

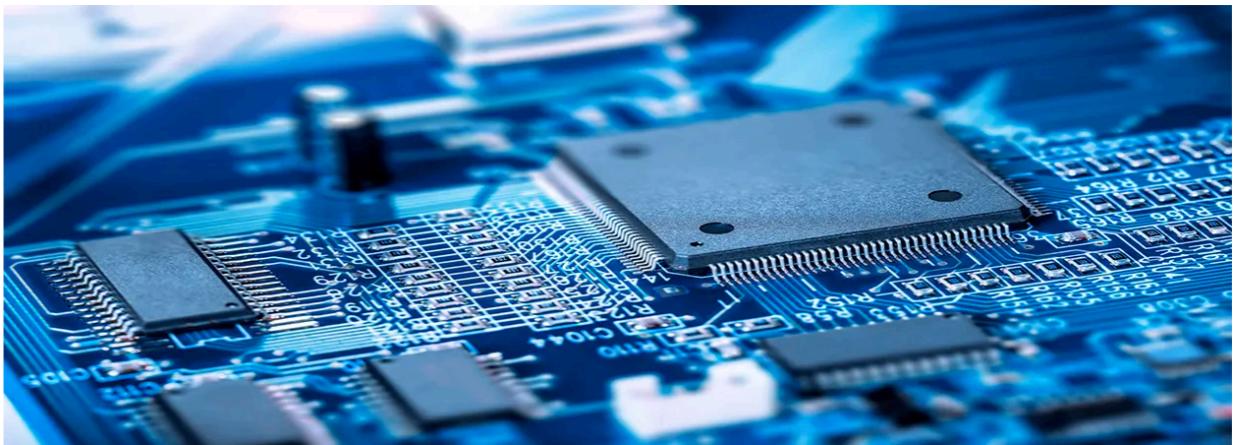
02 Logic and Proofs

CS201 Discrete Mathematics

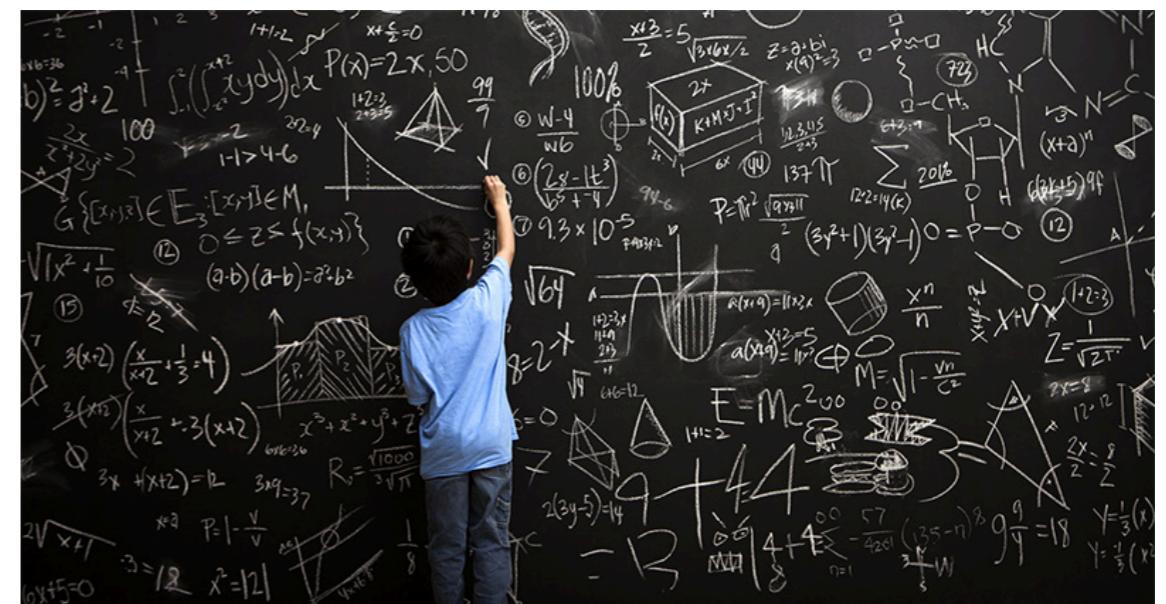
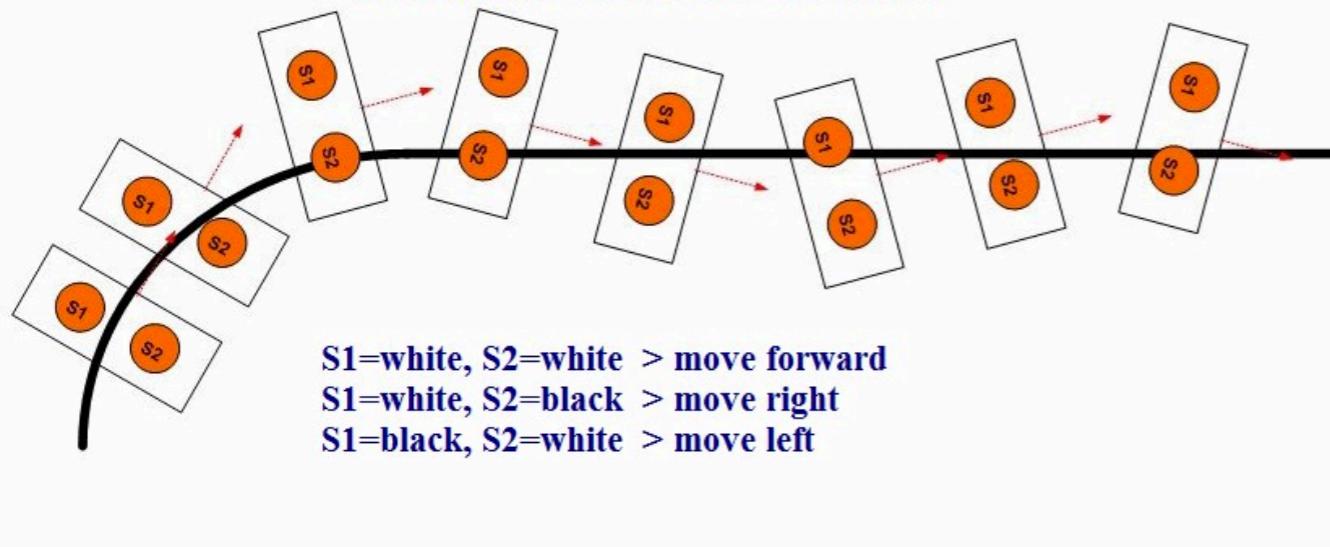
Instructor: Shan Chen

What is Logic?

- Logic is the basis of all mathematical reasoning
 - syntax of statements
 - meaning of statements
 - rules of logical inference



Line follower robot algorithm with 2 infrared reflective sensors



Propositional Logic

Propositions

- **Proposition:** a **declarative** statement that is **either true or false**
 - * *declarative: making an explicit statement*
- Examples:
 - SUSTech is located in Shenzhen. T (*true*)
 - $1 + 1 = 2$ T (*true*)
 - $2 + 2 = 3$ F (*false*)
- Counter-Examples:
 - No parking. *where?*
 - How old are you? *questions are not declarative*
 - $x + 2 = 5$ *x is uncertain*
 - She is very talented. *who?*

Propositions: More Examples

- Are the following sentences propositions?
 - It will rain in Shenzhen tomorrow.
 - $P = NP$
 - There are other life forms on other planets in the universe.
- **Yes!** They are declarative, i.e., either true or false.
 - It's OK that you do not know if the statement is true or false.

Compound Propositions

- **Compound proposition:** a proposition that is built from multiple elementary propositions using logical connectives
- Example:
 - Proposition A: **It rains outside.**
 - Proposition B: **We will watch a movie.**
 - A new proposition: **If it rains outside, then we will watch a movie.**
- Logical connectives:
 - Negation
 - Conjunction
 - Disjunction
 - Exclusive or
 - Implication
 - Biconditional

Negation (not)

- Let p be a proposition. The proposition “It is not the case that p .” is called the **negation of p** , denoted by $\neg p$, and read as “**not p** ”.
 - Example:
 - p SUSTech is located in Shenzhen. T
 - $\neg p$ SUSTech is **not** located in Shenzhen. F
It is **not the case** that SUSTech is located in Shenzhen.
 - More examples:
 - $5 + 2 = 8$ $5 + 2 \neq 8$
 - 10 is a prime number. 10 is **not** a prime number.
 - Classes begin at 8:00am. Classes **do not** begin at 8:00am.

Truth Table (not)

- **Truth table:** displays relationships between truth values (T or F) of different propositions.

p	$\neg p$
T	F
F	T

Rows: contain all possible truth values of proposition p

Conjunction (and)

- Let p and q be propositions. The conjunction of p and q , denoted by $p \wedge q$, is true when both p and q are true and false otherwise.
- Example:
 - p SUSTech is located in Shenzhen.
 - q $5 + 2 = 8$
 - $p \wedge q$ SUSTech is located in Shenzhen and $5 + 2 = 8$
- More Examples:
 - There are infinitely many twin prime numbers and $2 + 2 = 3$
 - 2 is a prime number and 9 is a prime power.

Disjunction (or)

- Let p and q be propositions. The **disjunction** of p and q , denoted by $p \vee q$, is **true** when p or q is **true** and false otherwise.
- Example:
 - p SUSTech is located in Shenzhen.
 - q $5 + 2 = 8$
 - $p \vee q$ SUSTech is located in Shenzhen **or** $5 + 2 = 8$
- More Examples:
 - There are infinitely many twin prime numbers **or** $2 + 2 = 3$
 - 2 is a prime number **or** 9 is a prime power.

Exclusive Or (xor)

- Let p and q be propositions. The exclusive or of p and q , denoted by $p \oplus q$, is true when either p or q is true (i.e., exactly one of p, q is true) and false otherwise.
- Example:
 - p SUSTech is located in Shenzhen.
 - q $5 + 2 = 8$
 - $p \oplus q$ either SUSTech is located in Shenzhen or $5 + 2 = 8$
- More Examples:
 - either There are infinitely many twin prime numbers or $2 + 2 = 3$
 - either 2 is a prime number or 9 is a prime power.

Truth Table (and, or, xor)

- The truth table for conjunction and disjunction

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

Rows: contain all possible ($2^2 = 4$) truth values of p and q

Implication

- Let p and q be propositions. The **implication** (also known as **conditional statement**) “if p , then q ”, denoted by $p \rightarrow q$, is **false** when p is **true** and q is **false**, and **true** otherwise.
 - p is called the **hypothesis** or **premise** and q is called the **conclusion**
 - Example: If you get 100 on the final, then you get an A.

Is this grading rule false when you don't get 100 on the final? NO!

- Truth table:

p	q	$p \rightarrow q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

- Note: $p \rightarrow q$ is equivalent to $\neg p \vee q$ (compare their truth tables)

Implication

- $p \rightarrow q$ is read in a variety of equivalent ways:
 - if p then q
 - p implies q
 - p is sufficient for q
 - q is necessary for p
 - q follows from p
 - q unless $\neg p$ * *this means $q \vee \neg p$*
 - p only if q
- Example:
 - If you get 100 on the final, then you get an A.

p

q

Implication

- The **converse** of $p \rightarrow q$ is $q \rightarrow p$.
- The **contrapositive** of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- The **inverse** of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.
- Examples: (p : you get 100 on the final q : you get an A)
 - $p \rightarrow q$ If you get 100 on the final, then you get an A.
 - $q \rightarrow p$ If you get an A, then you get 100 on the final.
 - $\neg q \rightarrow \neg p$ If you don't get an A, then you don't get 100 on the final.
 - $\neg p \rightarrow \neg q$ If you don't get 100 on the final, then you don't get an A.
- Which one is **logically equivalent** to implication $p \rightarrow q$
 - contrapositive $\neg q \rightarrow \neg p$

Biconditional

- Let p and q be propositions. The **biconditional statement** (also known as **biimplication**) “ p if and only if q ”, denoted by $p \leftrightarrow q$, is **true** if p and q have the same truth values, and false otherwise.
 - the opposite of $p \leftrightarrow q$ is exclusive or $p \oplus q$
- $p \leftrightarrow q$ is read in the following ways:
 - p if and only if q (or “ p iff q ” for short)
 - p is necessary and sufficient for q
 - If p then q , and conversely.

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

The Propositional Logic Basics

- **Proposition:** a declarative statement that is either true or false
- **Compound proposition:** a proposition that is built from multiple elementary propositions using logical connectives
- **Logical connectives:**

• $\neg p$	<i>Negation</i>	• $p \oplus q$	<i>Exclusive Or</i>
• $p \wedge q$	<i>Conjunction</i>	• $p \rightarrow q$	<i>Implication</i>
• $p \vee q$	<i>Disjunction</i>	• $p \leftrightarrow q$	<i>Biconditional</i>
- **Order of precedence:** $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$ (if same: from left to right)
 - Example: do you understand this formula? $p \rightarrow q \rightarrow r \vee \neg s \wedge t$
It can be rewritten using parentheses as $(p \rightarrow q) \rightarrow (r \vee (\neg s \wedge t))$
 - Xor is incomparable with $\wedge \vee$, but we have $\neg > \oplus > \rightarrow > \leftrightarrow$.

Exercise (2 mins)

- p : 2 is a prime (T) q : 6 is a prime (F)
- Determine the truth value of the following logical formulas:
 - $\neg p$
 - $p \wedge q$
 - $p \wedge \neg q$
 - $p \vee q$
 - $p \oplus q$
 - $p \rightarrow q$
 - $q \rightarrow p$
 - $p \leftrightarrow q$

Exercise (2 mins)

- p : 2 is a prime (T) q : 6 is a prime (F)
- Determine the truth value of the following logical formulas:
 - $\neg p$ F
 - $p \wedge q$ F
 - $p \wedge \neg q$ T
 - $p \vee q$ T
 - $p \oplus q$ T
 - $p \rightarrow q$ F
 - $q \rightarrow p$ T
 - $p \leftrightarrow q$ F

Exercise (3 mins)

- Construct a truth table for $p \vee q \rightarrow \neg r$

p	q	r	$\neg r$	$p \vee q$	$p \vee q \rightarrow \neg r$

Hint: decompose the proposition and enumerate all possible truth values, e.g., recall the truth table for $p \rightarrow q$

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

Exercise (3 mins)

- Construct a truth table for $p \vee q \rightarrow \neg r$

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

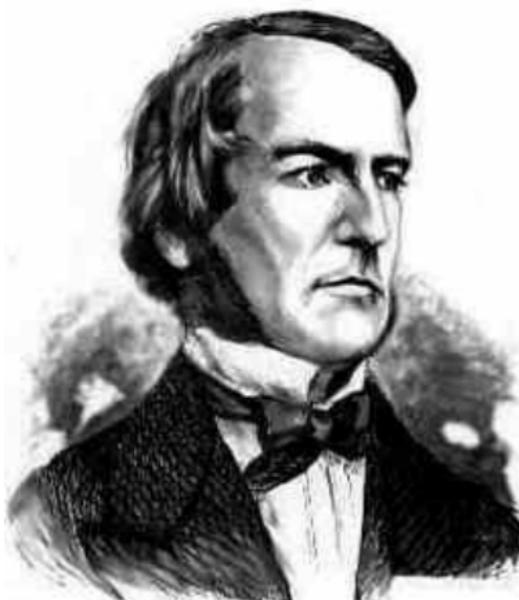
Computer Representation of T/F

- **Bit**: a unit that represents two possible values: 1 (T) or 0 (F)
- **Bit string**: a sequence of bits (might be empty)
 - Its length is the number (might be zero) of bits in the string.
- **Bitwise operations**: replace T and F respectively with 1 and 0
 - C++ bitwise operators: not (\sim), and ($\&$), or ($|$), xor (\wedge).
 - Example: **bitwise disjunction (or)** operation

$$\begin{array}{r} 1011\ 0011 \\ \vee \underline{0110\ 1010} \\ 1111\ 1011 \end{array}$$

Boolean Algebra

- Boolean algebra is intimately connected to propositional logic:
 - focusing on Boolean variables, i.e., with only 2 values 1 (T) and 0 (F)
 - invented by British mathematician **George Boole** (1815~1864)
 - independent from Leibniz's logic work in the 17th century
 - mathematical foundation of digital/logic circuits

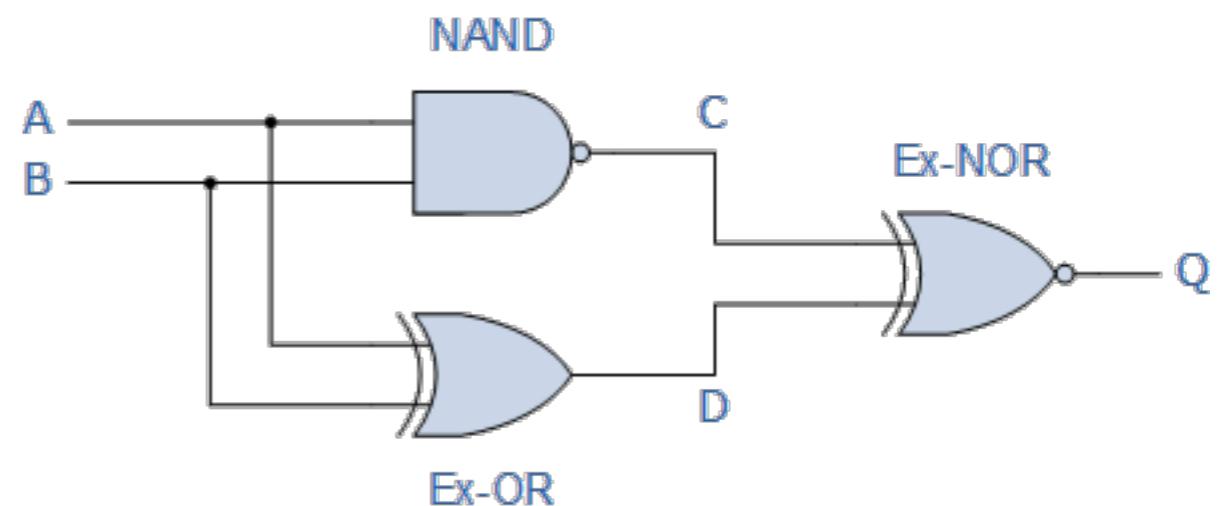
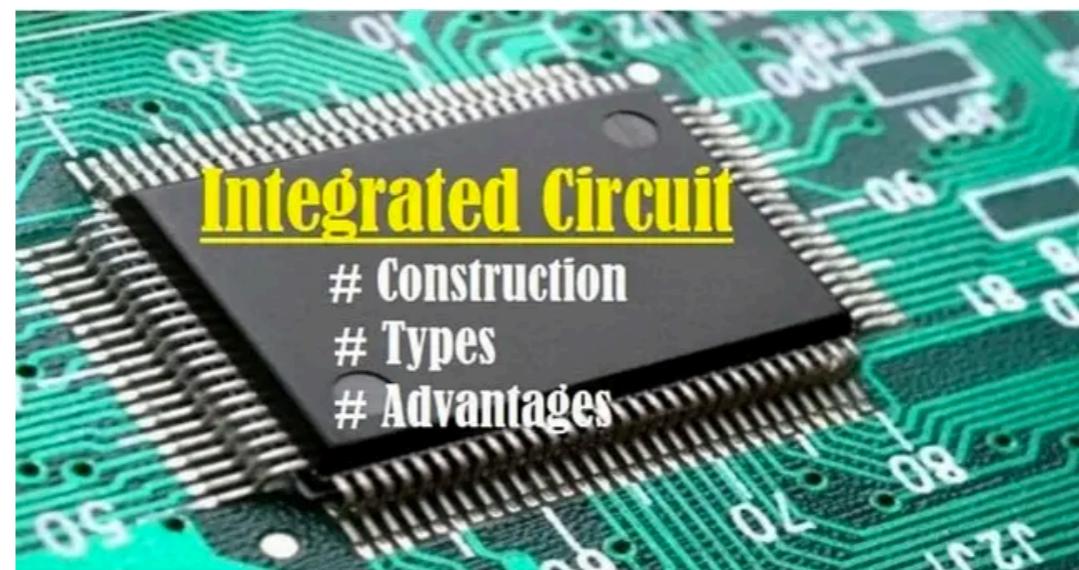
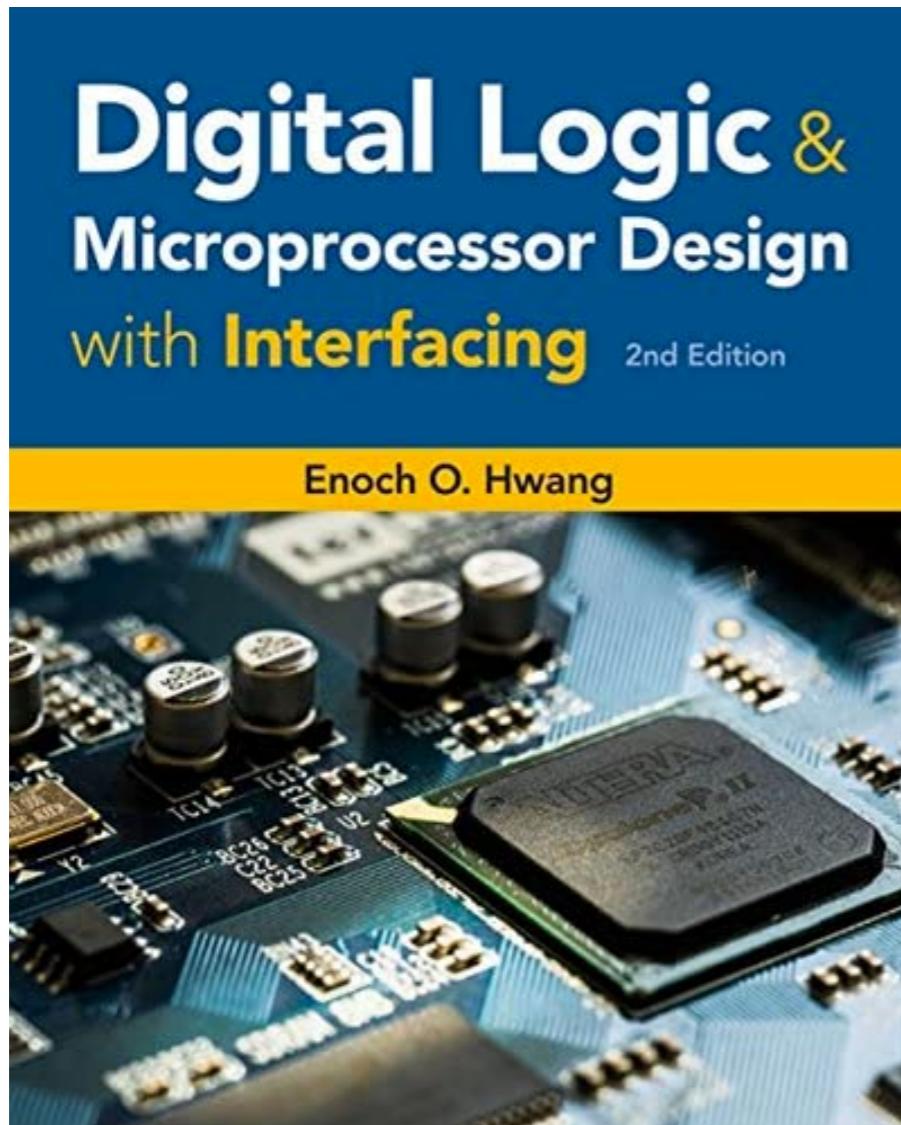


Although Boole's work was not originally perceived as particularly interesting, even by other mathematicians, he is now regarded as one of the founders of the field of computer science.

Applications of Logic

Design of Logic Circuits

- Hardware of digital devices (e.g., computers, phones, etc.)



Boolean Search

- Search with logical operators: and, or, not, etc.

Google

Advanced Search

Find pages with...

To do this in the search box

all these words:

|

Type the important words: tricolor rat terrier

this exact word or phrase:

Put exact words in quotes: "rat terrier"

any of these words:

Type OR between all the words you want:
miniature OR standard

none of these words:

Put a minus sign just before words you don't want:
-rodent, -"Jack Russell"

numbers ranging from:

to

Put 2 periods between the numbers and add a unit of measure:
10..35 lb, \$300..\$500, 2010..2011

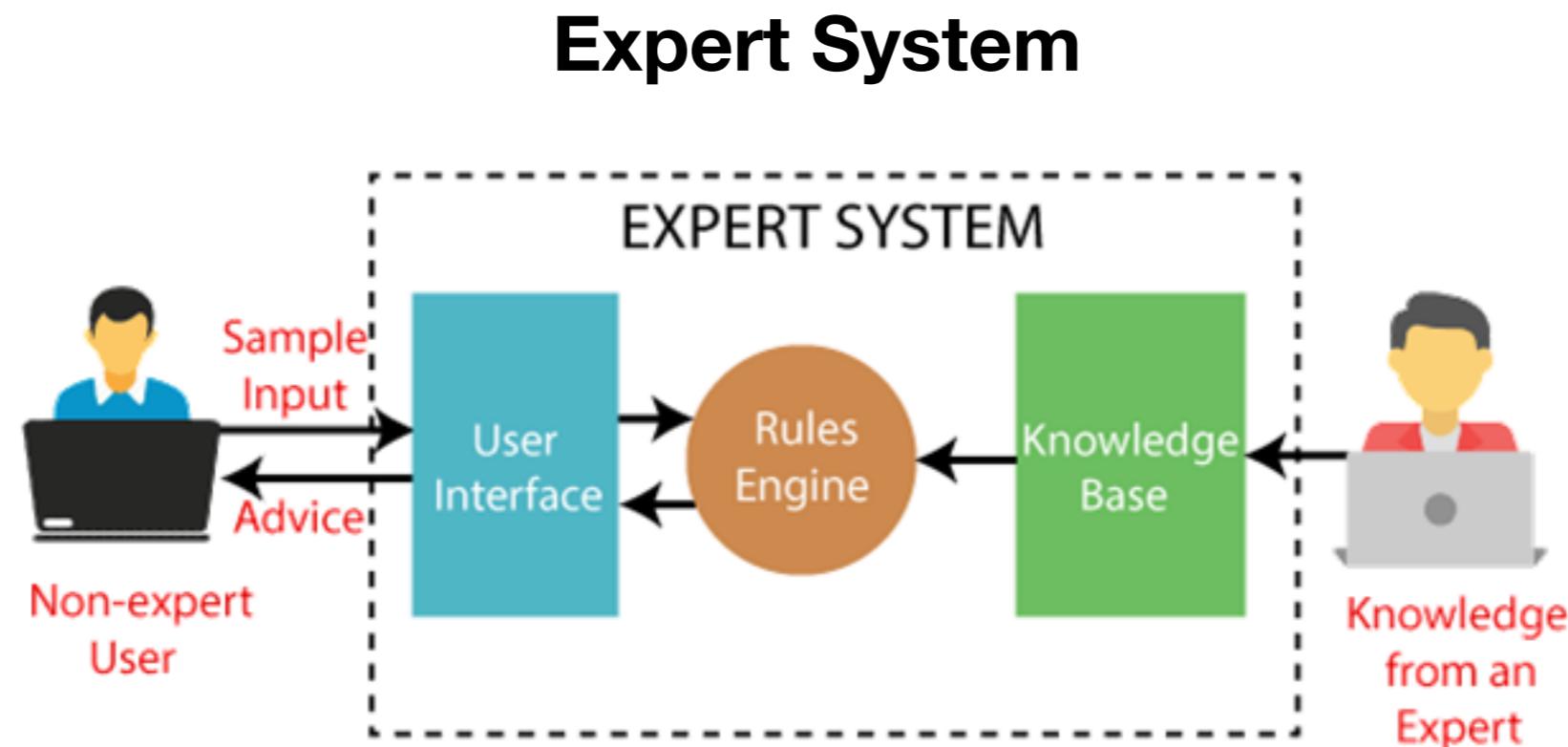
Logical Inference

- Process of reasoning from premises to logical conclusions
- Example:
 - Statement: **If** you are older than 13 **or** you are with your parents **then** you can watch this movie
 - Elementary propositions:
 - p - you are older than 13
 - q - you are with your parents
 - r - you can watch this movie
 - Translation: $p \vee q \rightarrow r$
 - Logical inference example:
 - Suppose p is true (i.e., you are older than 13), then with the help of logic we can infer that r is true (i.e., you can watch this movie).

** looks trivial? actually inference is very powerful in many tasks...*

Inference in Artificial Intelligence

- Artificial intelligence builds programs that act intelligently:
 - Programs often rely on symbolic manipulations (logical inference).

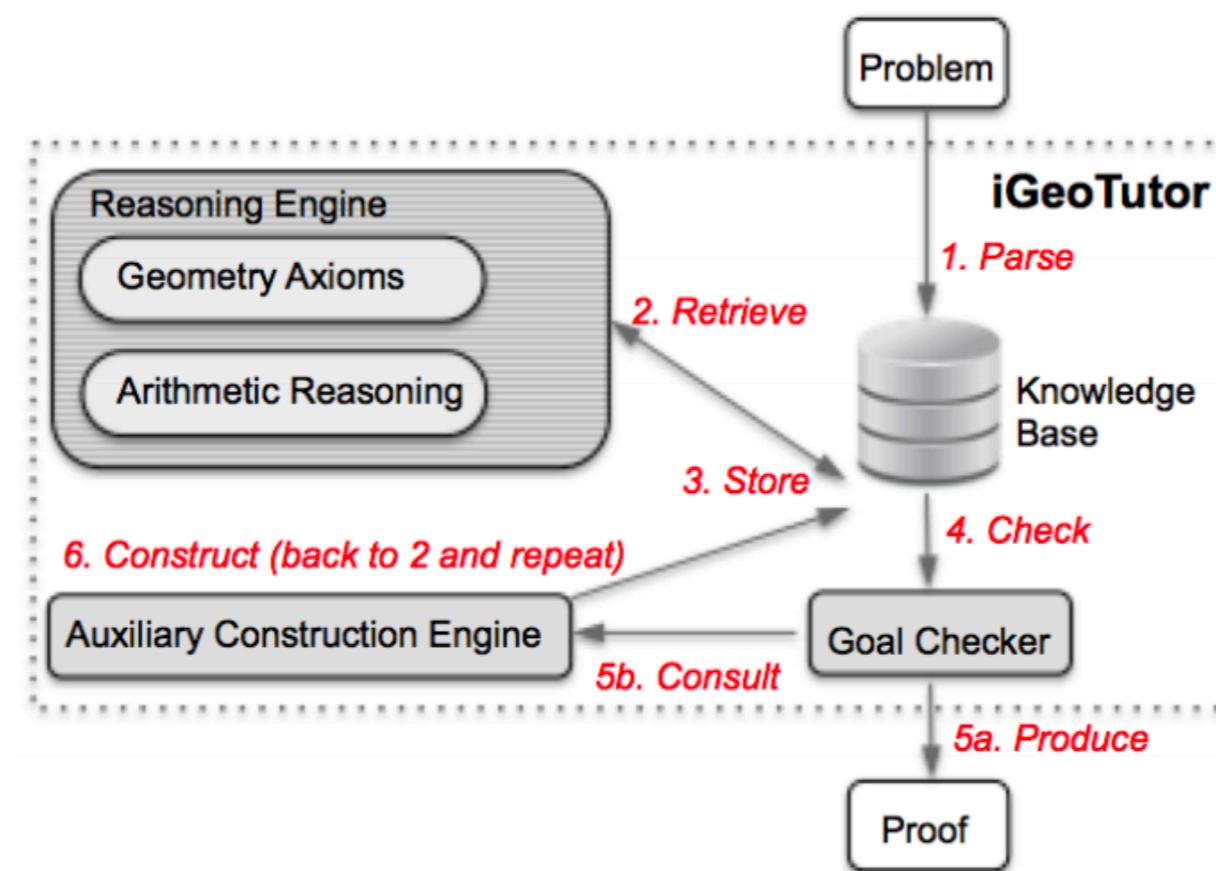


<https://www.javatpoint.com/expert-systems-in-artificial-intelligence>

Inference in Artificial Intelligence

- Artificial intelligence builds programs that act intelligently
 - Programs often rely on symbolic manipulations (logical inference).

Automated Theorem Proving



* Wang and Su, *Automated Geometry Theorem Proving for Human-Readable Proofs*, IJCAI 2015

What's Next...

- Logical equivalence (basis of proofs and circuit design)
 - important laws of logical equivalence
- Predicate logic (remedies limitations of propositional logic)
 - predicates, quantifiers, etc.
- Proofs
 - rules of inference (formal proofs)
 - theorem proving methods (informal proofs)

Assignments

- Deadline for Assignment 1: Oct 11
- Requirements:
 - Write your solutions in English (otherwise 50% penalty).
 - Submit a single PDF file on Blackboard (otherwise 20% penalty).
- DO NOT CHEAT! Plagiarism will be punished severely.
 - It's OK to form study groups and share ideas, but do not plagiarize!
- Reminder: Please submit your Declaration Form (Assignment 0) on Blackboard. (Otherwise, your course grade will be 0.)
 - It must carry your authentic handwritten signature: signing on a tablet is OK, but simply typing in your name is NOT allowed.

Logical Equivalence

Vocabulary

- **Tautology:** a compound proposition that is *always true* for all possible truth values
- **Contradiction:** a compound proposition that is *always false* for all possible truth values
- **Contingency:** a compound proposition that is neither a tautology nor a contradiction

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

Equivalent Propositions

- Two propositions are **equivalent** if they **always** have the **same truth value**.
- Example:
 - Consider the two pieces of codes taken from two different versions of **merge sort**. Do they do the same thing?

```
(1) if (((i+j ≤ p+q) && (i ≤ p) &&  
      ((j > q) || (List1[i] ≤ List2[j]))))  
(2) List3[k] = List1[i]  
(3) i = i+1  
(4) else  
(5) List3[k] = List2[j]  
(6) j = j+1  
(7) k = k+1
```

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))  
      || ((i+j ≤ p+q) && (i ≤ p)  
            && (List1[i] < List2[j]))))  
(2) List3[k] = List1[i]  
(3) i = i+1  
(4) else  
(5) List3[k] = List2[j]  
(6) j = j+1  
(7) k = k+1
```

Equivalent Propositions

- Two propositions are **equivalent** if they **always** have the **same truth value**.
- Example:
 - Consider the two pieces of codes taken from two different versions of **merge sort**. Do they do the same thing?

```
(1) if (((i+j ≤ p+q) && (i ≤ p) &&  
      ((j > q) || (List1[i] ≤ List2[j]))))
```

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))  
      || ((i+j ≤ p+q) && (i ≤ p)  
            && (List1[i] ≤ List2[j]))))
```

- Let's rewrite the above "if conditions" using

$s \sim (i + j \leq p + q)$, $t \sim (i \leq p)$, $u \sim (j > q)$, $v \sim (List1[i] \leq List2[j])$

(1): $s \wedge t \wedge (u \vee v)$

(1'): $(s \wedge t \wedge u) \vee (s \wedge t \wedge v)$

- Now set $w \sim (s \wedge t)$

(1): $w \wedge (u \vee v)$

(1'): $(w \wedge u) \vee (w \wedge v)$

Equivalent Propositions

- Two propositions are **equivalent** if they **always** have the **same truth value**.
- Example:
 - Consider the two pieces of codes taken from two different versions of **merge sort**. Do they do the same thing?

$$(1) w \wedge (u \vee v)$$

w	u	v	$u \vee v$	$w \wedge (u \vee v)$
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

$$(1') (w \wedge u) \vee (w \wedge v)$$

w	u	v	$w \wedge u$	$w \wedge v$	$(w \wedge u) \vee (w \wedge v)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

- Now set $w \sim (s \wedge t)$

$(1): w \wedge (u \vee v)$ **is equivalent to** $(1'): (w \wedge u) \vee (w \wedge v)$

* *this is actually one of the distributive laws that we will see soon*

Equivalent Propositions

- The propositions p and q are called **logically equivalent** if $p \leftrightarrow q$ is a **tautology**, denoted by $p \equiv q$ or $p \Leftrightarrow q$.
- Equivalent propositions are **important** for **logical reasoning** since they can be replaced with each other and can help us:
 - make logical arguments
 - infer new propositions (e.g., in proofs)
- Examples:
 - $p \rightarrow q \equiv \neg p \vee q$ implication can be represented as a **disjunction**
* *this later will be referred to as the useful law*
 - $p \rightarrow q \equiv \neg q \rightarrow \neg p$ implication is equivalent to its **contrapositive**

Important Logical Equivalences

- Identity laws
 - $p \wedge T \equiv p$
 - $p \vee F \equiv p$
- Domination laws
 - $p \vee T \equiv T$
 - $p \wedge F \equiv F$
- Idempotent laws
 - $p \vee p \equiv p$
 - $p \wedge p \equiv p$
- Commutative laws
 - $p \vee q \equiv q \vee p$
 - $p \wedge q \equiv q \wedge p$
- Associative laws
 - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
 - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Distributive laws
 - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
 - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Important Logical Equivalences

- De Morgan's laws

- $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$

- Absorption laws

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

- Double negation law

- $\neg(\neg p) \equiv p$

- Negation laws

- $p \vee \neg p \equiv T$
- $p \wedge \neg p \equiv F$

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

- Useful law

- $p \rightarrow q \equiv \neg p \vee q$

* known as conditional-disjunction equivalence
but we call it useful law for convenience

Using Logical Equivalences

- Equivalences can be used in proofs:
 - a proposition can be transformed using logical equivalences
- Example:
 - Show that $(p \wedge q) \rightarrow p$ is a tautology
 - Verify with the truth table:

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

* proving via a truth table is valid but involves tedious calculations

Using Logical Equivalences

- Equivalences can be used in proofs:
 - a proposition can be transformed using logical equivalences
- Example:
 - Show that $(p \wedge q) \rightarrow p$ is a tautology
 - Proof:

$$\begin{aligned}(p \wedge q) \rightarrow p &\equiv \neg(p \wedge q) \vee p \\ &\equiv (\neg p \vee \neg q) \vee p \\ &\equiv (\neg q \vee \neg p) \vee p \\ &\equiv \neg q \vee (\neg p \vee p) \\ &\equiv \neg q \vee T \\ &\equiv T\end{aligned}$$

Useful
De Morgan's
Commutative
Associative
Negation
Domination

Exercise (2 mins)

- Show that $p \rightarrow q \equiv \neg q \rightarrow \neg p$

- Identity laws

- $p \wedge T \equiv p$
- $p \vee F \equiv p$

- Domination laws

- $p \vee T \equiv T$
- $p \wedge F \equiv F$

- Idempotent laws

- $p \vee p \equiv p$
- $p \wedge p \equiv p$

- Double negation law

- $\neg(\neg p) \equiv p$

- Commutative laws

- $p \vee q \equiv q \vee p$
- $p \wedge q \equiv q \wedge p$

- Associative laws

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

- Distributive laws

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

- De Morgan's laws

- $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$

- Absorption laws

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

- Negation laws

- $p \vee \neg p \equiv T$
- $p \wedge \neg p \equiv F$

- Useful law

- $p \rightarrow q \equiv \neg p \vee q$

Exercise (2 mins)

- Show that $p \rightarrow q \equiv \neg q \rightarrow \neg p$

- Proof: $\neg q \rightarrow \neg p \equiv \neg(\neg q) \vee \neg p$
 $\equiv q \vee \neg p$
 $\equiv \neg p \vee q$
 $\equiv p \rightarrow q$

Useful

Double negation

Commutative

Useful

Exercise (5 mins)

- Show that $\neg(p \oplus q) \equiv p \leftrightarrow q$

Hint: by definition $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

- | | | |
|---|---|--|
| ○ Identity laws <ul style="list-style-type: none">• $p \wedge T \equiv p$• $p \vee F \equiv p$ | ○ Commutative laws <ul style="list-style-type: none">• $p \vee q \equiv q \vee p$• $p \wedge q \equiv q \wedge p$ | ○ De Morgan's laws <ul style="list-style-type: none">• $\neg(p \vee q) \equiv \neg p \wedge \neg q$• $\neg(p \wedge q) \equiv \neg p \vee \neg q$ |
| ○ Domination laws <ul style="list-style-type: none">• $p \vee T \equiv T$• $p \wedge F \equiv F$ | ○ Associative laws <ul style="list-style-type: none">• $(p \vee q) \vee r \equiv p \vee (q \vee r)$• $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | ○ Absorption laws <ul style="list-style-type: none">• $p \vee (p \wedge q) \equiv p$• $p \wedge (p \vee q) \equiv p$ |
| ○ Idempotent laws <ul style="list-style-type: none">• $p \vee p \equiv p$• $p \wedge p \equiv p$ | ○ Distributive laws <ul style="list-style-type: none">• $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$• $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ | ○ Negation laws <ul style="list-style-type: none">• $p \vee \neg p \equiv T$• $p \wedge \neg p \equiv F$ |
| ○ Double negation law <ul style="list-style-type: none">• $\neg(\neg p) \equiv p$ | | ○ Useful law <ul style="list-style-type: none">• $p \rightarrow q \equiv \neg p \vee q$ |

Exercise (5 mins)

- Show that $\neg(p \oplus q) \equiv p \leftrightarrow q$

- Proof:
$$\begin{aligned}\neg(p \oplus q) &\equiv \neg((p \wedge \neg q) \vee (\neg p \wedge q)) && \text{Definition} \\ &\equiv \neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q) && \text{De Morgan's} \\ &\equiv (\neg p \vee \neg(\neg q)) \wedge (\neg(\neg p) \vee \neg q) && \text{De Morgan's} \\ &\equiv (\neg p \vee q) \wedge (p \vee \neg q) && \text{Double negation} \\ &\equiv (p \rightarrow q) \wedge (q \rightarrow p) && \text{Useful} \\ &\equiv p \leftrightarrow q && \text{Definition}\end{aligned}$$

Predicate Logic

Limitations of Propositional Logic

- **Propositional logic** describes the logic world in terms of **elementary propositions** and their **logical combinations**.
- Can we use propositional logic to express the following?
 - p : “**Every** integer squared is ≥ 0 ” q : “ $3^2 \geq 0$ ”
Given that p is true, then q is also true as a **special case** of p .
 - r : “**Some** of the integers are prime” s : “2 is prime”
Given that s is true, then r is also true as **evidenced** by s .
- **No!** If $p \rightarrow q$ (or its equivalent) is not given as a premise, then the truth value of p cannot infer the truth value of q .
- **Solution:** Use **variables** to describe **objects in a group (universe)** and make statements about some or all objects in the group by **quantifying** the variables.

Predicate Logic

- **Predicate logic** remedies propositional logic by allowing for making **statements** with **variables** and **quantifiers**.
- Basic building blocks:
 - **Constant** – models a **specific** object
Examples: “1”, “SUSTech”...
 - **Variable** – represents an object in a group (**universe**)
Examples: $x, y, z\dots$ * *the universe can be people, numbers, etc.*
 - **Predicate** – represents **properties** or **relations** among objects
Examples: *Student(x), Married(A, B)\dots*
 - **Quantifier** - shown later

Predicates

- A **predicate** $P(x)$ assigns a value T or F to each x depending on whether the property $P(x)$ holds or not for x .
- Example:
 - Consider $Prime(x)$ where the universe of discourse is integers:

$Prime(2)$ T

$Prime(6)$ F

...

Is $Prime(x)$ a proposition?

No! ...but after the substitution for x it becomes one.

Predicates (Generalized)

- A **predicate** $P(x_1, x_2, \dots, x_n)$ is a statement that contains n variables x_1, x_2, \dots, x_n and it **becomes a proposition** when all variables x_i are substituted by **specific values**.
- The **universe (domain)** of **predicate variables** (x_1, x_2, \dots, x_n) is the **set of all values** that may be substituted for the variables.
- The **truth set** of the predicate $P(x_1, x_2, \dots, x_n)$ is the **set of all values** of the predicate variables (x_1, x_2, \dots, x_n) such that the proposition $P(x_1, x_2, \dots, x_n)$ is true.
- What is the relation between the truth set and universe?
 - The truth set is a **subset** of the universe.

Example

- Let $P(x)$ be the predicate “ $x^2 > x$ ” where the universe is all real numbers.

- What are the truth values of $P(2)$ and $P(1)$?

$$P(2) = T$$

$$P(1) = F$$

- What is the truth set of $P(x)$?

$$x > 1 \text{ or } x < 0$$

Exercise (1 min)

- Let $Q(x, y)$ be the predicate “ $x = y + 3$ ” where the universe is all pairs of real numbers.
 - What are the truth values of $Q(1, 2)$ and $Q(3, 0)$?
 - What is the truth set of $Q(x, y)$?

Exercise (1 min)

- Let $Q(x, y)$ be the predicate “ $x = y + 3$ ” where the universe is all pairs of real numbers.
 - What are the truth values of $Q(1, 2)$ and $Q(3, 0)$?
 $Q(1, 2) = F$
 $Q(3, 0) = T$
 - What is the truth set of $Q(x, y)$?
 $(r, r - 3)$ for all real numbers r

Compound Statements

- **Compound statements** are obtained from multiple **statements** (including predicates and propositions) via **logical connectives**.
- Examples:
 - $\text{Prime}(2) \wedge \text{Prime}(3)$
Translation: “Both 2 and 3 are primes.” (T)
 - $\text{City}(\text{Shenzhen}) \vee \text{River}(\text{Shenzhen})$
Translation: “Shenzhen is a city or a river.” (T)
 - $\text{CS-major}(x) \rightarrow \text{Student}(x)$
Translation: “If x is CS-major then x is a student.”
** not a proposition because x is not explicit*

Predicates vs Propositions

- A predicate of form $P(x)$ is **not a proposition** because there are **many objects** that it can be applied to.
- However, with predicates, predicate logic allows us to
 - **explicitly manipulate the objects** with variables, and
 - capture **quantified statements** with **quantifiers**, where variables are substituted for to make statements about a group of objects.

Quantified Statements

- **Universally** quantified statements
 - Example: “All CS-major graduates have to pass CS201.”
(This is true **for all** CS-major graduates.)
- **Existentially** quantified statements
 - Example: “Some CS-major students graduate with honor.”
(This is true **for some** students.)

Universal Quantification

- The universal quantification of $P(x)$ is the proposition: “ $P(x)$ is true for all values of x in the universe of discourse.” This is denoted by $\forall x P(x)$ and expressed as “for every x , $P(x)$ is true”.
 - \forall is called the universal quantifier
- Example: $P(x)$: “ $x > x - 1$ ” where the universe is all real numbers
 - What is the truth value of $\forall x P(x)$?
 T
 - Is $P(x)$ a proposition?
No. Many possible substitutions.
 - Is $\forall x P(x)$ a proposition?
Yes. It is true if and only if $P(x)$ is true for all x from the universe.

Existential Quantification

- The existential quantification of $P(x)$ is the proposition: “There exists an element in the universe of discourse such that $P(x)$ is true .” This is denoted by $\exists x P(x)$ and expressed as “there is an x such that $P(x)$ is true”.
 - \exists is called the existential quantifier
- Example: $P(x)$: “ $x > 5$ ” where the universe is all real numbers
 - What is the truth value of $\exists x P(x)$?
 T
 - Is $P(x)$ a proposition?
No. Many possible substitutions.
 - Is $\exists x P(x)$ a proposition?
Yes. It is true if and only if there exists an x from the universe such that $P(x)$ is true.

Exercise (2 mins)

- $P(x)$: “ $x \geq 0$ ” where x is a natural number
 - What is the truth value of $\forall x P(x)$?
- $Q(x)$: “ $x = x + 2$ ” where x is a real number
 - What is the truth value of $\exists x Q(x)$?
- $C(x)$: *CS-major(x) \wedge Honor-student(x)* where x is a SUSTech student
 - * assume all CS-major students graduate with honor
 - What is the truth value of $\forall x C(x)$?
 - What is the truth value of $\exists x C(x)$?

Exercise (2 mins)

- $P(x)$: “ $x \geq 0$ ” where x is a natural number
 - What is the truth value of $\forall x P(x)$?
 T
- $Q(x)$: “ $x = x + 2$ ” where x is a real number
 - What is the truth value of $\exists x Q(x)$?
 F
- $C(x)$: *CS-major(x) \wedge Honor-student(x)* where x is a SUSTech student
 - * assume all CS-major students graduate with honor
 - What is the truth value of $\forall x C(x)$?
 F
 - What is the truth value of $\exists x C(x)$?
 T

Summary of Quantified Statements

- When are $\forall x P(x)$ and $\exists x P(x)$ true and false?

Statement	When true?	When false?
$\forall x P(x)$	$P(x)$ true for all x	There is an x where $P(x)$ is false.
$\exists x P(x)$	There is some x for which $P(x)$ is true.	$P(x)$ is false for all x .

- Suppose that the elements in the universe can be enumerated as a_1, a_2, \dots, a_n , then:
 - $\forall x P(x)$ is true whenever $P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n)$ is true
 - $\exists x P(x)$ is true whenever $P(a_1) \vee P(a_2) \vee \dots \vee P(a_n)$ is true

The Universe Matters

- The truth values of $\exists x P(x)$ and $\forall x P(x)$ depend on both **the predicate $P(x)$** and the universe.
- Example: $P(x)$: “ $x < 2$ ”
 - universe: **the positive integers**
 $\exists x P(x) - T$ $\forall x P(x) - F$
 - universe: **the negative integers**
 $\exists x P(x) - T$ $\forall x P(x) - T$
 - universe: **$\{3, 4, 5\}$**
 $\exists x P(x) - F$ $\forall x P(x) - F$

Precedence of Quantifiers

- The quantifiers \forall and \exists have higher precedence than all other logical operators, i.e., $\forall/\exists > \neg > \wedge > \vee > \rightarrow > \leftrightarrow$
 - When xor is concerned: $\forall/\exists > \neg > \oplus > \rightarrow > \leftrightarrow$
- Example: what does $\exists x P(x) \vee Q(x)$ mean?
 - It means $(\exists x P(x)) \vee Q(x)$ rather than $\exists x (P(x) \vee Q(x))$

Translation with Quantifiers

- Statement: “All SUSTech students are smart.”
 - universe: all SUSTech students
translation: $\forall x \text{ Smart}(x)$
 - universe: all students
translation: $\forall x (\text{At}(x, \text{SUSTech}) \rightarrow \text{Smart}(x))$
What about this? $\forall x (\text{At}(x, \text{SUSTech}) \wedge \text{Smart}(x))$
** this means every student is at SUSTech and is smart!*
 - universe: all people
translation: $\forall x (\text{Student}(x) \wedge \text{At}(x, \text{SUSTech}) \rightarrow \text{Smart}(x))$

Translation with Quantifiers

- Statement: “Someone at SUSTech is smart.”
 - universe: all SUSTech affiliates
translation: $\exists x \text{ Smart}(x)$
 - universe: all people
translation: $\exists x (\text{At}(x, \text{SUSTech}) \wedge \text{Smart}(x))$
What about this? $\exists x (\text{At}(x, \text{SUSTech}) \rightarrow \text{Smart}(x))$
** this is even true when there is someone who is not at SUSTech and nobody at SUSTech is smart!*

Negation of Quantified Statements

- Example 1: “Nothing is perfect.”
 - translation 1: $\neg \exists x \text{ Perfect}(x)$
 - translation 2: $\forall x \neg \text{Perfect}(x)$ (“Everything is imperfect.”)
- Conclusion 1: $\neg \exists x P(x)$ is equivalent to $\forall x \neg P(x)$
- Example 2: “Not all horses are white.”
 - translation 1: $\neg \forall x (\text{Horse}(x) \rightarrow \text{White}(x))$
 - translation 2: $\exists x (\text{Horse}(x) \wedge \neg \text{White}(x))$ (“There is a nonwhite horse.”)
logically equivalent to $\exists x \neg(\text{Horse}(x) \rightarrow \text{White}(x))$ why?
 - * derived from De Morgan’s and useful laws
- Conclusion 2: $\neg \forall x P(x)$ is equivalent to $\exists x \neg P(x)$

Negation of Quantified Statements

- De Morgan's laws (logical equivalence) for quantifiers

Negation	Equivalent Statement	When Is Negation True?	When False?
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every x , $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x .

Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.
- Example 1: “Every real number has its corresponding negative.”
 - a real number is denoted by x and its negative as y
 - a predicate $P(x, y)$ denotes “ $x + y = 0$ ”
 - **Translation:** $\forall x \exists y P(x, y)$
- Example 2: “There is a person who loves everybody.”
 - variables x and y each denote a person
 - a predicate $L(x, y)$ denotes “ x loves y ”
 - **Translation:** $\exists x \forall y L(x, y)$

Exercise (3 mins)

- Variables x, y denote people, and $L(x, y)$ denotes “ x loves y ”.
Translate the following to quantified formulas.
 1. Everybody loves Raymond.
 2. Everybody loves somebody.
 3. There is somebody whom everybody loves.
 4. There is somebody whom Raymond doesn't love.
 5. There is somebody whom no one loves.
 6. There is exactly one person whom everybody loves. * *try $=, \neq$*

Exercise (3 mins)

- Variables x, y denote people, and $L(x, y)$ denotes “ x loves y ”.
Translate the following to quantified formulas.
 1. Everybody loves Raymond.
 2. Everybody loves somebody.
 3. There is somebody whom everybody loves.
 4. There is somebody whom Raymond doesn't love.
 5. There is somebody whom no one loves.
 6. There is exactly one person whom everybody loves. * *try $=, \neq$*

- Solutions:**

- | | |
|-------------------------------------|---|
| 1. $\forall x L(x, \text{Raymond})$ | 4. $\exists y \neg L(\text{Raymond}, y)$ |
| 2. $\forall x \exists y L(x, y)$ | 5. $\exists y \forall x \neg L(x, y)$ |
| 3. $\exists y \forall x L(x, y)$ | 6. $\exists y (\forall x L(x, y) \wedge \forall z (\forall x L(x, z) \rightarrow z = y))$ |

Order of Quantifiers

- The order of nested quantifiers **matters** if quantifiers are of **different** types.
 - Example: $\forall x \exists y L(x, y) \neq \exists y \forall x L(x, y)$ $L(x, y)$ denotes “*x loves y*”
 - $\forall x \exists y L(x, y)$: *Everybody loves somebody*
 - $\exists y \forall x L(x, y)$: *There is someone who is loved by everyone*
- The order of nested quantifiers **does not matter** if quantifiers are of the **same** type.
 - Example: $\forall x \forall y (\text{Parent}(x, y) \rightarrow \text{Child}(y, x))$
 - This means: for all x and y , if x is a parent of y , then y is a child of x .
 - $\forall y \forall x (\text{Parent}(x, y) \rightarrow \text{Child}(y, x))$ means the same

Quantifications of Two Variables

Statement	When True?	When False
$\forall x \forall y P(x, y)$	$P(x, y)$ is true for every pair x, y .	There is a pair x, y for which $P(x, y)$ is false.
$\forall y \forall x P(x, y)$		
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y .
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y .	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y
$\exists y \exists x P(x, y)$		

Negating Nested Quantifiers

- Example: “for every real number x , there exists a real number y such that $xy = 1$.”
- Translation: $\forall x \exists y (xy = 1)$
- Negation: $\neg \forall x \exists y (xy = 1)$
 - $\equiv \exists x \neg \exists y (xy = 1)$ *De Morgan's* $P(x)$: $\exists y (xy = 1)$
 - $\equiv \exists x \forall y \neg(xy = 1)$ *De Morgan's* $Q(x, y)$: $xy = 1$
 - $\equiv \exists x \forall y (xy \neq 1)$ *Definition*
- What is the negation of $\forall x \exists y P(x, y)$? What about $\exists x \forall y P(x, y)$?
 - $\neg \forall x \exists y P(x, y) \equiv \exists x \forall y \neg P(x, y)$
 - $\neg \exists x \forall y P(x, y) \equiv \forall x \exists y \neg P(x, y)$

Formal Proofs

Vocabulary

- **Axiom (or postulate):** a statement or proposition which is regarded as being established, accepted, or self-evidently **true**
 - E.g., “A straight line segment can be drawn joining any two points.”
- **Theorem:** a statement that can be **proved to be true**
 - E.g., “There are infinitely many prime numbers.”
- **Proof:** a **valid argument** that establishes the truth of a theorem
- **Lemma:** a less important theorem that can be **proved to be true**, and is **used in proving other theorems**
- **Corollary:** a statement that can be **established directly from a theorem**
- **Conjecture:** a statement that is **being proposed to be true**

Theorems

- Typically, a theorem looks like this:

$$p_1 \wedge p_2 \wedge \dots \wedge p_n \rightarrow q$$

premises *conclusion*

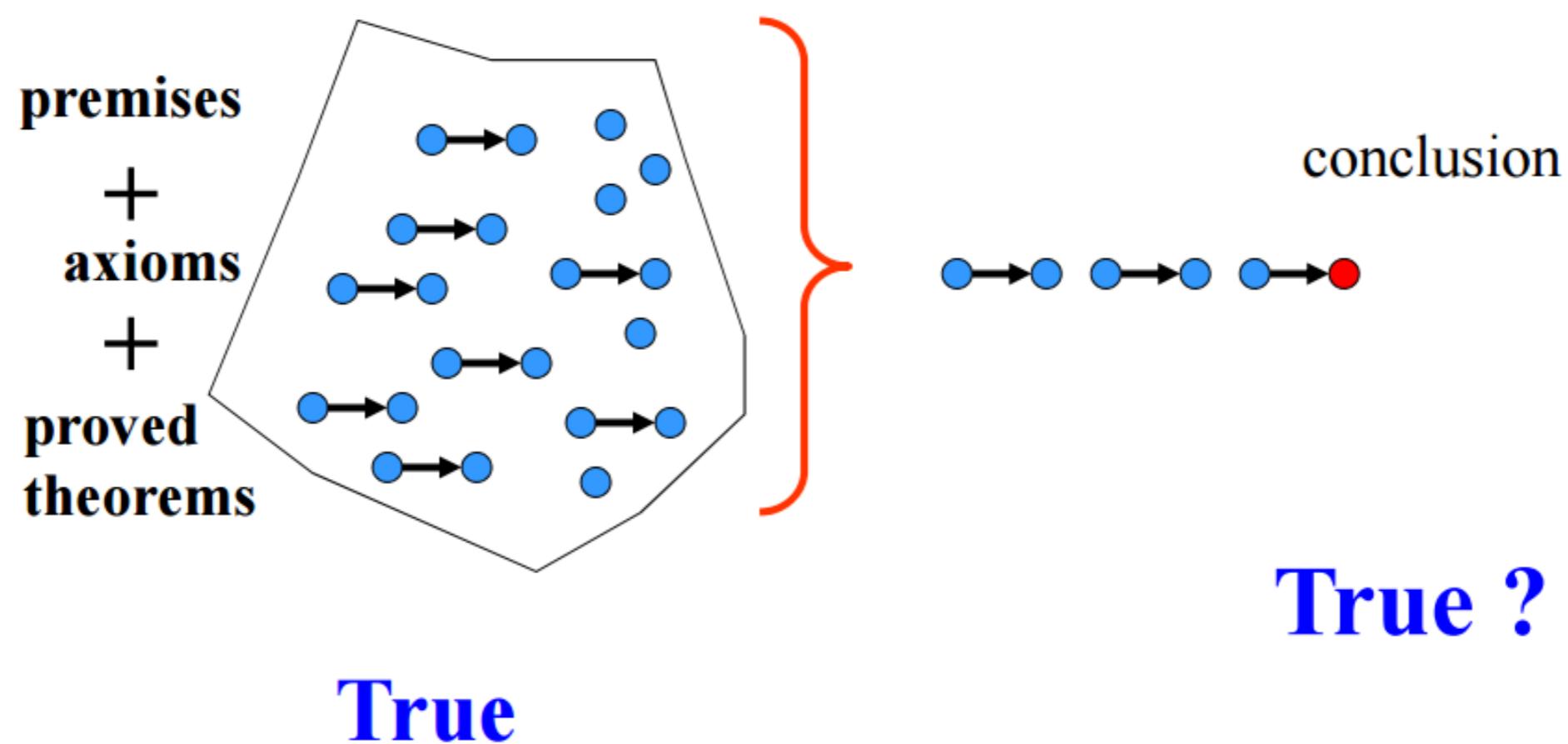
- Example: Fermat's little theorem

- If p is a prime and a is an integer not divisible by p , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Formal Proofs

- In **formal proofs**, steps follow **logically** from the set of premises, axioms, lemmas, and proved theorems.



Using Logical Equivalences

- Proofs based on logical equivalences: a statement can be transformed using a sequence of equivalence rewrites until some conclusion can be reached.
- Example:
 - Show that $(p \wedge q) \rightarrow p$ is a tautology
 - Proof:
$$\begin{aligned}(p \wedge q) \rightarrow p &\equiv \neg(p \wedge q) \vee p && \text{Useful} \\ &\equiv (\neg p \vee \neg q) \vee p && \text{De Morgan's} \\ &\equiv (\neg q \vee \neg p) \vee p && \text{Commutative} \\ &\equiv \neg q \vee (\neg p \vee p) && \text{Associative} \\ &\equiv \neg q \vee T && \text{Negation} \\ &\equiv T && \text{Domination}\end{aligned}$$

Rules of Inference for Propositional Logic

- **Rules of inference** (premises are true implies conclusion is true)
 - allow to infer new **true** statements from existing true statements
 - represent **logically valid** inference patterns
- List of rules:
 - **Modus ponens**
 - **Modus tollens**
 - **Hypothetical syllogism**
 - **Disjunctive syllogism**
 - **Addition**
 - **Simplification**
 - **Conjunction**
 - **Resolution**

Rules of Inference for Propositional Logic

- Modus ponens (affirming the antecedent):

$$\frac{p \rightarrow q \quad p}{\therefore q}$$

corresponding tautology:
 $((p \rightarrow q) \wedge p) \rightarrow q$

- Example:

- p “It is raining.”
- q “I will study discrete math.”
- $p \rightarrow q$ “If it is raining, then I will study discrete math.”
- p “It is raining.”
- q “Therefore, I will study discrete math.”

Rules of Inference for Propositional Logic

- Modus tollens (denying the consequent):

$$\frac{p \rightarrow q \quad \neg q}{\therefore \neg p}$$

corresponding tautology:

$$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$$

- Example:

- p “It is raining.”
- q “I will study discrete math.”
- $p \rightarrow q$ “If it is raining, then I will study discrete math.”
- $\neg q$ “I will **not** study discrete math.”
- $\neg p$ “Therefore, it is **not** raining.”

Rules of Inference for Propositional Logic

- Hypothetical syllogism:

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

corresponding tautology:
$$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$$

- Disjunctive syllogism:

$$\frac{p \vee q \quad \neg p}{\therefore q}$$

corresponding tautology:
$$((p \vee q) \wedge \neg p) \rightarrow q$$

Rules of Inference for Propositional Logic

- Addition:

$$\frac{p}{\therefore p \vee q}$$

corresponding tautology:

$$p \rightarrow (p \vee q)$$

- Simplification:

$$\frac{p \wedge q}{\therefore q}$$

corresponding tautology:

$$(p \wedge q) \rightarrow q$$

** of course we also have $(p \wedge q) \rightarrow p$*

Rules of Inference for Propositional Logic

- Conjunction:

$$\frac{\begin{array}{c} p \\ q \end{array}}{\therefore p \wedge q}$$

corresponding tautology:

$$(p) \wedge (q) \rightarrow p \wedge q$$

- Resolution:

$$\frac{\begin{array}{c} \neg p \vee r \\ p \vee q \end{array}}{\therefore q \vee r}$$

corresponding tautology:

$$(\neg p \vee r) \wedge (p \vee q) \rightarrow (q \vee r)$$

* note that p is either true or false

Example

- Premises:
 - “It is not sunny this afternoon and it is colder than yesterday.” $\neg p \wedge q$
 - “We will go swimming only if it is sunny.” $r \rightarrow p$
 - “If we do not go swimming then we will take a canoe trip.” $\neg r \rightarrow s$
 - “If we take a canoe trip, then we will be home by sunset.” $s \rightarrow t$

- Show that all these lead to a conclusion:

- “We will be home by sunset.” t

p “It is sunny this afternoon.”

q “It is colder than yesterday.”

r “We will go swimming.”

s “We will take a canoe trip.”

t “We will be home by sunset.”

Example

- Translation:

- premises: $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s, s \rightarrow t$
- conclusion: t

- Proof:

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Exercise (3 mins)

- Prove that the premises $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s$ imply $\neg q \rightarrow s$.

Exercise (3 mins)

- Prove that the premises $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s$ imply $\neg q \rightarrow s$.
- Proof:

Step	Reason
1. $p \rightarrow q$	Premise
2. $\neg q \rightarrow \neg p$	Contrapositive of (1)
3. $\neg p \rightarrow r$	Premise
4. $\neg q \rightarrow r$	Hypothetical syllogism using (2) and (3)
5. $r \rightarrow s$	Premise
6. $\neg q \rightarrow s$	Hypothetical syllogism using (4) and (5)

Rules of Inference for Quantified Statements

- Universal instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

- Universal generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

- Existential instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

- Existential generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example

- Premises:
 - “A student in this class has not read the book.” $\exists x(C(x) \wedge \neg B(x))$
 - “Everyone in this class passed the first exam.” $\forall x(C(x) \rightarrow P(x))$
 - Show that all these lead to a conclusion:
 - “Someone who passed the first exam has not read the book.”
 $\exists x(P(x) \wedge \neg B(x))$
- $C(x)$ “ x is in this class.”
- $B(x)$ “ x has read the book.”
- $P(x)$ “ x passed the first exam.”

Example

- Translation:

- premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \rightarrow P(x))$
- conclusion: $\exists x(P(x) \wedge \neg B(x))$

- Proof:

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

Informal Proofs

Informal Proofs

- Formal proofs can be extremely long and hard to follow.
- In practice, the proofs of theorems designed for human consumption are almost always informal proofs:
 - Informal proofs are not expressed in any formal language of logic.
 - Axioms being assumed and rules of inference being used are not explicitly stated, more than one rule of inference may be used in each step, steps may be skipped, etc.
 - One must always watch the consistency of the proof made.
 - Logic and inference rules can help decide soundness of the proof.
- Next, we use informal proofs to illustrate different methods of theorem proving, i.e., proof strategy.

Methods of Theorem Proving

- Basic methods to prove theorems:
 - Direct proof
 $p \rightarrow q$ is proved by showing that if p is true then q follows
 - Proof by contraposition
 $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$ is true
 - Proof by contradiction
shows that “theorem is false” leads to **contradiction** (e.g., $r \wedge \neg r$)
 - Proof by cases
gives proofs for all possible cases
 - Proof by equivalence
 $p \leftrightarrow q$ is replaced with $(p \rightarrow q) \wedge (q \rightarrow p)$
- * *proof by induction will be covered in later lectures*

Direct Proof

- $p \rightarrow q$ is proved by showing that **if p is true then q follows.**
- Example: Prove that “**if n is odd, then n^2 is odd.**”

- Proof:

Assume that the hypothesis is true, i.e., **n is odd.**

That is, $n = 2k + 1$ where k is an integer.

Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Therefore, **n^2 is odd.**

Proof by Contraposition

- $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$ is true.
- Example: Prove that “if $3n + 2$ is odd, then n is odd.”
 - Proof:

Assume that n is even, i.e., $n = 2k$, where k is an integer.
Then, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
Therefore, $3n + 2$ is even.

Proof by Contradiction

- To prove $p \rightarrow q$ is true, assume p is true but q is false ($p \wedge \neg q$), then show a **contradiction** to p or $\neg q$, or other settled results.
- Example: Prove that “if $3n + 2$ is odd, then n is odd.”
 - Proof:

Assume that $3n + 2$ is odd and n is even,
Then, $n = 2k$ for some integer k , and $3n + 2 = 2(3k + 1)$.
Thus, $3n + 2$ is even.
This is in **contradiction** to the assumption that $3n + 2$ is odd.
Therefore, if $3n + 2$ is odd, n is odd.
- How to prove an isolated proposition q is true (with no explicit premise) by contradiction?
 - Assume $\neg q$ is true (i.e., q is false) and show a **contradiction** to $\neg q$ or other settled results.

Proof by Cases

- In order to show $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$, it is equivalent to show $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$. *Why?*

$$\begin{aligned} & (p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q \\ \equiv & \neg(p_1 \vee p_2 \vee \dots \vee p_n) \vee q && \text{Useful} \\ \equiv & (\neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n) \vee q && \text{De Morgan's} \\ \equiv & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \dots \wedge (\neg p_n \vee q) && \text{Distributive} \\ \equiv & (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q) && \text{Useful} \end{aligned}$$

- Example: Prove that “ $|x||y| = |xy|$ for real numbers x, y .”

- Proof: (4 cases)

$$\begin{array}{ll} x \geq 0, y \geq 0 & x \geq 0, y < 0 \\ x < 0, y \geq 0 & x < 0, y < 0 \end{array}$$

Proof by Equivalence

- To prove $p \leftrightarrow q$, show $(p \rightarrow q) \wedge (q \rightarrow p)$.
- Example: Prove that “an integer n is odd if and only if n^2 is odd”
 - Proof: (sketch)
 - Proof of $p \rightarrow q$: direct proof
 - Proof of $q \rightarrow p$: proof by contraposition

Vacuous Proof and Trivial Proof

- **Vacuous proof:** To prove $p \rightarrow q$, if p is **always false**, then $p \rightarrow q$ is always true.
- Example: Let $P(n)$ denote “if $n > 1$ then $n^2 > n$ ”. Show $P(0)$.
 - Proof: Since the **premise $0 > 1$ is always false**, $P(0)$ is true.
- **Trivial proof:** To prove $p \rightarrow q$, if q is **always true**, then $p \rightarrow q$ is always true.
- Example: Let $P(n)$ denote “if $a \geq b$ then $a^n \geq b^n$ ”. Show $P(0)$.
 - Proof: Since the **conclusion $a^0 \geq b^0$ is always true**, $P(0)$ is true.

Proofs with Quantifiers

- Universally quantified statements $\forall x P(x)$
 - positive: prove the property **holds for all** examples
e.g., **proof by cases** to divide the proof into different parts
 - negative: **disprove universal** statements
e.g., show **counterexamples**
- Existentially quantified statements $\exists x P(x)$
 - positive: **constructive**
e.g., **find a specific example** to show the statement holds
 - negative: **nonconstructive**
e.g., **proof by contradiction**

Example

- Prove that “ $\sqrt{2}$ is irrational.” (Rational numbers are of the form $\frac{m}{n}$, where $m, n \neq 0$ are co-prime integers.)
- Proof by contradiction:

Suppose that $\sqrt{2}$ is rational, i.e., there exist integers m and n such that $\sqrt{2} = \frac{m}{n}$ and the greatest common divisor of m, n is 1.

Then, we have $m^2 = 2n^2$, and hence m is even.

Let $m = 2k$ for some integer k . It then follows that $4k^2 = 2n^2$, i.e., $2k^2 = n^2$, so n is also even.

This means the two even numbers m, n must have a common divisor 2, which contradicts the assumption.

* very elegant :) do you agree?

Exercise (5 mins)

- Prove that “there are infinitely many prime numbers.” (a prime number is a natural number > 1 that is not divisible by any smaller natural number except 1) *Hint: proof by contradiction*

Exercise (5 mins)

- Prove that “there are infinitely many prime numbers.” (a prime number is a natural number > 1 that is not divisible by any smaller natural number except 1) *Hint: proof by contradiction*

- Proof:

Suppose that there are only a finite number of primes.

Then, there exists some largest prime number p , and we can list all prime numbers in ascending order: $2, 3, 5, 7, 11, \dots, p$.

Let $n = (2 \times 3 \times 5 \times \dots \times p) + 1$ be the product of all primes plus 1. Then $n > 1$ and n cannot be divided by any prime number in the above list. This means that n is also prime. * why?

Obviously, n is larger than all the primes in the above list. This contradicts the assumption that p is the largest prime number.

* also very elegant :) don't you agree?

“... mathematical logic is and must be the basis for software design ... mathematical analysis of designs and specifications have become central activities in computer science research...”

Edsger W. Dijkstra (1930–2002), Dutch computer scientist

03 Sets and Functions

To be continued...

Project (optional, $-1 \sim +5$ points)

- Submit a **self-contained report** with **clear references**, together with supplementary materials (e.g., demo, codes, etc.) if any.
 - **Individual** project (no teamwork): do it only if you really have time
 - **Pick your own topic** related to this course.
If you have no clue, refer to “Writing Projects” in your textbook for examples, but avoid topics that are too easy or not technical at all.
 - Must involve some **technical details**.
E.g., “the history of the word algorithm” is not considered technical.
- Grading is based on **quality**: **scope**, **depth**, **workload**, **writing**, etc.
 - If your report is too hard to follow, **you may even get -1 point for wasting our time**. Many prior projects got 0 points for low quality.
 - **DO NOT** submit projects from other courses, which is **plagiarism** and will be punished severely!