since $2^{10} = 1024$, you don't want to do a 10-variable table.

Example: Is it true that $(p \vee q)' \equiv p' \vee q'$?

Example: Is it true that $(p \vee q)' \equiv p' \vee q'$?

p	q	$p \vee q$	$(p \vee q)'$	p'	q'	$p' \vee q'$
T	T	T	F	F	F	F
T	F	T	F	F	T	T
F	T	T	F	T	F	T
F	F	F	T	T	T	T

Propositional Equivalence (cont'd)

Example: Is it true that $(p \vee q)' \equiv p' \vee q'$?

p	q	$p \vee q$	$(p \vee q)'$	p'	q'	$p' \vee q'$
T	T	T	F	F	F	F
T	F	T	F	F	T	T
F	T	T	F	T	F	T
F	F	F	T	T	T	T

So it is *not* true that $(p \vee q)' \equiv p' \vee q'$!

Propositional Equivalence (cont'd)

Example: Rather than $(p \vee q)' \equiv p' \vee q'$, the correct formula is $(p \vee q)' \equiv p' \wedge q'$

Propositional Equivalence (cont'd)

Example: Rather than $(p \vee q)' \equiv p' \vee q'$, the correct formula is $(p \vee q)' \equiv p' \wedge q'$

p	q	$p \vee q$	$(p \vee q)'$	p'	q'	$p' \wedge q'$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

The formula $(p \wedge q)' \equiv p' \vee q'$ is also correct.
These formulas

$$(p \vee q)' \equiv p' \wedge q'$$
$$(p \wedge q)' \equiv p' \vee q'$$

are called *deMorgan's laws*.

Propositional Equivalence (cont'd)

Some well-known propositional laws (we haven't proved them all):

Double Negation	$(p')' \equiv p$
Idempotent	$p \wedge p \equiv p$
Idempotent	$p \vee p \equiv p$
Commutative	$p \wedge q \equiv q \wedge p$
Commutative	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Associative	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Distributive	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
DeMorgan	$(p \wedge q)' \equiv (p') \vee (q')$
DeMorgan	$(p \vee q)' \equiv (p') \wedge (q')$
Modus Ponens	$[(p \Rightarrow q) \wedge p] \Rightarrow q$
Modus Tollens	$[(p \Rightarrow q) \wedge q'] \Rightarrow p'$
Contrapositive	$(p \Rightarrow q) \equiv (q' \Rightarrow p')$
Implication	$(p \Rightarrow q) \equiv (p' \vee q)$

Propositional Equivalence (cont'd)

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' \,.$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Propositional Equivalence (cont'd)

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' .$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Example: Show that $(A \cap B)' = A' \cup B'$.

Propositional Equivalence (cont'd)

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' \,.$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Example: Show that $(A \cap B)' = A' \cup B'$.

Solution: Must show that any element of $(A \cap B)'$ is an element of $A' \cup B'$, and vice versa. But

$$x \in (A \cap B)' \iff (x \in A \cap B)'$$

Propositional Equivalence (cont'd)

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' \,.$$

It turns out that we can use a propositional law to easily prove the analogous set identity.
Example: Show that $(A \cap B)' = A' \cup B'$.
Solution: Must show that any element of $(A \cap B)'$ is an element of $A' \cup B'$, and vice versa. But

$$x \in (A \cap B)' \iff (x \in A \cap B)' \iff (x \in A \wedge x \in B)'$$

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' .$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Example: Show that $(A \cap B)' = A' \cup B'$.

Solution: Must show that any element of $(A \cap B)'$ is an element of $A' \cup B'$, and vice versa. But

$$\begin{aligned} x \in (A \cap B)' &\iff (x \in A \cap B)' \iff (x \in A \wedge x \in B)' \\ &\iff (x \in A)' \vee (x \in B)' \end{aligned}$$

Propositional Equivalence (cont'd)

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' \,.$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Example: Show that $(A \cap B)' = A' \cup B'$.

Solution: Must show that any element of $(A \cap B)'$ is an element of $A' \cup B'$, and vice versa. But

$$\begin{aligned} x \in (A \cap B)' &\iff (x \in A \cap B)' \iff (x \in A \wedge x \in B)' \\ &\iff (x \in A)' \vee (x \in B)' \\ &\iff (x \in A') \vee (x \in B') \end{aligned}$$

The preceding table is similar to the table of set identities from Chapter 1, e.g., we have

$$(p \wedge q)' \equiv p' \vee q' \qquad \text{and} \qquad (A \cap B)' = A' \cup B' .$$

It turns out that we can use a propositional law to easily prove the analogous set identity.

Example: Show that $(A \cap B)' = A' \cup B'$.

Solution: Must show that any element of $(A \cap B)'$ is an element of $A' \cup B'$, and vice versa. But

$$\begin{aligned} x \in (A \cap B)' \iff (x \in A \cap B)' &\iff (x \in A \wedge x \in B)' \\ &\iff (x \in A)' \vee (x \in B)' \\ &\iff (x \in A') \vee (x \in B') \\ &\iff x \in A' \cup B', \end{aligned}$$

as required. $\square$

Once we've proved a given propositional law, we can use it to help prove new ones.

Example: Let's prove the *exportation identity*

$$[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)].$$

We have

$$(p \wedge q) \Rightarrow r \equiv (p \wedge q)' \vee r \qquad \text{implication}$$

Propositional Equivalence (cont'd)

Once we've proved a given propositional law, we can use it to help prove new ones.

Example: Let's prove the *exportation identity*

$$[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)].$$

We have

$$\begin{aligned} (p \wedge q) \Rightarrow r &\equiv (p \wedge q)' \vee r && \text{implication} \\ &\equiv (p' \vee q') \vee r && \text{DeMorgan} \end{aligned}$$

Once we've proved a given propositional law, we can use it to help prove new ones.

Example: Let's prove the *exportation identity*

$$[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)].$$

We have

$$\begin{aligned}(p \wedge q) \Rightarrow r &\equiv (p \wedge q)' \vee r && \text{implication}\\ &\equiv (p' \vee q') \vee r && \text{DeMorgan}\\ &\equiv p' \vee (q' \vee r) && \text{associative}\end{aligned}$$

Once we've proved a given propositional law, we can use it to help prove new ones.

Example: Let's prove the *exportation identity*

$$[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)].$$

We have

$$\begin{aligned}
(p \wedge q) \Rightarrow r &\equiv (p \wedge q)' \vee r && \text{implication} \\
&\equiv (p' \vee q') \vee r && \text{DeMorgan} \\
&\equiv p' \vee (q' \vee r) && \text{associative} \\
&\equiv p' \vee (q \Rightarrow r) && \text{implication}
\end{aligned}$$

Once we've proved a given propositional law, we can use it to help prove new ones.

Example: Let's prove the *exportation identity*

$$[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)].$$

We have

$$\begin{aligned}
(p \wedge q) \Rightarrow r &\equiv (p \wedge q)' \vee r && \text{implication} \\
&\equiv (p' \vee q') \vee r && \text{DeMorgan} \\
&\equiv p' \vee (q' \vee r) && \text{associative} \\
&\equiv p' \vee (q \Rightarrow r) && \text{implication} \\
&\equiv p \Rightarrow (q \Rightarrow r) && \text{implication}
\end{aligned}$$

as required. $\square$

Propositional Equivalence (cont'd)

- **Duality:** If p is a proposition that only uses the operations $'$, $\wedge$, and $\vee$. If we replace all instances of $\wedge$, $\vee$, T, and F in p by $\vee$, $\wedge$, F, and T, respectively, we get a new proposition p^*, which is called the *dual* of p.

Propositional Equivalence (cont'd)

- **Duality:** If p is a proposition that only uses the operations $'$, $\wedge$, and $\vee$. If we replace all instances of $\wedge$, $\vee$, T, and F in p by $\vee$, $\wedge$, F, and T, respectively, we get a new proposition p^*, which is called the *dual* of p.
- **Example:** The duals of

$$p \wedge (q \vee r) \qquad \text{and} \qquad (p \wedge q) \vee (p \wedge r)$$

are

$$p \vee (q \wedge r) \qquad \text{and} \qquad (p \vee q) \wedge (p \vee r).$$

Propositional Equivalence (cont'd)

- **Duality:** If p is a proposition that only uses the operations $'$, $\wedge$, and $\vee$. If we replace all instances of $\wedge$, $\vee$, T, and F in p by $\vee$, $\wedge$, F, and T, respectively, we get a new proposition p^*, which is called the *dual* of p.
- **Example:** The duals of

$$p \wedge (q \vee r) \qquad \text{and} \qquad (p \wedge q) \vee (p \wedge r)$$

are

$$p \vee (q \wedge r) \qquad \text{and} \qquad (p \vee q) \wedge (p \vee r).$$

- **Duality Principle:** If two propositions (which only use the operations $'$, $\wedge$, and $\vee$) are equivalent, then their duals are equivalent. (Be lazy—save half the work!)

Example: Since the duals

$$p \wedge (q \vee r) \qquad \text{and} \qquad (p \wedge q) \vee (p \wedge r)$$

are

$$p \vee (q \wedge r) \qquad \text{and} \qquad (p \vee q) \wedge (p \vee r)$$

Propositional Equivalence (cont'd)

Example: Since the duals

$$p \wedge (q \vee r) \qquad \text{and} \qquad (p \wedge q) \vee (p \wedge r)$$

are

$$p \vee (q \wedge r) \qquad \text{and} \qquad (p \vee q) \wedge (p \vee r)$$

and we had earlier proved that

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r),$$

Example: Since the duals

$$p \wedge (q \vee r) \qquad \text{and} \qquad (p \wedge q) \vee (p \wedge r)$$

are

$$p \vee (q \wedge r) \qquad \text{and} \qquad (p \vee q) \wedge (p \vee r)$$

and we had earlier proved that

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r),$$

we now know that

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r).$$

"for free".

Example: Since the duals of

$$(p \vee q)' \qquad \text{and} \qquad p' \wedge q'$$

are

$$(p \wedge q)' \qquad \text{and} \qquad p' \vee q'$$

and we had earlier proved that

$$(p \vee q)' \equiv p' \wedge q',$$

Propositional Equivalence (cont'd)

Example: Since the duals of

$$(p \vee q)' \qquad \text{and} \qquad p' \wedge q'$$

are

$$(p \wedge q)' \qquad \text{and} \qquad p' \vee q'$$

and we had earlier proved that

$$(p \vee q)' \equiv p' \wedge q',$$

we now know that

$$(p \wedge q)' \equiv p' \vee q'$$

"for free".

Sometimes you can prove a statement with a direct approach.

Indirect Proofs

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Solution: Let m be an odd number; want to show that m^2 is odd.

Indirect Proofs

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Solution: Let m be an odd number; want to show that m^2 is odd.

- Write $m = 2n + 1$ for $n \in \mathbb{Z}$.

Indirect Proofs

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Solution: Let m be an odd number; want to show that m^2 is odd.

- Write $m = 2n + 1$ for $n \in \mathbb{Z}$.
- Then

$$m^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1.$$

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Solution: Let m be an odd number; want to show that m^2 is odd.

- Write $m = 2n + 1$ for $n \in \mathbb{Z}$.
- Then

$$m^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1.$$

  Let $k = 2n^2 + 2n \in \mathbb{Z}$. Then $m^2 = 2k + 1$,

Sometimes you can prove a statement with a direct approach.

Example: Show that the square of an odd number is also an odd number.

Solution: Let m be an odd number; want to show that m^2 is odd.

- Write $m = 2n + 1$ for $n \in \mathbb{Z}$.
- Then

$$m^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1.$$

Let $k = 2n^2 + 2n \in \mathbb{Z}$. Then $m^2 = 2k + 1$, and so m^2 is odd. $\square$

Indirect Proofs (cont'd)

Sometimes a "frontal attack" doesn't work. So we use an "sneak attack", more properly called an *indirect proof*.

Indirect Proofs (cont'd)

Sometimes a "frontal attack" doesn't work. So we use an "sneak attack", more properly called an *indirect proof*.

Two such techniques:

- *Proof by contradiction.* Show that if the statement to proved is false, then a contradiction results.

Sometimes a "frontal attack" doesn't work. So we use an "sneak attack", more properly called an *indirect proof*.
Two such techniques:

- *Proof by contradiction.* Show that if the statement to proved is false, then a contradiction results.
- *Proving the contrapositive.* Rather than directly proving an implication $p \Rightarrow q$, prove its contrapositive $q' \Rightarrow p'$.

Example: Show that if the square of an integer is even, then that integer is even.

Indirect Proofs (cont'd)

Example: Show that if the square of an integer is even, then that integer is even.

Solution: Let $m \in \mathbb{Z}$. We want to show that

$$m^2 \text{ is even} \Rightarrow m \text{ is even.}$$

Example: Show that if the square of an integer is even, then that integer is even.

Solution: Let $m \in \mathbb{Z}$. We want to show that

$$m^2 \text{ is even} \Rightarrow m \text{ is even.}$$

We can do this by establishing its contrapositive.

Indirect Proofs (cont'd)

Example: Show that if the square of an integer is even, then that integer is even.

Solution: Let $m \in \mathbb{Z}$. We want to show that

$$m^2 \text{ is even} \Rightarrow m \text{ is even}.$$

We can do this by establishing its contrapositive.
But the contrapositive is

$$m \text{ is odd} \Rightarrow m^2 \text{ is odd},$$

Indirect Proofs (cont'd)

Example: Show that if the square of an integer is even, then that integer is even.

Solution: Let $m \in \mathbb{Z}$. We want to show that

$$m^2 \text{ is even} \Rightarrow m \text{ is even}.$$

We can do this by establishing its contrapositive.
But the contrapositive is

$$m \text{ is odd} \Rightarrow m^2 \text{ is odd},$$

which we did previously. So we're done!! $\square$

Indirect Proofs (cont'd)

Example: Show that $\sqrt{2}$ is an irrational number.

Example: Show that $\sqrt{2}$ is an irrational number.

Solution: Let's do a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, let's assume that $\sqrt{2} \in \mathbb{Q}$, and show how this leads to a contradiction.

Example: Show that $\sqrt{2}$ is an irrational number.

Solution: Let's do a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, let's assume that $\sqrt{2} \in \mathbb{Q}$, and show how this leads to a contradiction.
So write $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms"). Then

Indirect Proofs (cont'd)

Example: Show that $\sqrt{2}$ is an irrational number.

Solution: Let's do a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, let's assume that $\sqrt{2} \in \mathbb{Q}$, and show how this leads to a contradiction.
So write $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms"). Then

$$\begin{aligned} \sqrt{2} = \frac{p}{q} \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2 \text{ is even} \\ &\Rightarrow p \text{ is even (see previous slide)} \\ &\Rightarrow p = 2r \text{ for some positive integer } r \\ &\Rightarrow (2r)^2 = p^2 = 2q^2 \qquad \text{(Remember that } p^2 = 2q^2\text{!)} \\ &\Rightarrow 4r^2 = 2q^2 \Rightarrow 2r^2 = q^2 \Rightarrow q^2 \text{ is even} \\ &\Rightarrow q \text{ is even (again using previous slide)} \end{aligned}$$

Indirect Proofs (cont'd)

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.

Indirect Proofs (cont'd)

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.
We wrote $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms").

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.
We wrote $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms").
Previous slide: Both p and q are even, i.e., they are both exact integer multiples of 2.

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.
We wrote $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms").
Previous slide: Both p and q are even, i.e., they are both exact integer multiples of 2.
This contradicts the assumption that p, q have no common factor (other than 1)!

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.
We wrote $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms").
Previous slide: Both p and q are even, i.e., they are both exact integer multiples of 2.
This contradicts the assumption that p, q have no common factor (other than 1)!
Hence we cannot write $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1.

Example (cont'd): Show that $\sqrt{2}$ is an irrational number.

Solution (cont'd): We're doing a proof by contradiction. Rather than showing $\sqrt{2} \notin \mathbb{Q}$, we are trying to show how the assumption $\sqrt{2} \in \mathbb{Q}$ leads to a contradiction.
We wrote $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1 (i.e., the fraction p/q is "reduced to lowest terms").
Previous slide: Both p and q are even, i.e., they are both exact integer multiples of 2.
This contradicts the assumption that p, q have no common factor (other than 1)!
Hence we cannot write $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}^+$, where $q \neq 0$ and where p and q have no common factor other than 1.
Hence $\sqrt{2} \notin \mathbb{Q}$. $\square$

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

We now have

- $b \Rightarrow d$, using (1), (3), transitive law.

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

We now have

- $b \Rightarrow d$, using (1), (3), transitive law.
- $(d')' \Rightarrow c'$, using (2), contrapositive law.

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

We now have

- $b \Rightarrow d$, using (1), (3), transitive law.
- $(d')' \Rightarrow c'$, using (2), contrapositive law.
- $d \Rightarrow c'$, since $(d')' \equiv d$ (double negation law).

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

We now have

- $b \Rightarrow d$, using (1), (3), transitive law.
- $(d')' \Rightarrow c'$, using (2), contrapositive law.
- $d \Rightarrow c'$, since $(d')' \equiv d$ (double negation law).
- Hence transitive law gives $b \Rightarrow c'$. $\square$

An Example From Lewis Caroll

Given the following facts:

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Prove that babies cannot manage crocodiles.

Let b, c, d, and l denote the status of being a baby, being able to manage a crocodile, being despised, and being logical. Then

1. $b \Rightarrow l'$.
2. $c \Rightarrow d'$.
3. $l' \Rightarrow d$.

We now have

- $b \Rightarrow d$, using (1), (3), transitive law.
- $(d')' \Rightarrow c'$, using (2), contrapositive law.
- $d \Rightarrow c'$, since $(d')' \equiv d$ (double negation law).
- Hence transitive law gives $b \Rightarrow c'$. $\square$

See text for a 10-fact example.

Predicate Logic

Want to symbolically state the classical syllogism

- All men are mortal.
- Socrates is a man.
- Therefore,

Want to symbolically state the classical syllogism

- All men are mortal.
- Socrates is a man.
- Therefore, Socrates is mortal.

Want to symbolically state the classical syllogism

- All men are mortal.
- Socrates is a man.
- Therefore, Socrates is mortal.

Let

$$\text{man}(x) = \text{“}x \text{ is a man''}$$
$$\text{mortal}(x) = \text{“}x \text{ is mortal''}$$

We can agree that man(Socrates) is (was?) true and that

$$\text{man}(x) \Rightarrow \text{mortal}(x) \text{ for any person } x.$$

Our natural conclusion?

Want to symbolically state the classical syllogism

- All men are mortal.
- Socrates is a man.
- Therefore, Socrates is mortal.

Let

$$\text{man}(x) = \text{“}x \text{ is a man”}$$
$$\text{mortal}(x) = \text{“}x \text{ is mortal”}$$

We can agree that man(Socrates) is (was?) true and that

$$\text{man}(x) \Rightarrow \text{mortal}(x) \text{ for any person } x.$$

Our natural conclusion? mortal(Socrates) is true.

Predicate Logic (cont'd)

- A *predicate* is a formula that contains a variable, that becomes a proposition when we substitute a particular value for the variable.
- In other words, plug in a value and get a truth value (T or F).
- Examples: $\text{man}(x)$ or $\text{mortal}(x)$.
- Can have more than one variable, e.g.,

$$\text{older}(x, y) = \text{“}x \text{ is older than } y\text{”}.$$

Predicate Logic (cont'd)

For example, suppose that four(t) means that $t \in \mathbb{Z}$ is divisible by 4 (in other words, t is an exact multiple of 4). Then:

x	four(x)	truth value of four(x)
$\vdots$	$\vdots$	$\vdots$
-4	-4 is divisible by 4	T
-3	-3 is divisible by 4	F
-2	-2 is divisible by 4	F
-1	-1 is divisible by 4	F
0	0 is divisible by 4	T
1	1 is divisible by 4	F
2	2 is divisible by 4	F
3	3 is divisible by 4	F
4	4 is divisible by 4	T
$\vdots$	$\vdots$	$\vdots$

Quantifiers

- How to transform a predicate $p(x)$ (where x varies over a set S) into a proposition?

Quantifiers

- How to transform a predicate $p(x)$ (where x varies over a set S) into a proposition?
- **Universal quantification:** We ask that $p(x)$ be true for *all* $x \in S$. We let

$$\forall\, x \in S, p(x)$$

denote the proposition "For all elements $x \in S$, $p(x)$ is true."

Quantifiers

- How to transform a predicate $p(x)$ (where x varies over a set S) into a proposition?
- **Universal quantification:** We ask that $p(x)$ be true for *all* $x \in S$. We let

  $$\forall x \in S, p(x)$$

  denote the proposition "For all elements $x \in S$, $p(x)$ is true."
- **Existential quantification:** We ask that $p(x)$ be true for *some* $x \in S$. We let

  $$\exists x \in S : p(x)$$

  denote the proposition "There exists some $x \in S$ such that $p(x)$ is true."

Quantifiers

- How to transform a predicate $p(x)$ (where x varies over a set S) into a proposition?
- **Universal quantification:** We ask that $p(x)$ be true for *all* $x \in S$. We let
$$\forall\, x \in S, p(x)$$
denote the proposition "For all elements $x \in S$, $p(x)$ is true."
- **Existential quantification:** We ask that $p(x)$ be true for *some* $x \in S$. We let
$$\exists\, x \in S \colon p(x)$$
denote the proposition "There exists some $x \in S$ such that $p(x)$ is true."
- Note the slight punctuation difference (comma vs. colon).

- Let

$$\text{four}(x) = \text{``}x \text{ is divisible by four.''} \qquad \text{for any } x \in \mathbb{Z}.$$

  - $\forall x \in \mathbb{Z}, \text{four}(x)$ is

- Let

$$\text{four}(x) = \text{“}x \text{ is divisible by four.”} \qquad \text{for any } x \in \mathbb{Z}.$$

  - $\forall\, x \in \mathbb{Z}, \text{four}(x)$ is false.
  - $\exists\, x \in \mathbb{Z}\colon\ \text{four}(x)$ is

Quantifiers (cont'd)

- Let

$$\text{four}(x) = \text{“}x \text{ is divisible by four.”} \qquad \text{for any } x \in \mathbb{Z}.$$

    - $\forall\, x \in \mathbb{Z}, \text{four}(x)$ is false.
    - $\exists\, x \in \mathbb{Z}\colon\ \text{four}(x)$ is true.

- Let
$$\text{four}(x) = \text{“}x \text{ is divisible by four.”} \qquad \text{for any } x \in \mathbb{Z}.$$
    - $\forall\, x \in \mathbb{Z}, \text{four}(x)$ is false.
    - $\exists\, x \in \mathbb{Z}\colon\ \text{four}(x)$ is true.
- Consider the predicate $x > y$ over $x, y \in \mathbb{Z}$.
    - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x > y$ is

- Let

$$\text{four}(x) = \text{“}x \text{ is divisible by four.”} \qquad \text{for any } x \in \mathbb{Z}.$$

  - $\forall\, x \in \mathbb{Z}, \text{four}(x)$ is false.
  - $\exists\, x \in \mathbb{Z}\colon\ \text{four}(x)$ is true.
- Consider the predicate $x > y$ over $x, y \in \mathbb{Z}$.
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x > y$ is false
  - $\exists\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Z} : x > y$ is

Quantifiers (cont'd)

- Let

$$\text{four}(x) = \text{“}x \text{ is divisible by four.”} \qquad \text{for any } x \in \mathbb{Z}.$$

  - $\forall\, x \in \mathbb{Z}, \text{four}(x)$ is false.
  - $\exists\, x \in \mathbb{Z}\colon\ \text{four}(x)$ is true.
- Consider the predicate $x > y$ over $x, y \in \mathbb{Z}$.
  - $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x > y$ is false
  - $\exists\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Z} : x > y$ is true

Some Rules for Using Predicates

- **Classical syllogism:** Suppose that
  - $p(x)$ and $q(x)$ are predicates, with x varying over some set S.
  - $p(x) \Rightarrow q(x)$ for any $x \in S$.

Some Rules for Using Predicates

- **Classical syllogism:** Suppose that
  - $p(x)$ and $q(x)$ are predicates, with x varying over some set S.
  - $p(x) \Rightarrow q(x)$ for any $x \in S$.

  Suppose further that $p(a)$ is true for some $a \in S$.

Some Rules for Using Predicates

- **Classical syllogism:** Suppose that
  - $p(x)$ and $q(x)$ are predicates, with x varying over some set S.
  - $p(x) \Rightarrow q(x)$ for any $x \in S$.

  Suppose further that $p(a)$ is true for some $a \in S$.
  Then $q(a)$ is true.

- **Classical syllogism:** Suppose that
  - $p(x)$ and $q(x)$ are predicates, with x varying over some set S.
  - $p(x) \Rightarrow q(x)$ for any $x \in S$.

  Suppose further that $p(a)$ is true for some $a \in S$.
  Then $q(a)$ is true.
  We can write this symbolically as

$$[\forall\, x \in S, p(x) \Rightarrow q(x) \wedge a \in S \wedge p(a)] \Rightarrow q(a)].$$

Some Rules for Using Predicates

- **Classical syllogism:** Suppose that
  - $p(x)$ and $q(x)$ are predicates, with x varying over some set S.
  - $p(x) \Rightarrow q(x)$ for any $x \in S$.

  Suppose further that $p(a)$ is true for some $a \in S$.
  Then $q(a)$ is true.
  We can write this symbolically as

$$[\forall\, x \in S, p(x) \Rightarrow q(x) \wedge a \in S \wedge p(a)] \Rightarrow q(a)].$$

- **Negation laws:**

$$[\exists\, x \in S \colon p(x)]' \equiv [\forall\, x \in S, p'(x)]$$

and

$$[\forall\, x \in S, p(x)]' \equiv [\exists\, x \in S \colon p'(x)].$$

Predicates Having More Than One Variable

- Any given variable might not be quantified.
- The quantified variables might be quantified differently.
- **Example:** Let P be a set of people, T be a set of temperatures. Define "beach(p, t)" to mean that "person p will go to the beach if the temperature reaches t degrees".

  Quantification choices?

  - No quantification. beach(p, t) is a two-variable predicate.

Predicates Having More Than One Variable

- Any given variable might not be quantified.
- The quantified variables might be quantified differently.
- **Example:** Let P be a set of people, T be a set of temperatures. Define "beach(p, t)" to mean that "person p will go to the beach if the temperature reaches t degrees".

  Quantification choices?
  - No quantification. beach(p, t) is a two-variable predicate.
  - We can quantify in one variable.
    Quantifying over p gives the following predicates in t:

$$\exists\, p \in P\colon\ \text{beach}(p, t)$$

$$\forall\, p \in P, \text{beach}(p, t).$$

Predicates Having More Than One Variable

- Any given variable might not be quantified.
- The quantified variables might be quantified differently.
- **Example:** Let P be a set of people, T be a set of temperatures. Define "beach(p, t)" to mean that "person p will go to the beach if the temperature reaches t degrees".

  Quantification choices?
  - No quantification. beach(p, t) is a two-variable predicate.
  - We can quantify in one variable.
    Quantifying over p gives the following predicates in t:

$$\exists\, p \in P : \text{ beach}(p, t)$$
$$\forall\, p \in P, \text{beach}(p, t).$$

    Quantifying over t gives the following predicates in p:

$$\exists\, t \in T : \text{ beach}(p, t)$$
$$\forall\, t \in T, \text{beach}(p, t).$$

Predicates Having More Than One Variable (cont'd)

- Quantification example (cont'd)
  - We can quantify in both variables, getting the propositions:

$$\begin{gathered} \exists\, p \in P\colon [\exists\, t \in T\colon\ \text{beach}(p,t)] \\ \exists\, p \in P\colon [\forall\, t \in T, \text{beach}(p,t)] \\ \forall\, p \in P, [\exists\, t \in T\colon\ \text{beach}(p,t)] \\ \forall\, p \in P, [\forall\, t \in T, \text{beach}(p,t)]. \end{gathered}$$

(Many people would omit the brackets.)