# MA112:
# Discrete Mathematics

Waleed A. Yousef, Ph.D.,

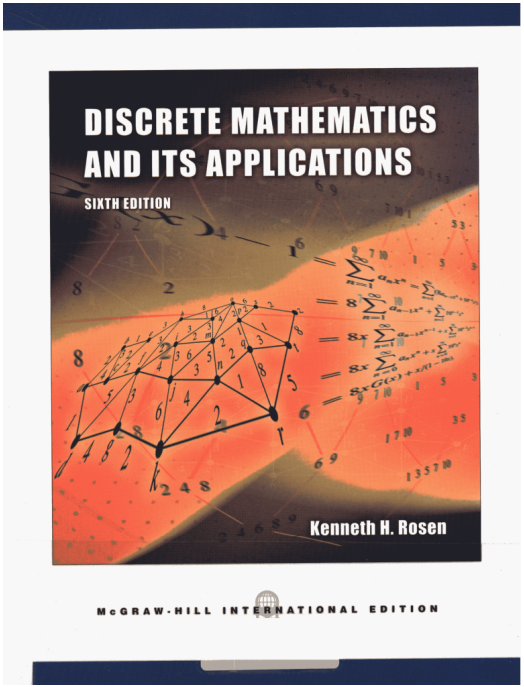
Human Computer Interaction Lab.,
Computer Science Department,
Faculty of Computers and Information,
Helwan University,
Egypt.

May 9, 2016

**Lectures follow:**

Rosen, K. H., 2007. Discrete mathematics and its applications, 6th Edition. McGraw-Hill Higher Education, Boston.

URL http://www.loc.gov/catdir/toc/ecip0612/2006012468.htmlhttp://www.loc.gov/catdir/enhafy0702/2006012468-d.htmlhttp://www.loc.gov/catdir/enhancements/fy0737/2006012468-b.html



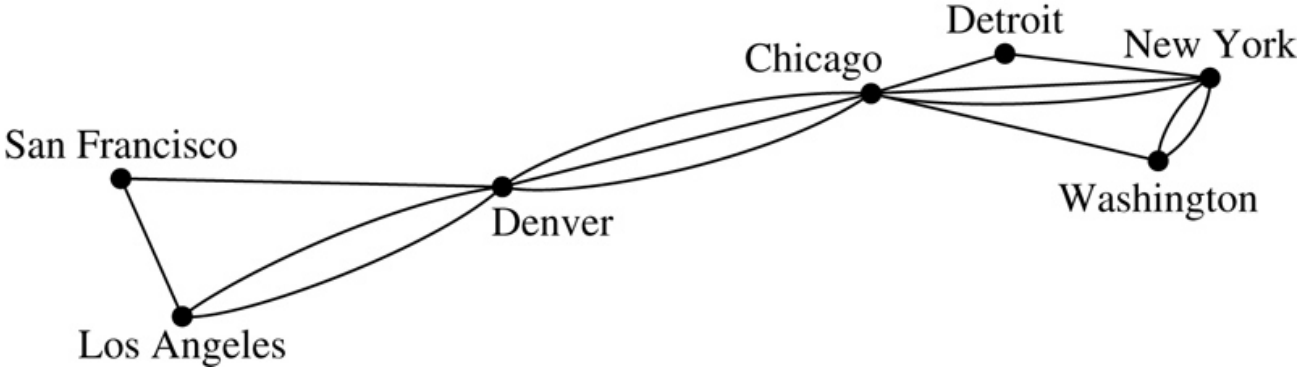
# Course Objectives

- Developing rigorous treatment.
- Developing mathematical foundations to CS.
- Building intuition.
- Linking to CS applications (Rosen has great practical examples)
- Introducing students to "Mathematical Computing" (we will use "Sage")

**Let's see how Mathematics is the pillars of Engineering and CS by illustrating the book's chapters**

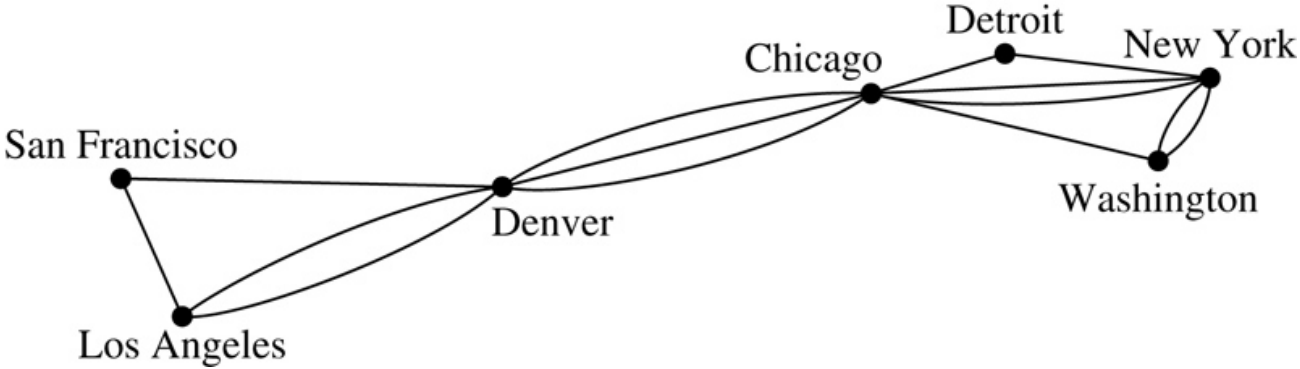
## Chapter 9: Graphs





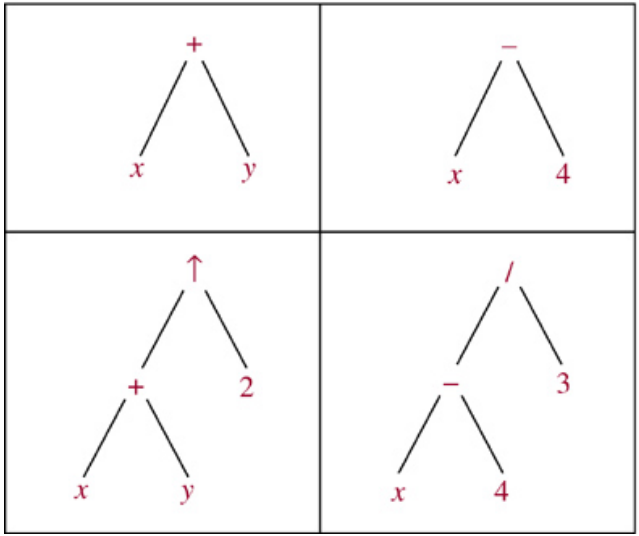
## Chapter 9: Graphs

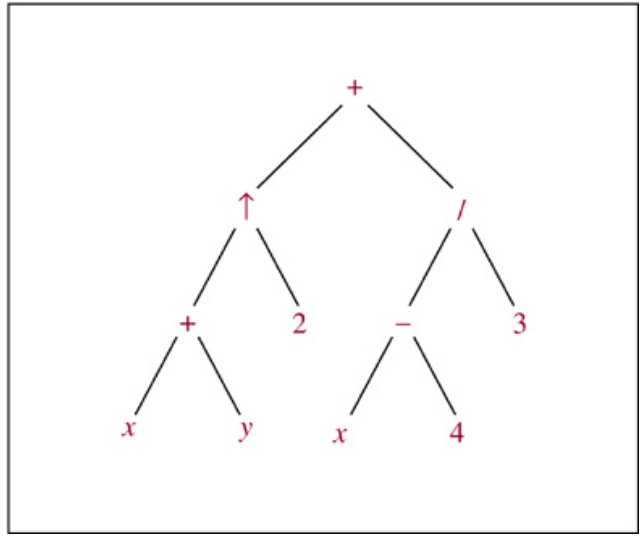




## Chapter 10: Trees

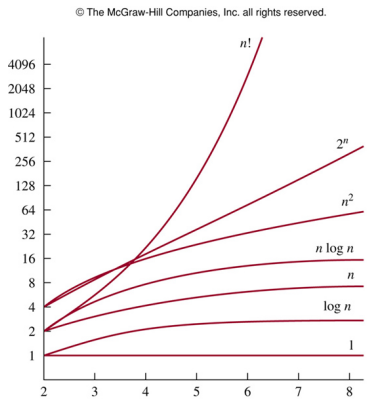


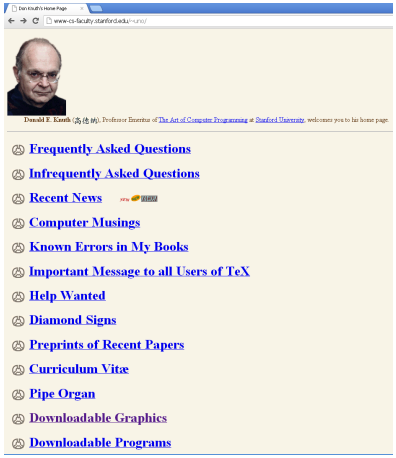


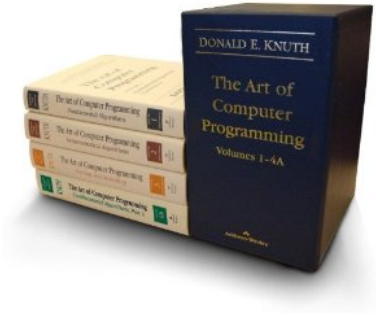




## Chapter 4: Induction and Recursion

# Chapter 3: Algorithms, Chapter 5: Counting, Chapter 7: Advanced Counting



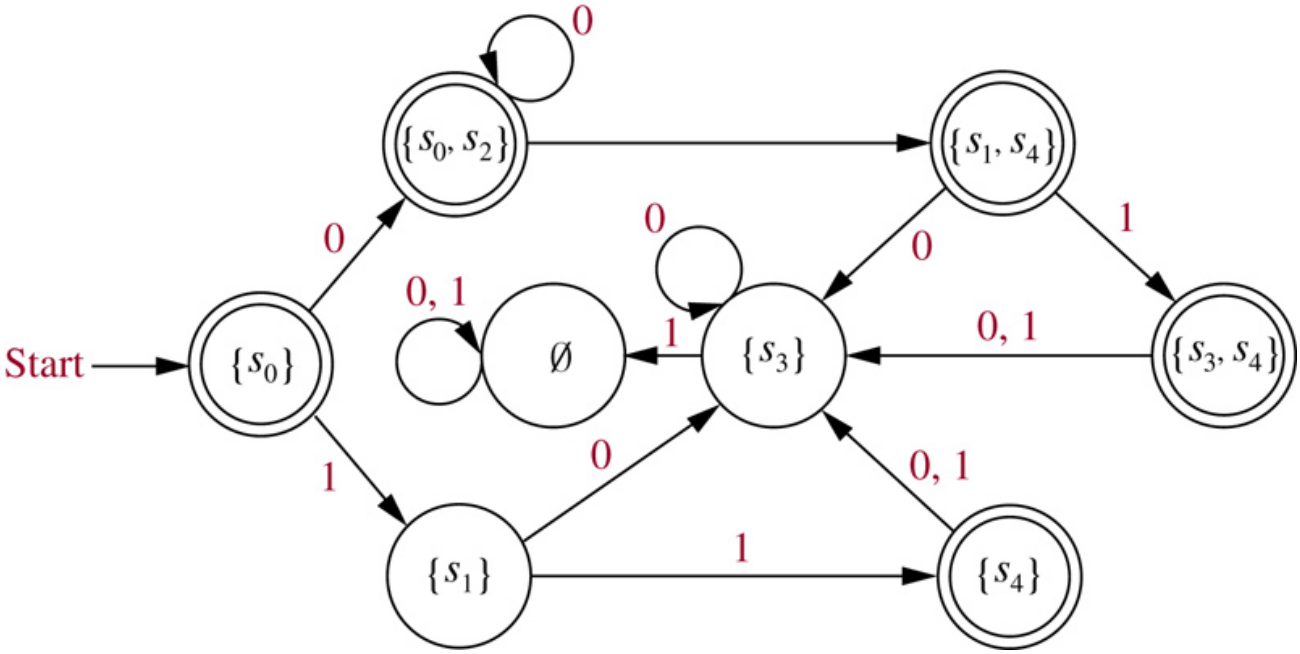



# Chapter 11: Boolean Algebra

*Boolean Expressions for the 16 Functions of Two Variables*

| Boolean Functions | Operator Symbol | Name | Comments |
|---|---|---|---|
| $F_0 = 0$ | | Null | Binary constant 0 |
| $F_1 = xy$ | $x \cdot y$ | AND | $x$ and $y$ |
| $F_2 = xy'$ | $x/y$ | Inhibition | $x$, but not $y$ |
| $F_3 = x$ | | Transfer | $x$ |
| $F_4 = x'y$ | $y/x$ | Inhibition | $y$, but not $x$ |
| $F_5 = y$ | | Transfer | $y$ |
| $F_6 = xy' + x'y$ | $x \oplus y$ | Exclusive-OR | $x$ or $y$, but not both |
| $F_7 = x + y$ | $x + y$ | OR | $x$ or $y$ |
| $F_8 = (x + y)'$ | $x \downarrow y$ | NOR | Not-OR |
| $F_9 = xy + x'y'$ | $(x \oplus y)'$ | Equivalence | x equals $y$ |
| $F_{10} = y'$ | $y'$ | Complement | Not $y$ |
| $F_{11} = x + y'$ | $x \subset y$ | Implication | If $y$, then $x$ |
| $F_{12} = x'$ | $x'$ | Complement | Not $x$ |
| $F_{13} = x' + y$ | $x \supset y$ | Implication | If $x$, then $y$ |
| $F_{14} = (xy)'$ | $x \uparrow y$ | NAND | Not-AND |
| $F_{15} = 1$ | | Identity | Binary constant 1 |



**Chapter 1: Logic and Proofs, Chapter 2: Sets**

**Chapter 6: Probability**

# Mathematical Computing and Sage

# Contents

# Chapter 1

# The Foundations: Logic and Proofs

- Rules of Logic $\Longrightarrow$ meaning of mathematics and proofs $\Longrightarrow$ building computing areas and computer science in particular.
- Logic (this chapter) and Boolean Algebra (Ch. 11) are the foundations of hardware design. George Boole (1815-1864) "The laws of Thought".
- Logic rectifies, even, reasoning in real life.

## 1.1 Propositional Logic

### 1.1.1 Propositions

**Definition 1 (Proposition)** *A proposition is a declarative sentence (declaring a fact) that is either a true of false, but not both.* ■

Q.E.D. is an initialism of the Latin phrase “quod erat demonstrandum”, meaning "which is what had to be proven"

**Example 2 (propositions)** .

1. *“Cairo is the capital of Egypt.”*
2. *“*$5+3=8$*.”* ■

**Example 3 (not propositions)** .

1. *“What time is it?”*
2. *“*$x+1=2$*.”* ■

We can denote a proposition by a variable for future reference:
$p$ : “Cairo is the capital of Egypt.”

**Compound Propositions using connectives:** discussed by the English mathematician George Boole; let’s see.

**Definition 4 (NOT)** *Let $p$ be a proposition. the negation of $p$, denoted by $\neg p$, $p'$, or $\overline{p}$, and read "not $p$"is the statement: "It is not the case that $p$"*
*The truth value of $\neg p$ is the opposite of the truth value of $p$.*



**TABLE 1 The Truth Table for the Negation of a Proposition.**

| $p$ | $\neg p$ |
|---|---|
| T | F |
| F | T |

■

**Example 5** *Find the negation of the proposition "Today is Friday".*
***Solution:***
$p$ : *"Today is Friday".*
$\neg p$ : *"It is not the case that today is Friday".*
$\overline{p}$ : *"Today is not Friday".* ■

Of course, we could denote $\neg p$ by $q$; i.e., $q = \neg p$.

**Definition 6 (AND)** *Let $p$ and $q$ be propositions. The conjunction of $p$ and $q$, denoted by $p \wedge q$, is the proposition "$p$ and $q$". The conjunction $p \wedge q$ is true when both $p$ and $q$ are true and false otherwise.*



**TABLE 2 The Truth Table for the Conjunction of Two Propositions.**

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

■

**Example 7** *Find the conjunction of the propositions $p$: "Today is Friday" and $q$: "It is raining today".*
***Solution:***
*$p \wedge q$: "Today is Friday and it is raining today".* ■

**Hint:** In language (not mathematics), we may use the word "but" to mean "and". "Today is Friday but it is raining".

**Definition 8 (OR)** *Let $p$ and $q$ be propositions. The disjunction of $p$ and $q$, denoted by $p \vee q$, is the proposition "$p$ or $q$". The disjunction $p \vee q$ is false when both $p$ and $q$ are false and true otherwise.*



**TABLE 3 The Truth Table for the Disjunction of Two Propositions.**

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

■

**Example 9** *What is the disjunction of the two propositions $p$ : "Students who have taken Introduction to CS can enroll in this course", $q$ : "Students who have taken Calculus can enroll in this course".*

*$p \vee q$: "Students who have taken Introduction to CS or Students who have taken Calculus can enroll in this course"* ■

**Hint:** In language (not mathematics), we may use the word "or" to mean exclusive or not inclusive. E.g., in a restaurant menu: "Soup or salad comes with an entrée". In mathematics, we define this exclusiveness next.

Can you imagine that the computer processor is built and any software action you do is translated to ONLY those three mathematical function NOT, OR, AND!!!
Study "Digital Design" and "Computer Organization" to see.

**Definition 10 (XOR)** *Let $p$ and $q$ be propositions. The exlusive or of $p$ and $q$, denoted by $p \oplus q$, read as "p X-OR q", is the proposition that is true when exactly only one of $p$ and $q$ is true and false otherwise.*



**TABLE 4 The Truth Table for the Exclusive Or of Two Propositions.**

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| T | T | F |
| T | F | T |
| F | T | T |
| F | F | F |

■

### 1.1.2 Conditional Statements (talks about existence not absence of hypothesis!!)

**Definition 11 (Conditional Statement)** *Let $p$ and $q$ be propositions.*
*The conditional statement $p \to q$ is the proposition "if $p$, then $q$".*
*Also, $p$ is called the hypothesis (or antecedent or premise) and $q$ is called the conclusion (or consequence). The conditional statement $p \to q$ is false when $p$ is true and $q$ is false, and true otherwise.*

| ***Sufficiency*** | ***Necessity*** |
|---|---|
| *"if $p$ then $q$"* | *"$p$ only if $q$"* |
| *"$p$ is sufficient for $q$"* | *"$q$ is necessary for $p$"* |
| *"a sufficient condition for $q$ is $p$"* | *"a necessary condition for $p$ is $q$"* |
| *"if $p$, $q$"* | |
| *"$q$ if $p$"* | |
| *"$q$ when $p$"* | |
| *"$q$ whenever $p$"* | |
| *"$p$ implies $q$"* | |
| *"$q$ follows from $p$"* | |



**TABLE 5** The Truth Table for the Conditional Statement $p \to q$.

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

***Another subtle way:***
*"$q$ unless $\neg p$" (if you exclude the case that $\neg p$, then $q$ is true)* ■

**Example 12** .
*$p$: "you submit the homework", $q$: "you will get an A".*
*If "you submit the homework", then "you will get an A".*
*"you will get an A" ($q$) unless "you does not submit the homework" ($\neg p$).* ■

**Conditional Statements in Logic compared to human languages**

- more general
- the truth value is stemmed from our definition not from semantics.
- the truth value is independent of a cause-and-effect relationship between hypothesis and conclusion.

**Example 13** .
*"If today is Friday, then 2+3=5" (always true)*
*"If today is Friday, then 2+3=6" (False only when today is Friday!!)* ■

**Conditional Statement in Logic compared to programming**

- it is result is either true or false not execution

**Example 14** *What is the value of the variable y after the statement:*

```
if (2+2==4) then y:=3;
```

■

### 1.1.2.1 contrapositive, Converse, and Inverse

- The contrapositive of $p \rightarrow q$ is defined as $\neg q \rightarrow \neg p$ and takes the same truth value of the original statement.
- It is obvious, since $\neg q \rightarrow \neg p$ is false only when $\neg q = T$ and $\neg p = F$ (when $p = T$ and $q = F$ the same as the implication)
- We say both are equivalent (more to come later).
- The converse is: $q \rightarrow p$.
- The inverse is: $\neg p \rightarrow \neg q$.
- Of course both converse and inverse are equivalent because they are the contrapositive of each other.
- Neither is the same as the original implication. E.g., when $p = T,\ q = F$, the conditional statement is false; however, both converse and inverse are true.



**TABLE 5** The Truth Table for the Conditional Statement $p \rightarrow q$.

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

**Example 15** *The conditional statement: "The home team wins whenever it is raining" q: "The home team wins"; p: "it is raining" (q whenever p or if p then q)*

***contrapositive:*** $\neg q \rightarrow \neg p$ *"if the home team does not win then it is not raining".*
***converse:*** $q \rightarrow p$ *"if the home team wins then it is raining".*
***inverse:*** $\neg p \rightarrow \neg q$ *"if it is not raining, then the home team does not win"* ■

### 1.1.2.2 Biconditionals

**Definition 16 (BICONDITIONALS)** *Let $p$ and $q$ be propositions. the biconditional statement $p \leftrightarrow q$ is the propositions "$p$ if and only if". It is true when $p$ and $q$ have the same truth value and is false otherwise. It is also called bi-implications.*

| $p$ | $q$ | $p \to q$ | $q \to p$ | $(p \to q) \wedge (q \to p)$ |
|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $T$ | $F$ |
| $F$ | $T$ | $T$ | $F$ | $F$ |
| $F$ | $F$ | $T$ | $T$ | $T$ |



**TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.**

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

■

- $p \leftrightarrow q$ is true when both $p \to q$ and $q \to p$ are true.
- therefore, $p \leftrightarrow q = (q \to p) \wedge (p \to q)$ ($p$ if $q$ and $p$ only if $q$; i.e., $p$ if and only if $q$)
- sometimes written for simplicity, $p$ iff $q$.
- "$p$ is necessary and sufficient for $q$".
- "if $p$ then $q$ and conversely".

**Example 17** *"You can take the flight if and only if you buy a ticket". The following two cases are false: taking a flight without ticket / buying a ticket and not taking a flight.*

**Biconditionals and natural languages**:

- the wording “if and only if” is not used in natural languages.
- Biconditional in natural languages is implicit not explicit; so be cautious. e.g., disciplining your kid by saying “if you finish your meal you can have a candy”. You actually mean “iff”.

### 1.1.3 Truth Tables of Compound Propositions

**Example 18** *Construct the truth table of the compound statement:* $(p \vee \neg q) \longrightarrow (p \wedge q)$*:*



**TABLE 7** The Truth Table of $(p \vee \neg q) \rightarrow (p \wedge q)$.

| $p$ | $q$ | $\neg q$ | $p \vee \neg q$ | $p \wedge q$ | $(p \vee \neg q) \rightarrow (p \wedge q)$ |
|---|---|---|---|---|---|
| T | T | F | T | T | T |
| T | F | T | T | F | F |
| F | T | F | F | F | T |
| F | F | T | T | F | F |

■

### 1.1.4 Precedence of Logical Operators



**TABLE 8**
**Precedence of Logical Operators.**

| *Operator* | *Precedence* |
|---|---|
| $\neg$ | 1 |
| $\wedge$ | 2 |
| $\vee$ | 3 |
| $\rightarrow$ | 4 |
| $\leftrightarrow$ | 5 |

- Last example: $(p \vee \neg q) \longrightarrow (p \wedge q)$
- Remember that negation could be denoted by $p'$ or $\overline{p}$.

### 1.1.5 Translating English Sentences

- English, or any human language, is ambiguous.
- Translation to logical expression removes this ambiguity.
- We can manipulate and analyze text this way using rules of inference (Section 1.5).
- In translation, keep into mind the implicit usage of some connectives!!, e.g., "or" sometimes means "XOR", etc.

**Example 19** *Translate to logical expression:*
*"You can access the internet from campus only if you are a computer science major or you are not a freshman"*

$a$: *"You can access the internet from campus".*
$c$: *"You are a computer science major".*
$f$: *"You are a freshman".*
$a \rightarrow (c \vee \neg f)$



**TABLE 5** The Truth Table for the Conditional Statement $p \rightarrow q$.

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

**Example 20** *Translate to logical expression:*
*"You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old"*

$q$: *"You can ride the roller coaster".*
$r$: *"You are under 4 feet tall".*
$s$: *"You are older than 16 years old".*
*The solution should be:* $C \rightarrow \neg q$, *but what is* $C$*?*

| $r$ | $s$ | $C$ |
|---|---|---|
| $T$ | $T$ | $F$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ |

$C = r \wedge \neg s$

### 1.1.6 System Specifications

- Very important to translate system requirements to formal specifications to avoid ambiguity.
- This is done by design engineers, e.g., software engineers, and others.

**Example 21** *Using logical connectives express the following specifications:*
*"The automated reply cannot be sent when the file system is full"*

$p$: *"The automated reply can be sent".*
$q$: *"The file system is full".*
$q \rightarrow \neg p$

**Example 22** *Determine whether these system specifications are consistent:*
*"The diagnosis message is stored in the buffer or it is retransmitted"*
*"The diagnostic message is not stored in the buffer"*
*"If the diagnostic message is stored in the buffer, then it is retransmitted".*

$p$: *"The diagnostic message is stored in the buffer".*
$q$: *"The diagnostic message is retransmitted".*
$C = (p \vee q) \wedge (\neg p)(p \rightarrow q)$

| $p$ | $q$ | $(p \vee q)$ | $(\neg p)$ | $(p \rightarrow q)$ | $C$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $F$ | $T$ | $F$ |
| $T$ | $F$ | $T$ | $F$ | $F$ | $F$ |
| $F$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $F$ | $T$ | $T$ | $F$ |

### 1.1.7 Boolean Searches

- Search engines use logical connectives; you have to know them.
- AND is almost a default.

**Example 23** *Search for universities in Cairo or Alexandria.*

*(Cairo OR Alexandria) AND Universities*

### 1.1.8 Logic Puzzles

### 1.1.9 Logic and Bit Operations

- **bit** stands for **bi**nary digi**t** (after great statistician John Tukey)
- At the hardware level, it is just a wire with either a high voltage or zero voltage (hence the T and F analogy).
- a Boolean Variable, is either true or false (1 or 0).
- Please, check the introductory lecture of the "Digital Design" course to see the link.



**TABLE 9** Table for the Bit Operators *OR*, *AND*, and *XOR*.

| $x$ | $y$ | $x \vee y$ | $x \wedge y$ | $x \oplus y$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

## 1.2 Propositional Equivalences

**Definition 24 (Tautology, Contradiction, and Contingency)** *: A compound proposition that is always true is called tautology, and that one that is always false is called contradiction. A compound statement that is neither a tautology nor a contradiction is called contingency.* ■

**Example 25** *:*



**TABLE 1** Examples of a Tautology and a Contradiction.

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

■

**Definition 26 (Equivalence)** *: The compound propositions $p$ and $q$ are called logically equivalent if $p \leftrightarrow q$ is a tautology. We also denote $p \leftrightarrow q$ by $p \equiv q$ (**they produce same truth table**).*

**Example 27 (Ex. 2)** *Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are equivalent.*





**TABLE 3** Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$.

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

**TABLE 2** De Morgan's Laws.

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

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

■

**Example 28 (Ex. 3)** *Show that* $p \to q$ *and* $\neg p \vee q$ *are equivalent.*



**TABLE 4** Truth Tables for $p \neg q \vee$ and $p \to q$.

| $p$ | $q$ | $\neg p$ | $\neg p \vee q$ | $p \to q$ |
|---|---|---|---|---|
| T | T | F | T | T |
| T | F | F | F | F |
| F | T | T | T | T |
| F | F | T | T | T |

**Example 29 (Distributive Law, Ex. 4)** *: Show that* $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
*Number of rows* $= 2^3$



**TABLE 5** A Demonstration That $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ Are Logically Equivalent.

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

**TABLE 6 Logical Equivalences.**

| *Equivalence* | *Name* |
|---|---|
| $p \wedge \mathbf{T} = p$<br>$p \vee \mathbf{F} = p$ | Identity laws |
| $p \vee \mathbf{T} = \mathbf{T}$<br>$p \wedge \mathbf{F} = \mathbf{F}$ | Domination laws |
| $p \vee p \equiv p$<br>$p \wedge p \equiv p$ | Idempotent laws |
| $\neg(\neg p) \equiv p$ | Double negation law |
| $p \vee q \equiv q \vee p$<br>$p \wedge q = q \wedge p$ | Commutative laws |
| $(p \vee q) \vee r = p \vee (q \vee r)$<br>$(p \wedge q) \wedge r = p \wedge (q \wedge r)$ | Associative laws |
| $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$<br>$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | Distributive laws |
| $\neg(p \wedge q) \equiv \neg p \vee \neg q$<br>$\neg(p \vee q) \equiv \neg p \wedge \neg q$ | De Morgan's laws |
| $p \vee (p \wedge q) \equiv p$<br>$p \wedge (p \vee q) = p$ | Absorption laws |
| $p \vee \neg p = \mathbf{T}$<br>$p \wedge \neg p = \mathbf{F}$ | Negation laws |

- The associative law of disjunction allows us to define $p \vee q \vee r \vee \cdots$
- Similarly for conjunction, $p \wedge q \wedge r \wedge \cdots$
- Moreover, for De Morgan's laws:
- $\neg(p_1 \vee p_2 \vee \cdots p_n) \equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \neg p_n)$.
- $\neg(p_1 \wedge p_2 \wedge \cdots p_n) \equiv (\neg p_1 \vee \neg p_2 \vee \cdots \neg p_n)$.
- The proof is clear for three variables, but for $n$ variables will be proven by induction.

**Other equivalence statements:**



**TABLE 7 Logical Equivalences Involving Conditional Statements.**

$$p \to q \equiv \neg p \vee q$$

$$p \to q \equiv \neg q \to \neg p$$

$$p \vee q \equiv \neg p \to q$$

$$p \wedge q \equiv \neg (p \to \neg q)$$

$$\neg(p \to q) \equiv p \wedge \neg q$$

$$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$$

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

$$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$$

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



**TABLE 8 Logical Equivalences Involving Biconditionals.**

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

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

$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

**Example 30 (Ex. 5)** *Use De Morgan's laws to express the negation of:*
*"Ahmed has a cellphone and he has a laptop computer".*

$p$ : *"Ahmed has a cellphone".*
$q$ : *"Ahmed has a laptop computer"*
$\neg(p \wedge q) \equiv \neg p \vee \neg q$: *"Ahmed does not have a cellphone or he does not have a laptop computer".*

**Example 31 (Ex. 6)** *Prove that* $\neg(p \to q) \equiv (p \wedge \neg q)$.

- *Prove it by truth table (HW).*

  ***Proof (algebraically).***

$$\begin{aligned} \neg(p \to q) &\equiv \neg(\neg p \vee q) && \text{(by last example)} \\ &\equiv \neg(\neg p) \wedge \neg(q) && \text{(De Morgan)} \\ &\equiv p \wedge \neg q \end{aligned}$$

■

- *By computer SW (Sage):*

```
sage: f1 = propcalc.formula("~(p -> q)")
sage: f2 = propcalc.formula("~(~p | q)")
sage: f1==f2
True
sage: f1.truthtable()
p       q       value
False   False   False
False   True    False
True    False   True
True    True    False

sage: f2.truthtable()
p       q       value
False   False   False
False   True    False
True    False   True
True    True    False
```

**Remarks:**

- truth table size = $2^n$.
- SW is essential for large $n$.
- For very large $n$, it is impossible even for computers! For $n = 1000$ it may take trillions of years !!!
  $2^{1000} =$
  10715086071862673209484250490600018105614048117055336074437503883703510511249361224
  93198378815695858127594672917553146825187145285692314043598457757469857480393456777
  48242309854210746050623711418779541821530464749835819412673987675591655439460770629
  14571196477686542167660429831652624386837205668069376.
- Even 10 GHZ processor will not do it: $\frac{2^{1000}\times 10^{-10}}{60*60*24*365} \approx 10^{290}$ year!!!

**Example 32 (Ex. 8)** *Show that $p \wedge q \rightarrow (p \vee q)$ is a tautology.*

$$\begin{aligned} p \wedge q \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) && \text{(previous example)} \\ &\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{(De Morgan)} \\ &\equiv \neg p \vee p \vee \neg q \vee q \\ &\equiv True \vee True = True \end{aligned}$$

■

## 1.3 Predicates and Quantifiers

### 1.3.1 Introduction

We need to extend the power of propositional logic to accommodate for more general treatment; hence **Predicate Logic**.

**Example 33** *"Every computer connected to the university network is functioning properly"*
*Is the following true for the computer named MATH3:*
*"MATH3 is functioning properly"*

### 1.3.2 Predicates:

**Definition 34** *A predicate is a statement involving variable. The predicate $P(x)$ takes a propositional value (True or False) after assigning a value to $x$.*

**Example 35 (Ex. 1)** *Let $P(x)$ denotes the statement "$x > 3$". Therefore:*
*$P(4)$: "4>3", which is True*
*$P(2)$: "2>3", which is False*

**Example 36 (Ex. 2)** *Let $A(x)$: "Computer x is under attack by an intruder". Suppose that only CS2 and MATH1 are currently under attack by intruders. Therefore:*

*$A(CS1)$: "Computer CS1 is under attack by an intruder" is False*
*$A(CS2)$: is True*
*$A(MATH1)$ is True.*

**Example 37 (Ex. 3)** *Let $Q(x, y)$ denotes the statement "x=y+3". Therefore,*
*$Q(1,2)$ is False*
*$Q(3,0)$ is True*

**Example 38 (Ex. 6)** *In programming, all conditions are predicates:*

```
if (x > 0)
y = 3; //C-language code.
```

**Extension:** A predicate of the form $P(x_1, x_2, \cdots, x_n)$ is an $n$-ary predicate.

### 1.3.3 Quantifiers: (the whole field is called "Predicate Calculus")

- to scope a predicate over a range of values, "domain" or "universe of discourse", of the variable.
- "universal quantification" defines a domain of all possible values.
- "existential quantification" defines the existence of one or more values.

**Definition 39 (Universal Quantification, Def. 1)** .

- *The universal quantification of $P(x)$ is the statement: "$P(x)$ for all values of $x$ in the domain".*
- *It is denoted by "$\forall x\ P(x)$", and read as "for all $x$ $P(x)$".*
- *An element for which $P(x)$ is false is called a counterexample of "$\forall x\ P(x)$".*

**Example 40 (Ex. 8–10)** .

- *$P(x)$: "$x+1>x$" and the domain is all real numbers. Then the statement "$\forall x\ P(x)$" is true.*
- *$Q(x)$: "$x<2$" and the domain is all real numbers. Then "$\forall x\ Q(x)$" is false by a counterexample $x=3$.*
- *$P(x)$: "$x^2>0$" and the domain is all integers. "$\forall x\ P(x)$" is false by counterexample $x=0$.*
- *$P(x)$: "$x^2>0$" and the domain is all positive integers. "$\forall x\ P(x)$" is true.*

**Remark 1** *When all elements in a domain can be listed, i.e., $x_1, x_2, \cdots, x_n$, we can say*

$$\forall x\ P(x) \equiv P(x_1) \wedge P(x_2) \wedge \cdots P(x_n)$$

**Example 41 (Ex. 13)** *What is the truth value of* $\forall x\,(x^2 \geq x)$ *for the real numbers domain and integers domain?*

$$\begin{aligned} x^2 &\geq x \\ x^2 - x &\geq 0 \qquad \text{(if and only if)} \\ x(x-1) &\geq 0 \\ (x \leq 0) \ &\textit{or}\ (x \geq 1) \end{aligned}$$

*Then the statement is false for real numbers and true for integers.* ■

**Definition 42 (Existential Quantification, Def. 2)** .

- *The existential quantification of $P(x)$ is the statement:*
  *" There exists an element $x$ in the domain such that $P(x)$".*
- *It is denoted by "$\exists x\ P(x)$", and read as "there exists $x$ such that $P(x)$".*
- *Other readings "for at least one", "there is", "for some", etc.*

**Example 43 (Ex. 14, 15, 16)** .

- *$P(x)$: "$x>3$", and the domain is real numbers. Then, the statement "$\exists x\ P(x)$" is true.*
- *$Q(x)$: "$x = x+1$", and the domain is real numbers. Then, the statement "$\exists x\ Q(x)$" is false.*
- *$R(x)$: "$x^2 > 10$", and the domain is positive integers not exceeding 4. Then, "$\exists x\ R(x)$" is true.*

**Remark 2** *When all elements in a domain can be listed, i.e., $x_1, x_2, \cdots, x_n$, we can say*

$$\exists x\ P(x) \equiv P(x_1) \vee P(x_2) \vee \cdots P(x_n)$$



**TABLE 1 Quantifiers.**

| *Statement* | *When True?* | *When False?* |
|---|---|---|
| $\forall x\, P(x)$ | $P(x)$ is true for every $x$. | There is an $x$ for which $P(x)$ is false. |
| $\exists x\, P(x)$ | There is an $x$ for which $P(x)$ is true. | $P(x)$ is false for every $x$. |

### 1.3.4 Other Quantifiers

- We can define unlimited number of quantifiers
- E.g., "There exists two $x$ such that ...", or "there exists 100 values ...", etc.
- However, $\forall$ and $\exists$, along with propositional logic can suffice.
- Ex. "there exists a unique $x$ such that $P(x)$" can be expressed as:
  - $\exists! x\, P(x)$ or $\exists_1 x\, P(x)$.
  - $\exists x\, P(x)$ and for any $x_1$ and $x_2$ if both $P(x_1)$ and $P(x_2)$ are true then $x_1 = x_2$. (Prob. 52, Sec. 1.4)

### 1.3.5 Quantifiers with Restricted Domains

**Example 44 (Ex. 17)** *What does this mean (where the domain is $\mathcal{R}$):*

- $\forall x < 0\ (x^2 > 0)$.
- $\forall y \neq 0\ (y^3 \neq 0)$.
- $\exists z > 0\ (z^2 = 2)$.

**Remark 3 (Very Important (details are in Sec. 1.3.8))** *:*

$$\forall x < 0\ P(x) \equiv \forall x \left((x < 0) \rightarrow P(x)\right) \qquad \not\equiv \forall x \left((x < 0) \wedge P(x)\right) \texttt{ contracdiction.}$$
$$\exists x < 0\ P(x) \equiv \exists x \left((x < 0) \wedge P(x)\right) \qquad \not\equiv \exists x \left((x < 0) \rightarrow P(x)\right) \texttt{ tautology.}$$

### 1.3.6 Precedence of Quantifiers

All quantifiers have higher precedence than logical operators:

$$\forall x\ P(x) \vee Q(x) \equiv \big(\forall x\ P(x)\big) \vee Q(x) \quad \text{(def.)}$$
$$\not\equiv \forall x\ \big(P(x) \vee Q(x)\big) \quad \text{(def.)}$$

### 1.3.7 Binding Variables

**Example 45 (Ex. 18)** *In the statement* $\exists x\ (x + y = 1)$, *we say*

- $x$ *is bound by the quantifier* $\exists$.
- $y$ *is free*
- $x + y = 1$ *is the scope of the quantifier* $\exists$.

*However, for the statement* $\exists x\ \big(P(x) \wedge Q(x)\big) \vee \forall x\ R(x)$,

- *all variables are bound*
- *the scope of the quantifier* $\exists$ *is* $(P(x) \wedge Q(x))$.
- *the scope of the quantifier* $\forall$ *is* $R(x)$.
- *of course, no need for re-using another variable; e.g.,* $\exists x\ (P(x) \wedge Q(x)) \vee \forall y\ R(y)$

■

### 1.3.8 Logical Equivalence Involving Quantifiers

**Definition 46 (Def. 3)** *Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional function.*
***We denote this by*** $S \equiv T$ ***or*** $S \leftrightarrow T$ ***or sometimes*** $S = T$.

**HW: Prove all the following:**

$$\forall x \left(P(x) \wedge Q(x)\right) \equiv \forall x\, P(x) \wedge \forall x\, Q(x) \qquad \text{(Sec. 1.3 Ex. 19)}$$
$$\exists x \left(P(x) \vee Q(x)\right) \equiv \exists x\, P(x) \vee \exists x\, Q(x) \qquad \text{(Sec. 1.3 prob. 45)}$$
$$\forall x \left(P(x) \leftrightarrow Q(x)\right) \not\equiv \forall x\, P(x) \leftrightarrow \forall x\, Q(x) \qquad \text{(Sec. 1.3 prob. 44)}$$
$$\forall x \left(P(x) \vee Q(x)\right) \not\equiv \forall x\, P(x) \vee \forall x\, Q(x) \qquad \text{(Sec. 1.3 prob. 50)}$$
$$\exists x \left(P(x) \wedge Q(x)\right) \not\equiv \exists x\, P(x) \wedge \exists x\, Q(x) \qquad \text{(Sec. 1.3 prob. 51)}$$
$$\forall x \left(P(x) \rightarrow Q(x)\right) \not\equiv \forall x\, P(x) \rightarrow \forall x\, Q(x) \qquad \text{(Sec. 1.3 prob. 43)}$$

And for any subset $\mathcal{S}$ of the domain

$$\forall x \in \mathcal{S}\ P(x) \equiv \forall x \left((x \in \mathcal{S}) \rightarrow P(x)\right) \qquad \not\equiv \forall x \left((x \in \mathcal{S}) \wedge P(x)\right)$$
$$\exists x \in \mathcal{S}\ P(x) \equiv \exists x \left((x \in \mathcal{S}) \wedge P(x)\right) \qquad \not\equiv \exists x \left((x \in \mathcal{S}) \rightarrow P(x)\right).$$

**Proof of Ex. 19:** $\forall x \left(P(x) \wedge Q(x)\right) \equiv \forall x\, P(x) \wedge \forall x\, Q(x)$**.**
**Sufficiency:** suppose that $\forall x \left(P(x) \wedge Q(x)\right)$ is true. Then, for arbitrary $a$, $P(a) \wedge Q(a)$ is true; then $P(a) = Q(a) = true$ (for arbitrary $a$). Therefore, $\forall x\, P(x) \wedge \forall x\, Q(x)$.
**Necessity:** suppose that $\forall x\, P(x) \wedge \forall x\, Q(x)$ is true. Then, $\forall x\, P(x) = \forall x\, Q(x) = true$. Then, for $x = a$, $P(a) = Q(a) = true$, which means $P(a) \wedge Q(a) = true$. We can do that for any $a$. Therefore, $\forall x \left(P(x) \wedge Q(x)\right)$ is true. ■

**Proof of Prob. 51:** $\exists x \left(P(x) \wedge Q(x)\right) \not\equiv \exists x\, P(x) \wedge \exists x\, Q(x)$**.**
**Sufficiency:**

**Necessity:**

■

**Hint:** We could have proved directly by counterexample had we realized its meaning!

### 1.3.9 Negating Quantified Expressions (De Morgan's laws for quantifiers)

**Example 47** *Negate Q: "Every student in your class has taken a course in calculus".*
*$P(x)$: "Student $x$ in your class has taken a course in calculus".*
*$Q : \forall x\, P(x)$, where the domain is the students in your class.*
*$\neg Q$: "it is not the case that every student in your class has taken a course in calculus".*
*$\neg Q$: "there is a student in your class has not taken a course in calculus". $\neg Q : \exists x\, \neg P(x)$.*

**Proof of $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$.** :
**Sufficiency:** Suppose that $\neg \forall x\, P(x)$ is true. Then, $\forall x\, P(x)$ is false, which means (by definition) there is at least one $x$ such that $P(x)$ is false; i.e., $\exists x\, \neg P(x)$.
**Necessity:** Suppose that $\exists x\, \neg P(x)$ is true. This means that there is at least $x = a$ such that $\neg P(a)$ is true, i.e., $P(a)$ is false. Hence, $\forall x\, P(x)$ is false, which means $\neg \forall x\, P(x)$ is true. ■

**Proof of $\neg \exists x\, Q(x) \equiv \forall x\, \neg Q(x)$.** very similar.

■

**Connection to De Morgan**



**TABLE 2** De Morgan's Laws 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 $x$. |

$$
\begin{aligned}
\forall x\, P(x) &\equiv \big(P(x_1) \wedge P(x_2) \wedge \cdots P(x_n)\big) \\
\neg\forall x\, P(x) &\equiv \neg\big(P(x_1) \wedge P(x_2) \wedge \cdots P(x_n)\big) \\
&\equiv \big(\neg P(x_1) \vee \neg P(x_2) \vee \cdots \neg P(x_n)\big) \\
&\equiv \exists x\, \neg P(x) \\
\exists x\, P(x) &\equiv \big(P(x_1) \vee P(x_2) \vee \cdots P(x_n)\big) \\
\neg\exists x\, P(x) &\equiv \neg\big(P(x_1) \vee P(x_2) \vee \cdots P(x_n)\big) \\
&\equiv \big(\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \neg P(x_n)\big) \\
&\equiv \forall x\, \neg P(x)
\end{aligned}
$$

**Hint: Why we did not use this proof?**

**Example 48 (Ex. 20)** . *Q: "There is an honest politician"*
*$H(x)$: "x is honest"*
*$Q : \exists x\ H(x)$, where the domain of x is all politicians.*
*$\neg Q : \neg\exists x\ H(x) \equiv \forall x\ \neg H(x)$: "All politicians are not honest."* ■

**Example 49 (Ex. 21)** *Negate both $\forall x\ (x^2 > x)$ and $\exists x\ (x^2 = 2)$.*

$$\neg\forall x\ (x^2 > x) \equiv \exists x\ \neg(x^2 > x) \equiv \exists x\ (x^2 \leq x).$$
$$\neg\exists x\ (x^2 = 2) \equiv \forall x\ \neg(x^2 = 2) \equiv \forall x\ (x^2 \neq 2).$$

■

**Example 50 (Ex. 22)** *Show that $\neg\forall x\ \big(P(x) \to Q(x)\big) \equiv \exists x\ \big(P(x) \wedge \neg Q(x)\big)$.*

$$\begin{aligned}\neg\forall x\ \big(P(x) \to Q(x)\big) &\equiv \exists x\ \neg\big(P(x) \to Q(x)\big)\\ &\equiv \exists x\ \big(P(x) \wedge \neg Q(x)\big) \qquad \text{(Ex. 31)}\end{aligned}$$

■

### 1.3.10 Translating from English into Logical Expressions (elaboration)

**Very important in:** Logic programming, AI, SWE, language understanding, among others.

**Example 51 (Ex. 23)** *Express, in predicates and quantifiers:*
*$P$: "Every student in this class has studied calculus".*

***Domain is students in the class:***
*$C(x)$: "$x$ has studied calculus".*
$P: \forall x\, C(x)$.

***Domain is all people:***
*$C(x)$: "$x$ has studied calculus".*
*$S(x)$: "Person $x$ is in class".*
$P: \forall x\, (S(x) \rightarrow C(x))$.
$P: \forall x\, (S(x) \wedge C(x))$ ***(Wrong)***.

***other possible courses are involved:***
*$Q(x,y)$: "$x$ has studied $y$".*
$P: \forall x\, Q(x, calculus)$.
$P: \forall x\, (S(x) \rightarrow Q(x, calculus))$.

■

**Example 52 (Ex. 24)** *Express the following two statements using predicates and quantifiers:*
$P$ : *"Some student in this class has visited Mexico"*
$Q$ : *"Every student in this class has visited either Canada or Mexico".*

***Domain is students in the class:***
$M(x)$ : *"$x$ has visited Mexico".*
$C(x)$ : *"$x$ has visited Canada".*
$P$ : $\exists x\, M(x)$.
$Q$ : $\forall x\, (C(x) \vee M(x))$.

***Domain is all people:***
$S(x)$*: "Person $x$ is in class".*
$P : \exists x\, (S(x) \wedge M(x))$.
$P : \exists x\, (S(x) \rightarrow M(x))$. (***Wrong***)
$Q : \forall x\, (S(x) \rightarrow (C(x) \vee M(x)))$.

***Hint:*** *$M(x)$ and $C(x)$ can be replaced, respectively, by: $V(x, Mexico)$ and $V(x, Canada)$.* ■

### 1.3.11 Using Quantifiers in System Specifications (elaboration)

**Example 53 (Ex. 25)** *Express, using predicates and quantifiers: P : "Every mail message larger than one megaby*
*will be compressed".*
*Q : "If a user is active, at least one network link will be available".*

***Domain of*** $m$ ***is all message:***
$S(m,1)$ : *"Size of message* $m$ *is larger than 1 MB".*
$C(m)$ : *"message* $m$ *will be compressed".*
$P$ : $\forall m\,(S(m,1) \rightarrow C(m))$.

***Domain of*** $u$ ***is all users:***
$A(u)$ : *"User* $u$ *is active".*
$S(n)$ : *"State of link* $n$ *is available".*
$Q$ : $\exists u\ A(u) \rightarrow \exists n\ S(n)$.
***HW:*** *is it equivalent to* $\forall u\ \big(A(u) \rightarrow \exists n\ S(n)\big)$.
***In general:*** $\forall u\ \big(A(u) \rightarrow R\big) \stackrel{?}{\equiv} \exists u\ A(u) \rightarrow R$

### 1.3.12 Examples from Lewis Carroll (elaboration on languages and reasoning)

**Example 54 (Ex. 27)** *The whole argument consists of premises and conclusion:*
***Premises:***
*"All hummingbirds are richly colored".*
*"No large birds live on honey".*
*"Birds that do not live on honey are dull in color".*
***Is this conclusion sound?***
*"Hummingbirds are small"*

***Formalization in Logic (soundness is deferred); domain is all birds:***
$P(x)$ : *"x is hummingbirds".*
$Q(x)$ : *"x is large".*
$R(x)$ : *"x lives on honey".*
$S(x)$ : *"x is richly in color".*

$$\forall x\,(P(x) \to S(x)).$$
$$\neg\exists x\,\big(Q(x) \wedge R(x)\big).$$ ($\neg\exists x\,\big(Q(x) \to R(x)\big)$ **is wrong**)
$$\forall x\,(\neg R(x) \to \neg S(x)).$$ (assuming not richly is dull)
$$\forall x\,(P(x) \to \neg Q(x)).$$ (assuming not large is small)

***Hint:*** *Why cannot we conclude the soundness (truthiness) using truth table as in system specification?*

### 1.3.13 Logic Programming

- Designed to reason using rules of predicate logic (lot of fun).
- **PROLOG** (**PRO**gramming in **LOG**ic) is an example.
- To the best of my knowledge, there is no "yet" a package supporting Logic Programming under Sage (please, watch the appendix lecture for Sage).
- I hope rigorous students start writing such a package in a graduation project.

### 1.3.14 More Proofs and Rigor (refer to Sec. 1.3.8 and prob. 46–47)

**Both terms are predicates**

$$\forall x \left(P(x) \wedge Q(x)\right) \equiv \forall x\ P(x) \wedge \forall x\ Q(x)$$
$$\exists x \left(P(x) \vee Q(x)\right) \equiv \exists x\ P(x) \vee \exists x\ Q(x)$$
$$\forall x \left(P(x) \vee Q(x)\right) \not\equiv \forall x\ P(x) \vee \forall x\ Q(x)$$
$$\exists x \left(P(x) \wedge Q(x)\right) \not\equiv \exists x\ P(x) \wedge \exists x\ Q(x)$$
$$\forall x \left(P(x) \rightarrow Q(x)\right) \not\equiv \forall x\ P(x) \rightarrow \forall x\ Q(x)$$
$$\cdots$$
$$\exists x \left(P(x) \rightarrow Q(x)\right) \equiv \forall x\ P(x) \rightarrow \exists x\ Q(x)$$
$$\equiv True \text{ for content.}$$

**Proof 1 of** $\exists x\ \left(P(x) \vee Q(x)\right) \equiv \exists x\ P(x) \vee \exists x\ Q(x)$**.** :

**Sufficiency:**

**Necessity:**

■

**A predicate and a proposition (null quantification)**

Of course

Of course

$$\forall x \left(P(x) \vee R\right) \equiv \forall x\ P(x) \vee R$$
$$\exists x \left(P(x) \wedge R\right) \equiv \exists x\ P(x) \wedge R$$
$$\forall x \left(R \rightarrow Q(x)\right) \equiv R \rightarrow \forall x\ Q(x)$$
$$\forall x \left(P(x) \rightarrow R\right) \equiv \exists x\ P(x) \rightarrow R \qquad \text{(HW of Ex. 53)}$$
$$\exists x \left(R \rightarrow Q(x)\right) \equiv R \rightarrow \exists x\ Q(x)$$
$$\exists x \left(P(x) \rightarrow R\right) \equiv \forall x\ P(x) \rightarrow R.$$

**Proof 2 of** $\exists x \left(P(x) \vee Q(x)\right) \equiv \exists x\ P(x) \vee \exists x\ Q(x)$**.** :

$$\begin{aligned}
\exists x \left(P(x) \vee Q(x)\right) &\equiv \neg\neg \exists x \left(P(x) \vee Q(x)\right) \\
&\equiv \neg \forall x\ \neg\big(P(x) \vee Q(x)\big) \\
&\equiv \neg \forall x \left(\neg P(x) \wedge \neg Q(x)\right) \\
&\equiv \neg\big(\forall x\ \neg P(x) \wedge \forall x\ \neg Q(x)\big) \\
&\equiv \neg\big(\neg \exists x\ P(x) \wedge \neg \exists x\ Q(x)\big) \\
&\equiv \exists x\ P(x) \vee \exists x\ Q(x)
\end{aligned}$$

■

**Proof 1 of** $\exists x \left(P(x) \wedge R\right) \equiv \exists x\, P(x) \wedge R$**.**
**Sufficiency:** works, of course, as last time when we proved: $\exists x \left(P(x) \wedge Q(x)\right) \not\equiv \exists x\, P(x) \wedge \exists x\, Q(x)$

**Necessity:** works now because R.H.S has only one existing $x$

■

**Proof 2 of** $\exists x \left(P(x) \wedge R\right) \equiv \exists x\, P(x) \wedge R$**.** Set $R$ to True and False the proof is immediate. ■

**Proof of** $\exists x \left(P(x) \rightarrow R\right) \equiv \forall x\, P(x) \rightarrow R$**.**

$$\begin{aligned}
\exists x \left(P(x) \rightarrow R\right) &\equiv \exists x \left(\neg P(x) \vee R\right) \\
&\equiv \exists x\, \neg P(x) \vee \exists x\, R \\
&\equiv \neg \forall x\, P(x) \vee R \\
&\equiv \forall x\, P(x) \rightarrow R.
\end{aligned}$$

■

## 1.4 Nested Quantifiers

### 1.4.1 Introduction (why nested?)

**Example 55 (Ex. 1)** *: (for the domain $\mathcal{R}$.)*

$$\forall x \exists y\ (x+y=0) \equiv \forall x\ \big(\exists y\ (x+y=0)\big) \qquad \equiv \forall x\ Q(x). \qquad \text{(additive inverse)}$$

$$\forall x \forall y\ (x+y=y+x) \equiv \forall x\ \big(\forall y\ (x+y=y+x)\big) \qquad \equiv \forall x\ Q(x). \qquad \text{(commutative law)}$$

**Example 56** *:[Ex. 2] Translate to English, where the domain $\mathcal{R}$*

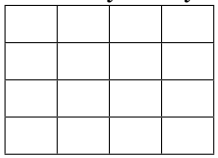
$$\forall x \forall y\ \big((x>0) \wedge (y<0) \rightarrow (xy<0)\big)$$

*"for every real number $x$ and for every real number $y$, if $x>0$ and $y<0$ then $xy<0$".*

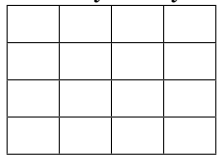
**Thinking of quantification as loops:**

```
for(x_1,..., x_n)
for(y_1,..., y_m )
print( ``the truth value is'' P(x, y));
```

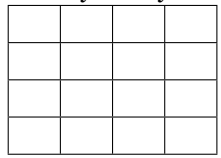
$\forall x \forall y\ P(x,y)$



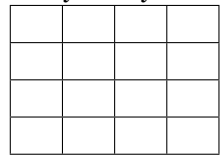
$\forall x \exists y\ P(x,y)$



$\exists x \forall y\ P(x,y)$



$\exists x \exists y\ P(x,y)$



Which is special case of which? If $P(x,y)$ : $x+y=0$, then which is true and which is false?

### 1.4.2 The Order of Quantifiers

$$\forall x \forall y\ P(x,y) \equiv \forall y \forall x\ P(x,y).$$
$$\exists x \exists y\ P(x,y) \equiv \exists y \exists x\ P(x,y).$$
$$\forall x \exists y\ P(x,y) \not\equiv \exists y \forall x\ P(x,y).$$

**Ex.:** $P(x,y):\ x+y=0.$

**Example 57 (Ex. 5)** *Let* $Q(x,y,z):\ x+y=z$*:*

$$\forall x \forall y \exists z\ Q(x,y,z) = True.$$
$$\exists z \forall x \forall y\ Q(x,y,z) = False.$$

### 1.4.3 Translating Mathematical Statements into Statements Involving nested Quantifiers

**Example 58 (Ex. 6)** *"the sum of two positive integers is always positive"*

$$\forall x > 0 \forall y > 0\ (x + y > 0) \equiv \forall x \forall y \left((x > 0) \wedge (y > 0) \rightarrow (x + y > 0)\right),$$

*where the domain is all integers.*

**Proof of multiple domain restriction.**

$$\forall x \in S\ P(x) \equiv \forall x \left((x \in S) \rightarrow P(x)\right) \equiv \forall x \left(\neg(x \in S) \vee P(x)\right).$$

$$\begin{aligned}
\forall x \in S_1 \forall y \in S_2 P(x, y) &\equiv \forall x \in S_1 \Big(\forall y \in S_2 P(x, y)\Big) \\
&\equiv \forall x \left(\neg(x \in (S_1)) \vee \forall y \in S_2\ P(x, y)\right) \\
&\equiv \forall x \left(\neg(x \in (S_1)) \vee \forall y \left(\neg(y \in S_2) \vee P(x, y)\right)\right) \\
&\equiv \forall x \forall y \left(\neg\big(x \in (S_1) \wedge (y \in S_2)\big) \vee P(x, y)\right) \\
&\equiv \forall x \forall y \left(\big((x \in (S_1) \wedge (y \in S_2)\big) \rightarrow P(x, y))\right).
\end{aligned}$$

■

**Example 59 (Ex. 7)** *"Every real number except zero has a multiplicative inverse"*

$$\forall x \neq 0\ \exists y\ (xy = 1) \equiv \forall x \left(x \neq 0 \rightarrow \exists y\ (xy = 1)\right)$$

### 1.4.4 Translating from nested Quantifiers into English

**Example 60 (Ex. 9)** *Translate the statement, (where the domain of both x and y are all students in school):*
$\forall x \left(C(x) \vee \exists y \left(C(y) \wedge F(x,y)\right)\right)$
$C(x)$ : *"x has a computer",*
$F(x,y)$ : *"x and y are friends",*

***inside:*** *Student x has a computer or there exists a student y who has a computer and is a friend to x.*

*For every student x in the school, x has a computer or there is a student y such that y has a computer and is a friend to x.*
***Said differently:*** *Every student in the school has a computer or is a friend to a student who has a computer.*

***NOT:*** *Every student in the school has a computer or for every student in the school there exists one of his friends who has a computer.* ■

**Example 61 (Ex. 10)** *Translate to English, (where the domain of x, y, z is all students in school):*
$\exists x \forall y \forall z \left((F(x,y) \wedge F(x,z) \wedge (y \neq z) \rightarrow \neg F(y,z))\right)$
$F(x,y)$ : *"x and y are friends".*

***inside:*** *if x and y are friends and x and z are friends and y is different from z then y and z are not friends.*

*There is a student x such that for all students y and all students z, other than y, if x and y are friends and x and z are friends then y and z are not friends.*
***Said differently:*** *there is a student none of whose friends are also friends with each other.* ■

### 1.4.5 Translating English Statements into Logical Expressions (elaboration)

**Example 62 (Ex. 11)** *Express "If a person is female and is a parent, then this person is someone's mother" using predicates and quantifiers, where domain is all people.*
$F(x)$ : *"$x$ is female".*
$P(x)$ : *"$x$ is parent".*
$M(x,y)$ : *$x$ is the mother of $y$.*

$$\forall x \left((F(x) \wedge P(x)) \rightarrow \exists y\, M(x,y)\right) \equiv \forall x \exists y \left((F(x) \wedge P(x)) \rightarrow M(x,y)\right).$$

**Example 63 (Prob. 52, and abstraction of Ex. 12)** *Express $\exists! x\, P(x)$ in terms of $\forall$ and $\exists$ (revisiting Sec. 1.3.4)*

$$\begin{aligned}
\exists! x\, P(x) &\equiv \exists x \left(P(x) \wedge \forall y \neq x\, \neg P(y)\right) \\
&\equiv \exists x \left(P(x) \wedge \forall y\, (y \neq x \rightarrow \neg P(y))\right) \\
&\equiv \exists x \left(P(x) \wedge \forall y (P(y) \rightarrow y = x)\right).
\end{aligned}$$

### 1.4.6 Negating Nested Quantifiers

**Example 64 (Ex. 14)** *Negate* $\forall x \exists y\ (xy = 1)$, *which of course is not true, so that no negation precedes a quantifier.*

$$\begin{aligned} \neg \forall x \exists y\ (xy = 1) &\equiv \exists x \neg \exists y\ (xy = 1) \\ &\equiv \exists x \forall y\ \neg (xy = 1) \\ &\equiv \exists x \forall y\ (xy \neq 1) \end{aligned}$$



**TABLE 1 Quantifications of Two Variables.**

| *Statement* | *When True?* | *When False?* |
|---|---|---|
| $\forall x \forall y P(x, y)$<br>$\forall y \forall x P(x, y)$ | $P(x, y)$ is true for every pair $x, y$. | There is a pair $x, y$ for which $P(x, y)$ is false. |
| $\forall x \exists y P(x, y)$ | 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. |
| $\exists x \exists y P(x, y)$<br>$\exists y \exists x P(x, y)$ | There is a pair $x, y$ for which $P(x, y)$ is true. | $P(x, y)$ is false for every pair $x, y$. |

### 1.4.7 Prenex Normal Form (PNF)

**Prove the following, of course, same domain for $x, y$**

$$\forall x \forall y (P(x) \wedge Q(y)) \equiv \forall x P(x) \wedge \forall x Q(x)$$
$$\forall x \forall y (P(x) \vee Q(y)) \equiv \forall x P(x) \vee \forall x Q(x) \quad \text{(prob. *48)}$$
$$\forall x \exists y (P(x) \wedge Q(y)) \equiv \forall x P(x) \wedge \exists x Q(x) \quad \text{(prob. *49-a)}$$
$$\forall x \exists y (P(x) \vee Q(y)) \equiv \forall x P(x) \vee \exists x Q(x) \quad \text{(prob. *49-b)}$$
$$\exists x \forall y (P(x) \wedge Q(y)) \equiv \exists x P(x) \wedge \forall x Q(x)$$
$$\exists x \forall y (P(x) \vee Q(y)) \equiv \exists x P(x) \vee \forall x Q(x)$$
$$\exists x \exists y (P(x) \wedge Q(y)) \equiv \exists x P(x) \wedge \exists x Q(x)$$
$$\exists x \exists y (P(x) \vee Q(y)) \equiv \exists x P(x) \vee \exists x Q(x)$$

**It is extremely tedious to write those 8 statements. Elegantly, rigorously, and more compactly, they can be written as:**

$$q_1 x q_2 y \left(P(x) \Diamond Q(y)\right) \equiv q_1 x\, P(x) \Diamond q_2 x\, Q(x),$$

where $q_i, i = 1,2$ is either $\exists$ or $\forall$ and $\Diamond$ is either $\vee$ or $\wedge$.

**Proof 1.** using sufficiency and necessity as book solutions ■

**Proof 2.** follows immediately from the null quantification statements in Sec. 1.3.14. ■

**Definition 65 (PNF, Prob. 49*)** *A statement is in prenex normal from (PNF) if it is of the form*

$$q_1 x_1 q_2 x_2 \cdots q_k x_k P(x_1, x_2, \cdots, x_k),$$

*where each* $q_i,\ i = 1, 2, \cdots, k$ *is either* $\exists$ *or* $\forall$*, and* $P(x_1, x_2, \cdots, x_n)$ *is a predicate involving no quantifier.*

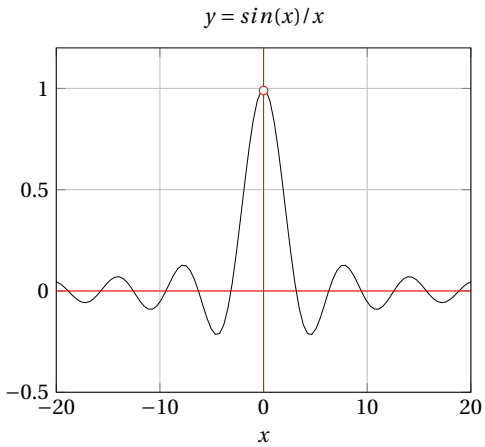
**Example 66 (Prob. 50(c))**

$$\begin{aligned} \exists x\ P(x) \to \exists x\ Q(x) &\equiv \left(\neg \exists x\ P(x)\right) \vee \left(\exists x\ Q(x)\right) \\ &\equiv \forall x\ \neg P(x) \vee \exists x\ Q(x) \\ &\equiv \forall x \exists y\ \left(\neg P(x) \vee Q(y)\right) \end{aligned}$$

**Lemma 67 (Prob. 51**)** *Every logical statement can be written in an equivalent PNF.*

**Proof.** Recall Prob. 45, Sec. 1.2, where: $\wedge$, $\vee$, and $\neg$ were proven to be complete. ■

### 1.4.8 For Mathematics Lovers: example from calculus*




**Example 69 (Ex. 8)** *Express the expression of limit using quantifiers:*
*We say that* $\lim_{x\to a} f(x) = L$ *if for every real number* $\epsilon > 0$ *there exists a real number* $\delta > 0$ *such that* $|f(x) - L| < \epsilon$ *whenever* $|x - a| < \delta$.

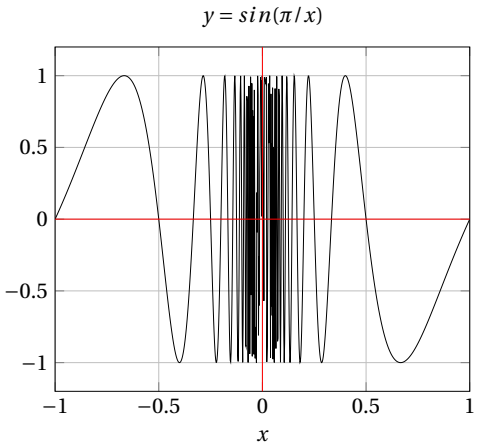
$$\forall \epsilon > 0\ \exists \delta > 0 \forall x\ \big((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\big),$$

*where the domain of* $\epsilon$, $\delta$, $x$ *is the real numbers.*

**Definition 68 (not rigorous)** *We say:*
*"the limit of* $f(x) = L$*, as* $x$ *approaches* $a$*,"*

$$\lim_{x\to a} f(x) = L,$$

*if we can make the values of* $f(x)$ *arbitrarily close to* $L$ *(as close to* $L$ *as we like) by taking* $x$ *to be sufficiently close to* $a$ *(on either side of* $a$*) but not equal to* $a$.




**Example 70 (Ex. 16)** $\lim_{x\to a} f(x)$ *does not exist means that:*

$$\forall L \lim_{x\to a} f(x) \neq L$$

$$\lim_{x\to a} f(x) = L \equiv \forall\epsilon > 0\ \exists\delta > 0 \forall x \left((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\right)$$

$$\begin{aligned}
\lim_{x\to a} f(x) \neq L &\equiv \neg\forall\epsilon > 0\ \exists\delta > 0 \forall x \left((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\right) \\
&\equiv \exists\epsilon > 0 \neg\exists\delta > 0 \forall x \left((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\right) \\
&\equiv \exists\epsilon > 0 \forall\delta > 0 \neg\forall x \left((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\right) \\
&\equiv \exists\epsilon > 0 \forall\delta > 0 \exists x \neg\left((|x-a| < \delta) \rightarrow (|f(x) - L| < \epsilon)\right) \\
&\equiv \exists\epsilon > 0 \forall\delta > 0 \exists x \neg\left(\neg(|x-a| < \delta) \vee (|f(x) - L| < \epsilon)\right) \\
&\equiv \exists\epsilon > 0 \forall\delta > 0 \exists x \left((|x-a| < \delta) \wedge (|f(x) - L| \geq \epsilon)\right)
\end{aligned}$$

*At last,* $\lim_{x\to a} f(x)$ *does not exist means*

$$\forall L \exists\epsilon > 0 \forall\delta > 0 \exists x \left((|x-a| < \delta) \wedge (|f(x) - L| \geq \epsilon)\right)$$

## 1.5 Rules of Inference

### 1.5.1 Introduction: towards building sound reasoning and proof

- Valid Arguments in Propositional Logic
- Rules of Inference for Propositional Logic
- Using Rules of Inference to Build Arguments
- Fallacies
- Rules of Inference for Quantified Statements
- Combining Rules of Inference for Propositions and Quantified Statements

### 1.5.2 Valid Arguments in Propositional Logic

**Definition 71 (Argument, Def. 1)** *:*

- *An* `argument` *in propositional logic is a sequence of propositions*
- *all but the final proposition in the argument are called* `premises` *the final is called the* `conclusion`*.*
- *an argument is* `valid` *if the truth of all its premises implies the truthiness of its conclusion.*
- *An* `argument form` *is a sequence of compound propositions involving propositional variables.*
- *An argument form is* `valid` *if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true;*
  ***i.e.,*** $(p_1 \wedge p_2 \wedge \cdots p_n) \rightarrow q$ ***is a tautology*** ■

**Example 72** *: **Argument:***
*"If you have a current password, then you can log onto the network"*

*"You have a current password"*

*Therefore,*
*"You can log onto the network"*

***Argument Form:***

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

$\big((p \rightarrow q) \wedge p\big) \rightarrow q$ *is a tautology.* ■

### 1.5.3 Rules of Inference for Propositional Logic

- For many variables, truth tables are very tedious.
- For predicates, no way of of writing truth of infinite values of variables.
- **Rules of Inference** are building blocks to derive more rules.
- **Modus Ponens** is the basis: $\big((p \to q) \wedge p\big) \to q$ is a tautology.

**Example 73 (Ex. 2)** *Valid argument with a false conclusion!!*
*"if* $\sqrt{2} > 3/2$*, then* $(\sqrt{2})^2 > (3/2)^2$*. Since we know that* $\sqrt{2} > (3/2)$*, consequently,* $(\sqrt{2})^2 = 2 > (3/2)^2 = (9/4)$*".*

## Basic rules of inference (prove as HW.)



**TABLE 1** Rules of Inference.

| *Rule of Inference* | *Tautology* | *Name* |
|---|---|---|
| $p$<br>$p \to q$<br>$\therefore q$ | $[p \wedge (p \to q)] \to q$ | Modus ponens |
| $\neg q$<br>$p \to q$<br>$\therefore \neg p$ | $[\neg q \wedge (p \to q)] \to \neg\ p$ | Modus tollens |
| $p \to q$<br>$q \to r$<br>$\therefore p \to r$ | $[(p \to q) \wedge (q \to r)] \to (p \to r)$ | Hypothetical syllogism |
| $p \vee q$<br>$\neg p$<br>$\therefore q$ | $[(p \vee q) \wedge \neg\ p] \to q$ | Disjunctive syllogism |
| $p$<br>$\therefore p \vee q$ | $p \to (p \vee q)$ | Addition |
| $p \wedge q$<br>$\therefore p$ | $(p \wedge q) \to p$ | Simplification |
| $p$<br>$q$<br>$\therefore p \wedge q$ | $[(p) \wedge (q)] \to (p \wedge q)$ | Conjunction |
| $p \vee q$<br>$\neg p \vee r$<br>$\therefore q \vee r$ | $[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$ | Resolution |

**Example 74 (Addition, Ex., 3)** *:*
*"It is below freezing now. Therefore, it is either below freezing or raining now."*

**Example 75 (Hypothetical syllogism, Ex. 5)** *:*
*"If it rains today, then we will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. therefore, if it rains today, then we will have a barbecue tomorrow."*

### 1.5.4 Using Rules of Inference to Build Arguments (recall Ex. 1.3.12)

**Example 76 (Ex. 6)** *: Show that the hypotheses "It is not sunny this afternoon and it is colder than yesterday", "We will go swimming only if it is sunny", "If we do not go swimming, then we will take a canoe trip", and "If we take a canoe trip, then we will be home by sunset" lead to the conclusion "We will be home by sunset".*

*"$p$: 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".*
***Premises (Hypotheses):*** $\neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t$.

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

```
sage: f = propcalc.formula("((~p & q) & (r -> p) & (~r -> s) & (s -> t)) -> t")

sage: f
((~p&q)&(r->p)&(~r->s)&(s->t))->t

sage: f.truthtable()
p       q       r       s       t       value
False   False   False   False   False   True
False   False   False   False   True    True
False   False   False   True    False   True
False   False   False   True    True    True
False   False   True    False   False   True
False   False   True    False   True    True
False   False   True    True    False   True
False   False   True    True    True    True
False   True    False   False   False   True
False   True    False   False   True    True
False   True    False   True    False   True
False   True    False   True    True    True
False   True    True    False   False   True
False   True    True    False   True    True
False   True    True    True    False   True
False   True    True    True    True    True
True    False   False   False   False   True
True    False   False   False   True    True
True    False   False   True    False   True
True    False   False   True    True    True
True    False   True    False   False   True
True    False   True    False   True    True
True    False   True    True    False   True
True    False   True    True    True    True
True    True    False   False   False   True
True    True    False   False   True    True
True    True    False   True    False   True
True    True    False   True    True    True
True    True    True    False   False   True
True    True    True    False   True    True
True    True    True    True    False   True
True    True    True    True    True    True
```

**Example 77 (Ex. 7)** : ***Premises:*** $p \to q$, $\neg p \to r$, $r \to s$,
***Conclusion:*** $\neg q \to s$.
***Key:*** $\neg q \to \neg p$.

```
sage: f = propcalc.formula("((p -> q) & (~p -> r) & (r -> s)) -> (~q -> s
    )")

sage: f
((p->q)&(~p->r)&(r->s))->(~q->s)

sage: f.truthtable()
p       q       r       s       value
False   False   False   False   True
False   False   False   True    True
False   False   True    False   True
False   False   True    True    True
False   True    False   False   True
False   True    False   True    True
False   True    True    False   True
False   True    True    True    True
True    False   False   False   True
True    False   False   True    True
True    False   True    False   True
True    False   True    True    True
True    True    False   False   True
True    True    False   True    True
True    True    True    False   True
True    True    True    True    True
```

### 1.5.5 Resolution: $\big((p \vee q) \wedge (\neg p \vee r)\big) \rightarrow (q \vee r)$

- Intuitive.
- "disjunctive syllogism" is a special case: $(p \vee q) \wedge (\neg p) \rightarrow q$.
- Another special case, put $q = r$: $\big((p \vee q) \wedge (\neg p \vee q)\big) \rightarrow q$
- Since $\wedge$, $\vee$, $\neg$ are complete, we can put all statements as POS as well as SOP.
- This is the form that theorem proofing and reasoning SW relies on.

**Example 78 (Ex. 7 again)** *: **Premises:*** $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s \equiv (\neg p \vee q) \wedge (p \vee r) \wedge (\neg r \vee s)$
***Conclusion:*** $\neg q \rightarrow s$

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

### 1.5.6 Fallacies: "Doing something wrong while thinking of its soundness"

**The following two statements are NOT tautology:**

$$\big((p \to q) \wedge q\big) \to p \qquad \text{(Fallacy of using converse)}$$
$$\big((p \to q) \wedge \neg p\big) \to \neg q \qquad \text{(Fallacy of using inverse)}$$

- This is a not "valid argument".
- However, "conclusion" could be true.

**Example 79 (Ex. 10)** *"if you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book."*

## 1.5.7 Rules of Inference for Quantified Statements



**TABLE 2 Rules of Inference for Quantified Statements.**

| *Rule of Inference* | *Name* |
|---|---|
| $\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$ | Universal instantiation |
| $\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, P(x)}$ | Universal generalization |
| $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c}$ | Existential instantiation |
| $\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$ | Existential generalization |

**Problems with universal generalization**

- $c$ must be arbitrary; (what about, e.g., $P(3)$)?
- nothing especial about the value of $c$.
- dividing by $c$ !!
- you could use the variable $x$ itself.
- proving $\forall x\,(P(x) \wedge Q(x)) \equiv \forall x\, P(x) \wedge \forall x\, Q(x)$.
- proving universal transitivity.

**universal modus ponens**

$$\forall x\,\big(P(x) \to Q(x)\big)$$
$$P(a)$$
$$\therefore Q(a)$$

**universal modus tollens**

$$\forall x\,\big(P(x) \to Q(x)\big)$$
$$\neg Q(a)$$
$$\therefore \neg P(a)$$

**universal transitivity, (hypothetical syllogism)**

$$\forall x\,\big(P(x) \to Q(x)\big)$$
$$\forall x\,\big(Q(x) \to R(x)\big)$$
$$\therefore \forall x\,\big(P(x) \to R(x)\big)$$

**Example 80 (Ex. 12)** *"Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science".*

| | | |
|---|---|---|
| $D(x)$ : *"x in disc. math. class"* | 1. $\forall x \left(D(x) \rightarrow C(x)\right)$ | |
| $C(x)$ : *"x took a course in CS"* | 2. $D(Marla)$ | |
| $D(Marla)$ | 3. $C(Marla)$ | (universal Modus ponens, (1) and (2)) |

**Example 81 (Ex. 13)** *Show that the premises "A student in this class has not read the book", and "Everyone in this class passed the first exam" imply the conclusion that "Someone who passed the first exam has not read the book".*

| | | |
|---|---|---|
| $C(x)$ : *"x is in this class"* | 1. $\exists x \left(C(x) \wedge \neg B(x)\right)$ | |
| $B(x)$ : *"x has read the book"* | 2. $C(a) \wedge \neg B(a)$ | (existential instantiation from (1)) |
| $P(x)$ : *"x passed the first exam"* | 3. $C(a)$ | (simplification using (2)) |
| $\exists x \left(C(x) \wedge \neg B(x)\right)$ | 4. $\neg B(a)$ | (simplification using (2)) |
| $\forall x \left(C(x) \rightarrow P(x)\right)$ | 5. $\forall x \left(C(x) \rightarrow P(x)\right)$ | |
| $\exists x \left(P(x) \wedge \neg B(x)\right)$. | 6. $P(a)$ | (universal modus ponens from (3) and (5)) |
| | 7. $P(a) \wedge \neg B(a)$ | (conjunction from (4) and (6)) |
| | 8. $\exists x \left(P(x) \wedge \neg B(x)\right)$. | (existential generalization from (7)) |

# 1.6 Introduction to Proofs (back to objectives of Ch. 1)

## 1.6.1 Introduction

- a proof is a valid argument: premises are previous theorems.
- We usually prove theorem **informally**, as opposed to formal argument.
- **Formal** proofs are perfect to computers and theorem proof SW (all detailed steps exist).
- "it is obvious that", "it is tedious to show that", ...and other painful statements.

## 1.6.2 Some Terminology

**Theorem** .
**Proposition** .
**Lemma** .
**Corollary** .
**Axiom** . (if $a > b$ and $b > c$ then $a > c$)
**Conjecture** .

## 1.6.3 Understanding How Theorems Are Stated (formal vs. informal)

"If $x > y$, where $x$ and $y$ are positive real numbers, then $x^2 > y^2$".
"For all positive real numbers $x$ and $y$, if $x > y$, then $x^2 > y^2$".
$\forall x \forall y\ (x \in \mathcal{R}^+ \wedge y \in \mathcal{R}^+ \rightarrow x^2 > y^2)$.

### 1.6.4 Methods of Proving Theorems

We will show several methods of proving theorems:

### 1.6.5 Direct Proofs (start from $p$ reach $q$): $p \to q$

**Example 82 (Ex. 1)** *Given the following definition (**as we always should resort to**), prove that "if $n$ is an odd integer, then $n^2$ is odd".*

***Definition 83*** *The integer $n$ is even if there exists an integer $k$ such that $n = 2k$, and $n$ is odd if there exists an integer $k$ such that $n = 2k+1$.*

*$P(n)$: "$n$ is odd"*
*$Q(n)$: "$n^2$ is odd"*
$\forall n\,(P(n) \to Q(n))$.

$$\begin{aligned} n &= 2k+1 \\ n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 2(2k^2+2k)+1 \\ &= 2m+1, \end{aligned}$$

*where $m = 2k^2+2k$ is an integer.* ■

***Hint:***

- *Nothing special about $n$; hence, $\forall n\,\big(P(n) \to Q(n)\big)$.*
- *some "formal steps may be missing".*

### 1.6.6 Proof by Contraposition

- if direct proof reaches dead end or very difficult.
- (start from $\neg q$ reach $\neg p$): $p \to q \equiv \neg q \to \neg p$.
- This is a usual proof strategy, we always try different proofs.

**Example 84 (Ex. 3)** *Prove that if $3n+2$ is odd, where $n$ is an integer, then $n$ is odd.*
***Direct proof:***

$$\begin{aligned} 3n+2 &= 2k+1 \\ n &= (2k-1)/3. \end{aligned}$$

***proof by contraposition:*** *Suppose that $n$ is even; then for some integer $k$,*

$$\begin{aligned} n &= 2k \\ 3n+2 &= 6k+2 \\ &= 2(3k+1), \end{aligned}$$

*which is even.* ■

**Example 85 (Ex. 4)** *Prove that if $n = ab$, where $a$ and $b$ are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.*
*Suppose that the conclusion is False, i.e.,* $\neg\big((a \leq \sqrt{n}) \vee (b \leq \sqrt{n})\big) \equiv (a > \sqrt{n}) \wedge (b > \sqrt{n})$

$$a > \sqrt{n}$$
$$b > \sqrt{n}$$
$$ab > n.$$
$$ab \neq n.$$

### 1.6.7 Vacuous and Trivial Proofs

- for proving special cases needed to prove the general case.
- $p \rightarrow q$ is true when $p$ is false (vacuous).
- $p \rightarrow q$ is true when $q$ is true (trivial).

**Example 86 (Ex. 5)** *Let $P(n)$ : "$\forall n$ If $n > 1$, then $n^2 > n$", where the domain is all integers.*

*Vacuously, $P(0)$ is true since: $0 > 1 \rightarrow 0 > 0$ is true.* ■

**Example 87 (Ex. 6)** *Let $P(n)$ : "If $a$ and $b$ are positive integers with $a \geq b$, then $a^n \geq b^n$, where the domain is all integers."*

*Trivially, $P(0)$ is true since: $a^0 \geq b^0$ regardless to the hypothesis.* ■

### 1.6.8 Proofs by Contradiction

- To prove $p$, while direct proof is difficult, we start with $\neg p$ to reach contradiction (False):

$$\neg p \rightarrow False \equiv p \vee False \equiv p$$

- You started with something, using sound rules of inference and true premises (except possibly the first one) then reached False. This means that $(\neg p) \wedge \cdots$ is False (or $p$ is True).
- This "False" can be in the form of a contradiction $\neg p \rightarrow (r \wedge \neg r)$.

**Example 88 (Ex. 10: very nice proof)** *Prove that $\sqrt{2}$ is irrational.*

*$P$ : $\sqrt{2}$ is irrational. Suppose that $\neg P$, i.e., $\sqrt{2}$ is rational, i.e., $\exists a \exists b$ ($\sqrt{2} = a/b$), where $a$, $b$ are integers with no common factors. Actually, we assumed $\neg p \wedge r$, where $r$ : "no common factor between $a$ and $b$".*

$$\sqrt{2} = a/b$$
$$a^2 = 2b^2,$$

*which means $a^2$ is even, and hence is $a$ (from the contraposition of "$a$ is odd $\rightarrow$ $a^2$ is odd").*

$$(2c)^2 = 2b^2$$
$$4c^2 = 2b^2$$
$$b^2 = 2c^2;$$

*therefore, $b^2$ is even and hence is $b$. So, both $a$ and $b$ are even and have a common factor of 2; a contradiction (common factor AND not common factor).*

#### 1.6.8.1 Proof by contradiction for conditional statements (similar to contraposition)

To prove $p \to q$, we start with both $p \wedge \neg q$ (not only $\neg q$) to reach contradiction (False)

$$\big((p \wedge \neg q) \to False\big) \equiv \neg(p \wedge \neg q) \vee False \equiv (\neg p \vee q) \equiv p \to q$$

**Example 89 (Ex. 3 again)** *Prove that if $3n+2$ is odd, where $n$ is an integer, then $n$ is odd.*
***proof by contraposition:*** *Suppose that $n$ is even; then for some integer $k$,*

$$\begin{aligned} n &= 2k \\ 3n+2 &= 6k+2 \\ &= 2(3k+1), \end{aligned}$$

***proof by contradiction:*** *Assume that $n$ is even ($\neg q$ as in contraposition) and $3n+2$ is odd ($p$). Then, we reach $3n+2$ is even (a contradiction).* ■

#### 1.6.8.2 Proof by contradiction for direct proofs

To prove $p \to q$ (directly) suppose $p \wedge \neg q$ and reach $q$.

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

.

### 1.6.9 Proof of Equivalence

#### 1.6.9.1 Proof of equivalence of two statements

**Example 90 (Ex. 12)** *Prove the theorem that "If n is a positive integer, then n is odd* ***iff*** $n^2$ *is odd"*

- *We have proven, in a previous example by direct proof, ("n odd* $\rightarrow n^2$ *is odd ").*
- *The other direction does not seem possible by direct proof: suppose* $n = 2k$*, then* $n^2 = 4k^2 = 2(2k^2)$*, an even integer (contradicting* $n^2$ *is odd); the proof is complete* ■

#### 1.6.9.2 Proof of equivalence of more than one statement

$$\left(p_1 \leftrightarrow p_2 \leftrightarrow \cdots p_n\right) \equiv \left((p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1)\right)$$

**Proof.** Draw a circle to see sufficiency and necessity

. ■

**Hint:**

- number of implications to be proven is just $n$, which is much more efficient to prove $2n_{C_2} = n(n-1)$ implications.
- We establish any chain; e.g., $p_3 \rightarrow p_1 \rightarrow p_2 \rightarrow p_3$.

**Example 91 (Ex. 13)** *Show that the following statements about integers are equivalent:*

$p_1 : n$ *is even.*
$p_2 : n-1$ *is odd.*
$p_3 : n^2$ *is even.*

***proof of:*** $p_1 \to p_2$
$n = 2k$, *then* $n-1 = 2k-1 = 2(k-1+1)-1 = 2(k-1)+1$, *which is odd.*

***proof of:*** $p_2 \to p_3$
$n-1 = 2k+1$, *then* $n = 2(k+1)$, $n^2 = 2(2(k+1)^2)$, *which is even.*

***proof of:*** $p_3 \to p_1$ ***(a common mistake is to prove*** $p_1 \to p_3$***; not a loop)***
$p_3 \to p_1 \equiv \neg p_1 \to \neg p_3 \equiv$ *"if n is odd then* $n^2$ *is odd", which has been proven in the previous example. The proof is complete* ■

### 1.6.10 (Dis)Proof by Counterexample

This is to show that $\forall x\ P(x)$ is False.

**Example 92 (Ex. 14)** *Show that the statement "Every positive integer is the sum of the squares of two integers"*
***Hint: (Just to remember)***

$$P(n) : \forall n \exists m \exists k\ (n > 0 \rightarrow n = m^2 + k^2)$$
$$\neg P(n) : \exists n \forall m \forall k\ (n > 0 \wedge n \neq m^2 + k^2).$$

***a counterexample:*** $n = 3$ ■

### 1.6.11 Mistakes in Proofs

#### 1.6.11.1 Dividing by Zero

$$\begin{aligned} 4-4 &= 4-4 \\ 2(2-2) &= (2-2)(2+2) \\ 2 &= 4 \\ 1 &= 2 \end{aligned}$$

#### 1.6.11.2 Dropping a Case in Negation

$$\neg(n<0) \equiv n \geq 0$$

#### 1.6.11.3 Replacing a step by non-equivalent step

$$\sqrt{x+3} = x-3 \tag{1.1}$$
$$x+3 = (x-3)^2 \tag{1.2}$$
$$x^2-7x+6 = 0 \tag{1.3}$$
$$(x-1)(x-6) = 0 \tag{1.4}$$
$$(x=1) \vee (x=6) \tag{1.5}$$

**Hint:** The final statement is true; however, this is not the solution set of $\sqrt{x+3} = x-3$!! It is the solution set of $x+3 = (x-3)^2$ (for simplicity: $x=3 \rightarrow x^2 = 9$).

#### 1.6.11.4 Fallacy of Affirming the Conclusion (using the converse)

$$p \to q \not\equiv q \to p.$$

**Wrong Proof for.** "If $n^2$ is positive, then $n$ is positive".
If $n$ is positive, then $n^2$ is positive. Hence, since we already know that $n^2$ is always positive then $n$ must be positive as well; which completes the proof ■

#### 1.6.11.5 Fallacy of Denying the Hypothesis (using the inverse)

$$p \to q \not\equiv \neg p \to \neg q.$$

**Wrong Proof for.** "If $n$ is not positive, then $n^2$ is not positive".
It is quite trivial to prove the lemma; however, we show it for completeness. We already have proven that if $n$ is positive then $n^2$ is positive. Since $n$ is not positive, then $n^2$ is not positive follows immediately. ■

#### 1.6.11.6 Fallacy of Begging the Question (circular argument)

**Wrong Proof for.** "If $n^2$ is even then $n$ is even" (although the conclusion itself is true)
Since $n^2$ is even, then $\exists k$ such that $n^2 = 2k$. We can freely choose $k$ to be in the form $k = 2m^2$. Therefore, $n^2 = 4m^2$; and hence $n = 2m$, an even number. ■

### 1.6.12 Just a Beginning

## 1.7 Proof Methods and Strategy

### 1.7.1 Introduction

- We continue what we have started in Sec. 1.6
- We elaborate here other methods of proof.
- We emphasize that proof strategy has a piece of art: conjecture, then try a direct proof, then try another proof by contradiction, then probably try to disprove by a counterexample, etc.

### 1.7.2 Exhaustive Proof and Proof by Cases

$$\big((p_1 \vee p_2 \vee \cdots \vee p_n) \to q\big) \equiv \big((p_1 \to q) \wedge (p_2 \to q) \wedge \cdots (p_n \to q)\big)$$

$$\begin{aligned}\big((p_1 \vee p_2 \vee \cdots \vee p_n) \to q\big) &\equiv \neg(p_1 \vee p_2 \vee \cdots \vee p_n) \vee q \\ &\equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \neg p_n) \vee q \\ &\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \cdots (\neg p_n \vee q) \\ &\equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \cdots (p_n \to q)\end{aligned}$$

**Example 93 (exhaustive, Ex. 1)**
*For positive integers, prove that* $(n+1)^2 \geq 3^n$, *where* $n = 1, 2$.

*Just substitute for* $n = 1, 2$. ■

**Example 94 (exhaustive, Ex. 2)** *Prove that the only consecutive 2 integers that are less than 100 and are perfect powers are 8 and 9.*

| $n$ | $n^2$ | $n^3$ | $n^4$ | $n^5$ | $n^6$ | $n^7$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 16 | 32 | 64 | |
| 3 | 9 | 27 | 81 | | | |
| 4 | 16 | 64 | | | | |
| 5 | 25 | | | | | |
| 6 | 36 | | | | | |
| 7 | 49 | | | | | |
| 8 | 64 | | | | | |
| 9 | 81 | | | | | |
| 10 | 100 | | | | | |

■

**HINT** (for computer scientists): simulation does NOT prove; and sometimes even cannot (P. 26)

**Example 95 (by cases, Ex. 3)** *Prove that if $n$ is an integer then $n^2 \geq n$.*
*The proof is quite easy and we show it here just for completeness.*

$n \geq 1$ *: multiplying both sides by $n$ gives $n^2 \geq n$.*

$n \leq -1$ *: then, $n^2 \geq 1$, which means $n^2 \geq 1 > -1 \geq n$*

$n = 0$ *: then $n^2 \geq n$.* ■

**Example 96 (Fallacy of a non-rigorous generalization by a young computer scientist or engineer)** *:*
*Since we have proved that $n^2 \geq n$ for $n \leq -1$ and $1 \leq n$, it will be true of course for the numbers in between when $n \in \mathcal{R}$.*

***This is based on the following invalid argument:***

$$\forall n\ (if\ n \leq -1 P(n))$$
$$\forall n\ (if\ n \geq 1 P(n))$$
$$\hline$$
$$\therefore \forall n\ (if\ -1 \leq n \leq 1 P(x))$$

**Example 97 (by case, Ex. 4)** *If $n$ is an integer, Conjecture something about the first digit of $n^2$ then try to prove/disprove it.*

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, $\cdots$ *It seems that it is either* 0, 1, 4, 5, 6, 9 *only!!*
***more towards conjecture:***

```
sage: for i in range(1000000):
....:     if not ((i^2 % 10) in {0, 1, 4, 5, 6, 9}):
....:         print(i)
....:
```

$\forall n$, $n = (10a+b)$, *then* $n^2 = 100a^2+20ab+b^2 = 100a^2+10(2ab)+b^2$. *Therefore, the first digit of* $n^2$ *comes, as well, from the first digit of* $n$*; i.e.,* $b$.

| $b$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $b^2$ | 0 | 1 | 4 | 9 | 16 | 25 | 36 | 49 | 64 | 81 |

*why this is not exhaustive proof?*

■

### 1.7.3 The Role of Open Problems

Many famous problem remains open (not proved and not disproved); they are conjectures.

**Example 98 (Fermat's Last Theorem (more than 3 centuries ago))** *The equation*

$$x^n + y^n = z^n$$

*has no solution for* $x,\ y,\ z$*, with* $xyz \neq 0$*, whenever* $n$ *is an integer with* $n > 2$*.*

- $n = 1$*: has solutions for all integers.*
- $n = 2$*: this is the well known Pythagorean theorem.*
- $n \geq 3$*: has no solution.*

**Example 99 (The** $3x+1$ **conjecture (Ulam's, Collatz, and others))** *: Consider the following transform:*

$$T(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 3n+1 & \text{if } n \text{ is odd} \end{cases}.$$

*Then, for any integer* $n$ *applying* $T$ *successively ends up with 1.*

**HW:** write an efficient algorithm to check all numbers from 1 to $N$.

**"Without Loss of Generality (WLOG)": not a proof method; it is just for short**

**Example 100 (Ex. 4)** *Show that* $|xy| = |x||y|$*, where* $x$ *and* $y$ *are real numbers.*

*The proof is clear when any or both of variables is zero.*

$x, y$ **are positive** *:*

$x, y$ **are negative** *:*

**WLOG,** $x > 0,\ y < 0$ *:*

*Other wording could be:* $x < 0,\ y > 0$ *follows similarly.*
***HINT:*** *always take care when you loose generality and assume WLOG*

### 1.7.4 Existence Proofs: $\exists x\, P(x)$

**Example 101 (constructive existence, Ex. 10)** *Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways*

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

***HW**: write a computer program to find the first such number.*

**Example 102 (nonconstructive existence, Ex. 11)** *Show that there exist irrational numbers $x$ and $y$ such that $x^y$ is rational.*

*Let $x = y = \sqrt{2}$. If $\sqrt{2}^{\sqrt{2}}$ is rational we are done. If not then let $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, then $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$.*

*Therefore, the two numbers are: $\sqrt{2}$ and either $\sqrt{2}$ or $\sqrt{2}^{\sqrt{2}}$*

■

### 1.7.5 Uniqueness Proofs: (remember Ex. 63)

**Example 103 (Ex. 13)** *Show that for $a \neq 0$, $y = ax + b$ has a unique solution in $x$.*

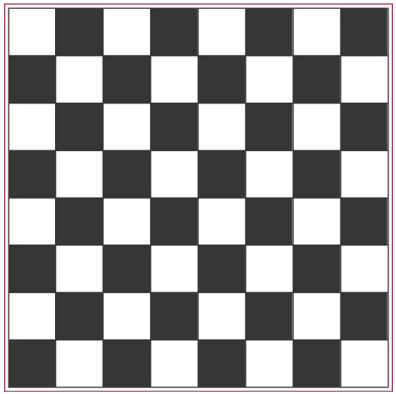
*Solve for $x$, and call the solution $x_1$; then $x_1 = (y - b)/a$. Suppose there is another solution $x_2$,*

$$\begin{aligned} y &= ax_1 + b \\ y &= ax_2 + b \\ 0 &= a(x_1 - x_2). \end{aligned}$$

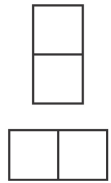
*either $a = 0$ or $x_1 = x_2$.* ■

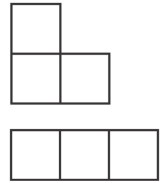
### 1.7.6 Tilings (even games are based on Mathematics)











**Example 104 (Constructive existence, Ex. 18)** *Can we tile the standard checkerboard using dominoes? Sure, using 32 dominoes. (one arrangement proves existence)* ■

**Example 105 (Contradiction, Ex. 19)** *Can we tile the checkerboard after removing one corner? Suppose we can; then* $2n = 63$*, where* $n$ *is an integer, a contradiction.* ■

**Example 106 (Ex., 20)** *Can we tile the checkerboard after removing 2 diagonal corners?*
***First try proving****:* $(2n = 62$*; i.e.,* $n = 31)$*; seems very difficult after trying many tilings.*
***Ok, try disproving****: number of white* $= 32 - 2$*, number of black* $= 32$*. Suppose we can tile them; the total number of white should equals to the total number of black; a contradiction.* ■

### 1.7.7 Additional Proof Methods and Related Issues (in subsequent chapters)

**Many things remaining for "proofs" and "theorems"**

- Induction
- Recursion
- "Halting Theorem": there is a problem that cannot be solved using any procedure!!
- $\cdots$ many others.

# Chapter 2

# Basic Structures:
# Sets, Functions, and Sequences and Sums

## 2.1 Sets

### 2.1.1 Introduction

- A very fundamental structure that almost all other structures are composed of.
- We will rely on the "naive set theory" rather than "axiomatic set theory".
- The "naive set theory" (by Cantor) leads to "Russel's Paradox".

**Definition 107 (Def. 1, 2)** *A "set" is an unordered collection of objects (also called elements, or members). A "set" is said to "contain" its elements.*
***Hint:*** *We did not define what is an "object" (not very rigorous as opposed to the axiomatic set theory)!!*

*If $a$ is an element of $A$, we say $a \in A$; and if not we say $a \notin A$ ($\equiv \neg(a \in A)$).* ■

**Example 108 (Ex. 1–5)** *How to write a set:*

$$
\begin{aligned}
V &= \{a,e,i,o,u\} = \{i,o,u,e,a\} && \text{(set of vowels)}\\
M &= \{1,2,3,\cdots,9\} && \text{(set of integers less than 10)}\\
O &= \{1,3,5,7,9\} && \text{(set of odd integers less than 10)}\\
&= \{x \,:\, x \text{ is odd positive less than } 10\}\\
&= \{x \mid x \text{ is odd positive less than } 10\}\\
\mathbb{Z}^+ &= \{1,2,\cdots\} && \text{(set of positive integers)}\\
\mathbb{N} &= \{0,1,2,\cdots\} && \text{(set of natural numbers)}\\
\mathbb{Z} &= \{\cdots,-2,-1,0,1,2,\cdots\} && \text{(set of integers)}\\
\mathbb{Q} &= \{p/q \mid p,q \in \mathbb{Z}, q \neq 0\} && \text{(set of rational numbers)}\\
\mathbb{R}. & && \text{(set of real numbers)}\\
\{\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}\} & && \text{(set containing four elements, each is a set)}
\end{aligned}
$$

■

**Example 109** *Consider the set $A = \{\{a\},\{a,b\},c\}$; then*

$$
\begin{aligned}
c &\in A\\
\{a\} &\in A\\
a &\notin A
\end{aligned}
$$

**Definition 110** *Two sets are equal if they have the same elements. Said differently, we say that:*

$$A = B \text{ if } \forall x\ (x \in A \leftrightarrow x \in B) \text{ is True.}$$

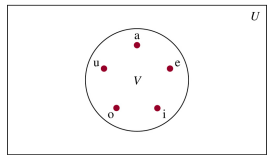
■

**Example 111 (very good to set back to def., Ex. 6)** $\{1,3,5\} = \{3,1,5\} = \{1,3,3,3,5,1\}$ ■

**Example 112 (More notation, Ex. 7)** *:*

- *Venn Diagram of set of vowels $V$, along with the universe $U$.*






- *Empty set: $\phi = \{\}$; this is not as $\{\phi\}$; e.g., empty directory.*
- *Singleton set (one element set):* $\{a\}$, $\{\{1,2,3\}\}$

**Definition 113 (Subset and Proper subset, Def., 4)** *:*
*The set $A$ is said to be a subset of $B$ $(A \subseteq B)$ if every element of $A$ is also an element of $B$. Said differently, we say that:*

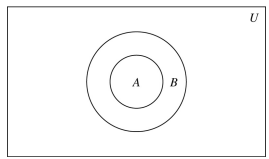
$$A \subseteq B \text{ if } \forall x\ (x \in A \rightarrow x \in B) \text{ is True.}$$

*The set $A$ is said to be a **proper subset** of $B$ $(A \subset B)$ if $A \subseteq B$ and there exist some elements in $B$ that do not belong to $A$. Said differently, we say that:*

$$A \subset B \text{ if } \forall x\ (x \in A \rightarrow x \in B) \wedge \exists x\ (x \in B \wedge x \notin A) \text{ is True.}$$

■






**Remark 4** *$A \subset B \rightarrow A \subseteq B$ but not the vise versa; this is clear since*

$$A \subset B \equiv (\forall x\ (x \in A \rightarrow x \in B)) \wedge (\exists x\ (x \in B \wedge x \notin A)) \equiv (A \subseteq B) \wedge (\exists x\ (x \in B \wedge x \notin A))$$

**Example 114 (Ex. 8)** *In the first example:*

$$O \subset \mathbb{Z}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

**Example 115** *Prove that if sets A and B are equal is equivalent to both are subsets of each others.*

$$\begin{aligned} A = B &\equiv \forall x\ (x \in A \leftrightarrow x \in B) \\ &\equiv \forall x\ \big((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)\big) \\ &\equiv \forall x\ (x \in A \rightarrow x \in B) \wedge \forall x\ (x \in B \rightarrow x \in A) \\ &\equiv (A \subseteq B) \wedge (B \subseteq A). \end{aligned}$$

**Theorem 116 (Thm. 1)** *For every set S, $\phi \subseteq S$ and $S \subseteq S$.*

**Proof.** The proof is trivial, but we show it for the sake of completeness.
From the definition: $\forall x\ (x \in A \rightarrow x \in B)$ is vacuously true for the first statement and tautologically true for the second; the proof is complete. ■

**Definition 117 (Def. 5-6)** *If there are exactly n distinct elements in S, we say that S is **finite set** and its **Cardinality** is $|S| = n$. And if S is not finite we call it **infinite**.*

**Example 118 (Ex. 9–12)** *:*

- *A* : *set of odd positive integers less than 10;* $|A| = 5$.
- $|\phi| = 0$.
- *Set of positive integers (infinite)*

### 2.1.2 The Power Set

**Definition 119 (Def. 7)** *The power set of the set $S$ ($P(S)$) is the set of all subsets of the set $S$.* ■

**Remark 5** *We will prove that if $|S| = n$, then*

$$|P(S)| = {}^nC_0 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_n = 2^n$$

**Example 120 (Ex. 13–14)** *: $S = \{0,1,2\}$*

$$\begin{aligned} P(S) &= \{\phi, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\} \\ |P(S)| &= 1+3+3+1 = 2^3 = 8 \\ P(\phi) &= \{\phi\} \\ P(\{\phi\}) &= \{\phi, \{\phi\}\}. \end{aligned}$$

**Remark 6** *Observe that for any set $S$, we have proven that $\phi \subseteq S$ and $S \subseteq S$; then:*

$$\begin{aligned} \phi &\in P(S) \\ S &\in P(S) \\ \{\phi\} &\subseteq P(S) \\ \{S\} &\subseteq P(S). \end{aligned}$$

■

### 2.1.3 Cartesian Products

- to define ordering as opposed to sets.
- a sub-field of computer science, i.e., databases, is founded on Cartesian products and Relations.

**Definition 121 (Def. 8)** *The **ordered** $n$-**tuple** $(a_1, a_2, \cdots, a_n)$ is the ordered collection that has $a_1$ as its first element, $a_2$ as the second, etc. We say that two $n$-tuples $a$ and $b$ are equal if $a_i = b_i$, $1 \leq i \leq n$.*

**Definition 122 (Def. 9)** *Let $A$ and $B$ be sets. The **Cartesian product** of $A$ and $B$, denoted by $A \times B$, is the set of all ordered pairs $(a, b)$, where $a \in A$ and $b \in B$. Said differently,*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

**Example 123 (Ex. 16)** *$A = \{1, 2\}$, $B = \{a, b, c\}$, then $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$.*

```
for(i=1, i<=|A|, i++)
        for(j=1, j<=|B|, j++)
                (A[i], B[j]); // C-like pseudo-code.
```

**Definition 124 (Generalization, Def. 10)** *The Cartesian product of the sets $A_1$, $A_2$, $\cdots$, $A_n$ is defined as:*

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i,\ 1 \leq i \leq n\}$$

**Example 125 (Ex. 18)** *$A = \{0, 1\}$, $B = \{1, 2\}$, $C = \{0, 1, 2\}$; then*

$$A \times B \times C = \{(0,1,0), (0,1,1), (0,1,2), (0,2,0), (0,2,1), (0,2,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2)\}$$

### 2.1.4 Using Set Notation with Quantifiers

We have previously proved it in Sec. 1.3.8

### 2.1.5 Truth Sets of Quantifiers

If the domain is $D$, then the truth set of the predicate $P(x)$ is

$$\{x \in D \mid P(x)\}$$

**Example 126 (Ex. 20)** *if the domain is $\mathbb{Z}$, then the truth set of "$|x| = 1$" is the set $\{-1, 1\}$*

## 2.2 Set Operations

### 2.2.1 Introduction

**Definition 127 (Def. 1–5)** *Let $A$ and $B$ be two sets; we define:*
**union** $A \cup B$ *: is the set that contains elements in either of them*

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

**intersection** $A \cap B$ *: is the set that contains elements in both of them.*

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

**disjoint** *: $A$ and $B$ are said disjoint if $A \cap B = \phi$.*

**difference** $A - B$ *: is the set that contains elements in $A$ but not $B$.*

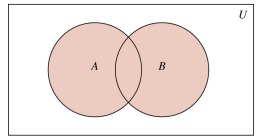
$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

**complement** $\overline{A}$ *: is the set that contains elements not in $A$ (with respect to some $U$); i.e., $U - A$*

$$\overline{A} = \{x \mid \neg(x \in A)\} = \{x \mid x \notin A\} = \{x \mid True \wedge x \notin A\} = \{x \mid x \in U \wedge x \notin A\} = U - A$$

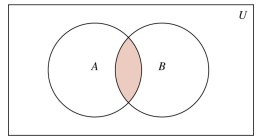
**Example 128 (Ex. 1–9)** $A = \{1,3,5\}$, $B = \{1,2,3\}$, $U = \{1,2,3,\cdots,6\}$*; then*
$A \cup B = \{1,2,3,5\}$, $A \cap B = \{1,3\}$, $A - B = \{5\}$, $\overline{A} = \{2,4,6\}$





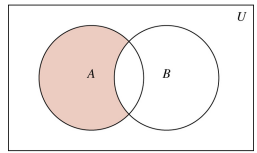

$A \quad B$ is shaded.





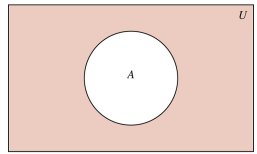

$A \quad B$ is shaded.






$A - B$ is shaded.






$\overline{A}$ is shaded.

### 2.2.2 Set Identities

- Very parallel to logic identities,:
- As in logical equivalence, can be proven by:

1. truth table
2. set builder
3. both are subsets of each other
4. algebraically

$$p(x): x \in A$$
$$q(x): x \in B$$
$$False = x \in \phi$$
$$True = x \in U$$
$$p(x) \wedge q(x) = x \in A \wedge x \in B$$
$$p(x) \vee q(x) = x \in A \vee x \in B$$
$$\neg p(x) = x \in \overline{A}.$$

**Remember $p \rightarrow q$:**



**TABLE 6 Logical Equivalences.**

| *Equivalence* | *Name* |
|---|---|
| $p \wedge \mathbf{T} \equiv p$<br>$p \vee \mathbf{F} \equiv p$ | Identity laws |
| $p \vee \mathbf{T} \equiv \mathbf{T}$<br>$p \wedge \mathbf{F} \equiv \mathbf{F}$ | Domination laws |
| $p \vee p \equiv p$<br>$p \wedge p \equiv p$ | Idempotent laws |
| $\neg(\neg p) \equiv p$ | Double negation law |
| $p \vee q \equiv q \vee p$<br>$p \wedge q \equiv q \wedge p$ | Commutative laws |
| $(p \vee q) \vee r \equiv p \vee (q \vee r)$<br>$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | Associative laws |
| $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$<br>$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | Distributive laws |
| $\neg(p \wedge q) \equiv \neg p \vee \neg q$<br>$\neg(p \vee q) \equiv \neg p \wedge \neg q$ | De Morgan's laws |
| $p \vee (p \wedge q) \equiv p$<br>$p \wedge (p \vee q) \equiv p$ | Absorption laws |
| $p \vee \neg p \equiv \mathbf{T}$<br>$p \wedge \neg p \equiv \mathbf{F}$ | Negation laws |



**TABLE 1 Set Identities.**

| *Identity* | *Name* |
|---|---|
| $A \cup \varnothing = A$<br>$A \cap U = A$ | Identity laws |
| $A \cup U = U$<br>$A \cap \varnothing = \varnothing$ | Domination laws |
| $A \cup A = A$<br>$A \cap A = A$ | Idempotent laws |
| $\overline{(\overline{A})} = A$ | Complementation law |
| $A \cup B = B \cup A$<br>$A \cap B = B \cap A$ | Commutative laws |
| $A \cup (B \cup C) = (A \cup B) \cup C$<br>$A \cap (B \cap C) = (A \cap B) \cap C$ | Associative laws |
| $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$<br>$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ | Distributive laws |
| $\overline{A \cup B} = \overline{A} \cap \overline{B}$<br>$\overline{A \cap B} = \overline{A} \cup \overline{B}$ | De Morgan's laws |
| $A \cup (A \cap B) = A$<br>$A \cap (A \cup B) = A$ | Absorption laws |
| $A \cup \overline{A} = U$<br>$A \cap \overline{A} = \varnothing$ | Complement laws |

**Example 129 (Ex. 10–14)** *Prove that* $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

1. ***Truth Table (membership table)***

| $A$ | $B$ | $A \cap B$ | $\overline{A \cap B}$ | $\overline{A}$ | $\overline{B}$ | $\overline{A} \cup \overline{B}$ |
|---|---|---|---|---|---|---|
| $x \in A$ | $x \in B$ | $x \in A \wedge x \in B$ | $\neg(x \in A \wedge x \in B)$ | $x \notin A$ | $x \notin B$ | $x \notin A \vee x \notin B$ |
| $p$ | $q$ | $p \wedge q$ | $\neg(p \wedge q)$ | $\neg p$ | $\neg q$ | $\neg p \vee \neg q$ |
| $T$ | $T$ | $T$ | $F$ | $F$ | $F$ | $F$ |
| $T$ | $F$ | $F$ | $T$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $F$ | $T$ | $T$ | $F$ | $T$ |
| $F$ | $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |

2. ***Set builder***

$$\neg(x \in A \wedge x \in B) \equiv \neg(x \in A) \vee \neg(x \in B)$$
$$\neg(x \in A \cap B) \equiv x \in \overline{A} \vee x \in \overline{B}$$
$$x \in \overline{A \cap B} \equiv x \in \overline{A} \cup \overline{B}$$
$$\left\{x \mid x \in \overline{A \cap B}\right\} = \left\{x \mid x \in \overline{A} \cup \overline{B}\right\}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

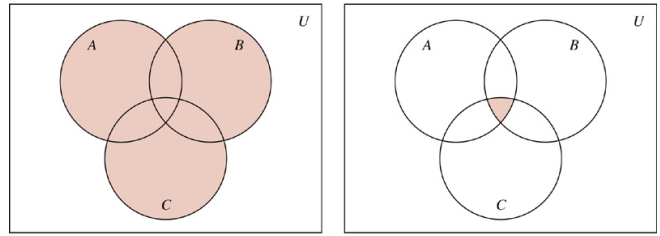
3. $x \in \overline{A \cap B} \leftrightarrow x \in \overline{A} \cup \overline{B}$ ***(both are subsets of each other)***
   ***Sufficiency:*** *suppose that* $x \in \overline{A \cap B}$ *then ...* $x \in \overline{A} \vee x \in \overline{B}$
   ***Necessity:*** *suppose that* $x \in \overline{A} \vee x \in \overline{B}$ *then ...* $x \in \overline{A \cap B}$.

4. ***Algebraically (after proving some identities)****: Prove that:* $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$

$$\overline{A \cup (B \cap C)} = \overline{A} \cap \overline{B \cap C} = \overline{A} \cap (\overline{B} \cup \overline{C}) = (\overline{B} \cup \overline{C}) \cap \overline{A}.$$

### 2.2.3 Generalized Unions and Intersections






(a) $A \cup B \cup C$ is shaded. (b) $A \cap B \cap C$ is shaded.

From the associative law, $A \cup B \cup C$ and higher unions is well defined; therefore,

**Definition 130 (Def. 6)** *The union of a collection of sets is the set that contains those elements that are member of at least one set in the collection. We denote:*

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

**Definition 131 (Def. 7)** *The intersection of a collection of sets is the set that contains those elements that are members of all the sets in the collection. we denote:*

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

**Example 132 (Ex. 16)** *Let $A_i = \{i, i+1, i+2, \cdots\}$, $1 \leq i$; then (**HW:** prove that)*

$$A_1 = \mathbb{Z}^+ \qquad \text{(by construction)}$$

$$\bigcup_{i=1}^{n} A_i = \{1,2,3,\cdots\} \cup \{2,3,4,\cdots\} \cup \{3,4,5,\cdots\} \cup \cdots \cup \{n, n+1, \cdots\} = \{1,2,3,\cdots\} = A_1$$

$$\bigcap_{i=1}^{n} A_i = \{1,2,3,\cdots\} \cap \{2,3,4,\cdots\} \cap \{3,4,5,\cdots\} \cap \cdots \cap \{n, n+1, \cdots\} = \{n, n+1, \cdots\} = A_n$$

***More notation:***

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$$

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots$$

***More notation:*** *suppose that $I = \{1,5,6\}$ then*

$$\bigcup_{i \in I} A_i = A_1 \cup A_5 \cup A_6$$

$$\bigcap_{i \in I} A_i = A_1 \cap A_5 \cap A_6$$

***Of course:***

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{Z}^+} A_i$$

**Example 133 (Ex. 17)** *Let $A_i = \{1,2,3,\cdots,i\}$, $1 \le i$. Prove that $\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}^+$ and $\bigcap_{i=1}^{\infty} A_i = \{1\}$.*
*First try to construct it (but it, **of course**, needs a proof):*

$$\bigcup_{i=1}^{\infty} A_i = \{1\} \cup \{1,2\} \cup \{1,2,3\} \cup \cdots = \{1,2,3,\cdots\}$$
$$\bigcap_{i=1}^{\infty} A_i = \{1\} \cap \{1,2\} \cap \{1,2,3\} \cap \cdots = \{1\}.$$

***Proof.***

- ***Proving*** $\bigcup_{i=1}^{\infty} A_i \subseteq \mathbb{Z}^+$
  *for $n \in \bigcup_{i=1}^{\infty} A_i$, then it has to belong to one of the individual sets (from the definition of union), e.g., $A_k$. Then, $1 \le n \le k$ and hence $n \in \mathbb{Z}^+$.*

- ***Proving*** $\mathbb{Z}^+ \subseteq \bigcup_{i=1}^{\infty} A_i$
  *Suppose $n \in \mathbb{Z}^+$, then $n \in A_n$ (from the def. of $A_n$) and hence belongs to the union of all $A_i$.*

***HW:*** *prove the second part using the same method.* ■

### 2.2.4 Computer Representation of Sets (Homework)

**Example 134 (Very fast example)** *Consider the universal set* $U = \{1,2,3,\cdots,10\}$*; then*

$$A = \{1,3,5,7,9\} \longrightarrow 10\ 1010\ 1010 \quad \text{(locations)}$$

$$\overline{A} = \{2,4,6,8,10\} \longrightarrow 01\ 0101\ 0101 \quad \text{(simple complement)}$$

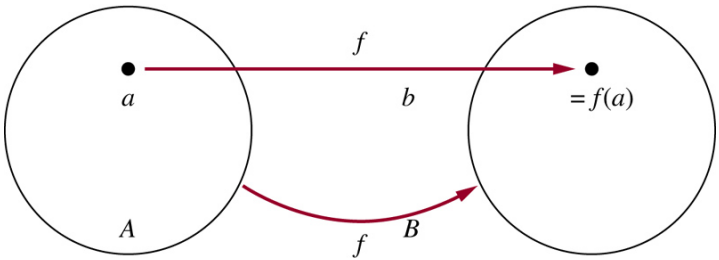
*Intersection and union are done with bit-wise operations (so fast).*

## 2.3 Functions

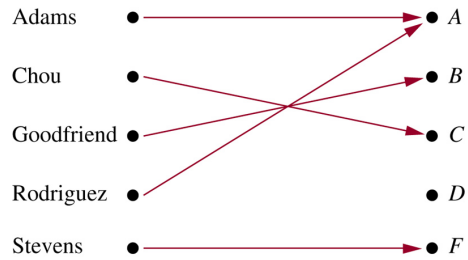
### 2.3.1 Introduction

- The concept of "functions" is extremely important in Mathematics, and Computer Science.
- Elementary example (grade assignment in class):
- Direct assignment (as figure), equation (as $f(x) = x + 1$), or computer program







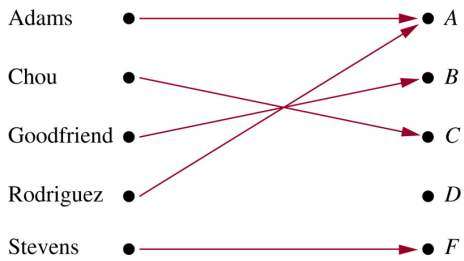

**Definition 135 (Def. 1–2)** *Let $A$ and $B$ be **nonempty** sets. A function $f$ from $A$ to $B$ is an assignment of exactly one element of $B$ to each element of $A$. We write $f(a) = b$ if $b$ is a unique element of $B$ assigned by the function $f$ to the element $a$ of $A$. We write $f : A \to B$ (also called mapping or transformation, or $f$ maps $A$ to $B$).*
*We say that $A$ is the domain of $f$ and $B$ is the codomain of $f$; $b$ is the image of $a$, and $a$ is the pre-image of $b$.*
*The range of $f$ is the set of all images of elements of $A$.* ■

**Hint:** Two functions are equal if the domain, codomain, and assignment are the same.

**Example 136 (Ex. 1)**

$$Domain = \{Adams, Chou, Godfriend, Rodriguea, Stevens\}$$
$$Codomain = \{A, B, C, D, F\}$$
$$Range = \{A, B, C, F\} \neq Codomain$$






**Example 137 (Ex. 4)** *Let $f : \mathbb{Z} \to \mathbb{Z}$ assign the square of an integer to this integer. Then, $f(x) = x^2$, where the domain is $\mathbb{Z}$ and **we take** the codomain to be $\mathbb{Z}$ (as well). The range will be $\{0, 1, 4, 9, \cdots\}$*

**Example 138 (Ex. 5)** *In programming, the domain and codomain are often specified for a function:*

```
float TestFunction(int x){
    ...
}
```

**Definition 139 (Ex. 3)** *Let $f_1$ and $f_2$ be functions from $A$ to $\mathbb{R}$. Then, $f_1 + f_2$ and $f_1 f_2$ are also functions from $A$ to $\mathbb{R}$ defined by:*

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

**Example 140 (Ex. 6)** *$f_i : \mathbb{R} \to \mathbb{R}$, $i = 1,2$, $f_1(x) = x^2$, $f_2(x) = (x - x^2)$. Then*

$$\begin{aligned} (f_1 + f_2)(x) = f_1(x) + f_2(x) &= (x^2) + (x - x^2) &&= x \\ (f_1 f_2)(x) = f_1(x) f_2(x) &= (x^2)(x - x^2) &&= x^3 - x^4. \end{aligned}$$

**Definition 141 (Def. 4)** *Consider $f : A \to B$. The image of the set $S$ ($\subseteq A$) is the subset of $B$ that consists of the images of the elements of $S$; we denote it by $f(S)$. It is*

$$f(S) = \{t \mid \exists s \in S\ (t = f(s))\} = \{f(s) \mid s \in S\}$$

**Example 142 (Ex. 7)** *$A = \{a,b,c,d,e\}$, $B = \{1,2,3,4\}$, $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$, $f(e) = 1$. Then the image of $S = \{b,c,d\}$ is the set $f(S) = \{1,4\}$.* ■

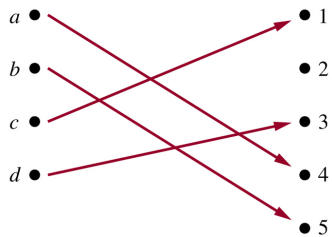
### 2.3.2 One-to-One and Onto Functions

**Definition 143 (Def. 5)** *A function $f$ is said to be one-to-one (or injective), if $f(a) = f(b)$ implies that $a = b$, for all $a, b$ in the domain of $f$. Said differently:*

$$\forall a \forall b (f(a) = f(b) \rightarrow a = b) \equiv \forall a \forall b (a \neq b \rightarrow f(a) \neq f(b)).$$

**Example 144 (one-to-one, Ex. 8)** *:*






**Example 145 (not one-to-one, Ex. 9)** $f(x) = x^2,\ x \in \mathbb{R}$.

$$b = a^2 \rightarrow a = \pm\sqrt{b}$$

***However:*** *if we restrict the domain to $\mathbb{R}+$ or $\mathbb{Z}+$ it will be injective.* ■

**Definition 146 ("increasing" Def. 6)** *A function $f$, whose domain and codomain are subsets of $\mathbb{R}$, is called increasing if $f(x) \leq f(y)$, and strictly increasing if $f(x) < f(y)$, whenever $x < y$ and $x, y$ belong to the domain.*

$$\forall x \forall y (x < y \rightarrow f(x) \leq f(y)) \qquad \text{(increasing)}$$
$$\forall x \forall y (x < y \rightarrow f(x) < f(y)) \qquad \text{(strictly increasing)}$$

*Similarly, $f$ is called decreasing if $f(x) \geq f(y)$, and strictly decreasing, if $f(x) > f(y)$, whenever $x < y$.*

$$\forall x \forall y (x < y \rightarrow f(x) \geq f(y)) \qquad \text{(decreasing)}$$
$$\forall x \forall y (x < y \rightarrow f(x) > f(y)) \qquad \text{(strictly decreasing)}$$

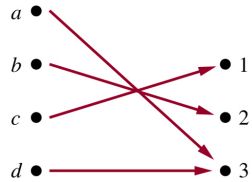
■

**Remark 7** *of course if the function is strictly (increasing/decreasing) it will be injective* $\forall x \forall y \, (x < y \rightarrow f(x) < f(y))$ *, which of course implies $f(x) \neq f(y)$.*

**Definition 147 (Def. 7)** *The function $f : A \to B$ is called onto (or surjective) if $\forall b \in B \; \exists a \in A \; (f(a) = b)$.*

**Example 148 (Ex. 11–12)** *This function is onto*



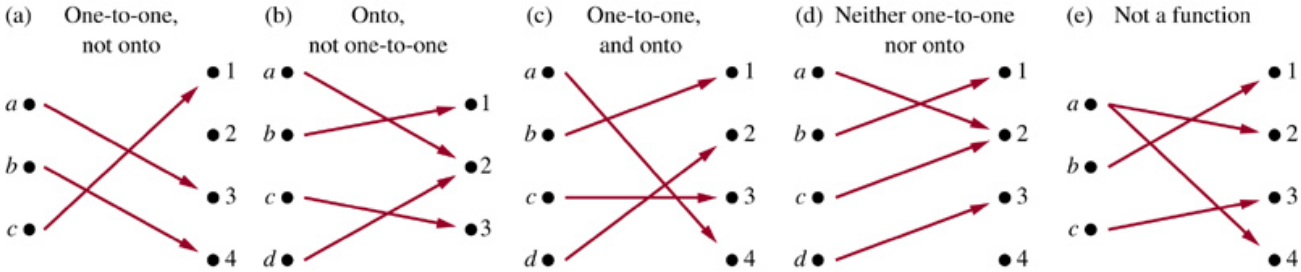



*The function $f(x) = x^2$ both domain and codomain are $\mathbb{R}$, is not onto (e.g., -1 has no pre-image)*

**Definition 149 (Def. 8)** *A function is called one-to-one correspondence (or bijection) if it is both injection and surjection.*

**Example 150 (4 possible combinations between injection-surjection)** *:*





**Example 151 (Prob. 75)** *Let $S$ be a set with $|S| = m$; then there is a bijection between $S$ and the set $\{1, 2, \cdots, m\}$. Show that there is a bijection between $S$ and $T$, where $|T| = m$.*

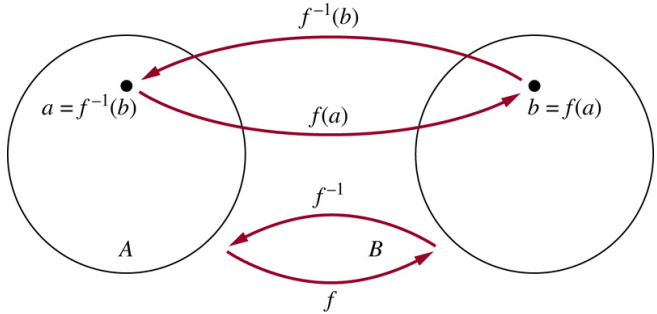
***Proof.*** *$S = \{s_1, s_2, \cdots, s_m\}$; $M = \{1, 2, \cdots, m\}$. Therefore, set $f : S \to M$, $f(s_i) = i,\ i = 1, 2, \cdots, m$*
***Injection:*** *for $s_i \neq s_j$ (which means $i \neq j$), $f(s_i) = i \neq j = f(s_j)$.*
***Surjection:*** *$\forall i \in M\ \exists s_i\ (f(s_i) = i)$; which complete the proof.*

*For $T = \{t_1, t_2, \cdots, t_m\}$, of course similarly, $g(s_i) = t_i$ is a bijection.* ■

### 2.3.3 Inverse Function and Compositions of Functions

**Definition 152 (Def. 9)** *Let $f : A \to B$ be a one-to-one correspondence (bijection);The inverse function of $f$ is the function that assigns to an element $b \in B$ the unique element of $a \in A$, such that $f(a) = b$; we denote $f^{-1}(b) = a$.*






**Remark 8 (Why bijection is necessary for defining inverse function)** *:*

- *if not one-to-one (injection), $f(a_1) = f(a_2) = b$; hence $f^{-1}(b)$ is not a function.*
- *if not onto (surjection), $\exists b \in B$ has no pre-image; hence $f^{-1}(b)$ has no meaning.*
- *Therefore, a bijection is also called invertible.*

**Example 153 (Ex. 17)** *For $f(x) = x+1$, and both the domain and codomain are $\mathbb{R}$; then $f$ is of course, one-to-one and onto; hence invertible:*

$$y = f(x) = x+1$$
$$x = f^{-1}(y) = y-1.$$

**Example 154 (Ex. 18–19)** *Let $f(x) = x^2$*

1. *if the domain and codomain are $\mathbb{R}$ then it is not bijection and hence has no inverse.*
2. *if the domain and codomain are $\mathbb{R}+$ then it is bijection:*
   ***one-to-one**: $f(x_1) = f(x_2) \rightarrow x_1^2 = x_2^2 \rightarrow x_1 = x_2$ (positive domain).*
   ***onto**: $\forall y \in \mathbb{R}+ \;\; y = x^2 \rightarrow x = \sqrt{y}$*
   *and hence invertible:*

$$y = f(x) = x^2$$
$$x = f^{-1}(y) = \sqrt{y} \qquad \text{(positive domain)}$$

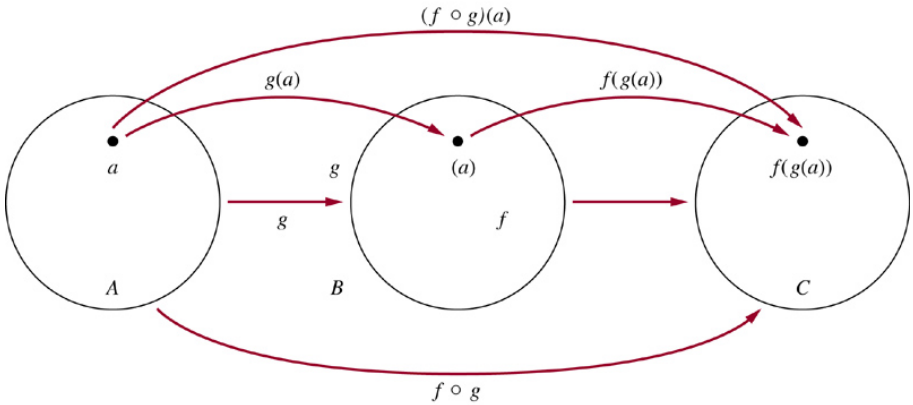
**Definition 155 (Def. 10)** *Consider $g : A \to B$ and $f : B \to C$. The composition of $f$ and $g$, denoted by $f \circ g$, is defined as*

$$(f \circ g)(x) = f\big(g(x)\big)$$

**Remark 9** *of course*

- *the range of $g$ must be a subset of the domain of $f$.*
- $f \circ g \neq g \circ f$.





**Example 156 (Ex. 21)** *Let $f, g : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x + 3$, $g(x) = 3x + 2$; then*

$$(f \circ g)(x) = f\left(g(x)\right) = 2(3x + 2) + 3 = 6x + 7$$
$$(g \circ f)(x) = g\left(f(x)\right) = 3(2x + 3) + 2 = 6x + 11$$

**Remark 10** *The identity function*

$$\iota_A : A \to A,\ \iota(x) = x$$

*is a bijection and is obtained by $f^{-1} \circ f$, $\forall f$*

$$f^{-1}\left(f(a)\right) = a$$
$$f\left(f^{-1}(b)\right) = b$$

### 2.3.4 The Graphs of Functions

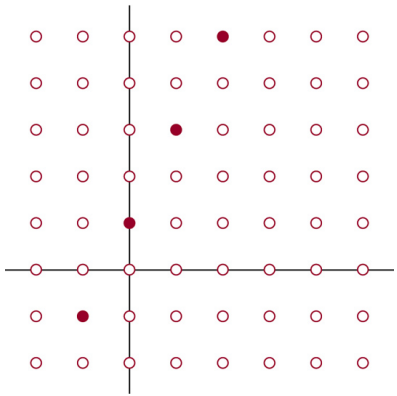
**Definition 157 (Def. 11)** *Consider $f : A \to B$. The graph of the function $f$ is the set of ordered pairs*

$$\{(a,b) \mid a \in A \text{and} f(a) = b\}$$

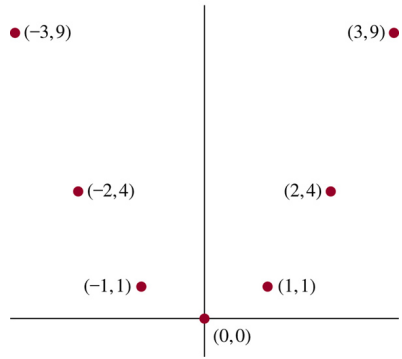
***Hint:*** *It is clear that the graph of $f$ is a subset of the Cartesian product $A \times B$.* ■

**Example 158 (Ex. 22–23)** *The functions $f(n) = 2n+1$ and $f(x) = x^2$ both from $\mathbb{Z}$ to $\mathbb{Z}$:*







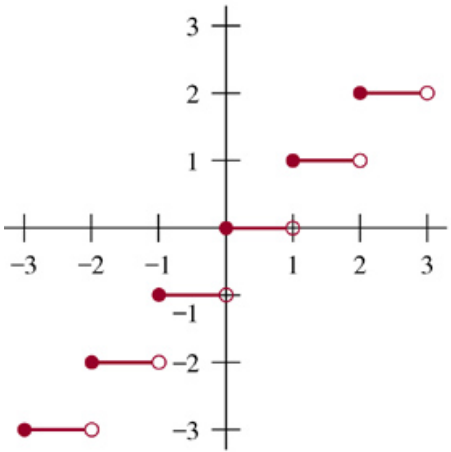


### 2.3.5 Some Important Functions (really important in CS-related proofs)

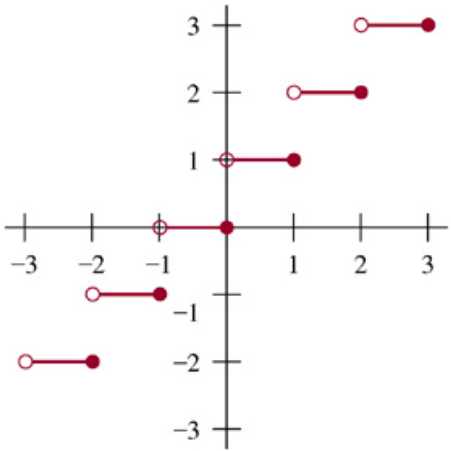
**Definition 159 (Def. 12)** *The floor function ($\lfloor x \rfloor$) assigns to the real number $x$ the* ***largest integer less than or eq***
*to $x$. The ceiling function ($\lceil x \rceil$) assigns the* ***smallest integer larger than or equal*** *to $x$.*
***Equivalent def.*** *We start from the def. of $\lfloor x \rfloor$ and $\lceil x \rceil$ to reach an equivalent def.:*

$$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1 \quad \equiv \quad 0 \le x - \lfloor x \rfloor < 1 \quad \equiv \quad x = \lfloor x \rfloor + \epsilon,\ 0 \le \epsilon < 1$$
$$\lceil x \rceil - 1 < x \le \lceil x \rceil \quad \equiv \quad 0 \le \lceil x \rceil - x < 1 \quad \equiv \quad x = \lceil x \rceil - \epsilon,\ 0 \le \epsilon < 1.$$





(a) $y = [x]$



(b) $y = [x]$

**Example 160 (Ex. 25)** *Min. # of bytes to represent 100 bits is* $\lceil 100/8 \rceil = 13$ *bytes.* ■

**Lemma 161** *More properties (**let's visualize the meaning**):*

**TABLE 1 Useful Properties of the Floor and Ceiling Functions.**
($n$ is an integer, $\boldsymbol{x}$ is a real number)

| | |
|---|---|
| (1a) | $\lfloor x \rfloor = n$ if and only if $n \le x < n+1$ |
| (1b) | $\lceil x \rceil = n$ if and only if $n-1 < x \le n$ |
| (1c) | $\lfloor x \rfloor = n$ if and only if $x-1 < n \le x$ |
| (1d) | $\lceil x \rceil = n$ if and only if $x \le n < x+1$ |
| (2) | $x-1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x+1$ |
| (3a) | $\lfloor -x \rfloor = -\lceil x \rceil$ |
| (3b) | $\lceil -x \rceil = -\lfloor x \rfloor$ |
| (4a) | $\lfloor x+n \rfloor = \lfloor x \rfloor + n$ |
| (4b) | $\lceil x+n \rceil = \lceil x \rceil + n$ |

**Proof. complete proof is left as HW.**

***1.*** From the definition $\big((1a)\ and\ (1c)\big)$; $\big((1b)\ and\ (1d)\big)$

***2.*** $1^{st}$ and $2^{nd}$ ineq (1c); $3^{rd}$ and $4^{th}$ ineq (1d)

***3.*** $\lfloor x \rfloor \le x \le \lceil x \rceil$; then $-\lceil x \rceil \le -x \le -\lfloor x \rfloor$ **done?** We should go as:

$$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1 \qquad \text{(def. of floor)}$$
$$-\lfloor x \rfloor - 1 < -x \le -\lfloor x \rfloor \qquad (2.1)$$
$$\lceil x \rceil - 1 < x \le \lceil x \rceil \qquad \text{(def. of ceiling)}$$
$$-\lceil x \rceil \le -x < -\lceil x \rceil + 1. \qquad (2.2)$$

Eq. (2.1) proves (3b) and Eq. (2.2) proves (3a).

***4.***

$$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1 \qquad \text{(def of floor)}$$
$$(\lfloor x \rfloor + n) \le x + n < (\lfloor x \rfloor + n) + 1 \qquad (2.3)$$
$$\lceil x \rceil - 1 < x \le \lceil x \rceil \qquad \text{(def. of ceiling)}$$
$$(\lceil x \rceil + n) - 1 < x + n \le (\lceil x \rceil + n). \qquad (2.4)$$

Eq. (2.3) proves (4a) and Eq. (2.4) proves (4b).

■

**Example 162 (Ex. 27)** *Prove that* $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.

***Proof. Let's visualize the meaning first (an example for proof by case):***

$$\begin{aligned} x &= n + \epsilon,\ 0 \le \epsilon < 1 \\ \lfloor x \rfloor &= n \\ 2x &= 2n + 2\epsilon \\ x + 1/2 &= n + (\epsilon + 1/2) \end{aligned}$$

***Case 1:*** $0 \le \epsilon < 1/2 \ \equiv\ 0 \le 2\epsilon < 1 \ \equiv\ 1/2 < \epsilon + 1/2 < 1$,
*which leads to:* $\lfloor 2x \rfloor = 2n,\ \lfloor x + 1/2 \rfloor = n$.

***Case 2:*** $1/2 \le \epsilon < 1 \ \equiv\ 1 \le 2\epsilon < 2 \ \equiv 0 \le 2\epsilon - 1 < 1 \equiv\ 0 \le \epsilon - 1/2 < 1/2$

$$\begin{aligned} 2x &= 2n + 2\epsilon \\ &= (2n + 1) + (2\epsilon - 1) \\ \lfloor 2x \rfloor &= 2n + 1 \\ x + 1/2 &= n + (\epsilon + 1/2) \\ &= (n + 1) + (\epsilon - 1/2) \\ \lfloor x + 1/2 \rfloor &= n + 1 \end{aligned}$$

■

**Example 163 (Ex. 28)** *Prove or disprove* $\forall x \forall y\ \lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.
***visualize first****; then a counter example:* $x = y = 0.01$. ■

### 2.3.6 Other important functions

**Definition 164** *The factorial function* $f : \mathbb{N} \to \mathbb{Z}+$, *and denoted by* $f(n) = n!$, *is defined as*

$$n! = \begin{cases} 1 & n = 0 \\ 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n & 1 \leq n \end{cases}$$

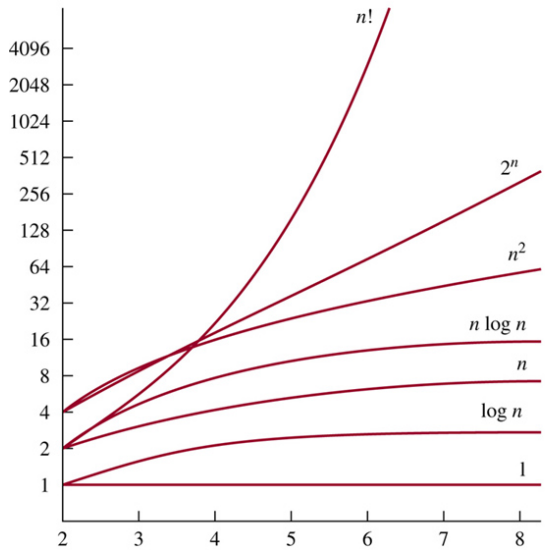
- too rapid (as will be seen in complexity)
- take care in programming (type size):

```
int Factorial(int n){
  for(int product=1; n>=1; n--)
    product*=n;
  return product;
}
```

- Stirling approximate formula:

$$n! \sim \sqrt{2\pi n}(n/e)^n.$$





## 2.4 Sequences and Summations

### 2.4.1 Introduction

- Very important in Mathematics.
- Very important in Computer Science (in particular, analysis of algorithms, data structures, strings, etc.)

### 2.4.2 Sequences

**Definition 165 (Def. 1)** *A sequence is a function from a subset of the set of integers (usually either the set* $\{0,1,2,\cdots\}$ *or the set* $\{1,2,3,\cdots\}$*) to a set S.* $f : \mathbb{N}+ \rightarrow S$

***Notation and Remarks:***

- $a_n = f(n)$*: denotes the image of the integer n; and we call it a term in the sequence.*
- $\{a_n\}$ *: the sequence itself (of course notation abuse; but known from the context).*
- *n is called the index; and domain is discrete.*

■

**Example 166 (Ex. 1)** *The sequence* $\{a_n\}$*, where* $a_n = 1/n$*, is:*

$$a_1, a_2, a_3, \cdots \equiv 1, 1/2, 1/3, \cdots$$

**Definition 167 (Def. 2)** *A geometric progression (series) is the sequence:* $a, ar, ar^2, \cdots, ar^n, \cdots,$ *where the* $a,\ r \in \mathbb{R}$.

**Hint:** of course, it is a discrete analogue to $f(x) = ar^x,\ x \in \mathbb{R}$.

**Example 168 (geometric series examples, Ex. 2)**

| | | |
|---|---|---|
| $b_n = (-1)^n$ | $\{b_n\} = 1,\ -1,\ 1,\ -1,\ \cdots$ | $a = 1,\ r = -1$ |
| $c_n = 2 \cdot 5^n$ | $\{c_n\} = 2,\ 10,\ 50,\ 250,\ \cdots$ | $a = 2,\ r = 5$ |
| $d_n = 6 \cdot (1/3)^n$ | $\{d_n\} = 6,\ 2,\ 2/3,\ 2/9,\ 2/27,\ \cdots$ | $a = 6,\ r = 1/3.$ |

**Definition 169 (Def. 3)** *An arithmetic progression (series) is the sequence:* $a, a+d, a+2d, \cdots, a+nd, \cdots,$ *where,* $a, d \in \mathbb{R}$.

**Example 170 (arithmetic series examples, Ex. 3)**

| | | |
|---|---|---|
| $s_n = -1 + 4n$ | $\{s_n\} = -1,\ 3,\ 7,\ 11,\ \cdots$ | $a = -1,\ d = 4$ |
| $t_n = 7 - 3n$ | $\{t_n\} = 7,\ 4,\ 1,\ -2,\ \cdots$ | $a = 7,\ d = -3$ |

### 2.4.3 Special Integer Sequences (conjecture the rule of the sequence)



- no particular rule of thumb; trial and error, related to pattern recognition.
- theoretically speaking, infinite rules exist to fit a finite initials of a sequence.
- computer SW must help in complicated sequences.

**TABLE 1 Some Useful Sequences.**

| *nth Term* | *First 10 Terms* |
|---|---|
| $n^2$ | 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, . . . |
| $n^3$ | 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, . . . |
| $n^4$ | 1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, . . . |
| $2^n$ | 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, . . . |
| $3^n$ | 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, . . . |
| $n!$ | 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, . . . |

**Example 171 (Ex. 5–8)**

$1, 1/2, 1/4, 1/8, \cdots$ $\quad a_n = 1/2^n = (1)(1/2)^n$ (geometric)

$5, 11, 17, 23, 29, \cdots$ $\quad a_n = 5+6n$ (arithmatic)

$1, 2, 2, 3, 3, 3, 4, 4, 4, 4, \cdots$ (HW. write it in closed form)

**index transformation (C language as example):**

$a_n$, $n = 0, 1, 2, \cdots$, we can substitute $m = n+1$ (then $m = 1, 2, 3, \cdots$). E.g.,

$$a_n = 5+6n,\ n = 0, 1, 2, \cdots \equiv a_m = 5+6(m-1) = -1+6m,\ m = 1, 2, 3, \cdots$$

### 2.4.4 Summations

#### 2.4.4.1 Notations and Basics

Consider the sequence: $a_0,\ a_1,\ a_2,\ \cdots,\ a_m\ \cdots,\ a_n,\ \cdots,\ a_p$

$$a_m + a_{m+1} + a_{m+2} + \cdots + a_n = \sum_{j=m}^{n} a_j = \sum_{m \le i \le n} a_i$$

```
s=0;
for(int i=m; i <= n; i++)
   s+= a[i];
```

**Lemma 172** *Consider* $\{x_n\}$, $\{y_n\}$; *then*

$$\sum_{i=m}^{n} (ax_i + by_i) = a \sum_{i=m}^{n} x_i + b \sum_{i=m}^{n} y_i.$$

**Proof.** is immediate by commutative and associative laws.

$$\sum_{i=m}^{n} (ax_i + by_i) = (ax_m + by_m) + \cdots + (ax_n + by_n) = (ax_m + \cdots + ax_n) + (by_m + \cdots + by_n) = a \sum_{i=m}^{n} x_i + b \sum_{i=m}^{n} y_i.$$

■

**Example 173 (Ex. 9)** $a_n = 1/n,\ n = 1,\ 2,\ \cdots \qquad \sum_{j=10}^{100} a_j = \sum_{j=10}^{100} \frac{1}{j}$

```
sage: j=var('j')
sage: sum(1/j, j, 10, 100)
32885835761679513760951913715533243583283 /
   1394407504594249543290676178706246071136 0
```

**Theorem 174 (summation of geometric series, Thm. 1)** *If $a,\ r \in \mathbb{R},\ r \neq 0$, then*

$$a + ar + ar^2 + \cdots + ar^n = \sum_{j=0}^{n} ar^j = \begin{cases} \frac{ar^{n+1}-a}{r-1} & \texttt{if } r \neq 1 \\ (n+1)a & \texttt{if } r = 1. \end{cases}$$

**Proof.** Set $S = \sum_{j=0}^{n} ar^j$. If $r = 1$, then clearly $S = \sum_{j=0}^{n} a = a(n+1)$. If $r \neq 1$, then

$$\begin{aligned} rS &= \sum_{j=0}^{n} ar^{j+1} \\ &= \sum_{k=1}^{n+1} ar^k \\ &= \sum_{k=0}^{n} ar^k - a + ar^{n+1} \\ &= S + (ar^{n+1} - a) \\ S &= \frac{ar^{n+1} - a}{r-1}. \end{aligned} \qquad (r \neq 1)$$

■

**Example 175 (Another good example for rigorous treatment)** *Find $\sum_{i=0}^{n}(-1)^i$ and $\sum_{i=0}^{\infty}(-1)^i$*

$$\sum_{i=0}^{n}(-1)^i = \frac{(1)(-1)^{n+1}-1}{(-1)-1} = \frac{(-1)^{n+1}-1}{-2} = -1 = \begin{cases} 0 & n \texttt{ is odd} \\ 1 & n \texttt{ is even.} \end{cases}$$

$$\sum_{i=0}^{\infty}(-1)^i = 1 + (-1) + 1 + (-1) + \cdots = 0 \qquad \text{(What do you think?)}$$

**Example 176 (Ex. 13)**

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij = \sum_{i=1}^{4}(i+2i+3i) = \sum_{i=1}^{4} 6i = 6+12+18+24 = 60.$$

```
sage: i, j= var('i, j')
sage: sum(sum(i*j, j, 1, 3), i, 1, 4)
60
```

```
s=0;
for(int i=1; i <= 4; i++)
   for(int j=1; j <= 3; j++)
      s+= i*j;
```

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij = \sum_{j=1}^{3} ij\Big|_{i=1} + \sum_{j=1}^{3} ij\Big|_{i=2} + \sum_{j=1}^{3} ij\Big|_{i=3} + \sum_{j=1}^{3} ij\Big|_{i=4} = \sum_{j=1}^{3} j + \sum_{j=1}^{3} 2j + \sum_{j=1}^{3} 3j + \sum_{j=1}^{3} 4j.$$

**Of course:** for finite limits:

$$\sum_i \sum_j = \sum_j \sum_i$$

**Notation:**

$$\sum_{n\in\{0,\,2,\,4\}} a_n = a_o + a_2 + a_4.$$

**TABLE 2** Some Useful Summation Formulae.

| *Sum* | *Closed Form* |
|---|---|
| $\sum_{k=0}^{n} ar^k \ (r \neq 0)$ | $\frac{ar^{n+1}-a}{r-1}, r \neq 1$ |
| $\sum_{k=1}^{n} k$ | $\frac{n(n+1)}{2}$ |
| $\sum_{k=1}^{n} k^2$ | $\frac{n(n+1)(2n+1)}{6}$ |
| $\sum_{k=1}^{n} k^3$ | $\frac{n^2(n+1)^2}{4}$ |
| $\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$ | $\frac{1}{1-x}$ |
| $\sum_{k=1}^{\infty}, kx^{k-1}, \lvert x\rvert < 1$ | $\frac{1}{(1-x)^2}$ |



**Example 177 (Ex. 15)**

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2$$
$$= \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6}$$
$$= 338,350 - 40425 = 297925.$$

**Example 178 (Ex. 16)**

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}, \quad x \neq 1$$
$$\sum_{k=0}^{\infty} x^k = \lim_{n\to\infty} \frac{x^{n+1}-1}{x-1} = \frac{1}{1-x}, \quad |x| < 1$$

### 2.4.5 Cardinality

- We had defined the Cardinality of a finite set to be the number of its elements.
- Then, we had proven that (Ex. 151, Prob. 75) there is a bijection between two finite sets with same cardinality. With almost the same trivial proof we can show immediately that:

  **Corollary 179** *If there is a bijection between two finite sets, then they have the same cardinality.* ■

- Can we generalize the definition to include infinite sets by saying:

  **Definition 180 (Def. 4)** *To sets $A$, $B$ have the same cardinality if there is a bijection from $A$ to $B$.* ■

- exactly as we have done in the length of $p$-dimensional vector:

$$\|X\| = \sum_{i=1}^{p} x_i^2,\ p = 1,2,3 \qquad \text{(this is a proof)}$$

$$\|X\| = \sum_{i=1}^{p} x_i^2,\ p = 1,2,3,\cdots. \qquad \text{(this is a definition)}$$

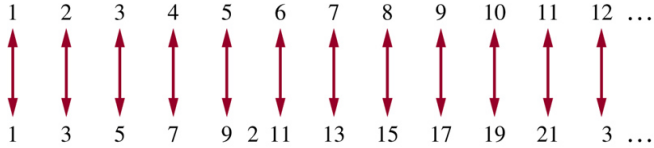
- But if they are infinite, how they do not have the same cardinality? How $\infty \neq \infty$

  **Example 181** *Two line segments, $x$, $2x$; $f(x) = 2x$ (this is a bijection)*

**Definition 182 (Def. 5)** *A set that is either finite or has the same cardinality as the set of positive integers is called **countable**. A set that is not countable is called **uncountable**. When an infinite set $S$ is countable, we say $|S| = \aleph_0$ (aleph null).*
***Hint:*** *think of $|\mathbb{Z}+| = \aleph_0$ as the smallest $\infty$.* ■

**Example 183 (Ex. 18)** *Show that the set of odd positive integers is a countable set.*






*Then* $f(n) = 2n-1 : \mathbb{Z}+ \to \{1, 3, 5, \cdots\}$ *is the required bijection.*
***Injection:*** $f(n) = f(m) \to 2n-1 = 2m-1 \to n = m$
***Onto:*** *Suppose that* $t$ *is an odd integer in the range, then* $t = 2n-1$ *and* $\exists n = (t+1)/2$ *in the domain* ■

**Remark 11** *The bijection* $f : \mathbb{Z}+ \to S$ *is established if we can list the elements of* $S$ *in a sequence indexed by the positive integers* ($a_n = f(n)$). *This makes it easier to find the bijection if the closed from is difficult.*

**Example 184 (Ex. 19)** *Show that the set of all integers is countable.*

$$\begin{array}{ccccccc} & 1 & 2 & 3 & 4 & \cdots \\ 0 & & & & & \\ & -1 & -2 & -3 & -4 & \cdots \end{array}$$

This listing is equivalent to mapping even to positive numbers and odd to negative numbers.

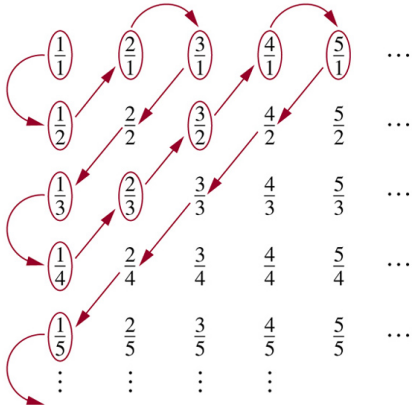
$$a_n = \begin{cases} n/2 & n = 2, 4, 6, \cdots \\ -(n-1)/2 & n = 1, 3, 5, \cdots . \end{cases} \qquad n = \begin{cases} 2t & t > 0 \\ -2t+1 & t \le 0. \end{cases}$$

It is clear that $a_n = a_m \to n = m$, then one-to-one; and every $t$ has a pre-image $n$, then onto.

**Example 185 (Ex. 20)** *Show that the set of positive rational numbers is countable.*



Terms not circled are not listed because they repeat previously listed terms



■

**Example 186 (Ex. 21)** *Show that the set or real numbers is uncountable !!*
*(the $\infty$ of $\mathbb{R}$ is too dense w.r.t. the $\infty$ of $\mathbb{Z}+$; hence, there is no one-to-one correspondence.)*

**Sketch of Proof.**

$$r_1 = 0.d_{11}d_{12}d_{13}\cdots$$
$$r_2 = 0.d_{21}d_{22}d_{23}\cdots$$
$$r_3 = 0.d_{31}d_{32}d_{33}\cdots$$
$$\vdots$$

Construct a new real number: $0.d_1d_2d_3\cdots$ ■

# Philosophical Issues: common fallacies in reasoning

***1.*** **Life, Reasoning, and Predicates**
Our life is almost predicates; however the variable, almost, is omitted that casts it as a proposition. Here contradiction may apparently arise while it is not. **Example**
$P$ : "students are not allowed to talk"
$Q$ : "students are allowed to talk"
**In fact:** it could be $P(t)$ and $Q(t)$ where $t$ is time, status, condition, etc.

***2.*** **In Definitions, "if and only if", Is Redundant.**
**Definition** The integer $n$ is even *if and only if* there exists an integer $k$ such that $n = 2k$. ■

***3.*** **Logic: Stochastic or Deterministic?**
"If you study you pass" (in general; it is stochastic)

***4.*** **Binary vs. Continuous Logic**
Things are not binary/Boolean (True or False) things usually span a continuum.
$P$ : "He is clever"
In fact, his cleverness is continuous (how much is he clever?)

***5.*** **Hidden Assumptions**
"Isn't accepting this deal better than being poor?"
**Wrong assumption 1:** Things are superfluously binary
**Wrong assumption 2:** "Not accepting this deal" ≡ or → "being poor"

# Bibliography

Rosen, K. H., 2007. Discrete mathematics and its applications, 6th Edition. McGraw-Hill Higher Education, Boston.
URL http://www.loc.gov/catdir/toc/ecip0612/2006012468.htmlhttp://www.loc.gov/catdir/enhancements/fy0702/2006012468-d.htmlhttp://www.loc.gov/catdir/enhancements/fy0737/2006012468-b.html