a	b	and
0	1	0
1	1	1

Slidebook on Discrete Mathematics

$\leftrightarrow$

Masud Hasan

$\forall$ $\exists$

Version: 03-05-2021

Preface

<u>In the name of Allah, The Most Merciful, The Most Beneficent</u>

<u>All praises and all achievements are due to Him</u>

Slidebook can be a new concept, where pages are more in content than traditional lecture slides and are written in a little informal way. A slidebook is more like how an instructor would deliver his/her lectures for a course as well as how a student would take notes while s/he attends the lectures. It is more in content than lecture slides, but less than a textbook. Still, pages of a slidebook can be projected as slides by the instructor, which can reduce the extra effort required by an instructor to prepare lecture slides based on some textbooks.

A slidebook is prepared by looking at some well-known textbooks of the current time. Students are strongly encouraged to look into those textbooks in addition to the slidebook for more examples and exercises, and for more content on the topics. For this slidebook, a list of textbooks are given at the end, and a mapping of its lectures with sections of the textbook of Ref. [1] is provided on the website of this slidebook in Ref. [8].

The content of this slidebook can be suitable for a one-semester first course on discrete mathematics for undergraduate students in computer science and related discipline. The level of difficulty in the content and exercises are medium.

In this slidebook, almost every slide contains examples, and exercises are putted just after the relevant examples, instead of putting them together in batches by sections. Most of the slides contain a sticky note highlighting the important notes related to the slide content and that can be recalled for better understanding of the slide content. Figures and tables are also pushed to the right side as much as possible.

A website in Ref. [8] contains additional information and content about this slidebook.

Table of Content

Lecture 1
Introduction and Preliminaries

And your god is the One God (Allah) … (Quran 2:163)

Lectures/Topics

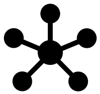
1. Introduction and Preliminaries
2. Logic (Propositional Logic)
3. Implication and Bi-conditional
4. Logical Equivalences
5. Predicates and Quantifiers
6. Rules of Inference
7. Sets
8. Relations and Functions
9. Induction and Recursion
10. Counting
11. Probability
12. Graphs and Trees

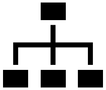
- **Exercise:**
- Have you heard any of these terms (from 2 to 12) before in your earlier (high school, diploma) studies?
- Can you imagine how these terms can be related to mathematics, science, computer science, engineering, medical science, humanities, or some other discipline?

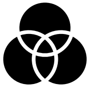
Motivation

- What is the meaning of “discrete”?
- **Answer:** Different, independents, separate, not of same type
- So, what is “discrete mathematics”?
- **Answer:** Mathematical topics that are different, independent, separate, not of same type
- Why do we learn different mathematical topics?
- **Answer:** Because, computer science and related disciplines use these different topics at different places
- Discrete mathematics is also called **discrete structures**

a	b	and
0	1	0
1	1	1







Some Warmup Preliminaries

- Before we go to the main topics, we need to recall some simple mathematical preliminaries from our school life
- In some preliminaries, we shall use the terms “correct” and “wrong” instead of “true” and “false”
- Because we were not used to in “true” or “false” before
- **> and ≥:** If $a > b$ is correct, then $a \geq b$ is also correct
- **Example:** $7 > 5$ is correct, so $7 \geq 5$ is correct
- If $a \geq b$ is correct, then $a > b$ may not be correct, because it may happen that $a = b$
- **Example:** $5 \geq 5$ is correct, but $5 > 5$ is not correct
- **Exercise:** Repeat the above examples for < and ≤
- **Exercise:** Repeat the examples for fractions (7.3, 3.9, …)

≥ is > or =

one OK, OK

≤ is < or =

one OK, OK

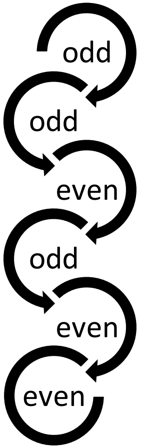
<, -, and Inverse

- If a < b is correct, then -a > -b is correct, -a < -b is wrong
- **Example:** 3 < 4 is correct, so -3 > -4 is correct, but -3 < -4 is wrong
- **Inverse** of x is $\frac{1}{x}$
- If a < b is correct, then (inverse of a) > (inverse of b) is correct, that means, $\frac{1}{a} > \frac{1}{b}$ is correct
- **Example:** -5 < -2 is correct, so, $\frac{1}{-5} > \frac{1}{-2}$. This is -0.2>-0.5
- **Exercise:** If a < b is correct, then $\frac{1}{-a} ? \frac{1}{-b}$ is correct. What is "?" here? Is it ">" or "<"?
- **Exercise:** Repeat everything above with >, -, and inverse

(-big) is small
(-small) is big
1/big is small
1/small is big

Odd, Even Integers

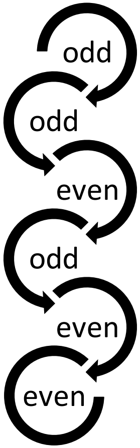
- **Integer** means whole number, such as 2, 5, 0, -3, -1, etc. (not fractions like 3.7, 0.11, -21.19, -7.3, etc.)
- **Odd** means odd integer and **even** means even integer
- 0 is even
- 1, 3, 5, …, -1, -3, -5, … are odd
- 0, 2, 4, 6, …, -2, -4, -6, … are even
- odd + 1 = even
- odd – 1 = even
- even + 1 = odd
- even -1 = odd
- **Exercise:** Odd + 2 = odd or even?
- **Exercise:** Even – 2 = odd or even?



Odd-even relations can be tricky

Odd, Even Integers

- odd + odd = ~~odd~~ even. **Example:** 5 + 3 = 8
- even + even = even. **Exercise:** Find some examples
- even + odd = odd. **Example:** 4 + 3 = 7
- odd – odd = ~~odd~~ even. **Example:** (-7) - (-3) = -4
- even – even = even. **Exercise:** Find some examples
- even – odd = odd. **Exercise:** Find some examples
- odd – even = odd. **Example:** (-7) - 2 = -9
- **Exercise:**
  - – odd – odd = even or odd? Show some examples
  - – even – even = even or odd? Show some examples
  - odd + odd + odd = ? Why? Show examples
  - – even – even – even = ? Why? Show examples



Odd-even relations can be tricky

Odd, Even Integers

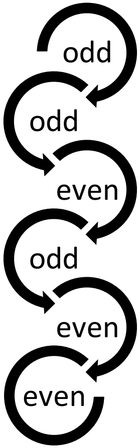
- Even = 2k   // for some integer k. k may be even or odd
- **Example:** 8 = 2*4, 10 = 2*5
- odd = 2k + 1 // for some integer k. k may be even or odd
- **Example:** 9=2*4+1, 11=2*5+1
- **Exercise:**
  - 2k-1 is even or odd? Why?
  - Try some examples of 2k-1
  - Can there be any other formula (instead of 2k and 2k+1) to represent odd and even?
  - $\frac{\text{odd}+\text{odd}}{2}$ = odd or even? Try some examples
  - What about $\frac{\text{even}+\text{even}}{2}$ and $\frac{\text{even}+\text{odd}}{2}$?

odd = 2k+1

even = 2k

Odd, Even Integers

- odd * odd = odd. **Example:** 5*3 = 15
- even * even = even **Example:** 8*2 = 16
- odd * even = even. **Example:** 5*(-2) = -10
- even/2 = may be even, may be odd!
- **Example:** 10/2 = 5, 12/2 = 6
- $(\text{even or odd})^0 = 1 = \text{odd}$
- $(\text{even})^{\text{positive even}} = \text{even}$. **Example:** $4^2 = 16$
- $(\text{even})^{\text{positive odd}} = \text{even}$. **Example:** $4^3 = 64$
- $(\text{odd})^{\text{positive even or positive odd}} = \text{odd}$. **Example:** $3^2 = 9$, $3^3 = 27$
- **Exercise:** $(-\text{odd})^{\text{positive even or positive odd}}$ = even or odd? Try some examples
- **Exercise:** What about $(-\text{even})^{\text{positive even or positive odd}}$?



Odd-even relations can be tricky

At least

- “At least” means same or more (more means bigger by value)
- **Example:** “At least 12” means 12 or more
  - So, 12 is at least 12
  - 13.5, 12.01, 1000, etc. are at least 12
  - But, less that 12 is not at least 12
  - So, 11, 11.99, -5, 2, etc. are not at least 12
- **Example:** “At least -4” means -4 or more
  - So, -4, -3.5, -2.1, 0, 4, etc. are at least -4
  - But, -4.01, -5, -100, -5.3, etc. are not at least -4
- **Exercise:** Find some values for “at least 0”
- **Exercise:** At least -4 is also at least -10. Why?

at least

=

same or more

At most

- "At most" means same or less (less means smaller by value)
- **Example:** "At most 12" means 12 or less
  - So, 12 is at most 12
  - 11, 11.99, -5, 2, etc. are at most 12
  - But, more that 12 is not at most 12
  - So, 13.5, 12.01, 1000, etc. are not at most 12
- **Example:** "At most -4" means -4 or less
  - So, -4, -4.01, -5, -100, -5.3, etc. are at most -4
  - But, -3.5, 0, 4, etc. are not at most -4
- **Exercise:** Find some values for "at most 0"
- **Exercise:** Find a value that is at most 10 and at least -5

at most

=

same or less

Non-negative, Non-positive

- 0 is not positive, not negative
- There is nothing like -0. Actually, -0 means 0
- "Non-negative" means 0 or positive
- So, "non-negative" and "at least 0" are same
- **Example:** 2, 4, 0, 9, 1 are some non-negative integers
- **Example:** 2.5, 4, 0, 0.1, 1 are some non-negative numbers
- "Non-positive" means 0 or negative
- So, "non-positive" and "at most 0" are same
- **Example:** -2, -4, 0, -9, -1 are some non-positive integers
- **Example:** -4, -0.01, -1.1, -1, 0 are some non-positive numbers

non-negative

=

zero or more

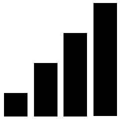
non-positive

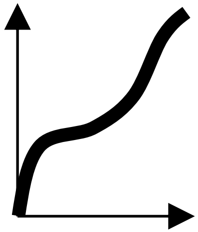
=

zero or less

Increasing

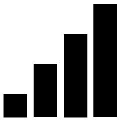
- The term "increasing" usually come with "sequence"
- "Increasing sequence" means left to right values are always bigger (same not allowed)
- **Example:** 12, 13, 23, 26, 101, … is an increasing sequence
- **Example:** 12, 13, 13, 12, 26, 26, 81, 31, … is not an increasing sequence because 13 after 13 and 31 after 81
- **Example:** Right side example (up) has increasing values with same increase speed (rate)
- **Example:** Right side example (below) is an increasing curve with different increasing speed at different places
- **Exercise:** Can you find some real-life examples of increasing sequence?

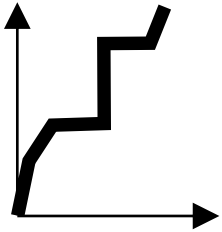




Non-decreasing

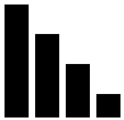
- "Non-decreasing sequence" means left to right values are same or bigger
- Increasing sequence is also non-decreasing
- **Example:** 5, 9, 14, 14, 17, 20, 20, 20, 23, 99, … is a non-decreasing sequence
- **Example:** 5, 9, 14, 16, 17, 18, 21, 25, 33, 99, … is a non-decreasing as well as an increasing sequence
- **Example:** 5, 9, 14, 16, 17, 18, 21, 20, 33, 99, … is not a non-decreasing sequence because of 20 after 21
- **Example:** See right-side pictures for more examples
- **Exercise:** Can you find some real-life examples of non-decreasing sequence?

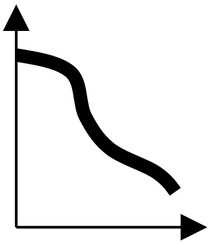




Decreasing

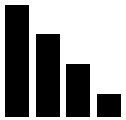
- “Decreasing sequence” means left to right values are always smaller (same not allowed)
- **Example:** 101, 26, 23, 13, 12 … is a decreasing sequence
- **Example:** 81, 65, 42, 26, 26, 19, 10, 12, … is not a decreasing sequence because 26 after 26 and 12 after 10
- **Example:** Right side example (up) has decreasing values with same decreasing speed (rate)
- **Example:** Right side example (below) is a decreasing curve with different decreasing speed
- **Exercise:** Repeat the above examples with both positive and negative values mixed together and draw the right-side curves accordingly?

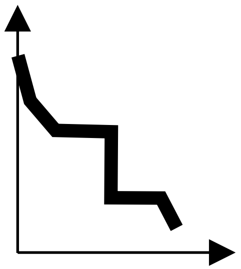




Non-increasing

- "Non-increasing sequence" means left to right values are same or less
- Decreasing sequence is also non-increasing
- **Example:** 99, 23, 20, 20, 20, 17, 14, 14, 9, 5, … is a non-increasing sequence
- **Example:** 99, 33, 25, 21, 18, 17, 16, 13, 9, 5, … is a non-increasing as well as a decreasing sequence
- **Example:** 99, 33, 20, 21, 18, 17, 16, 14, 9, 5, … is not a non-increasing sequence because 21 after 20
- **Exercise:** Can you repeat the above examples with negative and positive values mixed together and then redraw the right-side curves again?





Real Numbers

- A **rational** number can be represented by the fraction (ratio) of two integers as p/q, where q is non-zero
- **Example:** 1.5 (same as 3/2), 0.25 (same as 1/4), 22/7, etc. So, 1.5, 0.25, 22/7 are rational numbers
- An **irrational** number is a number that cannot be represented by a ratio of two integers
- **Example:** π (which is 3.14159…), $\sqrt{2}$ (which is 1.4142…)
- **Real** numbers include integers, rational and irrational numbers
- **Example:** 4/3, 5.8, $\sqrt{3}$, 13, 42, *e* (which is 2.71828…) are all real numbers
- **Exercise:** Find some other uncommon real numbers

Real:
Integer
Rational
Irrational

Binary Numbers

- The numbers that we usually see and use are **decimal**, such as 0, 1, 2, 3, 4, …, 9, 10, 11, …, 99, 100, 101, …
- Decimal numbers are composed of ten digits: 0,1,2,…,9
- In contrast, **binary** number has only two digits, 0 and 1
- **Example:**
  - 10011 is a binary number
  - 10023 is not a binary number as it has digits 2, 3
  - Observe that 10011 is also a decimal number, but its values in binary and decimal are different
- Binary numbers are mentioned by number of digits
- Leading digits are filled with 0 (see next slide …)
- **Exercise:** How many digits will be in ternary numbers?

Decimal digits: 0,1,2,…,9

Binary digits: 0 and 1

Binary Numbers Examples

- There is only two 1-digit binary numbers: 0 and 1
- Four 2-digits binary numbers are: 00, 01, 10, 11
    - Observe that, number after 01 is 10
    - This is like 10 after 09 in decimal
- 3-digits binary numbers are: 000, 001, 010, 011, 100, 101, 110, 111
    - Again, 100 after 011 is like 100 after 99 in decimal
- Binary numbers have equivalent decimal values
- For example: 00, 01, 10, 11 are equivalent to 0, 1, 2, 3
- Similarly, decimal value of 3-digits binary numbers are
- **Exercise:** Write 4-digit binary and equivalent decimal numbers

Binary	Decimal
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

Absolute Value

- **Absolute value** of a number is its value without sign
- So, if the sign is + (that means nothing), then the absolute value is the number itself
- But if the sign is -, then the absolute value is the number without the - sign
- It is denoted by two bars | | in the left and right sides of the number
- **Example:**
  - |-5| = 5
  - |5| = 5
  - |-23.75| = 23.75
  - |0| = 0

Absolute value means value without sign

Equality, Inequality

- **Equality** is another name of mathematical equation
- **Example:** Following expressions are equalities
  - $x+y = 5$
  - $(a+b)^2 - (a-b)^2 = 4ab$
- **Inequality** means if the expression has no “=“. Instead, it has $<$, $\neq$, $>$, $\geq$, $\leq$ etc.
- **Example:** The followings are inequalities
  - $x+y < 5$
  - $(a+b)^2 - (a-b)^2 \neq 4ab$
  - $a \geq c$
- Although $\geq$ and $\leq$ have “=“ within them, they are still inequalities

Equality: =

Inequality:
$< \; > \; \neq \; \geq \; \leq$

Factorial n (n!)

- **Factorial** of a non-negative integer n (written as n!) is:
  - $0! = 1$
  - If $n \geq 1$, then $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$
- **Example:**
  - $0! = 1$
  - $1! = 1$
  - $2! = 2 \cdot 1 = 2$
  - $3! = 3 \cdot 2 \cdot 1 = 6$
  - $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$
- For $n \geq 1$, $n!$ can also be written as $n \cdot (n-1)!$
- **Example:** $4! = 4 \cdot (4-1)! = 4 \cdot 3! = 4 \cdot 6 = 24$
- **Exercise:** Find 5!, 6!, 7!

$0! = 1$

$1! = 1$

$n! = n(n-1)! = n(n-1) \ldots 3 \cdot 2 \cdot 1$

log

- Definition of **log** is this: If $a^x = y$, then $x = \log_a y$
- **Example:**
  - $\log_{10}(1000) = 3$, because $10^3 = 1000$. Here, a=10, x=3, and y=1000
  - $\log_2 64 = 6$, because $2^6 = 64$. **Exercise:** Find a, x, y here
- Some **common formula** for log (here a, b, c > 0):
  - $\log_a a = 1$
  - $b^{\log_b a} = a$
  - $\log_a b^n = n\log_a b$
  - $\log_a(bc) = \log_a b + \log_a c$
  - $\log_a(1/b) = -\log_a b$
  - Next here
  - $\log_a b = \frac{\log_c b}{\log_c a}$
  - $\log_a b = \frac{1}{\log_b a}$
  - $a^{\log_b c} = c^{\log_b a}$

If $a^x = y$, then $x = \log_a y$

log

- Some examples of these formulas are given below:
- $\log_5 5 = 1$
- $2^{\log_2 9} = 9$
- $\log_{10} 5^2 = 2\log_{10} 5$
- $\log_2(63 * 45) = \log_2 63 + \log_2 45$
- $\log_e(1/9) = -\log_e 9$
- $\log_e 19 = \frac{\log_2 19}{\log_2 e}$
- $\log_3 9 = \frac{1}{\log_9 3}$
- $3^{\log_5 7} = 7^{\log_5 3}$
- **Exercise:** Find the value of $\log_2(4096)$
- **Exercise:** Find the value of $\log_2(0.125)$

If $a^x = y$,
then
$x = \log_a y$

ceil ($\lceil\ \rceil$) and floor ($\lfloor\ \rfloor$)

- Ceil of a number (integer or fraction) is denoted as $\lceil$number$\rceil$
- It is computed as follows:
  - $\lceil k \rceil$ = k, if k is an integer
  - $\lceil k \rceil$ = integer immediately bigger than k, if k is a fraction
- **Example:**
  - $\lceil 1.99 \rceil = 2$
  - $\lceil 3 \rceil = 3$
  - $\lceil 5.0 \rceil = 5$
  - $\lceil 19.000001 \rceil = 20$
- **Exercise:** Find $\lceil 0.99 \rceil$, $\lceil 0 \rceil$, $\lceil 3/2 \rceil$, $\lceil 0.0001 \rceil$

$\lceil k \rceil$ = k, if k integer
$\lceil k \rceil$ = next integer, if k fraction

ceil ($\lceil\ \rceil$) and floor ($\lfloor\ \rfloor$)

- Floor of a number (integer or fraction) is denoted as $\lfloor$number$\rfloor$
- It is computed as follows:
  - $\lfloor k \rfloor$ = k, if k is an integer
  - $\lfloor k \rfloor$ = integer immediately smaller than k, if k is a fraction. That means, just delete the fractional part
- **Example:**
  - $\lfloor 1.99 \rfloor = 1$
  - $\lfloor 3 \rfloor = 3$
  - $\lfloor 5.0 \rfloor = 5$
  - $\lfloor 19.000001 \rfloor = 19$
- **Exercise:** Find $\lfloor 0.99 \rfloor$, $\lfloor 0 \rfloor$, $\lfloor 3/2 \rfloor$, $\lfloor 0.0001 \rfloor$

$\lfloor k \rfloor$ = k, if k integer
$\lfloor k \rfloor$ = previous integer, if k fraction

mod (%)

- **mod** (also called **modulus**) of two integers **a mod b** is the remainder after a is divided by b
- It is also written as **a % b**
- **Example:**
  - 5 mod 3 = 2
  - 21 mod 9 = 3
  - 15 % 15 = 0
  - 0 mod 3 = 0
  - 77 mod 6 = 5
  - (any even integer) % 2 = 0
  - (any odd integer) % 2 = 1
- **Exercise:** Find 21 % 7, 33 % 9, 45 mod 7, 100 mod 10

mod means remainder

Lecture 2
Propositional Logic

Had there been within the heavens and earth gods besides Allah, they both would have been ruined. … (Quran 21:22)

Motivation

- Suppose that your final marks in this course is 80%
- You told your marks to your friend
- Then you asked your friend, what is his marks?
- He got 95% and was little shy to tell you that because he got much higher marks than you
- So he said, **at least** 80%
- Is your friend saying **truth** or **false**?
- Remember from Lecture 1, "at least" means same **or** more (≥)
- So, he is actually telling the truth, because 95% ≥ 80%
- This is a very simple example of **propositional logic**

95% is
at least 80% ✓

Proposition

- **Proposition** is a statement that is either true or false (not both) at the **time** when the statement is made
- "True" and "false" are called **truth values**
- Note that, "false" is also a truth value
- **Example:** The statement "2 - 2 = 0" is a proposition, because its truth value is true
- **Example:** "4 + 3 = -7" is a proposition with truth value false
- **Example:** "4 + x = 9" is not a proposition, because we do not know the value of x. Based on x, it may be true or false
- **Example:** Similarly, "x + y = z" is not a proposition

truth values are "true", "false"

Proposition

- **Example:**
  - "Today is Friday" is a proposition
  - Because, its truth value is either true or false
  - The truth value will be decided by the **moment/time** the statement is made
  - If it is made in a Friday, then it is true
  - If it is made in another day, then it is false
- Observe that, this example is different from the example "x+4=9" in the previous slide
- Because, in this example, "today" is not like x. Unlike x, "today" cannot have different values at a moment

Proposition?

- *Today is Friday* ✓
- $x+4 = 9$ ✗

Proposition

- **Example:**
  - "Solve this problem" is not a proposition
  - Because, it does not have any truth value
  - It is an order or instruction
  - It can have an outcome, such as
    - the problem is solved
    - the problem was tried but not finished
    - do nothing, just ignore the order
    - etc.
  - true or false is not a value of this statement
  - Actually, truth value is meaningless for this statement

Proposition?

- *Do this job* ✗
- *I did this job* ✓
- *Don't do this* ✗
- *He did this* ✓

Proposition

Proposition?

- How is he? ×
- He is fine ✓
- Who is he? ×
- He is Osman ✓

- **Example:**
  - "What is your name?" is not a proposition
  - Because, it is a question
  - It has an answer, but it does not have a truth value
  - The answer can be like this: "My name is Azad"
  - True or false cannot be a value of this question
  - Observe that (similarly in the previous example)
    - The answer "My name is Azad" can itself be true or false
    - So, "My name is Azad" has a truth value
    - But that does not give a truth value of the original question "What is your name?"

Proposition

- **Exercise:** For each of the following statement, decide whether it is a proposition or not. Give reason (why?) of your answer
  - $5 + 0 = 5$
  - My name is not Mubarak
  - Where do you live?
  - $4 + x > x$
  - Hasan and Hossain are brothers
- **Exercise:** It is difficult to decide whether the following statements are proposition or not. You can try yourself
  - I am not saying the truth
  - This statement is false

Proposition?

- *He is tall*
- *$x+4 > x$*
- *He is lying*

Compound Propositions

- So far, we have seen a single statement which may be a proposition or not
- However, most of the time logical statements are combination of one or more propositions with **logical operators**
- Those statements are called **compound propositions**
- There are five basic logical operators:
  - not ($\neg$)
  - and ($\wedge$)
  - or ($\vee$)
  - Implication ($\rightarrow$)
  - Bi-conditional ($\leftrightarrow$)

This lecture

Involved. So, a separate lecture

$\neg$

$\wedge$

$\vee$

$\rightarrow$

$\leftrightarrow$

Not ($\neg$)

- **Not** means negative, negation, opposite
- Its symbol is $\neg$
- It makes true to false, and false to true
- $\neg$P and "not P" are same
- If P is a proposition, then $\neg$P is the negative of P
- **Example:** Suppose that P is "Today is Friday"
  - Then, $\neg$P is "Today is not Friday"
- **Example:** Suppose that P is "Today is Friday"
  - Suppose that today (during this lecture) is Sunday
  - So, P is false and $\neg$P is true
  - Here, "Sunday" is true means "not Friday" is true
- **Exercise:** Do the above examples with P: "His age is 19"

true = $\neg$*false*

false = $\neg$*true*

Not (¬)

- **Example:** Consider P: "His car is white"
  - Negation of P (¬P) is: "His car is not white"
  - It can also be written in this way: "It is not true that his car is white"
  - Observe that "His car is black" is not a correct negation of P
  - Because, there can be many other colors, such as blue, green, red, etc. that are not white
  - So, writing "black" is not enough
  - Writing "not white" is enough, because it covers all other colors
- **Exercise:** Write the negation of "His car is not white"

¬white
=
not white

Not (¬)

- **Example:** Negative of “at least”
  - Remember, “at least” means same or more (≥)
  - So, negative of “at least” is less (<)
  - Note: “at most” is not the negative of “at least”
- **Example:** Negation of P: “His mark is at least 80”
  - Here, P is true or false based on term “at least”
  - P is true if the mark is 80 or more, like: 80, 85, 88, …
  - P is false if the mark is less than 80, like: 79, 2, 5, …
  - So, $\neg$P is: “His marks are less than 80”
- **Exercise:** Write the negative of “His mark is at most 90”
- **Exercise:** Why “at most” is not the negative of “at least”?

$\neg(\geq)$ *is* $<$

$\neg(\leq)$ *is* $>$

Not ($\neg$)

- **Example:** Suppose that P is: 3+4 = 8
  - Then, $\neg$P is: $3+4 \neq 8$
  - Here, P was false. Now, $\neg$P is true
- Observe that, in the above example, $\neg$P **cannot** be written as 3+4=7, 4+4=8, 3+3=6, etc.,--- although all of them are true
- Because, there can be many such true statements. $3+4 \neq 8$ covers all of them. So, writing $3+4 \neq 8$ is enough
- **Exercise:** Write the negative of the following propositions
  - 3+4 = 7
  - $3+4 \neq 7$

$\neg$*true* = *false*

$\neg$*false* = *true*

Double Negation

- "Not" can be applied as many times as you want
- If it is applied two times, then it is called **double negation**
- A double negation cancels each other, like minus minus is plus
- **Example:**
  - $\neg\neg P$ is P
  - $\neg\neg\neg P$ is $\neg P$
- **Example:**
  - Suppose that P is: "He is good"
  - Double negation of P ($\neg\neg P$) is: "He is good"
  - Logically "He is not not good" is the correct answer. But in English it is not a good way to write "not not"

$\neg\neg P = P$

$\neg\neg\neg P = \neg P$

$\neg\neg\neg\neg P = P$

Truth Table

- **Truth table** is a convenient way to understand how the truth values of a compound proposition can be achieved from given propositions
- For $\neg P$, the truth table is created as follows:
- In this table, P is given, and $\neg P$ is to be calculated
- It is created from left to right
- It has two columns, left one for P and right one for $\neg P$
- P has two rows for two possible values, one for true and another for false
- True and false are written as T and F for short
- For each row, the value of $\neg P$ is written in the right side
- Right side picture is the truth table for **not P ($\neg$P)**

Truth Table for **not P ($\neg$P)**	
P	$\neg P$
T	F
F	T

And ($\wedge$)

- **And** is applied to two given propositions P, Q
- Its symbol is $\wedge$
- It is written as P **and** Q, $P \wedge Q$
- **And** is also called **conjunction**
- **Example:**
  - Suppose P: "Today is Friday" and Q: "We go to pray"
  - Then, P **and** Q is: "Today is Friday and we go to pray"
- "**Conjunction** of P and Q", "P **and** Q", "$P \wedge Q$" are all same
- $P \wedge Q$ is a new compound proposition and has truth value
- **And** is true when both of P and Q are true
- If P or Q or both of them are false, then **and** is false
- **Exercise:** Write $P \wedge Q$ when P: "I go" and Q: "you go"

and ($\wedge$) means "both"

And ($\wedge$)

- **Example:** Consider P, Q from the previous example
  - If today is Friday and we are going to pray, then both P and Q are true, so $P \wedge Q$ is also true
  - So, "Today is Friday and we go to pray" is true
  - If today is Sunday, then P is false. So, $P \wedge Q$ is false
  - So, "Today is Friday and we go to pray" is false
  - If we do not go to pray, then Q is false. So, $P \wedge Q$ is false
  - So, "Today is Friday and we go to pray" is false
  - If today is not Friday and we also do not go to pray, then both P and Q are false. So, $P \wedge Q$ is false
  - So, "Today is Friday and we go to pray" is also false

$\wedge$ is true when both true

Truth Table for and ($\wedge$)

- **Example:** Truth table for $P \wedge Q$
  - There will be three columns: P, Q, $P \wedge Q$
  - Left side P, then Q, then $P \wedge Q$
  - P and Q are given, we shall find $P \wedge Q$
  - P and Q can be T or F
  - So, there will be four possible combinations of P and Q: TT, TF, FT, FF
  - So, four rows
  - $P \wedge Q$ is true only for TT. For other cases, it is false
  - The right-side picture is the truth table for $P \wedge Q$
- **Exercise:** In the truth table of $\neg P$, the number of rows was two. Here, it is four. Is there any formula here?

Truth Table for P **and** Q ($P \wedge Q$)

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Truth Table for and (∧)

- The operation **and** is **commutative**
- That means, P∧Q and Q∧P are the same
- Sometimes, for better understanding, the variables can be chosen close to the given statement
- For example, we can choose F for "Today is **F**riday" and P for "We are going to **P**ray"
- Sometimes, T and F are written as binary digits 1 and 0, so the four combinations are 00, 01, 10, 11
- Usually with T and F, it starts with TT and ends to FF
- With 0 and 1, it starts with 00 and ends to 11, because these are the four possible binary numbers by two digits
- **Example:** So, the truth table for **and** with 0 and 1 is this

Truth Table for **and** (∧)		
F	P	F∧P
0	0	0
0	1	0
1	0	0
1	1	1

Or ($\vee$)

- Similar to **and**, **or** is applied to two propositions P, Q
- Its symbol is $\vee$. It is written as P **or** Q, $P \vee Q$
- **Or** is also called **disjunction**
- Similar to **and**, **or** is also commutative: $P\vee Q$, $Q\vee P$ same
- **Example:** Suppose that P: “Today is Friday” and Q: “We go to pray”
  - Then, P **or** Q is: “Today is Friday **or** we go to pray”
  - “**disjunction** of P and Q”, “P **or** Q”, “$P\vee Q$” are all same
- $P\vee Q$ is a compound proposition and has a truth value
- **Or** is true when one or both of P and Q are true
- If both of P and Q is false, then **or** is false

or ($\vee$)
means
one or both

Or ($\vee$)

- **Example:** Consider P, Q from the previous example
  - If today is Friday, then P is true. So, $P \vee Q$ is true
  - That means, "Today is Friday or we go to pray" is true. It does not matter whether we go to pray or not
  - If we are going to pray, then Q is true. So, $P \vee Q$ is true
  - So, "Today is Friday or we go to pray" is true. It does not matter whether today is Friday or not
  - If today is not Friday and we are also not going to pray, then both P and Q are false. So, $P \vee Q$ is false
  - So, "Today is Friday or we go to pray" is false

$\vee$ is true means one or both true

Truth Table for or ($\vee$)

- **Example:** Truth table for $P \vee Q$
  - There will be three columns: P, Q, $P \vee Q$. Left side P, then Q, then $P \wedge Q$
  - P and Q are given, we shall find $P \vee Q$
  - P and Q can be T or F
  - So, four rows for PQ will be TT, TF, FT, FF
  - $P \vee Q$ is false for FF. For other cases, it is true
  - The right-side picture is the truth table for $P \vee Q$
- **Exercise:**
  - Which rows are similar in the truth tables of **and** and **or**? Why?
  - Draw the truth table of **or** with 0 and 1

Truth Table for P **or** Q ($P \vee Q$)

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive or (xor, ⊕)

- **Exclusive or** is also written as **xor**
- The symbol of **xor** is ⊕, and it is written as P⊕Q
- In English it is expressed as "**either … or**"
- Example: Suppose P: "Musa went" and Q: "Isa went"
  - Then P⊕Q: "Either Musa or Isa went"
- **Xor** is true when exactly one of P or Q is true
- If both P and Q are true or false, then **xor** is false
- Similar to **and** and **or, xor** is also commutative
- Example: From the previous example,
  - If both Musa and Isa were there, then P⊕Q is false
  - If only one of Musa and Isa went, then P⊕Q is true
  - If none of them went there, then P⊕Q is false

Truth Table for P xor Q (P⊕Q)

P	Q	P⊕Q
T	T	F
T	F	T
F	T	T
F	F	F

Multiple and ($\wedge$), Multiple or ($\vee$)

- **And** or **or** can be applied more than once
- **Example:**
  - $P1 \wedge P2 \wedge P3 \wedge \ldots \wedge Pn$ is a conjunction of n propositions
  - $P1 \vee P2 \vee P3 \vee \ldots \vee Pn$ is a disjunction of n propositions
- For multiple **and**, the compound statement is true when all the given propositions are true
- If any one is false, then it is false
- For multiple **or**, the compound statement is false when all the given propositions are false
- If any one is true, then it is true
- **Exercise:** In the truth table of **and** of three propositions P, Q, R, how many columns and rows will be there?

$\wedge \ \wedge \ \wedge \ \wedge \ \ldots$

$\vee \ \vee \ \vee \ \vee \ \ldots$

Multiple and ($\wedge$), Multiple or ($\vee$)

- **Example:** Truth table for $P \wedge Q \wedge R$ and $P \vee Q \vee R$ with 0, 1 (see in the right-side table) $\longrightarrow$
  - Five columns: P, Q, R, $P \wedge Q \wedge R$ and $P \vee Q \vee R$
  - 8 rows: 000, 001, …, 111
- **Number of rows in a truth table:**
  - If a compound statement has n variables, then number of rows will be 2^n
  - Because, each variable can have two values: T, F
  - So, total possible combination for n variables is: $2*2*\ldots$ n times = 2^n
  - This is same as the number of n-bit binary numbers

Truth Table for $P \wedge Q \wedge R$ and $P \vee Q \vee R$

P	Q	R	$P \wedge Q \wedge R$	$P \vee Q \vee R$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	0	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Truth Tables for Multiple $\wedge$, $\vee$, $\neg$, $\oplus$

- **And**, **or**, **not**, **xor** can appear together multiple times
- **Example:** Draw truth table for $(q \vee p) \wedge (p \wedge \neg q)$ with 0, 1
  - Two variables p, q. So, $2^2=4$ rows, from 00 to 11
  - Six columns: p, q, $\neg q$, $(q \vee p)$, $(p \wedge \neg q)$, $(q \vee p) \wedge (p \wedge \neg q)$
  - We go gradually from left to right

$\wedge$

$\vee$

$\neg$

$\oplus$

Truth Table for $(q \vee p) \wedge (p \wedge \neg q)$					
p	q	$\neg q$	$p \wedge \neg q$	$q \vee p$	$(q \vee p) \wedge (p \wedge \neg q)$
0	0	1	0	0	0
0	1	0	0	1	0
1	0	1	1	1	1
1	1	0	0	1	0

Truth Tables for Multiple $\wedge$, $\vee$, $\neg$, $\oplus$

- **Example:** Draw the truth table for $(p\wedge r)\vee(r\oplus q)$
  - We have three variables: p, q, r
  - So, $2^3 = 8$ rows, from TTT to FFF
  - Six columns: p, q, r, $(p\wedge r)$, $(r\oplus q)$, $(p\wedge r)\vee(r\oplus q)$
  - We go gradually from left to right →
- **Exercise:** Draw truth tables for:
  - $(p\vee\neg r)\vee(\neg r\vee p)\vee(r\vee\neg p)$
  - $\neg p\vee(\neg q\wedge p)$
  - $((p\vee q)\vee(r\oplus q))\wedge(p\vee r)$
  - $p\vee\neg p$
  - $(p\vee\neg q)\oplus q$

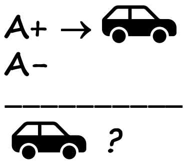
Truth Table for $(p\wedge r)\vee(r\oplus q)$					
p	q	r	$p\wedge r$	$r\oplus q$	$(p\wedge r)\vee(r\oplus q)$
T	T	T	T	F	T
T	T	F	F	T	T
T	F	T	T	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	T	T
F	F	F	F	F	F

Lecture 3
Implication and Bi-conditional

… and the reward of the hereafter is certainly much greater, if only they knew.
(Quran 16:41)

Motivation

- Suppose that your father told you this:
  - "**If** you get A+ in the exam, **then** he will give you a new car as a gift"
- After the exam, your grade is not A+, but A-
- After hearing your grade, your father still gives you a new car
- So, is your father doing something **true** according to his promise or doing something **false**?
- The answer of this question is very conceptual and at the heart of this lecture
- What your father is doing is **true**
- Actually, he is doing something more than his promise



Implication (→)

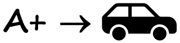
- **Implication** is applied to two given propositions P, Q
- Its symbol is → and written as P→Q
- Commonly, **implication** is stated in English as follows,
  - P implies Q
  - If P, then Q
  - Q, if P
  - If P is true, then Q is true
- **Example:** Consider the previous example
  - In short, your father told this: “If A+, then new car”
  - Here, P: A+, Q: new car
  - The statement of your father is the implication:

    A+ → new car

A+ → 

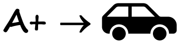
Implication ($\rightarrow$)

- **Example:** For this statement: “odd+odd implies even”
  - P: odd+odd, Q: even
  - It is the implication: (odd+odd) $\rightarrow$ even
- **Example:** Consider this statement: “(x>0), if (x-1 ≥ 0)”
  - Here, P: (x-1 ≥ 0), Q: x>0
  - The statement is the implication: (x-1 ≥ 0) $\rightarrow$ (x>0)
- **Example:** Consider this statement: “If (2>3) is true, then (3>4) is true”
  - Here, P: 2>3, Q: 3>4
  - The statement is the implication: (2>3) $\rightarrow$ (3>4)
- **Exercise:** Write the implication for “If it rains or if it is snowing, then it will be cold”



Implication ($\rightarrow$)

- In the previous examples we have seen how English sentences can be written as implications
- Now we see some examples where an implication can be written as English sentences
- **Example:** Suppose that A: Arif prays, B: Arif remains good. Then A $\rightarrow$ B can be stated in English as follows (all are same):
  - If Arif prays, then he remains good
  - Arif prays implies he remains good
  - Arif remains good, if he prays
  - If it is true that Arif prays, then it is also true that Arif remains good



Implication ($\rightarrow$)

- **Implication** is a proposition and has a truth value
- An **implication** $P \rightarrow Q$ is true in two cases:
  - When P is true and Q is also true
  - When P is false (no matter Q is true or false)
- $P \rightarrow Q$ is false when P is true, but Q is false
- Truth table for implication (see right side): $\longrightarrow$
  - Three columns: P, Q, $P \rightarrow Q$
  - P and Q are given, we would find $P \rightarrow Q$
  - Four rows: TT, TF, FT, FF
  - Only one case is false, all other true
- **Exercise:** Draw the truth table of implication with 0, 1

Truth Table for $P \rightarrow Q$

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Implication (→)

- **Example:** The truth value of an implication can be better understood by the previous example of "A+ → new car"
  - We shall see when "A+ → new car" becomes true or false
  - Let us see when "A+ → new car" becomes true
  - Suppose that you did not get A+ (so, A+ is false)
  - Now, whether your father gives you a new car or not (new car true or false), his promise remains true
  - So, this makes "A+ → new car" true for the two cases based on the new car is true or false
  - (continued to the next slide…)

Truth Table for A+ → 

A+		A+→ 
T	T	T
T	F	F
F	T	T
F	F	T

Implication ($\rightarrow$)

- (continued from the previous slide)
- There is another case when "A+ $\rightarrow$ new car" becomes true
- Suppose that you got A+ (so, A+ is true)
- Your father gives you a new car (new car is true)
- He keeps his promise, and everything is fine
- So, the implication "A+$\rightarrow$new car" remains true
- Finally, we see when "A+$\rightarrow$new car" is false
- Suppose that you got A+ (so, A+ is true), but your father does not give you a new car (so, new car is false). Your father breaks promise
- This makes the implication false

Truth Table for A+ $\rightarrow$ 

A+		A+$\rightarrow$ 
T	T	T
T	F	F
F	T	T
F	F	T

Bi-conditional (↔)

- **Bi-conditional** is applied to two given propositions P, Q
- Its symbol is ↔ and written as P↔Q
- P↔Q and Q↔P are same (detail we shall see latter)
- P↔Q is stated in English as follows,
  - P if and only if Q (or equivalently, Q if and only if P)
  - P iff Q (or equivalently, Q iff P)
- **Example:** Consider the "new car" example again
  - Suppose your father changes his promise as follows: "He will give you a new car if and only if you get A+"
  - Here, P: A+, Q: new car. The above statement is the biconditional: A+ ↔ new car (or similarly, new car ↔ A+)

A+ ↔ 

Bi-conditional (↔)

- **Example:** Consider this statement with integer x: "x^2 is even if and only if x is even"
  - Here, P: x is even, Q: x^2 is even
  - The statement is same as the bi-conditional $P \leftrightarrow Q$
- **Example:** Suppose that A: Arif prays, B: Arif remains good. Then $A \leftrightarrow B$ can be stated in English as follows (all are same):
  - Arif remains good if and only if he prays
  - Arif prays if and only if he remains good
  - If Arif prays, then he remains good and if Arif remains good, then he prays (This statement has two parts $A \rightarrow B$ and $B \rightarrow A$. See next next slide)

A+ ↔ 

Bi-conditional (↔)

- P↔Q is a proposition and has a truth value
- P↔Q is true when both P and Q are same
- P↔Q is false when P and Q are different
- ↔ is same as equivalence (=) between P and Q
- Truth table for implication (see here) ⟶
  - Three columns: P, Q, P ↔ Q
  - P and Q are given, we need to find P ↔ Q
  - Four rows: TT, TF, FT, FF
  - Two cases are true, two cases false
  - When P and Q are same, it is true
  - When P and Q are different, it is false
- **Exercise:** Draw the truth table of bi-conditional with 0, 1

Truth Table for P↔Q

P	Q	P↔Q
T	T	T
T	F	F
F	T	F
F	F	T

Bi-conditional (↔)

Truth Table for P↔Q from (P→Q)∧(Q→P)				
P	Q	P→Q	Q→P	P↔Q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

∧

- P↔Q has two parts: P→Q and Q→P
- Q→P can also be written as P←Q
- P→Q and P←Q combine to P↔Q
- P↔Q is actually (P→Q)∧(P←Q)
- P↔Q is true when both P→Q and Q→P are true
- If any of P→Q or Q→P is false, then P↔Q is false
- This can be better understood by extending the truth table by adding two more columns for P→Q and Q→P before P↔Q (see here)
- The table is computed from left to right (P, Q given)
- For computing P→Q and Q→P, we can go back and forth to the truth table of (→) in previous slides

Bi-conditional (↔)

Truth Table for A+ ↔ 		
A+		A+ ↔ 
T	T	T
T	F	F
F	T	F
F	F	T

- **Example:** Truth value of a bi-conditional can be better understood by the example "A+ ↔ new car"
  - Remember, the modified promise of your father: "He will give you a new car if and only if you get A+"
  - That means, A+ and new car should be the same
  - So, if A+, then new car. If no A+, then no new car
  - We can see this in the top-right corner truth table
  - When A+ and new car are same (first and last rows), (↔) becomes true
  - If they are different (two middle rows), (↔) is false
- **Exercise:** Truth tables of ↔ (in this slide) and → (in Slide 62-64) differ only in 3rd row. Why?

Truth Table for Compound Propositions

- **Example:** Draw the truth table by 0, 1 for:

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

  - We have two variables here: p, q
  - So, $2^2 = 4$ rows, from 00 to 11
  - Six columns: p, q, $\neg q$, $(q \vee p)$, $(p \wedge \neg q)$, $(q \vee p) \rightarrow (p \wedge \neg q)$
  - We go gradually from left to right
- **Exercise:** Draw truth tables for:
  - $(p \vee \neg q) \rightarrow (\neg q \vee p)$
  - $\neg p \rightarrow \neg q$
  - $(r \vee p \vee q) \rightarrow (r \wedge q)$
  - $(\neg p \leftarrow p) \leftarrow \neg p$
  - $(p \vee \neg q) \leftarrow (\neg q \vee p)$

Truth Table for $(q \vee p) \rightarrow (p \wedge \neg q)$

P	q	$\neg q$	$q \vee p$	$p \wedge \neg q$	$(q \vee p) \rightarrow (p \wedge \neg q)$
0	0	1	0	0	1
0	1	0	1	0	0
1	0	1	1	1	1
1	1	0	1	0	0

Truth Table for Compound Propositions

- **Example:** Draw the truth table for
  $(p \rightarrow r) \rightarrow (r \vee q)$
  - We have three variables: p, q, r
  - So, $2^3 = 8$ rows, from TTT to FFF
  - Six columns: p, q, r, $(p \rightarrow r)$, $(r \vee q)$, and $(p \rightarrow r) \rightarrow (r \vee q)$
  - We go gradually from left to right
- **Exercise:** Draw truth tables for:
  - $(p \rightarrow \neg r) \rightarrow (\neg r \vee p)$
  - $\neg p \rightarrow (\neg q \rightarrow \neg r)$
  - $(p \vee q) \rightarrow (r \wedge q)$
  - $(\neg p \rightarrow q) \rightarrow \neg p$

Truth Table for $(p \rightarrow r) \rightarrow (r \vee q)$

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

Truth Table for Compound Propositions

- **Example:** Draw truth table by 0, 1 for: $(p\wedge q)\leftrightarrow(\neg q\vee\neg p)$
  - Two variables p, q. So, $2^2 = 4$ rows, from 00 to 11
  - Six columns: p, q, $\neg p$, $\neg q$, $(p\wedge q)$, $(\neg q\vee\neg p)$, $(p\wedge q)\leftrightarrow(\neg q\vee\neg p)$
  - We gradually go from left to right
- **Exercise:** Draw truth table by 0, 1 for:
  - $\neg(p\wedge q)\leftrightarrow(\neg q\vee\neg p)$
  - $p\vee(q\leftrightarrow(\neg q\vee\neg p))$
  - $(p\leftrightarrow q)\vee((\neg q)\leftrightarrow(\neg p))$
  - $(p\oplus q)\leftrightarrow(\neg q\oplus\neg p)$
  - $((p\vee\neg q)\leftrightarrow(\neg q))\vee p)$
  - $(p\wedge q)\leftrightarrow(\neg(\neg q\vee\neg p))$

Truth Table for $(p\wedge q)\leftrightarrow(\neg q\vee\neg p)$

p	q	$\neg p$	$\neg q$	$p\wedge q$	$\neg q\vee\neg p$	$(p\wedge q)\leftrightarrow(\neg q\vee\neg p)$
0	0	1	1	0	1	0
0	1	1	0	0	1	0
1	0	0	1	0	1	0
1	1	0	0	1	0	0

Truth Table for Compound Propositions

- **Example:** Draw truth table for:
  $(p \rightarrow r) \leftrightarrow (r \vee q)$
  - We have three variables: p, q, r
  - So, $2^3 = 8$ rows, from TTT to FFF
  - Six columns: p, q, r, $(p \rightarrow r)$, $(r \vee q)$, $(p \rightarrow r) \leftrightarrow (r \vee q)$
  - We go gradually from left to right
- **Exercise:** Draw truth tables for:
  - $(p \leftrightarrow \neg r) \rightarrow ((\neg r) \oplus p)$
  - $\neg p \leftrightarrow \neg q$
  - $(\neg p \vee q) \leftrightarrow (r \leftrightarrow \neg q)$
  - $(\neg p \leftrightarrow p) \leftrightarrow \neg p$

Truth Table for $(p \rightarrow r) \leftrightarrow (r \vee q)$

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

Operator Precedence

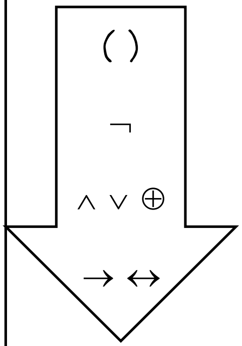
- **Precedence** means importance or priority in execution (who is executed first)
- If the logical operators $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$ and () appear together in a compound proposition, then they are executed by their precedence
- Same precedence executed from left to right by their appearance
- Precedence of these operators are (from high to low):

  ()

  $\neg$

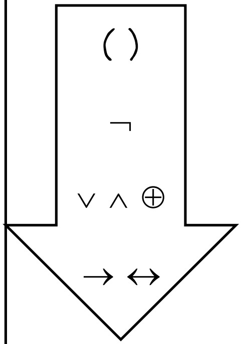
  $\wedge$, $\vee$, $\oplus$ same precedence

  $\rightarrow$, $\leftrightarrow$ same precedence



Operator Precedence

- **Example:** The proposition $p \lor q \land r$ is executed as $(p \lor q) \land r$
- **Example:** The proposition $\neg p \lor q$ is executed as $(\neg p) \lor q$
- **Example:** Step by step execution of $r \to \neg p \leftrightarrow q \land p \lor q$ by order of precedence (red color shows current step):
  - $r \to (\neg p) \leftrightarrow q \land p \lor q$ // $\neg$ is highest among all
  - $r \to (\neg p) \leftrightarrow (q \land p) \lor q$ // then $\land$, $\lor$ same, so left to right
  - $r \to (\neg p) \leftrightarrow ((q \land p) \lor q)$ // complete $\lor$ after $\land$
  - $(r \to (\neg p)) \leftrightarrow ((q \land p) \lor q)$ // $\to$, $\leftrightarrow$, same, left to right
  - $((r \to (\neg p)) \leftrightarrow ((q \land p) \lor q))$ // complete $\leftrightarrow$ after $\to$
- **Exercise:** Execute step by step
  - $r \to \neg(p \leftrightarrow q) \land p \lor q$
  - $(r \to p \leftrightarrow q) \oplus \neg p \lor q$



Contrapositive, Converse, Inverse

- **Contrapositive** of an implication $p \to q$ is $\neg q \to \neg p$
- Implication and contrapositive are logically equivalent
- Their values are same for all values of p, q
- This can be seen from the truth table
- The last two columns for $p \to q$ and $\neg q \to \neg p$ are same
- Their equivalency can be proven by other ways
- We shall see that in the next lecture
- **Exercise:** Write contrapositive for each of the following implications and verify their equivalency by truth table

  A+→ new car, $\neg q \to \neg p$, $\neg p \to q$, $q \to \neg p$, $\neg q \to q$, $p \to p$

Truth Table for $p \to q$ and $\neg q \to \neg p$

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

=

Contrapositive, Converse, Inverse

- Remember, $p \to q$ can be written in different ways
- The equivalency of $p \to q$ and $\neg q \to \neg p$ gives some more ways to write $p \to q$:
  - If no q, then no p // from $\neg q \to \neg p$
  - No q means no p // from the previous line
  - p only if q // from the previous line
  - q is necessary for p // from the previous line
  - p is sufficient for q // from $p \to q$ (if p, then p)
- Above five statements are all equivalent to $p \to q$ and $\neg q \to \neg p$
- **Exercise:** Rewrite the implication "A+$\to$ new car" in ways similar to the above five statements

implication

=

contrapositive

Contrapositive, Converse, Inverse

- $p \leftrightarrow q$ can also be expressed in new ways
- Remember, $p \leftrightarrow q$ means $p \rightarrow q$ **and** $q \rightarrow p$
- From the previous slide:
  - $p \rightarrow q$ is same as "p is sufficient for q"
  - $q \rightarrow p$ is same as "p is necessary for q"
- Combining them together, we can write $p \leftrightarrow q$ as
  - p is necessary and sufficient for q
- We can also see how $p \leftrightarrow q$ is same as "p if and only if q"
  - $q \rightarrow p$ is same as "p if q"
  - $p \rightarrow q$ is same as "p only if q" // from previous slide
  - Combining them together, we get "p if and only if q"
- **Exercise:** Do the above analysis for "A+$\leftrightarrow$ new car"

implication

=

contrapositive

Contrapositive, Converse, Inverse

- **Converse** of an implication $p \rightarrow q$ is $q \rightarrow p$
- **Inverse** of $p \rightarrow q$ is $\neg p \rightarrow \neg q$
- **Converse** and **inverse** are equivalent
- This can be seen from this truth table →
- Last two columns of $q \rightarrow p$ and $\neg p \rightarrow \neg q$ are same
- This equivalency can also be proven by contrapositive:
  - contrapositive of $q \rightarrow p$ is $\neg p \rightarrow \neg q$
  - From previous slides, implication and contrapositive are same. So, $q \rightarrow p$ and $\neg p \rightarrow \neg q$ are same
- **Exercise:** Show converse = inverse for the followings:
  A+→ new car, $\neg q \rightarrow \neg p$, $\neg p \rightarrow q$, $q \rightarrow \neg p$, $\neg q \rightarrow q$, $p \rightarrow p$

Truth Table for $q \rightarrow p$ and $\neg p \rightarrow \neg q$

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

=

Lecture 4
Logical Equivalences

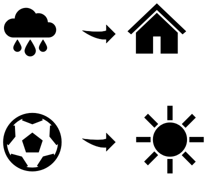
And not equal are the blind and the seeing, nor are those who believe and do righteous deeds and the evildoer. Little do you remember. (Quran 40:58)

Motivation

- Suppose that you and your friend are learning logic
- You two are trying to relate rain with playing
- You are relating them in this way:

  If it rains, then we shall not go to play
- But your friend is saying like this:

  If we are playing, then it is not raining
- Are these two statements same?
- Do they mean that rain and condition for not to play are equivalent to each other?
- This is **logical equivalence**
- This will be the topic of this lecture
- **Exercise:** Can you find some other examples like this?



Logical Equivalency by Truth Tables

- **Logical equivalence** between two compound propositions p and q can be shown in many ways
- The easiest way is to show it by truth table
- p and q are logically equivalent if their truth values are same for every rows in the table
- **Example:** Show that $(p \rightarrow q)$ and $(\neg p \vee q)$ are logically equivalent
  - Combined truth table for $(p \rightarrow q)$ and $(\neg p \vee q)$ is this
  - The two right-side columns are same for every row
  - So, they are logically equivalent
- $(\neg p \vee q)$ is used instead of $(p \rightarrow q)$ in many places and is called a **definition of implication**

Truth Table for $p \rightarrow q$ and $\neg p \vee q$

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

=

Logical Equivalency by Tautology

- If a compound proposition is always true (for all rows in its truth table) then it is called **tautology**
- If it is always false, then it is called **contradiction**
- **Example:** $p \lor \neg p$ is tautology
- **Example:** $p \land \neg p$ is contradiction
- **Example:** $p \land T$ is not tautology or contradiction
- See the right-side table for the above → three examples
- **Exercise:** Decide by truth table whether the followings are tautology, contradiction, or none
  - $p \land p$, $p \lor p$, $\neg p \lor \neg p$, $p \lor T$, $p \land F$, $\neg p \lor \neg p$, $p \lor F$, $T \lor F$

Truth Table for some Tautology and Contradiction

p	$\neg p$	T	$p \lor \neg p$	$p \land \neg p$	$p \land T$
T	F	T	T	F	T
F	T	T	T	F	F

Logical Equivalency by Tautology

- Suppose that p and q are two logically equivalent compound statements
- Their truth table can be extended by one more column for $p \leftrightarrow q$
- Since p and q are same for all rows, this column will be true for all rows, that means it will be tautology
- If they are not logically equivalent, then $p \leftrightarrow q$ is not tautology
- So, **logical equivalence** can also be defined as: p and q are logically equivalent if $p \leftrightarrow q$ is tautology. Otherwise, not

Truth Table for $p \leftrightarrow q$

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

Logical Equivalency by Tautology

- **Example:** $(p \rightarrow q)$ and $(\neg p \vee q)$ are logically equivalent as $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$ is tautology. See the truth table below

Truth Table for $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$					
p	q	$\neg p$	$p \rightarrow q$	$\neg p \vee q$	$(p \rightarrow q) \leftrightarrow (\neg p \vee q)$
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

p equivalent q

when

$p \leftrightarrow q$ tautology

- **Exercise:** Show by tautology that each of the following pairs of statements are logically equivalent:
(a) $(p \rightarrow \neg q)$ and $(q \rightarrow \neg p)$ **(b)** $(p \leftrightarrow q)$ and $(\neg p \leftrightarrow \neg q)$

Logical Equivalency by Tautology

- **Example:** Show that $\neg(p \vee q)$ and $(\neg p \wedge \neg q)$ are logically equivalent. This equivalency is called De-Morgan's law

Truth Table for De-Morgan Law: $\neg(p\vee q)\leftrightarrow(\neg p\wedge\neg q)$							
p	q	$\neg p$	$\neg q$	$p\vee q$	$\neg(p\vee q)$	$\neg p\wedge\neg q$	$\neg(p\vee q) \leftrightarrow (\neg p\wedge\neg q)$
T	T	F	F	T	F	F	T
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	F	T	T	T

- **Exercise:** The other part of De-Morgan's law is that $\neg(p\wedge q)$ and $(\neg p\vee\neg q)$ are logically equivalent. Prove this equivalency by tautology

Logical Equivalency by Tautology

- **Example:** $(p \to q) \to r$ and $p \to (q \to r)$ are not logically equivalent, because the last column is not tautology

Truth Table for $((p \to q) \to r)$ and $(p \to (q \to r))$							
p	q	r	$p \to q$	$(p \to q) \to r$	$q \to r$	$p \to (q \to r)$	$((p \to q) \to r) \leftrightarrow (p \to (q \to r))$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	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	T	F	F	T	F
F	F	T	T	T	T	T	T
F	F	F	T	F	T	T	F

p, q not equivalent when $p \leftrightarrow q$ is not tautology

Common Logical Equivalences

- So far, we have seen some pairs of logically equivalent propositions
- They commonly appear in logical statements
- They are also used to prove other logically equivalent propositions
- That's why they have some names
- Those are simple-but-conceptual
- The right-side table gives the most common list of them
- **Exercise:** Prove Associative law and Distributive law by tautology

Logical Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity law
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination law
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent law
$\neg\neg p \equiv p$	Double negation
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative law
$(p \vee q) \vee r \equiv p \vee (q \vee r) \equiv p \vee q \vee r$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \equiv p \wedge q \wedge r$	Associative law
$(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$ $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$	Distributive law
$\neg(p \vee q) \equiv (\neg p \wedge \neg q)$ $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$	De-Morgan's law
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation law

Common Logical Equivalences

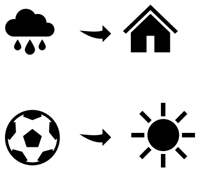
- Logical equivalences can be used to express some English statements in equivalent forms
- **Example:** Rephrase by double-negation:
  - "It is **not** true that he is **not** good" can be rephrased as "He is good" (it is like $\neg\neg$good = good)
- **Example:** Negation by De-Morgan's law
  - Negation of the statement "Omer's car is Toyota **and** white" by De-Morgan's law is "Omer's car is **not** Toyota **or not** white"
  - It is like $\neg$(Toyota$\wedge$white) = $\neg$Toyota$\vee\neg$white
- **Exercise:** Express the negation of "Ashraf or his brother is coming" by De-Morgan's law

…
associative law
…
distributive law
…
De-Morgan's law
…

Common Logical Equivalences

Logical Equivalence	Name
$p \rightarrow q \equiv \neg p \vee q$	Definition of implication
$p \rightarrow q \equiv \neg q \rightarrow \neg p$	Contrapositive
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	Definition of bi-conditional
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$	Bi-conditional of negations

- Right-side table gives some more common logical equivalences involving implication and bi-conditional
- **Example:** Rephrase by contrapositive
  - Recall the example at the beginning of this lecture
  - Your statement was: “If it rains, then no play”
  - By contrapositive, this is same as: “Play means not raining” (this was your friend’s statement)
  - So, your and your friend’s statements are equivalent
- **Exercise:** Can you rephrase the statement “new car iff A+” by “no new car iff no A+”? How?

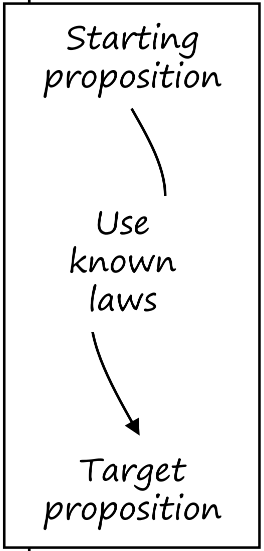


Logical Equivalency by Derivation

- We can show two propositions are logically equivalent by going from one proposition to other
- We can use existing know logical equivalences (laws) gradually one after another
- We can find those laws in the tables that we have seen
- At each step, we mention the name of the law used
- This method is called **logical equivalency by logical derivation**
- **Example:** Show by derivation that $p \rightarrow p$ is a tautology (that means, $p \rightarrow p$ and T are logically equivalent)

$p \rightarrow p \equiv \neg p \lor p$ // by the definition of implication

$\equiv T$ // by negation law



Logical Equivalency by Derivation

- **Example:** Show by logical derivation that $(p \rightarrow r) \vee (q \rightarrow r)$ and $(p \wedge q) \rightarrow r$ are logically equivalent
- **Solution:** $(p \rightarrow r) \vee (q \rightarrow r)$

$\equiv (\neg p \vee r) \vee (\neg q \vee r)$ // by definition of implication // applied twice

$\equiv (\neg p \vee r) \vee \neg q \vee r$ // by associative law

$\equiv \neg p \vee r \vee \neg q \vee r$ // by associative law

$\equiv \neg p \vee \neg q \vee r \vee r$ // by commutative law

$\equiv (\neg p \vee \neg q) \vee (r \vee r)$ // by associative law applied twice

$\equiv (\neg p \vee \neg q) \vee r$ // by idempotent law

$\equiv \neg (p \wedge q) \vee r$ // by De-Morgan's law

$\equiv (p \wedge q) \rightarrow r$ // by the definition of implication

Starting proposition

Use known laws

Target proposition

Logical Equivalency by Derivation

- **Example:** Show by logical derivation that $\neg((p \wedge q) \to p)$ is a contradiction (that means, $\neg((p \wedge q) \to p)$ and F are logically equivalent)

$$
\begin{aligned}
& \neg((p \wedge q) \to p) \\
& \equiv \neg(\neg(p \wedge q) \vee p) && \text{// by definition of implication} \\
& \equiv \neg\neg(p \wedge q) \wedge \neg p && \text{// by De-Morgan's law} \\
& \equiv (p \wedge q) \wedge \neg p && \text{// by double negation} \\
& \equiv \neg p \wedge (p \wedge q) && \text{// by commutative law} \\
& \equiv (\neg p \wedge p) \wedge q && \text{// by associative law} \\
& \equiv F \wedge q && \text{// by negation law} \\
& \equiv F && \text{// by domination law}
\end{aligned}
$$

- **Exercise:** Show the above contradiction by truth table

Starting proposition

Use known laws

Target proposition

Truth Tables vs Logical Derivations

- We have seen two techniques to prove logical equivalency: (1) truth tables and (2) logical derivation
- Both techniques have advantages over other
- Constructing truth tables are straight forward and easier
- But they are lengthy and have many rows and columns
- On the other hand, logical derivations are concise, but they are more conceptual and need more intellect
- **Exercise:** Prove logical equivalency of the following pairs of propositions by truth tables and by logical derivations **(a)** $(p \leftrightarrow \neg q)$ and $(\neg p \leftrightarrow q)$ **(b)** $(p \rightarrow q) \wedge (p \rightarrow r)$ and $p \rightarrow (q \wedge r)$ **(c)** $(p \wedge (\neg p \vee q)) \rightarrow q$ and T
  (d) $(q \wedge (q \rightarrow q)) \leftrightarrow \neg q$ and F

Truth tables easier, but lengthy

vs

Derivation shorter, but conceptual

Lecture 5
Predicates and Quantifiers

… whoever kills a person… (unjustly)… it is as if he has killed all mankind …
(Quran 5:32)

Motivation

- Is the answer of this question “**$x/2 < x$?**” true or false?
- At first look, this answer comes to the mind:

  True, because half of anything is of course smaller
- However, if we look carefully from mathematical point of view and also if we remember from Lecture 1, then:

  For $x > 0$, it is true. But for $x \leq 0$, it is false
- So, **for some values** of x it is true, **for some values** it is false
- We can also say, **for all values** of x it can be true of false
- Statements like “$x/2 < x$”, the terms “for some”, “for all” --- all these fall into **predicates** and **quantifiers**
- **Exercise:** Can you find some other examples like this?

$9/2 < 9$ ✓

$1/2 < 1$ ✓

$0/2 < 0$ ×

$0/2 = 0$ ✓

$-9/2 < -9$ ×

$-9/2 > -9$ ✓

Predicates

- "$x/2 < x$?" can be represented as: $P(x)$: $x/2 < x$
- Here x is a **variable**, P is called **predicate** and P(x) is called **propositional function**
- P(x) does not have a truth value without a value of x
- If x gets a value, then P(x) becomes a proposition (true or false)
- **Example:** Decide the truth value of P(0), P(-2) and P(3), where $P(x)$: $x/2 < x$
  - P(0) is $0/2<0$, which is $0 < 0$. So, false
  - P(-2) is $-2/2<-2$, which is $-1<-2$. So, false
  - P(3) is $3/2<3$, which is $1.5<3$. So, true
- **Exercise:** Find truth values of $P(x)$: $x/2>x$ for $x= 0, -2, 3$

Predicates with variable values become propositions

Predicates

- There can be two or more variables in a predicate
- **Example:** Consider P(x, y): x-y = -(y-x)
  - Here, P(x, y) is true **for all values** of x and y
- **Example:** Consider P(x, y): x-y = -(y-x). Verify that P(x) is true for P(3,2), P(0,0), P(-1,-2)
  - P(3,2) is 3-2 = -(2-3), which is 1 = -(-1). This is true
  - P(0,0) is 0-0 = -(0-0), which is 0 = -0, which is 0=0. So, true
  - P(-1,-2) is -1-(-2) = -(-2-(-1)), which is -1+2 = -(-2+1), which is 1 = -(-1), which is 1 = 1, so true
- **Exercise:** Find some values of x, y, z so that P(x, y, z): x+y < z becomes sometimes true and sometimes false

Predicates with values become propositions

Quantifiers

- "For some value", "for all value" are called **quantifiers**
- "For some value" is written as ∃ and is called **existential quantifier**
- "For all values" is written as ∀ and is called **universal quantifier**
- P(x) with ∃ or ∀ is written as ∃xP(x) or ∀xP(x)
- ∃xP(x) is read as "for some value of x, P(x)"
- ∀xP(x) is read as "for all values of x, P(x)"
- **Example:** If P(x): x < x*(-1), then ∃xP(x) reads as "there **exists** a value of x so that x < x*(-1)"
- **Example:** If P(x): x < x*(-1), then ∀xP(x) reads as "for **all** possible values of x, x < x*(-1)"

∃: existential quantifier

∀: universal quantifier

English vs. Mathematical Statements

- Propositions expressed in English can be written by predicates and quantifiers, and vice versa
- **Example:** Consider the statement: All persons have beard
  - This statement can be written as: $\forall x B(x)$, where x means a person and B(x) means x has beard
- **Example:** Consider this proposition: $\exists x H(x)$, where x is a student in this class and H(x) means x got 100% marks
  - This proposition can be written in English as "There is a student in this class who got 100% marks
- **Exercise:** Write "A man died" by predicate and quantifier
- **Exercise:** Write in English $\forall x G(x)$, where G(x): x is a girl

$\exists$: *some*

$\forall$: *all*

∀, Any, Every, All, Each

- When ∀ is expressed in English, the terms **any**, **all**, **every** are used in same meaning
- **Example:** Consider this proposition: $\forall x G(x)$, where $G(x)$: x is a good student in this class
  - This proposition can be stated in English as follows, all of which have the same meaning:
    - All students in this class are good
    - Any student in this class is good
    - Every student in this class is good
    - Each student in this class is good
- **Exercise:** Consider $\forall x P(x)$, where $P(x)$: x is a healthy man in this city. Write $P(x)$ by **all**, **every**, **any, each** as above

∀ =

any, every, all, each

∃, Some, Exists, At least one

- When ∃ is expressed in English, the terms **some**, **exists**, **at least one** are used in same meaning
- **Example:** Consider this proposition: ∃xG(x), where G(x): x is a good student in this class
  - This proposition can be stated in English as follows, all of which have the same meaning:
    - Some student in this class is good
    - There exists a student in this class who is good
    - At least one student in this class is good
- **Exercise:** Consider ∃xP(x), where P(x): x is a healthy man in this city. Express this proposition by **some**, **exists**, **at least one** as above

∃ =

some, exists,

at least one

Quantifiers

- $\exists xP(x)$ and $\forall xP(x)$ are propositions and have truth values
- $\exists xP(x)$ is true if for **at least** one value of x, P(x) is true
- $\exists xP(x)$ is false if for **every** value of x, P(x) is false
- **Example:** Suppose that, P(x): x = x*2. Then, $\exists xP(x)$ is true
  - Because, for x = 0, we get 0 = 0*2, which is 0 = 0 and is true. So, for x=0, $\exists xP(x)$ is true
- **Example:** Suppose that, P(x): x = x-1. Then, $\exists xP(x)$ is false
  - Because, no value of x can make x = x-1 (you can try)
- **Exercise:** Explain whether $\exists xP(x)$ is true or false for the following propositions:
  - P(x): $x < x*2$
  - P(x): $|x| < x$

$\exists$ true: when one true

$\exists$ false: when all false

Quantifiers

- $\forall xP(x)$ is true if for **any** value of x, P(x) is true
- $\forall xP(x)$ is false if at least one of x makes P(x) false
- **Example:** Suppose P(x): x = x*2. Then, $\forall xP(x)$ is false
  - Because, many values of x can make $\forall xP(x)$ false
  - For example, for x = 2, we get 2 = 2*2, which is false
- **Example:** Suppose P(x): x > x-1. Then, $\forall xP(x)$ is true
  - Because, x > x-1 means x-x > -1, which is 0 > -1. This is true, irrespective of the value of x
- **Exercise:** Explain whether $\forall xP(x)$ is true or false for the following propositions:
  - P(x): $x \neq x*2$
  - P(x): $|x| \geq x$

$\forall$ true: when all true

$\forall$ false: when one false

Domain

- Sometimes, $P(x)$ is expresses by mentioning more precisely the **range** or **set** of value of x
- That range is called the **domain of x**, or simply **domain**
- Domain can determine the truth value of $P(x)$
- **Example:** Suppose $P(x)$: $x^2 \geq x$ where the domain of x is the set of all integers. Then $\forall x P(x)$ is true
  - Because, $0^2 \geq 0$, $(-1)^2 \geq -1$, $2^2 \geq 2$, so on …
- **Example:** Suppose $P(x)$: $x^2 \geq x$ where the domain is real numbers (remember, real numbers include fractions)
  - Then, $\forall x P(x)$ is false, because for positive fraction less than 1, such as 0.1, 0.2, 0.5, etc., $x^2 \geq x$ is false
  - For example, $(0.5)^2 = 0.25 < 0.5$. So, $0.25 \geq 0.5$ is false

domain

[…]

English vs. Mathematical Statements

- **Example:** Write this English expression by predicates and quantifiers: “Every student in this class is good”
- **Solution 1:** $\forall x G(x)$, where x is a student, G(x) means x is good, and the domain of x is the students in this class
- **Solution 2:** If we change the domain of x as all students (including students outside of this class), then we need additional condition to check the student to be in this class:
  - If x is a student of this class, then x is good
  - By predicate and quantifier: $\forall x(C(x) \rightarrow G(x))$, where additionally C(x) means x is a student of this class
- **Wrong Solution:** We **cannot** write $\forall x(C(x) \wedge G(x))$
  - Because, it says all students are in this class and are good

domain
[…]

English vs. Mathematical Statements

- **Example:** Write by predicates and quantifiers: "Some person in this city visited Makkah"
- **Solution 1:** $\exists x(V(x))$, where x is a person, V(x) means x visited Makkah, and the domain of x is persons in this city
- **Solution 2:** If we take the domain of x as all persons (including those outside this city), then we need additional checking whether x is a person of this city:
  - For some x, x lives in this city and x visited Makkah
  - By predicates and quantifiers, this is: $\exists x(C(x) \wedge V(x))$, where additionally C(x) means x lives in this city
- **Wrong solution:** We **cannot** write $\exists x(C(x) \rightarrow V(x))$, because if C(x) is false (x not in this city), then the proposition still is true

domain

[...]

How ∃ and ∀ can be Related

- When $\forall x P(x)$ is true, then $\exists x P(x)$ is also true
- Because, $\forall x$ is true for all values of x, including the one that makes $\exists x P(x)$ true
- **Example:** Suppose that, $P(x)$: $x^2/2$ is even, where the domain is even integers.
  - Then $\forall x P(x)$ is true. Because, for any even x, $x = 2k$, for some integer k. So, $P(x)$: $x^2/2 = (2k)^2/2 = 4k^2/2 = 2k^2 = 2k' =$ even, where $k'=k^2$ is another integer
  - Now, we can say that $\exists x P(x)$ is also true, because $\forall x P(x)$ is true
- **Exercise:** Explain why $\exists x P(x)$ is false means $\forall x P(x)$ is also false

∀ *true*
means
∃ *true*

∃ *false*
means
∀ *false*

Counterexample

- Remember, to make $\forall x P(x)$ false, a single value of x is enough, although there may be many such values of x
- Showing $\forall x P(x)$ false with such a single value of x is called **counterexample**
- **Example:** Suppose, P(x): $x^3+1 > x^2$, with domain of all integers. Show that $\forall x P(x)$ is false by a counterexample
  - The counterexample can be shown for x = -1
  - Because, P(-1): $(-1)^3+1 > (-1)^2$, which is -1+1>1, false
- **Exercise:** Find counterexample to prove that the following propositions are false:
  - $\forall x P(x)$, with P(x): x is sour, where domain is all fruits
  - $\forall x P(x)$, P(x): x is sweet, with domain of all fruits

Counter-example = only 1 value for false

Negation of Quantifiers

- **Example:** Consider the statement: "All workers got bonus". What is the negation of this statement?
  - This is little tricky, as there can be two ways to think
    1. No worker got bonus (same as: All no bonus)
    2. Some worker did not get bonus
  - Which one is correct?
  - It becomes easy if we use predicate and quantifier
  - The statement with predicate and quantifier becomes: $\forall x B(x)$, with $B(x)$: person x got bonus
  - Now, remember, $\forall x B(x)$ becomes false when for **some** x, $B(x)$ is false (all values of x are not required)
  - So, the second way is correct (continue …)

not all

=

some not

Negation of Quantifiers

- (Continued from the previous slide…)
- We can write "did not get bonus" as $\neg B(x)$
- Then "some worker did not get bonus" becomes $\exists x \neg B(x)$
- Negation of $\forall x B(x)$ is written as $\neg \forall x P(x)$
- So, $\neg \forall x B(x)$ is $\exists x \neg B(x)$ (this is the answer)

- "$\neg \forall x B(x) = \exists x \neg B(x)$" holds for all universal quantifiers
- This is the **De-Morgan's law** for universal quantifier

$$\boxed{\text{De-Morgan's Law: } \neg \forall x B(x) = \exists x \neg B(x)}$$

- **Exercise:** Why way (1) in the previous slide is not correct?
- **Exercise:** By De-Morgan's Law find the negation of "all students in this class passed the final exam"

$$\neg \forall P(x) = \exists \neg P(x)$$

Negation of Quantifiers

- **Example:** Consider this statement "Some worker got bonus". What is the negation of this statement?
  - Again, there can be two ways to think for negation
    1. No worker got bonus (same as: All no bonus)
    2. Some worker did not get bonus
  - With predicate and quantifier, the statement becomes: $\exists x B(x)$ with $B(x)$: x got bonus
  - Now, remember, $\exists x B(x)$ becomes false when for **all** x, $B(x)$ is false (only some value of x is not enough)
  - So, the first way is correct, which can be written as "for every worker x, bonus was not given to x" (continued …)

not some

=

all not

Negation of Quantifiers

- (Continued from the previous slide…)
- This can be written as $\forall x \neg B(x)$
- So, we get $\neg\exists x B(x) = \forall x \neg B(x)$ (this is the answer)

- Again, the above negation holds for all existential quantifiers
- This is actually the second part of **De-Morgan's law**

$$\boxed{\text{De-Morgan's Law: } \neg\exists x B(x) = \forall x \neg B(x)}$$

- **Exercise:** Why way (2) in the previous slide is not correct?
- **Exercise:** By De-Morgan's Law find the negation of:
  - Some student in this class failed in the final exam
  - Each of them attended the ceremony
  - None of them missed the prayer

$$\neg\exists P(x) = \forall\neg P(x)$$

Negation of Quantifiers

- **Example:** Find the negation of $\forall x(x \geq 1)$

  $\neg\forall x(x \geq 1)$

  $= \exists x \neg (x \geq 1)$ // by De-Morgan law

  $= \exists x (x < 1)$
- **Example:** Find the negation $\exists x((x \geq 1) \vee (x < 5))$
- **Solution:** $\neg\exists x((x \geq 1) \vee (x < 5))$

  $= \forall x \neg((x \geq 1) \vee (x < 5))$ // De-Morgan law

  $= \forall x(\neg(x \geq 1) \wedge \neg(x < 5))$ // De-Morgan law of Lecture 4

  $= \forall x((x < 1) \wedge (x \geq 5))$
- **Exercise:** Find the negation of the followings:

  (a) $\forall x(p \rightarrow q)$ (b) $\forall x((x>1) \rightarrow (x \geq 0))$ (c) $\exists x((x \geq 0) \leftrightarrow (x \leq 0))$

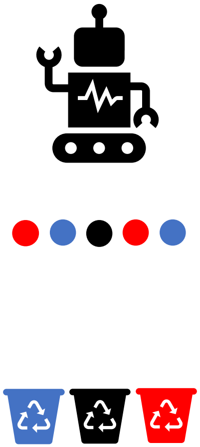
  (d) $\exists x(p \leftrightarrow q)$ (e) $\exists x((x \leq 0) \rightarrow (x<1))$ (f) $\forall x((x \geq 0) \leftrightarrow (x \leq 0))$

$\neg\forall = \exists\neg$

$\neg\exists = \forall\neg$

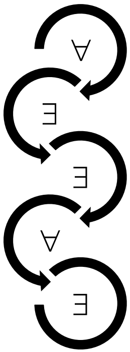
Nested Quantifiers: Motivation

- Quantifiers can appear in more than one, nested
- **Example:** Suppose you have a robot at your home that can sort items by colors. One day you give the robot this instruction: Put the balls into the baskets by their colors
  - To do this job, the robot will translate this instruction like this: For **each** ball x and for **some** basket y, if color x = color y, then put x in y. If color x $\neq$ color y, then do not put
  - This is same as: put x in y if and only if color x = color y
  - By predicate and quantifier, suppose C(x): Color of ball x, D(y): Color of basket y, P(x,y): Put x in y
  - Then the instruction is: $\forall x \exists y((C(x)=D(y)) \leftrightarrow P(x,y))$



Nested Quantifiers

- Each variable in nested quantifier has its own quantifier
- Quantifiers are applied from left to right
- Propositions with nested quantifiers have truth values
- **Example:** Consider this proposition: $\forall x \exists y (x-y=0)$
  - It reads as "for any x, there is a y so that x-y is 0"
  - The truth value of this proposition is true
  - Because, for any x (say, x=5), we can take y same as x (so, y=5 too)
  - This makes x-y as x-x = 0 (like 5-5=0)
  - So, x-y = 0 is true
  - So, for any x, we can find a y so that x-y = 0 is true
  - Therefore, $\forall x \exists y (x-y=0)$ is true



Meaning of multiple quantifiers are tricky

Nested Quantifiers

- Order of quantifiers is important when the quantifiers are mixed of $\forall$ and $\exists$
- Changing the order between $\forall$ and $\exists$ may change the meaning of the proposition
- **Example:**
  - Consider the two propositions $\forall x \exists y(x-y=0)$ and $\exists y \forall x(x-y=0)$
  - Here, $P(x,y)$ remains same, but $\forall x$ and $\exists y$ swapped
  - This swapping changes the meaning as well as the truth value of the proposition
  - The first one is the previous example and was true
  - The second one will be false (see next example …)

$\forall\exists \neq \exists\forall$

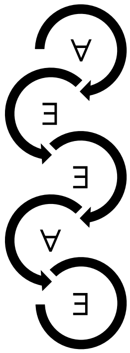
Nested Quantifiers

- **Example:** $\exists y \forall x(x-y=0)$ is false
  - The proposition reads as "there exists a y such that any value of x will give x-y=0"
  - Why this proposition is false?
  - Let us try some y
  - Let, y=5. Then, for x=5, x-y is 5-5=0, which is true
  - But for other x, say x=4, x-y is 4-5 = 0 is false
  - Actually, for any y, we can take x=y-1. That will make x-y=0 as (y-1)-y=0, which is -1=0. This is false
  - So, for every y, there is an x so that x-y=0 is false.
  - So, there is no y, for which $\forall x(x-y=0)$ is true
  - So, $\exists y \forall x(x-y=0)$ is false

$\forall\exists \neq \exists\forall$

Nested Quantifiers

- **Example:** Consider this proposition: $\forall x \forall y \exists z(x-y=z)$
  - It reads as "for any value of x and y, we can find a value of z so that x-y becomes same as z"
  - This proposition is true. Why?
  - Because, if we take z=x-y, then x-y=z becomes true
  - For example, take any x and any y, say x=7, y=2. Then take z = x-y=7-2=5. So, x-y=z becomes 7-2=5, which is 5=5, true
- **Example:** Consider this proposition: $\exists z \forall y \forall x(xyz=0)$
  - It reads as "there is a z, so that for any x and y, xyz=0
  - This proposition is true
  - Because, for z=0, xyz=xy*0=0, irrespective of x and y



Meaning of multiple quantifiers are tricky

English vs. Mathematical Statements

- Sometimes, in English expression, quantifiers and domains are not explicitly mentioned
- Those should be understood from the English meaning
- **Example:** Write this English expression by predicates and quantifiers: “Average of two even numbers is even”
- **Answer:** Here, no quantifiers or domain is mentioned
  - But the meaning of the expression is: “Average of **any** two even **integers** is even”
  - That means, “For any two integers, if they are even, then their average is even”
  - By predicates and quantifiers, $\forall x \forall y((x\%2=0) \wedge (y\%2=0) \rightarrow ((x+y)/2)\%2 = 0))$, where x, y are integers

domain

[…]

English vs. Mathematical Statements

- **Note:** It is **not important** to check whether a given statement is true or false. The statement in the previous example is actually false, because (2+4)/2 = 3 = odd. We only see the English meaning, not its truth value
- **Example:** Write by predicates and quantifiers: "Average of two odd numbers is not necessarily odd"
- **Solution:** Here, "not necessarily odd" means "not always odd". That means, "**sometimes** even"
  - So, the meaning of the expression is this: "For **some** pair of odd integers, their average is even integer"
  - By predicates and quantifiers, $\exists x \exists y((x\%2=1) \wedge (y\%2=1) \wedge ((x+y)/2)\%2=0))$, where x, y are integers

domain

[…]

Nested Quantifiers

- **Wrong Solution:** We **cannot** write in previous example $\exists x \exists y$ $((x\%2=1) \wedge (y\%2=1) \rightarrow ((x+y)/2)\%2=0))$. Why? See Slide 107
- **Exercise:** Write by predicates and quantifiers:
  - Multiplication of two odd integers is odd
  - Some integer may not have inverse (inverse of x is 1/x)
- **Exercise:** State the following propositions in English, and then write and prove their truth values
  (a) $\forall x \forall y \forall z(x+y>z)$ (b) $\exists x \exists y \exists z(x+y>z)$ (c) $\forall x \exists y(xy=x)$
  (b) $\exists x \forall y(xy \neq x)$ (e) $\exists x \exists y \forall z(xy=z)$
- **Exercise:** Explain what happens if you do some changes in the ordering of the quantifiers in the following two propositions (hint: no effect! See right-side box)
  (a) $\forall x \forall y \forall z(x+y<z)$ (b) $\exists x \exists y \exists z(x+y<z)$

$\forall x \forall y \forall z$ =
$\forall y \forall z \forall x$ =
...

$\exists x \exists y \exists z$ =
$\exists z \exists x \exists y$ =
...

Negation in Nested Quantifiers

- For multiple/nested quantifiers, negation works from left to right
- De-Morgan law is applied for each quantifier one by one from left to right
- Finally, the proposition is negated
- **Example:** Find the negation of $\forall y \exists x (x-y \neq 0)$

  $\neg \forall y \exists x (x-y \neq 0)$

  $= \exists y \neg \exists x (x-y \neq 0)$ // by De-Morgan law

  $= \exists y \forall x \neg (x-y \neq 0)$ // by De-Morgan law

  $= \exists y \forall x (x-y = 0)$
- **Exercise:** Find the negation of the following propositions: (a) $\exists x \exists y \forall z (yz=x)$, (b) $\exists x \exists y \forall z (x+z \rightarrow y)$

$\neg \forall = \exists \neg$

$\neg \exists = \forall \neg$

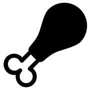
Lecture 6
Rules of Inference and Proof Techniques

… There is no deity except Him, so how are you deluded? (Quran 35:3)

Motivation

1. I like bread and meat
2. If I get rice, then I do not like bread
3. If I do not get rice, then I do not like meat

- From the above three statements, can we conclude this:
  4. I do not like meat
- Yes. How? This is called **rules of inference**: conclude or deduct something from the given statements
- But (1) implies that “I like meat”! This contradicts (4). So, is it possible to deduct some contradiction? Yes!
- These are what we shall see in this lecture
- **Exercise:** What else (like (4)) can you deduct from those three statements (1), (2), (3)?



Rules of Inference

- **Example:** Consider the following two statements
    1. If you get A+, then you are a good student
    2. You got A+
  - From these two statements, we can conclude that "you are a good student"
- **Example:** Consider the following two statements
    1. If I know the password, then I can access the network
    2. I know the password
  - From these two statements, we can conclude that "I can access the network"
- Why are the above deductions correct? (Next slides …)

$$\begin{array}{l} \textit{statement} \\ \textit{statement} \\ \dots \\ \textit{statement} \\ \hline \therefore\ \textit{conclusion} \end{array}$$

Modus ponens

- Two examples in the previous slide are of this form:

  $p \rightarrow q$ // in the first example, p: A+, q: good student

  $\underline{p \qquad}$ // in second example, p: password, q: access

  $\therefore q$ // $\therefore$ means "Therefore"
- This deduction is called **modus ponens**
- The deduction of q is correct. Because, from $p \rightarrow q$, if p is true, then q is also true. Nothing wrong is there
- Moreover, if we cannot deduct q, that means if q is false, then $p \rightarrow q$ would not hold. Because, p=T, q=F means $p \rightarrow q$ = F from the truth table of implication ($\rightarrow$)
- This is called **argument**, which validates modus ponens
- There is another way to show this validity (next slide …)

Modus ponens:

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

Modus ponens

- Modus ponens can be stated as follows:
  "$p \rightarrow q$ and p" implies q
- More mathematically, like this way: $((p \rightarrow q) \wedge p) \rightarrow q$
- The following truth table shows that $((p \rightarrow q) \wedge p) \rightarrow q$ is always true, that means a tautology

Truth Table for modus ponens				
p	q	$p \rightarrow q$	$(p \rightarrow q) \wedge p$	$((p \rightarrow q) \wedge p) \rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Modus ponens:

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

Modus tollens

- Modus ponens is the most basic rule of inference
- It can be used to establish other rules
- One such rule is **Modus tollens:**

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

- **Example:** Consider the following two statements
    1. If it rains, then the weather becomes cold
    2. The weather is not cold
  - From the above two statements, we can conclude than "it is not raining"
  - This is by Modus tollens

Modus tollens:

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

Modus tollens

- **Example:** Derive Modus tollens from Modus ponens
  - Consider this Modus ponens →

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

  - Remember, by contrapositive, $p \rightarrow q$ is same as $\neg q \rightarrow \neg p$
  - So, this Modus ponens can be written as

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

  - This is the Modus tollens

Modus tollens:

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

- **Exercise:** Verify Modus tollens by truth table

Common Rules of Inference

- In addition to Modus ponens and Modus tollens, there are some other common rules of inferences
- The right-side table shows the list →
- They are easy to understand and verify
- **Example:** Verify disjunctive syllogism
  - The first rule $p \vee q$ is true
  - So at least one p or q is true
  - But, by the second rule, $\neg p$ is true
  - So, p is false. So, q must be true
- **Exercise:** Verify remaining rules similarly
- **Exercise:** Verify them by truth tables

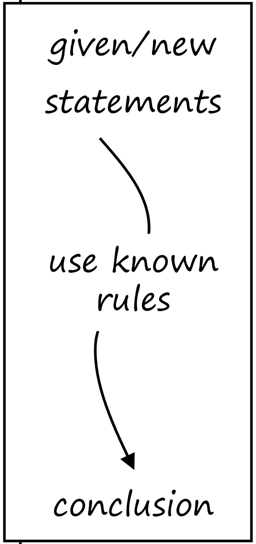
Rules	Name
$p \rightarrow q$ p $\therefore q$	Modus ponens
$p \rightarrow q$ $\neg q$ $\therefore \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
p $\therefore p \vee q$	Addition
$p \wedge q$ $\therefore p$	Simplification
p q $\therefore p \wedge q$	Conjunction

Deduction

- Rules of inferences can be used to **deduct** a statement (called **conclusion**) from some given statements
- **Example:** Consider the example that we saw at the beginning of this lecture (deduct 4 from 1, 2, 3):
  1. I like bread and meat
  2. If I get rice, then I do not like bread
  3. If I do not get rice, then I do not like meat

  ---
  4. $\therefore$ I do not like meat (conclusion)

  - We shall show that this deduction is correct
  - Suppose b: I like bread, m: I like meat, r: I get rice
  - Then the three given statements become as follows: (continues to the next slide …)



Deduction

- (Continued from the previous slide…)
  1. I like bread and meat $\longrightarrow$ $b \wedge m$
  2. If I get rice, then I do not like bread $\rightarrow$ $r \rightarrow \neg b$
  3. If I do not get rice, then I do not like meat $\neg r \rightarrow \neg m$
- We gradually derive (4) (which is $\neg m$) as follows:
  5. b // from (1) by simplification
  6. $\neg r$ // from (2) and (5) by Modus tollens
  7. $\neg m$ // from (3) and (6) by Modul ponens
- Observe that, from (1) we get m by simplification. But we have deducted $\neg m$. It does not mean the deduction is wrong. The given statements may be contradictory

given/new statements

use known rules

conclusion

Deduction

- **Example:** Show that the statements (1), (2) and (3)
  1. His car is Toyota or white
  2. I saw his car to be Ford
  3. A white car is comfortable in summer

  concludes 4.: His car is comfortable in summer
- **Solution:** Let t: Toyota, w: white, c: comfortable
  - Then (1), (2), (3) become:
    1. $t \vee w$
    2. $\neg t$ // "Ford" means "not Toyota"
    3. $w \rightarrow c$ // same as "white implies comfortable"
  - Continue to the next slide …

given/new statements

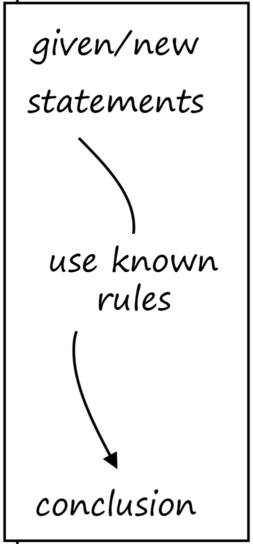
use known rules

conclusion

Deduction

- (Continued from the previous slide…)
- Now we derive (4) (which is c) gradually:
  5. w // from (1) and (2) by disjunctive syllogism
  6. c // form (3) and (5) by Modus ponens
- **Exercise:** Show that the Statements (1) to (4)
  1. If Omer does not pray, he does not feel well
  2. If Omer does not feel well, he becomes unjolly
  3. If Omer meets Mohammad, he becomes jolly
  4. Omer met Mohammad today

  concludes 5.: Omer prayed today
- **Exercise:** Create by yourself some exercises similar to the above example and exercise, and then solve



Two Common Mistakes

- **Example (Mistake 1):** Consider the following deduction
  1. If he takes ice cream, he gets cold
  2. He got cold
  ____
  3. $\therefore$ He took ice cream
  - At a first look, the above deduction looks correct, because cold means ice cream
  - But it is wrong. Because, there may be other means of getting cold, for example, swimming
  - This can be verified by truth table as follows:
  - Take p: ice cream, q: cold, and the above deduction as: $((p\rightarrow q)\wedge q)\rightarrow p$. Then, $((p\rightarrow q)\wedge q)\rightarrow p$ will not be tautology (**Exercise:** Complete that truth table)

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

Two Common Mistakes

- **Example (Mistake 2):** Consider the following deduction
    1. If he takes ice cream, he gets cold
    2. He did not take ice cream

    ---

    3. ∴ He will not get cold
  - Again, at a first look, the above deduction looks correct, because no ice cream means no cold
  - But it is wrong, because, he can get cold by other reason, for example because of swimming
  - This can also be verified by truth table as before
- **Exercise:** What happens if we change (1) in the two previous examples as follows: (1): He gets cold **if and only if** he takes ice cream?

$$\cancel{\begin{array}{l} p \to q \\ \neg p \\ \hline \therefore\ \neg q \end{array}}$$

Proof Techniques

- We have seen that deduction can be verified (**proven**) by arguments and by truth tables
- The verification by argument can be more formalized as **theorem** and its **proof**
- A theorem is given in the form: **if p, then q**
- Some common techniques for proving a theorem are:
  - Direct proof
  - Proof by contrapositive } Indirect proof
  - Proof by contradiction }
  - Proof by induction → Separate lecture
- Proof techniques can use known facts and known rules that we have seen before

direct proof

...

proof by contrapositive

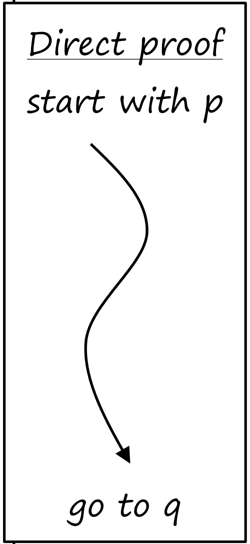
...

proof by Contradiction

...

Direct Proof

- Direct proof works in this way for proving **if p, then q**:
  - Start with p, gradually go to q, stop at q
- **Example:** Proof that square of an odd integer is odd
- Before proving this statement, let us clarify it
  - Here **Theorem** is: square of an odd integer is odd
  - This is same as **Theorem:** If n is odd, then n^2 is odd
  - Do we proof this theorem for only one value of n or for all value of n? That means, the quantifier of n is $\exists$ or $\forall$?
  - It is $\forall$, because the theorem means for all n
  - Moreover, the domain of n is all integers. So we need to prove this for any integer n (next slide …)



Direct Proof

- **Proof:** We now give a direct proof as follows:
  - We start with "p: n is odd" and go to "q: n^2 is odd"
  - Remember, for any integer n, n is odd means n=2k+1, for some integer k
  - So,
$$
\begin{aligned}
n^2 &= (2k+1)^2 \\
&= 4k^2 + 4k + 1 \\
&= 2(2k^2+2k) + 1 \\
&= 2k' + 1 \qquad \text{// } k' \text{ is another integer} \\
&= \text{odd integer (end of proof)}
\end{aligned}
$$
- **Exercise:** Prove the following theorems by direct proof:
  - Square of an even integer is even
  - Difference of two odd integers is even

Direct proof

start with p

go to q

Proof by Contrapositive

- Sometimes, it is convenient to use proof by contrapositive, instead of direct proof while proving **if p, then q**
- Proof by contrapositive works as follows:
  - Take the contrapositive of "if p, then q", which is**: if not q, then not p**
  - Then proof this contrapositive by direct proof
  - That means, start with not q and go to not p (like direct proof)
  - As we know that original implication is equivalent to its contrapositive, proving the contrapositive is equivalent to proving the original theorem

Proof by contrapositive

take $\neg q \to \neg p$

start with $\neg q$

go to $\neg p$

Proof by Contrapositive

- **Example:** Proof that if n^2 is odd, then n is odd
  - Before we proof this theorem by contrapositive, let us try to use direct proof
  - We shall see that using direct proof may not be convenient
  - For direct proof, we start with "p: n^2 is odd" and go to "q: n is odd"
  - $n^2 = \text{odd} = 2k+1$, so $n = \sqrt{(2k+1)}$
  - From here, we need to show that n is odd, that means $\sqrt{(2k+1)} = 2k'+1$ for some integer k'
  - Looks not easy!
  - Let us now try by proof by contrapositive (next ...)

Proof by contrapositive

take $\neg q \to \neg p$

start with $\neg q$

go to $\neg p$

Proof by Contrapositive

- **Proof by contrapositive:**
  - Original statement: **If n^2 is odd (p), then n is odd (q)**
  - Contrapositive: **If n not odd ($\neg$q), then n^2 not odd ($\neg$p)**
  - Start with "$\neg$q: n not odd"
  - n = not odd = even = 2k // k is integer
  - $n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2k'$ // $k' = (2k^2)$ is
    // another integer
  - So, n^2 = even = not odd
  - This ends the proof of the contrapositive as well as the original theorem
- **Exercise:** Proof by contrapositive: if n^3-1 is even, then n is odd. Explain why a direct proof is difficult here

Proof by contrapositive

take $\neg q \to \neg p$

start with $\neg q$

go to $\neg p$

Proof by Contradiction

- Proof by contradiction is little conceptual
- It works as follows for proving the theorem: **if p, then q**
  - We assume that p is true, **but q is false**
  - Then we reach something false (contradiction)
  - We need to use p (if required) during this journey
  - When we reach something false, it shows that our assumption was wrong at the beginning
  - That means, the assumption “q is false” was wrong
  - That means, “q is false” is false
  - So, q is true
  - This proves the theorem that “if p, then q” is correct

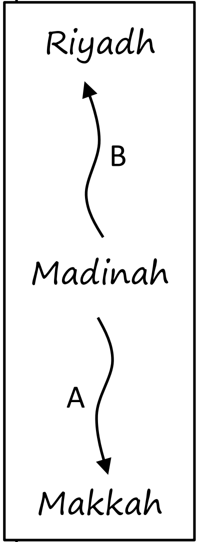
Proof by contradiction

assume $\neg q$

go to “false”

Proof by Contradiction: A Practical Example

- **Example:** Suppose there are two roads out from Madinah: A and B. Road A goes to Makkah and Road B to Riyadh. We want to prove this by proof by contradiction: If I want to go to Makkah from Madinah, then Road A is the correct road
- To prove this by proof by contradiction, we assume that Road A is a wrong road to Makkah from Madinah
- So, we start by Road B from Madinah
- After travelling Road B, we reach Riyadh, and realize that it is a wrong destination. So, we reached something false
- That means, somewhere there is a mistake
- After reviewing everything about our journey, we found no mistake. So, mistake is actually the initial assumption that Road A was wrong. That means, Road A is the correct road



Proof by Contradiction

- **Example:** Proof by contradiction: if n and m are odd integers, then mn is odd
- **Proof:** Here, p: n and m are odd, q: nm is odd
  - We assume that n and m are odd integers (p true), but mn is not odd (q false). That means, mn is even
  - n, m are odd, so $n = 2k+1$, $m=2k'+1$ for some integers k, k'
  - $mn=(2k+1)(2k'+1)=4kk'+2k+2k'+1=2(2kk'+k+k')+1$ $= 2k''+1$ for integer k'' (here, $k'' = 2kk'+k+k'$) = odd
  - This is false, because we assumed that mn is even
  - So, our initial assumption "mn is even" was wrong
  - So, mn is odd. This ends the proof

Proof by contradiction

assume $\neg q$

go to "false"

Proof by Contradiction

- **Example:** Proof by contradiction that 2^{odd} is even
- **Proof:**
  - Here p is not given. That means, there is nothing wrong in p. So, we can assume that p is true
  - Here, q: 2^{odd} is even
  - Suppose that q is false, that means, 2^{odd} is odd
  - Now, $2^{odd} = 2^{(2k+1)} = 2^{(2k)}2^{1}$ = (integer)*2 = even
  - This is false, because we assumed that 2^{odd} is odd
  - So, our initial assumption "2^{odd} is odd" was wrong
  - Therefore, 2^{odd} is even, and it completes the proof
- **Exercise:** Proof by contradiction:
  (a) 3^{even} is odd, (b) 3^{odd} = odd, (c) odd^{odd} = odd

Proof by contradiction

assume $\neg q$

go to "false"

Proof of Equivalence ($\leftrightarrow$)

- Sometimes, a theorem can be like this: **p if and only if q**
- Remember that "if and only if" means "$\leftrightarrow$"
- Also remember that $p \leftrightarrow q$ means $p \rightarrow q \wedge q \rightarrow p$
- So, to prove $p \leftrightarrow q$, we need **two proofs**, one for $p \rightarrow q$ and another for $q \rightarrow p$
- We can prove any of them first, and the other one next
- To proof each of them, we can use any proof technique that have seen before (direct proof, indirect proof, etc.)
- **Example:** Suppose that m is non-negative integer. Proof that 2^m is odd if and only if $m=0$
- Proof next slide…
- We can verify this theorem: Take m=0. So, $2^{m=0} = 1 =$ odd

proof $(p \leftrightarrow q)$
=
proof $(p \rightarrow q)$
+
proof $(q \rightarrow p)$

Proof of Equivalence ($\leftrightarrow$)

- **Proof:** Here, p: 2^m is odd, q: m=0. Moreover, $m \geq 0$
- **Part 1: Proof for $q \rightarrow p$ (if m=0, then 2^m is odd)**
  - We use direct proof
  - $2^m = 2^0 = 1$ = odd (end of proof of Part 1)
- **Part 2: Proof for $p \rightarrow q$ (if 2^m is odd, then m=0)**
  - We use proof by contrapositive
  - So, we shall proof that if $m \neq 0$, then $2^m \neq$ odd
  - $m \geq 0$ and $m \neq 0$ means, $m \geq 1$
  - Now, $2^{m \geq 1} = 2^{m-1+1} = 2^1 * 2^{m-1 \geq 0} = 2 *$(integer ≥ 1) = 2*(integer) = even $\neq$ odd (end of proof of Part 2)
- As we have proven both parts, the proof is complete
- **Exercise:** Prove that m^3 is even iff m is even

proof ($p \leftrightarrow q$)

=

proof ($p \rightarrow q$)

+

proof ($q \rightarrow p$)

Lecture 7
Sets

Let there be a group among you who call others to goodness… (Quran 3:104)

Definition, Examples

- **Set** is a **collection** (ordering not important) of **similar** elements
- Repetition of elements are allowed
- A set is denoted like this **{…, …, …, …}**, where the elements are enclosed by **{** and **}**
- **Example:**
  - D={2, 3, -2, 5} is a set of some integers
  - B={2, 3.5, -1.2, 3, 44} is a set of real numbers
  - A={cat, horse, cow} is a set of animals
  - S={7, 2, cat} is not a set of integers or a set of animals, as the elements are not of similar type
  - S= 5, 3, 4 is not a set, because { and } are missing

Set:

same type

unordered OK

repetition OK

{ } important

$=, \in, \notin$

- **Example:** Two sets {7, 1, 2, 3, 3} and {7, 1, 2, 3} are equal, because repetition of elements is not counted. So, {7, 1, 2, 3, 3}={7, 1, 2, 3}
- **Example:** Two sets {7, 1, 3, 3} and {1, 3, 3, 7} are equal, because ordering is not important. So, {7,1,3,3}={1,3,3,7}
- The symbol $\in$ denotes if an elements **is** in a set
- The symbol $\notin$ denotes if an elements **is not** in a set
- **Example:**
  - $-19 \in \{2, 7, 19, 0, -19, 5\}$
  - dog $\notin$ {cat, horse, cow, camel, donkey}
- **Exercise:** Write a set that is equal to {3, 3} but with different number of elements

$\in$: *in set*

$\notin$: *not in set*

Empty Set, Universal Set

- A set can be empty, with no elements, like this { }
- An **empty set** is denoted by ∅, so **∅={ }**
- An empty set is also called a **null set**
- A **universal set** contains all possible elements
- A universal set is denoted by **U**
- U is mentioned when another set is drawn from it
- **Example:**
  - A universal set of positive even integers is U={2, 4, 6, 8, …}
  - For set {7, 5, -9, 1}, the universal set can be the set of all integers or the set of all odd integers
- **Exercise:** What can be the universal set of {-3.4,-2,-1.5}?

∅: { }

U: all

Some Common Sets

- Some frequently used sets have their own notations
- **Example:**
  - **N** = {1, 2, 3, …} is the set of natural numbers
  - **Z** = {…, -3, -2, -1, 0, 1, 2, 3, …} is the set of integers
  - $\mathbf{Z}^+$ = {1, 2, 3, 4, 5, …} is the set of positive integers
  - $\mathbf{Z}^-$ = {-1, -2, -3, -4, -5, …} is the set of negative integers
  - **R** = The set of all real numbers
  - $\mathbf{R}^+$ = The set of all positive real numbers
  - $\mathbf{R}^-$ = The set of all negative real numbers
- All the sets in the above examples are universal sets
- **Exercise:** Find from other sources what is the set Q?

$\mathcal{N}$

$\mathcal{Z}$

$\mathcal{Z}^+$

$\mathcal{Z}^-$

$\mathcal{R}$

$\mathcal{R}^+$

$\mathcal{R}^-$

$\mathcal{Q}$

Cardinality

- **Cardinality** of a set A is the number of **distinct** elements in A
- It is denoted by |A|
- **Example:** If A = {1,2,7}, then |A| = 3
- **Example:** If A = {5,3,3,2,2,7,7,7}, then |A| = 4
- **Example:** $|\varnothing| = 0$
- When a set has infinite number of elements, then it is called an **infinite** set. Cardinality of an infinite set is infinite
- **Example:** N, Z, Z^+, Z^-, R, R^+, R^-, {all integers bigger than 5} are some infinite sets. Cardinality of all of them are infinite
- **Example:** If A = $\{x \in Z \mid$ x is even and positive}, then A = {2,4,6,8,10,…}. Here, |A| = infinite
- **Exercise:** If A={English alphabet}, then |A| = ?

Cardinality: Number of distinct element

Set Representation: Other Ways

- A set can be represented in many other ways
- A general form is like this **S = {x| condition on x}**
- It reads as: S is the set of x such that condition on x is satisfied
- **Example:** The set S of all positive integers that are 5 or more can be written as any of the following ways:
  - S = {positive integers that are 5 or more}
  - S = {x|x is a positive integer and at least 5}
  - $S = \{5, 6, 7, 8, \ldots\}$
  - $S = \{x \in Z^+ | x \geq 5\}$
  - $S = \{x | (x \in Z^+) \wedge (x \geq 5)\}$
- **Exercise:** Try to write the above set in another way

$S=\{x|condition\}$

Set Representation: Other Ways

- **Example:** Describe the following set by text and then write at least five elements of it: $\mathbf{S = \{x \in N \mid x\text{-}5 \notin N\}}$
- **Answer:**
  - **By text:** S is a set of natural numbers such that if we deduct 5 from each of them, then they are no longer natural numbers
  - **Five numbers:** We know N = {1, 2, 3, 4, 5, …}. So x is such that x-5 not in N. That means, $x-5 < 1$. So, $x < 6$.
  - There are only five such x in N, which are 1, 2, 3, 4, 5
  - So, **S = {1, 2, 3, 4, 5}**
  - Observe that 6, 7, 8, … are not in S. Because, in that case, $x-5 \geq 1$ and falls within N, which violates $x-5 \notin N$

$S=\{x \mid cond.\}$

Set Representation: Other Ways

- **Example:** Describe the following set by text and then write at least ten elements of it: **S = {$x^2 \in Z | x \notin Z$}**
- **Answer:**
  - **By text:** S is a set of integers whose roots are not integers (that means, roots are real number)
  - **Ten numbers:** Integers whose root is also integers are called perfect square, such as 1, 4, 9, 16, 25, …
  - So, S does not contain those perfect squares
  - Moreover, x^2 is positive
  - So, S is positive integers except perfect squares
  - Therefore, **S = {2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, …}**

S={x|cond.}

Set Representation: Other Ways

- **Example:** Describe the following set by text and then write some elements of it: $\mathbf{S = \{x>0 \wedge x<0\}}$
- **Answer:**
  - **Text:** S is the set of numbers that are both positive and negative
  - **Elements:** No element can be both positive and negative. So, the set is empty. $\mathbf{S = \{\ \}}$
- **Exercise:** For the following sets write their description by text and then write at least ten elements in the set:
  - $S = \{x \geq 0 \wedge x \leq 0\}$
  - $S = \{x \in Z \mid -x \in Z\}$
  - $S = \{x^2 \in N \mid x \notin N\}$

$S=\{x \mid condition\}$

Subset, Superset

- For two sets A and B, if all elements of A are also elements of B then A is called a **subset** of B and is denoted by $A \subseteq B$
- Observe that, B may have some other elements too
- B is also called a **superset** of A, and denoted as $B \supseteq A$
- **Example:** $\{2, 3, 4\} \subseteq \{4, 3, 5, 7, 2\}$, because 2, 3, 4 in the left-side set are also available in the right-side set
- **Example:** $\{3, 3, 3, 3, 3\} \subseteq \{2, 3\}$, because the left-side set has only one element '3', which is in the right-side set
- If some elements of A are not in B, then A is not a subset of B. It is denoted as $A \nsubseteq B$
- A={7,5,2}, B={2}. $A \nsubseteq B$, because 7, 5 are in A but not in B

subset: $\subseteq$

superset: $\supseteq$

Subset

- For any set A, $A \subseteq A$, because all elements of A are in A
- **Example:** $\{3, 4\} \subseteq \{3, 4\}$
- Empty set $\varnothing$ is a subset of any other set, including itself
- Because, "empty" or "nothing" is available in all sets
- **Example:** $\varnothing \subseteq \{3, 4\}$, $\varnothing \subseteq \varnothing$, $\varnothing \subseteq A$ for any set A
- For A and B, if both $A \subseteq B$ and $B \subseteq A$ are true, then $A=B$
  - Because, by $A \subseteq B$, all elements of A are in B
  - By $B \subseteq A$, all elements of B are A
  - So, A and B have same elements
- **Example:** $\{7,1,2\} \subseteq \{2,1,7\}$, $\{2,1,7\} \subseteq \{7,1,2\}$. So, $\{7,1,2\}=\{2,1,7\}$
- **Exercise:** Justify whether the followings are true or not:
  $\{0\} \subseteq \varnothing$, $\{1,1,1\} \supseteq \{1,1\}$, $\{1,1,1\}=\{1,1\}$, $\{x+1 \mid x \in N\} \not\subseteq \{x \mid x \in N\}$

$A \subseteq A$

$\varnothing \subseteq \varnothing$

$\varnothing \subseteq A$

$A \subseteq B \wedge B \subseteq A$

$=$

$A=B$

Proper Subset

- If A is a subset of B, but B has element that is not in A (that means $A \neq B$), then A is called a **proper subset** of B
- It is denoted as $A \subset B$ or $B \supset A$
- **Example:** $\{2, 3, 4\} \subset \{4, 3, 5, 7, 2\}$, because $\{2, 3, 4\}$ is a subset of $\{4,3,5,7,2\}$ and 7 is in B but not in A
- **Example:** $\{2,3,4\} \not\subset \{4,2,2,3\}$, because $\{2,3,4\}=\{4,2,2,3\}$
- A proper subset is also a subset, but the opposite is not true (there are subsets that are not proper subset)
- Proper subset can also be said as: $A \subset B = (A \subseteq B) \wedge (A \neq B)$
- **Exercise:** Justify whether the followings are true or not **(a)** $\varnothing \subset \varnothing$, $\varnothing \subset A$ for any non-empty set A **(b)** $\{x+1 \mid x \in N\} \subset \{x \mid x \in N\}$

$A \subseteq A$

$\varnothing \subseteq \varnothing$

$A \subseteq B \wedge B \subseteq A$

$=$

$A = B$

All Possible Subsets

- **Example:** How many subsets are there for A={4, 2, 3}?
  - Eight: { } (or ∅), {4}, {2}, {3}, {4,2}, {4,3}, {2,3}, {4,2,3}
  - There are no more. Why?
  - Because, we have considered all possible ways to create the subsets of A---{no element}, {1 element}, {2 elements}, and {all elements}
- **Example:** All possible subsets of {2, 3, 4, 5} are:
  ∅, {2}, {3}, {4}, {5}, {2,3}, {2,4}, {2,5}, {3,4}, {3,5}, {4,5}, {2,3,4}, {2,3,5}, {3,4,5}, {2,4,5}, {2,3,4,5} --- total 16
- **Example:** All possible subsets of ∅ is just ∅
- **Exercise:** Find all possible subsets of {1} and {1, 1, 2, 3, 4, 5, 6}

All possible subsets:
∅,
{1 element},
{2 elements},
…
{all elements}

All Possible Subsets

- There is another way to generate all subsets of A
- That technique also tells how many subsets are possible
- The technique is related to binary numbers as follows:
    - Total number of subsets $2^{|A|}$. How? (Remember, $|A|$ is cardinality of A)
    - For each element in A, there are 2 possibilities: (i) it is present in a subset (denote by binary 1) (ii) absent in a subset (denote by binary 0)
    - Over all $|A|$ elements, total number of possibilities is $2*2*\ldots*2$ ($|A|$ times) = $2^{|A|}$
    - Like (0/1)(0/1)(0/1)…$|A|$ times = $2^{|A|}$ binary numbers
    - Each binary number represents one subset

All possible subsets = $2^{|A|}$

All Possible Subsets

- **Example:** All possible subsets of A = {5,7,8}
  - |A| = 3, so the number of subsets is $2^3 = 8$
  - Take three binary digits for 5,7,8 from left to right
  - 8 possible binary numbers and the corresponding subsets are given in the right-side table
  - For example, 000 means 5, 7, 8 absent, so the subset is { }
  - 110 means 5, 7 present, 8 absent, so the subset is {5,7}
  - 111 means 5,7,8 present, so the subset is {5,7,8}
- **Exercise:** Find all possible subsets of ∅, {a, b, c, d, e}, {6, 7, 8, 5} by finding the corresponding binary numbers

000 → { }
001 → {8}
010 → {7}
011 → {7,8}
100 → {5}
101 → {5,8}
110 → {5,7}
111 → {5,7,8}

Set of Sets

- So far, we have seen that the elements of a set are numbers, animals, etc.
- But the elements themselves can be sets
- **Example:** A = {{1,2}, {3,4}, ∅, {5,6,1}}
  - Each element in this set itself is a set, including ∅
  - |A| is 4, because there are four elements inside
  - Observe that |A| is **not** 6. It is **wrong** to think that A has six different elements--- 1, 2, 3, 4, 5, 6. So, |A| will be 6. No!
- **Example:** {∅} is same as {{}}. It is a set with only one element, which is an empty set {}
- **Exercise:** Find all subsets of {∅} and {{1,2}, ∅, {5,6,1}}

All possible subsets

=

$2^{|A|}$

Power Set

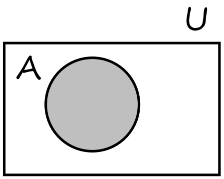
- **Power set** of a A is the set of all possible subsets of A
- It is denoted as $\mathcal{P}(A)$
- **Example:** Suppose that A={2,3,4}. Then $\mathcal{P}(A)$ = {∅, {2}, {3}, {4}, {2,3}, {2,4}, {3,4}, {2,3,4}}
- Cardinality of power set $|\mathcal{P}(A)|$ is $2^{|A|}$, which is the number of all possible subsets of A
- **Example:** In the previous example, $|\mathcal{P}(A)| = 2^{|A|} = 2^3 = 8$
- **Example:** Power set of {{1}, {2}} is {∅, {{1}}, {{2}}, {{1},{2}}} and its cardinality is 4
- **Example:** Power set of ∅ is {∅}
- **Exercise:** Find the power set and its cardinality for the following sets: {∅}, {{1,2},∅,{5,6,1}}, {1,1,1}, {1,2,3,4, 5}

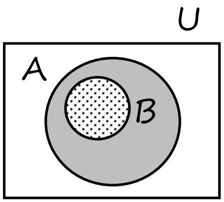
power set: set of all subsets

Set Operations

- Set operations are applied to one or more sets
- Output of a set operation is another set
- Some common set operations are: **union**, **intersection**, **complement**, **difference**
- Before we see set operations, we see **Venn diagram**
- Venn diagram is a very useful way of set representation
- By Venn diagram, a universe U is represented by a rectangle and a set A by a circle inside of U. See this
- Size and position of rectangle and circle are relative, not fixed
- **Example:** Venn Diagram of B⊂A
- **Exercise:** Draw Venn diagram of the universal set U

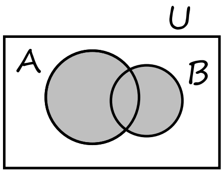
Venn diagram

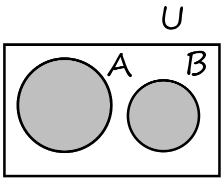




Union

- **Union** of two sets A and B is the set that contains all elements that are in A, or in B, or in both
- It is denoted as $A \cup B$
- Common elements of A and B are not repeated in $A \cup B$
- **Example:**
  - $\{2,3,4\} \cup \{3,4,5\} = \{2,3,4,5\}$
  - $\{2,3,4\} \cup \{2,3,4\} = \{2,3,4\}$
  - {goat, cow}∪{camel} = {goat, cow, camel}
- **Example:** Right-side pictures show the Venn diagram of $A \cup B$ (shaded area) when A and B have (i) common elements, (ii) no common elements
- **Exercise:** Draw the Venn diagram of $A \cup B$ when $A=B$





Union

- Union is like logical **or**
- $A \cup B$ can be considered like this: **(in A) or (in B)**
- Because, union of A and B is the elements that are **in A**, or **in B**, or **in both**
- So, $A \cup B$ can be written as $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$
- There are some simple-but-conceptual unions on sets
- Some of them are given below with brief justification:
  - $A \cup A = A$ // Repeated elements not counted
  - $A \cup B = B \cup A$ // Order does not matter for combining
  - $A \cup U = U$ // U contains all elements of A and more
  - $A \cup \varnothing = A$ // $\varnothing$ has nothing, so nothing to add with A
- **Exercise:** Draw the Venn diagram of $A \cup U$ and $A \cup \varnothing$

$A \cup A = A$

$A \cup B = B \cup A$

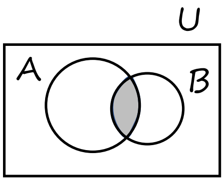
$A \cup U = U$

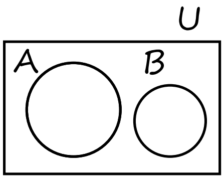
$A \cup \varnothing = A$

Intersection

- **Intersection** of two sets A and B is the set that contains only the elements that are common in A and B
- It is denoted as $A \cap B$
- If A and B have no common element, then $A \cap B$ is empty
- In that case, A and B are called **disjoint**
- **Example:**
  - $\{2,3,4\} \cap \{3,4,5\} = \{3,4\}$
  - $\{a,b,c\} \cap \{b,a,c\} = \{a,b,c\}$
  - $\{\text{goat, cow}\} \cap \{\text{camel}\} = \varnothing$
- **Example:** Right-side picture shows the Venn Diagram of $A \cap B$ (shaded area) when A and B are (i) not disjoint, and (ii) disjoint

Intersection





Intersection

- Intersection is like logical **and**
- $A \cap B$ can be considered like this: **(in A) and (in B)**
- Because, union is **in A and in B** (same as logical and)
- So, $A \cap B$ can be written as $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$
- Some simple-but-conceptual intersections on set:
  - $A \cap A = A$ // Common elements of A and A are A
  - $A \cap B = B \cap A$ // Order not important for finding
    // common elements
  - $A \cap U = A$ // All elements in A are also in U
  - $A \cap \varnothing = \varnothing$ // $\varnothing$ has nothing, so no common
- **Exercise:** Draw the Venn diagram of $A \cap U$ and $A \cap \varnothing$
- **Exercise:** What is $\varnothing \cap \varnothing$? Why?

$A \cap A = A$

$A \cap B = B \cap A$

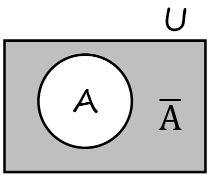
$A \cap U = A$

$A \cap \varnothing = \varnothing$

Complement

- **Complement** of a sets A is the set that contains all elements that are not in A
- It is denoted as $\overline{\mathrm{A}}$ or A^c
- It is important to mention the universal set U while finding $\overline{\mathrm{A}}$
- **Example:** Suppose that A = {2,3,4} and U is the set of all integers. Then $\overline{\mathrm{A}}$= {…, -5, -4, -3, -2, -1, 0, 1, 5, 6, 7, 8, …}
- **Example:** Suppose A = {1,2,3,4,…}, and U=**N**. Then $\overline{\mathrm{A}}$={ }
- **Example:** If A={x|x is even} and U=Z, then $\overline{\mathrm{A}}$={x|x is odd}
- **Example:** Right-side picture (shaded area) shows the Venn Diagram of $\overline{\mathrm{A}}$

Complement



Complement

- A^c can be written as $A^c = \{x \mid x \notin A\}$
- A pair of complements nullify each other, like double negation. That means, $(A^c)^c = A$. Why?
- Because, the second complement means the elements which are not in A^c. But the elements that are not in A^c are exactly the elements of A. So, $(A^c)^c = A$
- $\varnothing^c = U$ // $\varnothing$ has nothing, so $\varnothing^c$ has everything
- $U^c = \varnothing$ // U has everything, so U^c has nothing
- $A \cup A^c = U$ // Elements inside and outside of A form U
- $A \cap A^c = \varnothing$ // Inside and outside of A have nothing in //common
- **Exercise:** If $A = \{x \mid (x \notin \mathbf{Z}^+) \wedge (x \notin \mathbf{Z}^-)\}$ and $U = \mathbf{Z}$, then find A^c

$(A^c)^c = A$

$\varnothing^c = U$

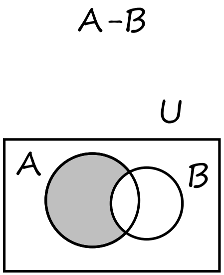
$U^c = \varnothing$

$A \cup A^c = U$

$A \cap A^c = \varnothing$

Difference

- **Difference** between two sets A and B (denoted as A-B) is a set that contains all elements of A that are not in B
- That means, common elements of A and B are deleted form A. See the Venn diagram of A-B (shaded area)
- A-B can be written as A-B = $\{x \mid (x \in A) \wedge (x \notin B)\}$
- **Example:** Suppose, A={2,3,9} and B={2,5,6,7}. Then A-B = {3,9}. Because, common element 2 is deleted from A
- **Example:** Suppose, A = {X, Y} and B={b, c}. Then A-B ={X, Y}. Because, no common element, so A-B remains as A
- **Example:** If A={x|x is even} and B={x|x is integer}, then A-B=∅. Because, B has both odd and even integers, and all even integers are deleted from A



Difference

- Some simple-but-conceptual set differences are:
- $A-B \neq B-A$ // Example: $A=\{1,2\}$, $B=\{2,3\}$, $A-B=\{1\}$, $B-A=\{3\}$
- $A-A = \varnothing$ // Everything of A are deleted from A
- $U-A = A^c$ // After deleting all of A from U, A^c remains
- $A-\varnothing = A$ // Nothing is removed from A, so A remains A
- $\varnothing-A = \varnothing$ // $\varnothing$ has nothing. Nothing can be deleted
  // from $\varnothing$. So, $\varnothing$ remains $\varnothing$
- **Exercise:**
  - Suppose, $A=\{x \mid x \in \mathbf{Z}\}$ and $B=\{x \notin \mathbf{Z}^+\}$. Find A-B and B-A
  - Is this true: $(A-B) \subseteq A$? Explain with some examples
  - Explain by Venn diagram why the followings are true:
    (i) $A-B=A-(A \cap B)$ **(ii)** $A-B=A \cap B^c$

$A-B \neq B-A$

$A-A = \varnothing$

$U-A=A^c$

$A-\varnothing = A$

$\varnothing-A = \varnothing$

Common Set Operations

- There are some other common set operations
- These common operations are frequently used to derive other set operations
- They have names too
- See the right-side table
- **Exercise:** Verify each law in the right-side table by drawing two Venn diagrams for the left side and the right-side of "=" and show that both are same

Set Operations	Name
$A \cap U = A$ $A \cup \varnothing = A$	Identity law
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination law
$A \cup A = A$ $A \cap A = A$	Idempotent law
$(A^c)^c = A$	Double complement
$A \cup B = B \cup A$ $A \cap A = B \cap A$	Commutative law
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative law
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive law
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De-Morgan's law
$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$	Complement law
$A\text{-}B = A \cap B^c$	Definition of "–"

Proving Set Operations

- Common rules are used to prove set operation results
- **Example:** Prove that $\overline{A \cup B \cup C} = \overline{A} \cap \overline{B} \cap \overline{C}$

$$\overline{A \cup B \cup C} = \overline{A \cup (B \cup C)} \quad \text{// Associative law}$$
$$= \overline{A} \cap \overline{(B \cup C)} \quad \text{// De-Morgan's law}$$
$$= \overline{A} \cap (\overline{B} \cap \overline{C}) \quad \text{// De-Morgan's law}$$
$$= \overline{A} \cap \overline{B} \cap \overline{C} \quad \text{// Associative law}$$

- **Example:** Show that $(A-B) \cap (B-C) = \varnothing$

$$(A-B) \cap (B-C) = (A \cap B^c) \cap (B \cap C^c) \quad \text{// Definition of “–”}$$
$$= (A \cap C^c) \cap (B \cap B^c) \quad \text{// Associative law}$$
$$= (A \cap C^c) \cap \varnothing \quad \text{// Complement law}$$
$$= \varnothing \quad \text{// Domination law}$$

$(A^c)^c = A$

$\varnothing^c = U$

$U^c = \varnothing$

$A \cup A^c = U$

$A \cap A^c = \varnothing$

Set Membership Tables

- **Set membership table** is like truth table
- '1' means the item is in the set,
  '0' means not in the set
- $\cup$ is like $\vee$, $\cap$ is like $\wedge$,
  complement is like $\neg$
- Set membership table can be used to verify set identities
- Two columns for left and right sides will be same
- **Example:** Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$ by set membership table
  - The right-side table is the answering table
  - Two columns for $\overline{A \cap B}$ and $\overline{A} \cup \overline{B}$ are same

Set Membership Table for $\overline{A \cap B} = \overline{A} \cup \overline{B}$

A	B	$\overline{A}$	$\overline{B}$	$A \cap B$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
0	0	1	1	0	1	1
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	1	0	0

=

Set Membership Tables

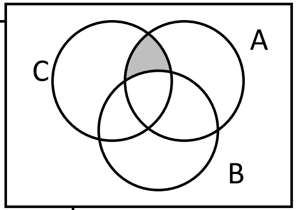
- **Example:** The below table proves $\overline{A \cup B \cup C} = \overline{A} \cap \overline{B} \cap \overline{C}$

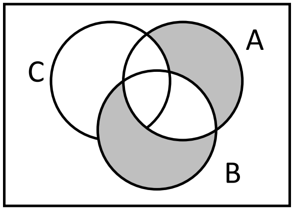
Set Membership Table for $\overline{A \cup B \cup C} = \overline{A} \cap \overline{B} \cap \overline{C}$										
A	B	C	$\overline{A}$	$\overline{B}$	$\overline{C}$	$A \cup B$	$A \cup B \cup C$	$\overline{A \cup B \cup C}$	$\overline{A} \cap \overline{B}$	$\overline{A} \cap \overline{B} \cap \overline{C}$
0	0	0	1	1	1	0	0	1	1	1
0	0	1	1	1	0	0	1	0	1	0
0	1	0	1	0	1	1	1	0	0	0
0	1	1	1	0	0	1	1	0	0	0
1	0	0	0	1	1	1	1	0	0	0
1	0	1	0	1	0	1	1	0	0	0
1	1	0	0	0	1	1	1	0	0	0
1	1	1	0	0	0	1	1	0	0	0

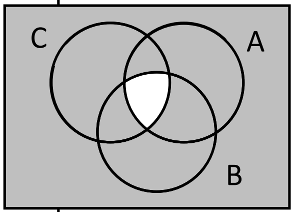
=

Proving Set Operations

- **Exercise:** Prove the followings by using common set operation rules and by set membership tables:
  - $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$
  - $(A-B) \cup (B-A) = (A \cup B) - (A \cap B)$
  - $(A \cap B) \cup \overline{A} = (B \cup \overline{A})$
- **Exercise:** Draw Venn diagram for
  - $\overline{A \cap B \cap C}$
  - $(A-B) \cup (B-A)$
  - $(A \cap B) \cup \overline{A}$
- **Exercise:** Write the expressions for the shaded area of these three Venn diagrams







Lecture 8
Relations and Functions

…And be mindful of Allah—in whose name you appeal to one another—and honor family relations. Surely Allah is ever watchful over you. (Quran 4:1)

Motivation

- Suppose a country maintains two **relationship** records, one for mother-child and another for husband-wife
- When a new couple get married, a new entry (husband name, wife name) is added in the husband-wife record
- When a child is born, a new entry (mother name, child name) is added in the mother-child record
- Now, after some years, the country needed the information about who is the father of which child
- They do not have any father-child record
- Can they find it from husband-wife and mother-child records?
- Yes. Relations are used in this type of applications

Husband-wife

+

Mother-child

$\Rightarrow$

Father-child

Relation Comes from Cartesian Product

- **Cartesian product** is important to understand relations
- **Cartesian product** or **cross product** happens between two or more sets
- Cartesian product is denoted by $\times$
- Cartesian product of two sets $A \times B$ is a set of all possible pair (a,b), where a comes from A and b comes from B
- In another way to say: $A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$
- **Example:** Suppose that A = {f, m} and B = {3, 4, 5}. Then $A \times B$ = {(f,3), (f,4), (f,5), (m,3), (m,4), (m,5)}
- **Example:** If A = {a,b} and B = {a}, then $A \times B$ = {(a,a), (b,a)}
- **Exercise:** Find $A \times B$ for A = {1,1,2} and B = {a,b,c,c}

Cartesian product $A \times B$

=

All possible pairs (a,b), $a \in A$, $b \in B$

Cartesian Product

- **Order** of a and b in the pair (a,b) is important for A×B
- **Example:** A={a,b}, B={2}. Then A×B={(2,a),(b,2)} is wrong
  - Because, the pair (2,a) is not a correct pair
  - 2 is not an element of A and a is not an element if B
  - The correct answer is A×B = {(a,2), (b,2)}
- **Example:** However, if A = {a,b} and B = {2}, then A×B = {(b,2), (a,2)} is correct, because {(b,2), (a,2)} and {(a,2), (b,2)} are same set
- **Exercise:** Explain which one is correct for {a,b}×{1,1,2}
  (i) {(a,1), (b,1), (b,2), (a,2)}
  (ii) {(a,1), (a,1) (a,2), (b,1), (b,1), (b,2)}
  (iii) {(1,a), (2,a), (1,b), (2,b)}

Order of a,b is important: (a,b) ≠ (b,a)

A×B×C×…

- Cartesian product can occur among more than two sets
- Each element in the resulting set is an **n-tuple** (like this: (…, …, .., … n elements)), where n is the number of input sets
- One element comes from each input set in order
- **Example:** If F = {a,b}, M = {2}, C = {x,y}, then F×M×C = {(a,2,x), (a,2,y), (b,2,x), (b,2,y))}
- **Example:** Suppose that, Father = {Ali}, Mother = {Neha}, Son = {Ashik, Salam}. Then, Father×Mother×Son = {(Ali, Neha, Ashik), (Ali, Neha, Salam)}
- **Exercise:** Find {a,b}×{1,2}×{x,y}×{p,q,r}. What is the cardinality of the resulting set?

Cartesian product for more than two sets: A×B×C×D…

What is Relation?

- **Example:** Consider two sets Men={Anis, Faisal} and Women={Tinni, Lota}
  - The set Men can be related **to** the set Women in many ways
  - For example, a relation **from** the set Men **to** the set Women could be father-daughter
  - Suppose that Anis is father of Lota. Then we can say that the pair (Anis, Lota) are related by father-daughter relation
  - But, at the same time, the pair (Faisal, Lota) cannot be related, because Lota cannot have two fathers
- **Exercise:** Find another relation from Men to Women

Relation …
from … to…

What is Relation?

- **Example:** We continue with the previous example: Two sets are Men={Anis, Faisal} and Women={Tinni, Lota}, and the relation is father-daughter
  - (Tinni, Anis) cannot be an example of the father-daughter relation
  - Because, a women cannot be a father and a man cannot be a daughter
  - So, father-daughter relation cannot be defined from the set Women to Men
- **Exercise:** Find by yourself another example similar to the above and then find some valid and invalid relations for that example

Relation …
from … to…

Define Relation

- From the previous examples, we can observe these:
  - A **relation** happens among the elements of two sets
  - A relation is a set of **some** (may not be all) **ordered** pair of elements from the two sets
  - So, relation is similar to cartesian product of the two sets, but a subset of cartesian product
- Formally, a relation R from set A to set B is defined as:
  - $R=\{(a,b) \mid a\in A \text{ and } b\in B\}$. So, $R\subseteq A\times B$
- It is said like this: "R is a **relation from** A **to** B", or like this: "A is **related to** B by the relation R"
- When $(a,b)\in R$, then we say that a is related to b by R

Relation

$\subseteq$

Cartesian product

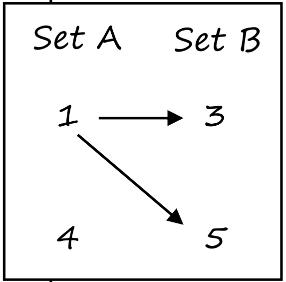
Representing Relation

- **Example:** Consider the two sets $A=\{1,4\}$, $B=\{3,5\}$ and the relation R from A to B as $R=\{(a,b) | a \in A, b \in B, \text{ and } |a-b| \geq 2\}$
  - This relation says that (a,b) is related if their difference (a-b or b-a) is at least two
  - So, $R=\{(1,3),(1,5)\}$
  - Observe that $A \times B = \{(1,3),(1,5),(4,3),(4,5)\}$
  - The pairs (4,3) and (4,5) are not in R, because these two pairs do not satisfy the condition $|a-b| \geq 2$
  - Moreover, (3,1) and (5,1) cannot be in R, although they satisfy the condition $|a-b| \geq 2$
  - Because, they violate the ordering of a, b

$(a,b) \in R$
may not imply
$(b,a) \in R$

Representing Relation

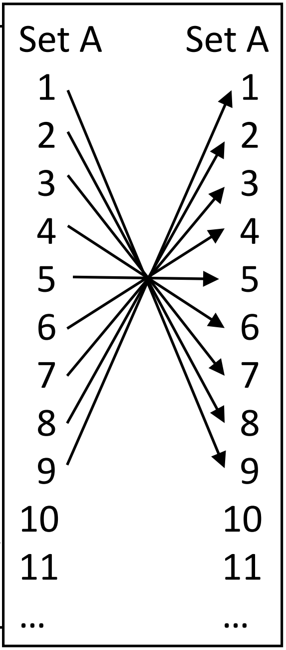
- A relation from A to B can be represented and understood in several other ways
- One easy way to represent in a graphical way as follows:
  - Put A in left side and B in right side
  - For every pair (a,b) in R, put an arrow from a to b
- **Example:** A graphical representation of the previous example is given in the right-side picture



- **Exercise:** Consider the two sets A={1,4}, B={3,5,9} and the relation R from A to B as R={(a,b)|a$\in$A, b$\in$B, and (a+b)$\geq$10}
  - Find A$\times$B, find R
  - Draw the graphical representation of R

Relation Within Same Set?

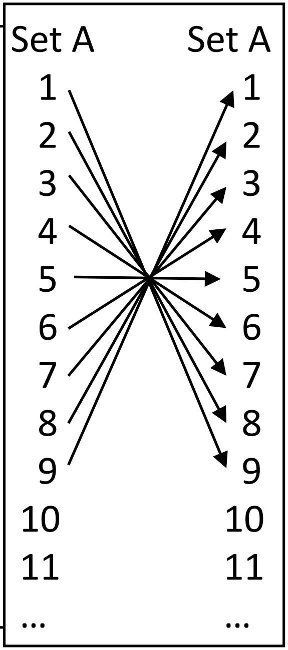
- A relation R can occur **on** same set A, from A to A
- In other way, in can happen that A=B and $R \subseteq A \times A$
- In that case, R is said to be **a relation on A**
- **Example:** Suppose that A is the set of positive integers and $R=\{(a,b)|a+b=10\}$ on A
  - Here both a and b come from A
  - R contains all pairs of positive integers of sum 10
  - There can be many such pairs, such as (1,9), (2,8), (9,1), (3,7), and so on…
  - Finally, $R=\{(1,9),(2,8),(3,7),(4,6),(5,5),(6,4),(7,3),(8,2),(9,1)\}$
  - A graphical representation of R is shown here



Relation Within Same Set?

- (Continued from the previous slide):
- There is no more pair in R, because any such pair will not sum up to 10. For example, $(2,9) \notin R$, because $2+9 = 11 \neq 10$
- Observe that, both (1,9) and (9,1) are in R, as a can be both 1 and 9 and b can be both 9 and 1
- Also observe that, (5,5) is not repeated. Because, repetition is not counted in a set

- **Example:** $R=\{(a,b) \mid 2^a = b\}$ on non-negative integers
  - R contains all pair of non-negative integer (a,b) so that $2^a = b$
  - For example, $2^2 = 4$, so (2,4) is in R (continued …)



Relation Within Same Set?

- (Continued from the previous slide…)
- (3,7) will not be in R, because $2^3 = 8 \neq 7$
- R will be a infinite set, because for any non-negative integer a, 2^a is another non-negative integer
- So, R contains $(a,2^a)$ for all $a \geq 0$
- Complete answer is:

  R = {(0,1),(1,2),(2,4),(3,8),(4,16),(5,32),…}

- **Exercise:** Find the set of the following relations on the set of integers: **(i)** $R1=\{(a,b) \mid a=b^2\}$ **(ii)** $R2=\{(a,b) \mid a-b \geq 0\}$
- **Exercise:** Are the following pairs members of the above relations R1, R2, or in both: (4,2), (-5,-3), (4,-2), (0,0), (1,-1), (-1,1), (1,1)?

Relation can be infinite set

Relation Types

- Relation can be of different types based on some properties
- Some common and interesting types are
  - Reflexive
  - Symmetric
  - Transitive
- All these relations are defined on same set A
- **Reflexive relation:** To be reflexive, a relation R must contain the pair (a,a) for every a in A
- **Example:** Suppose A={1,2,3} and R={(1,1),(2,1),(2,2),(2,3),(3,3)}
  - R is reflexive. Because, (1,1), (2,2) and (3,3) are in R

Reflexive

Symmetric

Transitive

…

Reflexive Relation

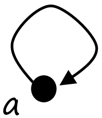
- **Example:** Suppose A={1,2,3} and R={(1,1),(2,1),(3,2),(2,3),(3,3)}
  - R is not reflexive, because (2,2) is missing in R
- **Example:** Relation $\leq$ on a set of numbers A is reflexive
  - Because, for any element a in A, we know that $a \leq a$
  - So, (a,a) is in R for all a in A
  - For example, if A = {1,3}, then R={(1,1),(1,3),(3,3)}.
  - As (1,1)} and (3,3) are there, R is reflexive
- **Example:** Relation < on a set of numbers is not reflexive
  - Because, for $a \in A$, (a,a) is not in R, as a<a is not true
  - For example, if A = {1,3}, then R={(1,3)}
  - As (1,1), (3,3) are not in R, R cannot be reflexive

Reflexive:

(a,a)

required

for all a

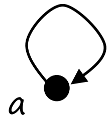


a

Reflexive Relation

- **Exercise:** Justify whether the following relations on the set A = {2,3,4} are reflexive or not
  a. R = {(2,2)}
  b. R = {(2,2),(3,3),(4,4)}
  c. R = {}
  d. R = {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)}
- **Exercise:** Justify whether the following relations on the set of positive integers are reflexive or not
  a. R = {(a,b)|a-b=0}
  b. R = {(a,b)|a+b=0}
  c. R = {(a,b)|Division of a by b is an integer}

Reflexive means: (a,a) required for all a



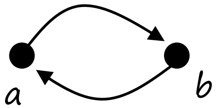
Symmetric Relation

- **Symmetric relation:**
  - A relation R to be symmetric, if a pair (a,b) is in R, then the pair (b,a) must also be in R. Here, $a \neq b$
  - (a,b) and (b,a) are called **symmetric pairs**
  - For a pair (a,a), it is not necessary to repeat (a,a) again in R. (a,a) is the symmetric pair of itself
- **Example:** Suppose A={1,2,3} and R={(1,1),(2,1),(1,2),(2,3),(3,2)}
  - R is symmetric, because, for each pair in R, the symmetric pair is also in R
  - (1,2) and (2,1) are in R, (2,3) and (3,2) are in R, and the remaining pair (1,1) is symmetric by itself

Symmetric means:

$(a,b) \rightarrow (b,a)$

for all existing (a,b)



Symmetric Relation

- **Example:** Suppose A={1,2,3} and R={(1,1),(2,1),(3,2),(2,3),(3,3)}
  - R is not symmetric, because for the pair (2,1), the symmetric pair (1,2) is absent in R
- **Exercise:** Justify whether the following relations on the set A = {2,3,4} are symmetric or not
  a. R1 = {(2,3)}
  b. R2 = {(2,3),(3,2)}
  c. R3 = { }
  d. R4 = {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3)}
  e. R5 = {(4,4),(3,3)}
  f. R6 = {(a,b) | |a-b|=1}

For symmetric: (a,a) is OK

Symmetric Relation

- **Example:** Relation < on a set of numbers is not symmetric
  - Because, if a pair (a,b) in R, then a < b. That means, $b \nless a$. So, the pair (b,a) cannot be in R
  - For example, if A = {1,2,3}, then R={(1,2),(1,3),(2,3)}
  - As $2 \nless 1$, R cannot have (2,1). Same for (3,1) and (3,2)
  - So, R is not symmetric
- **Exercise:** Similar to above example, explain whether the relation ≤ on a set of numbers is symmetric or not
- **Example:** Among a set of men, relation "brother" is symmetric
  - Because, if a is a brother of b, then b is a brother of a
  - So, if (a,b) is in the relation, then (b,a) is also there

brother: symmetric

≤, ≥, father-son: symmetric?

Transitive Relation

- **Transitive relation:**
  - For a relation R to be transitive, if two pairs (a,b) and (b,c) are in R, then the pair (a,c) must also in R
  - Here, a≠b and b≠c. But it is possible that a=c
  - The pair (a,c) is the **transitive pair** of (a,b) and (b,c)
- **Example:** Suppose A={1,2,3} and R={(1,1),(1,2),(2,1),(3,2),(2,3)}
  - R is not transitive. Because, for (3,2) and (2,1), the transitive pair (3,1) is missing
  - There are more violations, but one is enough
- **Exercise:** Find the other missing transitive pairs in the above example

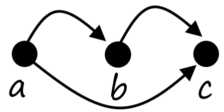
Transitive means:

$(a,b) \wedge (b,c)$

$\rightarrow (a,c)$

for all existing

(a,b), (b,c)



Transitive Relation

- **Example:** Suppose that A={1,2,3,4} and R={(1,1),(2,1),(1,2),(2,2),(1,3),(2,3),(3,3),(4,3)} on A
  - R is transitive, because all required transitive pairs are in R
  - We can check each pair one by one from left to right
  - No need to check (1,1)
  - For (2,1) and (1,2), the transitive pair (2,2) is there
  - For (2,1) and (1,3), the transitive pair (2,3) is there
  - For (1,2) and (2,1), the transitive pair (1,1) is there
  - For (1,2) and (2,3), the transitive pair (1,3) is there
  - No more pairs need to be checked. Because, for (1,3), (2,3) and (4,3), there is no pair like this (3, …)

If (a,b) but no (b,c), then (a,b) is OK

Transitive Relation

- **Exercise:** Justify why the following relations on the set A={1,2,3,4} are transitive or not, as written next to each
  a. R = {(1,1)} // transitive
  b. R = {(2,3),(3,2),(3,3),(2,2),(4,3)} // not transitive
  c. R = {} // transitive
  d. R = {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3), (4,4)}
  // transitive
- **Example:** Relation > on a set of numbers is transitive
  - Because, if two pairs (a,b) and (b,c) are in R, then a>b and b>c
  - This gives, a>c too. So, the pair (a,c) is in R
  - (Continued to the next slide …)

>, <:

transitive

Transitive Relation

- (Continued from the previous slide…)
- For example, if A = {1,2,3}, then R={(2,1),(3,1),(3,2)} is transitive
- Because, For (3,2) and (2,1), the transitive pair (3,1) is there in R
- No more pairs required checking

- **Exercise:** Like previous example, explain whether relation $\leq$ on a set of numbers is transitive or not
- **Exercise:** Explain why among a set of men, the relation "ancestor" would be transitive
- **Exercise:** Are these relations on integers transitive?
  (i) R={(a,b)|a-b=1} **(ii)** R={(a,b)| a=kb, where k is integer}

$\geq$, $\leq$, ancestor: transitive? (Ancestor means: father, grandfather, grandgrand-father, so on …)

Equivalence Relation

- **Equivalence relation:** A relation R is an equivalence when it is at the same time reflexive, symmetric and transitive
- **Example:** Suppose that A={a,b,c}
  - The relation R1={(a,a),(b,b),(b,c),(c,b),(c,c)} on A is equivalence relation
    - Because, all three properties are met (check it)
  - The relation R2={(a,a),(a,b),(b,a),(b,b),(b,c),(c,b),(c,c)} on A is not an equivalence relation
    - Because, R2 is reflexive and symmetric
    - But is it not transitive, because for (a,b) and (b,c), the transitive pair (a,c) is missing

Equivalence

=

reflexive $\wedge$

symmetric $\wedge$

transitive

Equivalence Relation

- **Exercise:** Justify whether the following relations on the set A = {2,3,4} are equivalence relations or not
  a. R = {(2,2)}
  b. R = {(2,3),(3,2),(3,3),(2,2)}
  c. R = {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)}
  d. R = {(a,b) | a-b=0}
- **Exercise:** For A={a,b,c} find a relation R for each of the following criteria
  - R is reflexive and symmetric, but not transitive
  - R is reflexive and transitive, but not symmetric
  - R is transitive and symmetric, but not reflexive
  - R is none of reflexive, symmetric or transitive

Equivalence

=

reflexive $\wedge$

symmetric $\wedge$

transitive

Relation in Three or More Sets

- Relation can happen among more than two sets
- **Example:** Consider three sets of men, women and children, denoted by F, M and C respectively
  - A "family" relation R on these three sets is $R \subseteq F \times M \times C$
  - Elements of R are 3-tuples, where each tuple represents a family of father-mother-child
  - For example, suppose that F={a,b}, M={p,q}, C={x,y,z}, and R={(a,q,x),(b,p,y),(b,p,z)}
    - R represents three families: (father a, mother q, and child x), (father b, mother p, and child y), and (father b, mother p, and child z)

$R \subseteq A \times B \times C \times D \ldots$

Composite Relation

- Two or more relations can be used to find new relations by applying different set operations
- Some common operations are **union**, **intersection**, **difference**, **composition**, etc.
- Union, intersection, difference --- we saw before in set
- Here, we see **composition**, as it is very useful and interesting
- **Composition** of two relations R1 and R2**:**
    - The idea is similar to transitivity of a relation
    - R1 **composite** R2 is denoted by $R1 \circ R2$
    - Suppose that R1 is from A to B and R2 is from B to C
    - Then, $R1 \circ R2 = \{(a,c) \mid (a,b) \in R1 \text{ and } (b,c) \in R2\}$

Union,
intersection,
difference,
composition,
...

$R1 \circ R2$

- **Example:** Consider three sets F, M and C representing the sets of Fathers, Mothers, and Children, respectively
  - Suppose that F={a,b}, M={p,q}, C={w,x,y,z}
  - Suppose that R1={(a,p),(b,q)} is a father-mother relation from F to M
  - Suppose that R2={(p,x),(p,z),(q,y)} is a mother-child relation from M to C
  - Then, $R1 \circ R2=\{(a,p),(b,q)\} \circ \{(p,x),(p,z),(q,y)\} = \{(a,x),(a,z),(b,y)\}$ is a relation from F to C
  - As discovered, $R1 \circ R2$ is exactly the father-child relation, because a is the father of x and z (by mother p), and b is the father of y (by mother q)

$$R1 \circ R2 = \{(a,c) \mid (a,b) \in R1 \wedge (b,c) \in R2\}$$

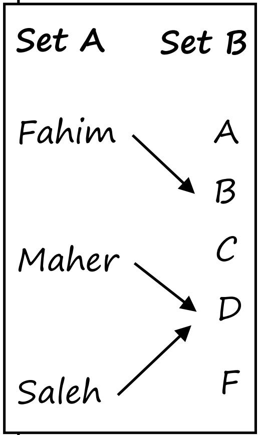
R1∘R2

- **Exercise:** Find R1∘R2 for the following relations which are given on the sets F={a,b}, M={p,q,r}, C={w,x,y,z}
  - R1={(a,p),(b,q),(a,r)} is from F to M
  - R2={(p,x),(p,z),(q,y),(r,w)} is form M to C
- A composition can be done involving same relation
- **Example:** For the relation R={(1,1),(2,1),(1,3)},
  R∘R = {(1,1),(2,1),(1,3)}∘{(1,1),(2,1),(1,3)} = {(1,1),(1,3),(2,1),(2,3)}
- **Example:** R∘R is useful in many ways. For example, if R={(a,c),(e,d),(d,a)} represents (ancestor, descendent) pairs, then R∘R={(e,a),(d,c)} discovers new such pairs
- **Exercise:** Find R∘R∘R, R∘R∘R∘R, …. Are they all same?

$R1 \circ R2 = \{(a,c) \mid (a,b) \in R1 \wedge (b,c) \in R2\}$

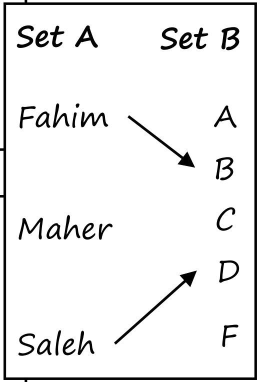
Functions

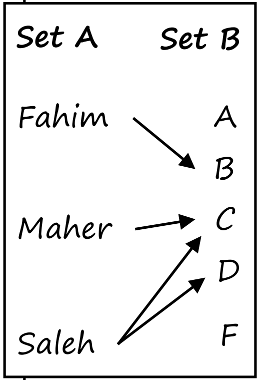
- **Functions** are special type of relations
- A **function f from A to B** is a relation from A to B such that for **every** element a$\in$A, there is **exactly one** element b$\in$B such that (a,b)$\in$f
- It is written as f : A$\rightarrow$B
- When (a,b)$\in$f, it is written as b = f(a)
- **Example:** Consider a set of students A={Fahim, Maher, Saleh} and a set of grades B={A, B, C, D, F}
    - f = {(Fahim, B), (Saleh, D), (Maher, D)} is a function
    - Above function can be represented by the right-side picture
    - In this example, f(Fahim)=B, f(Saleh)=D, f(Maher)=D



Negative Examples

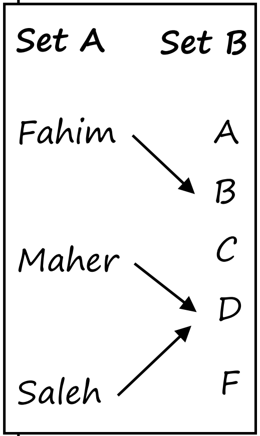
- **Example:** Consider a set of students A={Fahim, Maher, Saleh} and a set of grades B={A, B, C, D, F}
  - f: A→B = {(Fahim, B), (Saleh, D)} is not a function. Because, (Maher, …) is not available (see here)
  - f = {(Fahim, B), (Saleh, D), (Saleh, C), (Maher, D)} is not a function. Because, there are two values for Saleh: (Saleh, D) and (Saleh, C). (See here)
  - f={(Ashraf,D), (Fahim,X)} is not a function. Because, Ashraf is not in A. Similarly, X is not in B
- **Exercise:** Is f a function below from A={1,2} to B={c,d}? (i) f={(1,c), (1,d)}, (ii) f={(1,k),(2,d)}, (iii) f={(3,c),(4,d)}





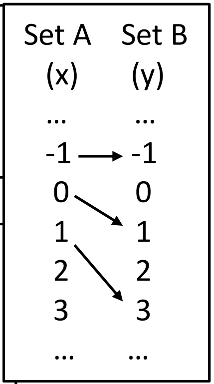
Definitions

- For a function f : A→B, the set A is called the **domain** of f and the set B is called the **codomain** of f
- In b = f(a), a is called the **argument** of f and b is called the **value** of f for a
- Some elements of B may not be values of elements of A
- **Range** of A is the set of elements of B who are values of some elements of A
- **Example:** In the right-side example,
  - f(Fahim) = B. Here, Fahim is an argument
  - Range of A is {B, D}
  - {A, C, F} are not values of some elements of A
- **Exercise:** Find all arguments and their values here

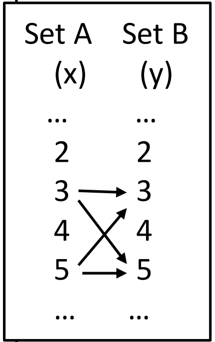


Examples

- **Example:** $F=\{(x,y) | x,y \in Z$ and $y=2x+1\}$ is a function
  - Domain and codomain of F are the set of all integers
  - Range of F is the set of all odd integers
  - Here, $y=F(x)=2x+1$. E.g., $F(0)=1$, $F(5)=11$, $F(-3)=-5$, etc.



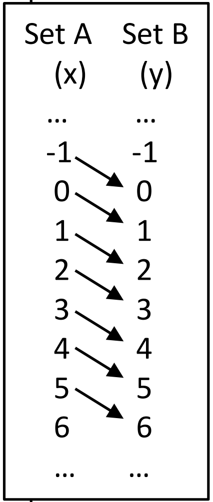
- **Example:** Relation $F=\{(x,y) | x,y \in N$ and $xy=odd\}$ is not a function, because for some x, there can be many y so that $xy=odd$
  - For example, (3,3), (3,5), (3,7) … all give $xy=odd$



- **Example:** Relation R={(father, child)} on the set of all people in this world is not a function
  - Because, for one father there can be many children
- **Exercise:** Is relation R={(child, father) a function? Why?

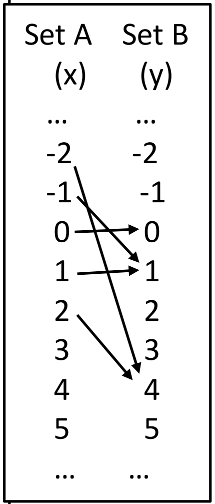
Onto, Injection, Bijection

- Consider a function f: A→B (see right-side examples)
- f is **onto** if every element of B is a value of some argument of A. That means, range of f is the codomain
- f is **injection** if different arguments have different values
- f is **bijection** (or **one-to-one**) if it is onto and injection
- **Example:** Consider f(x) = y = x+1 on set of integers
  - f is onto, because every integer y is the value of x=y-1. For example, for y=-2, x=-3; for y=0, x=-1; for y=4, x=3; etc.
  - f is injection, because if x1≠x2, then f(x1)=x1+1 ≠ f(x2) = x2+1. For example, f(1)=2, and f(2)=3. So, f(1)≠f(3)
  - As f is both onto and injection, it is one-to-one



Onto, Injection, Bijection

- Observe that for a bijection, A and B have same size
- **Example:** Consider the function $f(x) = y = x^2$ on set of integers (see here)
  - f is not onto, because not every integer y is a value
    - For example, there is no x such that $f(x) = 3$
  - f is not injection, because many y have different arguments. For example, $f(1) = 1$ and $f(-1) = 1$
  - As f is not onto or injection, it is not bijection either
- **Exercise:** Explain whether the function $f(x) = y = -x$ is onto, injection, and bijection?
- **Exercise:** Find a function that is onto but not injection
- **Exercise:** Find a function that is not onto but injection

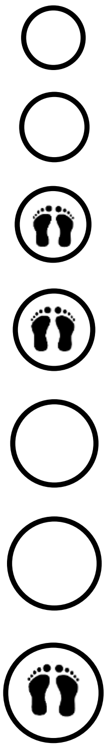


Lecture 9
Induction and Recurrence

And We have certainly given you, [O Muhammad], seven of the often repeated [verses] and the great Qur’an (Quran 15:87)

Induction: Motivation

- Suppose you are playing this game with your friends:
  - There are n small circles equally apart along a line
  - The game is to start from the first circle
  - Then go to the next circle with one jump and the two feet together, then to the next circle, and so on, and finally go to the last circle
  - The challenge is to keep the feet within a circle
- To succeed in this game you need to know two things:
  1. Start correctly from the first circle
  2. Jump correctly from one circle to the next (you can use/repeat/apply/**induce** this technique n-1 times)
- This idea of **correct start + repetition** is called **induction**



Induction

- **Induction** means influence on another or on the next
- Mathematically, induction is a technique to prove statements that are given by non-negative integer n
- By this technique:
  - If the starting step is true/correct
  - and if the current step is true/correct,
  - then the next step will also be true/correct
  - This will imply that the entire series is true/correct
- More formally, there are **two steps** of **proof by induction**
  - Base case (proof the starting step to be true)
  - Inductive step (prove (k+1)-th step from k-th step)

Base case

+

Induction step

Proof by Induction

- **Example:** Proof by induction: For $n \geq 1$, $1+2+3+\ldots+n=\frac{n(n+1)}{2}$
- **Proof:** We denote by $S(n)$: $1+2+3+\ldots+n = \frac{n(n+1)}{2}$
- **Base case:**
  - For the first step, n=1. We need to show S(1) is true
  - Left side of S(1) is 1, because summation stops at n=1
  - Right side of S(1) is $\frac{1(1+1)}{2} = 1$
  - Left side = right side. So, S(1) is true. Base case is correct
- **Induction step:**
  - We assume that Step k, that means S(k), is true
  - Using S(k), we show that S(k+1) is true (continued…)

Base case

+

Induction

step:

use

step k

Prove step

k+1

Proof by Induction

- (Continued from the previous slide…)
- S(k) is true means, S(k): $1+2+3+\ldots+k = \frac{k(k+1)}{2}$ holds
- We prove S(k+1): $1+2+3+\ldots+(k+1) = \frac{(k+1)(k+2)}{2}$ is true
- Left side of S(k+1): $1+2+3+\ldots+(k+1)$

  $= 1+2+3+\ldots+k+(k+1)$ // k was hidden, now exposed

  $= (1+2+3+\ldots+k)+(k+1)$

  $= \frac{k(k+1)}{2}+(k+1)$ // $(1+2+3+\ldots+k)$ is replaced by

  // $\frac{k(k+1)}{2}$ by S(k)

  $= \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$ = Right side of S(k+1)
- So, S(k+1) is true. Therefore, the proof is complete

Base case

+

Induction step:

use step k

Prove step k+1

Proof by Induction

- **Example:** Proof by induction: For $n \geq 1$, $1+3+5+\ldots+(2n-1)=n^2$
- **Proof:** We denote by S(n): $1+3+5+\ldots+(2n-1) = n^2$
- **Base case:** For first step, n=1. We need to show S(1) true
  - Left side of S(1) is 1, because summation stops at (2n-1) with n=1, which is (2*1-1) = (2-1) = 1
  - Right side of S(1) is $1^2 = 1$
  - Left side = right side. So, S(1) is true. Base case correct
- **Induction step:**
  - We assume that Step k, that means S(k), is true
  - Then using S(k), we shall show that S(k+1) is true
  - S(k) is true means, S(k): $1+2+3+\ldots+(2k-1) = k^2$ holds
  - (Continued …)

Base case

+

Induction step:

use step k

Prove step k+1

Proof by Induction

- (Continued from the previous slide…)
- We prove S(k+1): $1+3+5+\ldots+(2(k+1)-1) = (k+1)^2$ true
- Left side of S(k+1): $1+3+5+\ldots+(2(k+1)-1)$
  $= 1+2+3+\ldots+(2k-1)+(2(k+1)-1)$ // (2k-1) exposed
  $= (1+2+3+\ldots+(2k-1))+(2(k+1)-1)$
  $= k^2+(2(k+1)-1)$ // $(1+3+5+\ldots+(2k-1)) = k^2$ by S(k)
  $= k^2+2k+1 = (k+1)^2$ = Right side of S(k+1)
- So, S(k+1) is true and the proof is complete

- **Exercise:** Prove by induction:
  - $1^2+2^2+3^2\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}$
  - $1^3+2^3+3^3+\ldots+n^3 = (\frac{n(n+1)}{2})^2$

Base case

+

Induction step:

use step k

Prove step k+1

Proof by Induction

- **Example:** Proof by induction:

  For $n \geq 0$, $1+2+2^2+2^3+\ldots+2^n = 2^{n+1}-1$
- **Proof:** We denote by $S(n)$: $1+2+2^2+2^3+\ldots+2^n = 2^{n+1}-1$

  $\Rightarrow S(n): 2^0+2^1+2^2+2^3+\ldots+2^n = 2^{n+1}-1$
- **Base case:**
  - At first step, n=0. So, we need to show S(0) is true
  - S(0) left side: $2^0=1$, because summation stops at n=0
  - S(0) right side: $2^{0+1}-1 = 2^1-1 = 1$
  - Left side = right side. So, S(0) is true. Base case OK
- **Induction step:**
  - We assume that Step k, that means S(k), is true
  - Using S(k), we show that S(k+1) is true (continued …)

Base case

+

Induction step:

use step k

Prove step k+1

Proof by Induction

- (Continued from the previous slide)
- S(k) true means S(k): $1+2+2^2+2^3+\ldots+2^k = 2^{k+1}-1$ holds
- We prove S(k+1): $1+2+2^2+2^3+\ldots+2^{k+1} = 2^{k+1+1}-1$ true
- Left side of S(k+1): $1+2+2^2+2^3+\ldots+2^{k+1}$

  $= 1+2+2^2+2^3+\ldots+2^k+2^{k+1}$ // hidden 2^k now exposed

  $= (1+2+2^2+2^3+\ldots+2^k)+2^{k+1}$

  $= (2^{k+1}-1)+2^{k+1}$ // $(1+2+2^2+2^3+\ldots+2^k)$ replaced by

  // $2^{k+1}-1$ by S(k)

  $= 2\cdot2^{k+1}-1 = 2^1\cdot2^{k+1}-1 = 2^{k+1+1}-1$ = Right side of S(k+1)
- So, S(k+1) is true. Therefore, the proof is complete
- **Exercise:** Proof by induction:

  For $n\geq0$, $1+x+x^2+x^3+\ldots+x^n = \frac{x^{n+1}-1}{x-1}$

Base case

+

Induction

step:

use step k

Prove step

k+1

Proof by Induction

- In the base case, n can be other than 0 or 1
- In the induction step, "Assume S(k) is true" is also called **induction hypothesis** (**IHT**)
- **Example:** Proof by induction: For $n > 6$, $3^n < n!$
- **Proof:** We denote by $S(n)$: $3^n < n!$
  - Here, $3^n < n!$ is to be proven for n=7,8,9,…
  - So, the first step is for n=7
- **Base case:**
  - We need to prove $S(7)$: $3^7 < 7!$
  - Left side: $3^7 = 2187$
  - Right side: $7! = 7{\cdot}6{\cdot}5{\cdot}4{\cdot}3{\cdot}2{\cdot}1 = 5040$ // Remember
  - $2187 < 5040$. So, $S(7)$ is true. Base case correct

$n! = n{\cdot}(n-1)\ldots3{\cdot}2{\cdot}1$

Proof by Induction

- (Continued from the previous slide…)
- **Induction step:**
  - Induction Hypothesis (IHT): S(k): $3^k < k!$ is true
  - Using this induction hypothesis, we shall show that S(k+1): $3^{k+1} < (k+1)!$ is true
  - 3^{k+1}

    $= 3^k \cdot 3^1$

    $< k! \cdot 3$ // $3^k < k!$ by IHT

    $< k! \cdot (k+1)$ // $n \geq 7$ means $k \geq 7$. So, $(k+1) \geq 8$. So, $3 < k+1$

    $= (k+1)!$ // Remember $(k+1)! = (k+1) \cdot k!$
  - So, $3^{k+1} < (k+1)!$
  - This ends the proof

IHT:

Assume S(k) true

Proof by Induction

- **Exercise:** Proof the following statements by mathematical induction
  - For $n \geq 1$, $8^n - 3^n$ is divisible by 5 (divisible by 5 means, division of (8^n-3^n) by 5 is integer)
  - $2^n < n!$ for $n \geq 4$
  - $n^2 < 2^n$ for $n \geq 5$
  - $n! < n^n$ for $n>1$
  - n^2+n is even for $n \geq 1$
  - 6^n-1 is multiple of 5 for $n \geq 1$ (multiple of 5 is same as disable by 5)
- **Exercise:** What are the induction hypotheses in the above proofs

Base case

+

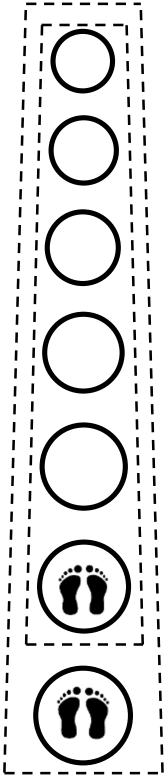
Induction step:

use step k

Prove step k+1

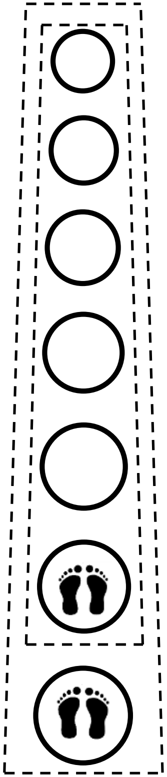
Recurrence: Motivation

- Again consider the game that we saw at the beginning
- This time we want to introduce a scoring system:
  - After a successful first jump you get n points, after second jump n-1 points, after third jump n-2 points, and so on… No more point at n-th circle
- How many total point one can achieve for n circles?
- There can be many ways to count this value
- Below is the method called **recurrence**
  - Start counting from Circle 1: n points after first jump. Current position: Circle 2
  - From Circle 2 count similarly: n-1 points for second jump. Current position: Circle 3 (continued …)



Recurrence: Motivation

- (Continued from the previous slide…)
  - Stop counting at Circle n, as there is only one circle where you are currently standing, and no more jump, so no point
- This scoring mechanism can be formulated like this:
  - Total Point for n circles = n+Total Point for n-1 circles
  - Total Point for 1 circle = 0
- There are two parts of the above formula
  - "Total Point" recursively appear in the right side. This is called **recursive equation**
  - "Total Point" has a terminating value (0 for 1 circle), which is called **terminating condition**



Solving Recurrences

- **Example:** Let us write the previous recurrence clearly
  - Let us denote by T(n) the "Total Points for n circles"
  - So, the recurrence becomes:

$$\mathrm{T(n)} = \begin{cases} \mathrm{n + T(n-1),} & \mathrm{for\ n > 1} \quad \text{// Recursive equation} \\ 0, & \mathrm{for\ n = 1} \quad \text{// Terminating condition} \end{cases}$$

  - Solving this recurrence means finding the value of T(n) in terms of n
  - In this example, that value of T(n) will give the total points for n circles
- But, how can we solve this recurrence?
- There are many ways to solve a recurrence
- We shall see an easy method called **iterative method**

Recurrence:

Recursive Equation

+

Terminating Condition

Solving Recurrences: Iterative Method

- **Iterative method:**
  - Expand the recursive equation from n to n-1, n-2, …
  - Stop when the terminating condition is reached
  - Find a summation pattern in the expended terms
  - Solve the summation by induction or known formula
- **Example:** Solve the following recurrence by iterative method

$$T(n) = \begin{cases} n + T(n-1), & \text{for } n > 1 \\ 0, & \text{for } n = 1 \end{cases}$$

- **Solution:**
  - When we expand T(n), we shall need the equation for T(n-1), T(n-2), and so on (Continued …)

Iterative method: Expand + Stop + Sum

Solving Recurrences: Iterative Method

- (Continued from the previous slide…)
- How to get the equation for T(n-1), T(n-2), …?
- Replacing n by n-1 in T(n), we get T(n-1)=(n-1)+T(n-2)
- Similarly, T(n-2) = (n-2)+T(n-3), and so on…
- Now we expand T(n):

T(n) = n+T(n-1)
= n+(n-1)+T(n-2) // use T(n-1)=(n-1)+T(n-2)
= n+(n-1)+(n-2)+T(n-3) // use T(n-2)=(n-2)+(T(n-3)
… continue until terminating condition T(1) is reached
= n+(n-1)+(n-2)+….+2+T(1) // Think why 2 before T(1)?
= n+(n-1)+(n-2)+….+2+0 // use T(n)=0 for n=1
(Continued …)

Get T(n-1): Replace n by n-1 in T(n)

Solving Recurrences: Iterative Method

(Continued from the previous slide…)

- Expansion is complete. Now we find a pattern/series

= 2+3+4+…+(n-2)+(n-1)+n…. // write in opposite way

- This is 1 short of our know series: 1+2+3+…+n
  = -1+1+2+3+…+n // -1 and +1 cancel each other

= -1 + (1+2+3+…+n) // replace (1+2+3+…+n) by $\frac{n(n+1)}{2}$

= -1 + $\frac{n(n+1)}{2}$ // we already proved this by induction

$= \frac{-2+n(n+1)}{2} = \frac{n^2+n-2}{2} = \frac{n^2+2n-n-2}{2} = \frac{n(n+2)-1(n+2)}{2}$

$= \frac{(n+2)(n-1)}{2}$

- This is the final answer and ends the solution

Try to find a series of summation

Solving Recurrences: Iterative Method

- **Example:** Solve the following recurrence by iterative method. Assume that n is power of 2.

$$T(n) = \begin{cases} 1 + T(n/2), & \text{for } n > 1 \\ 0, & \text{for } n = 1 \end{cases}$$

- **Solution:** n is power of 2, so $n = 2^k$. This gives $k = \log_2 n$
  - $T(n) = 1+T(n/2)$ // first/given expansion
  - If we replace n by n/2, we get $T(n/2) = 1 + T(n/2^2)$
  - So, $T(n) = 1+1+T(n/2^2))$ // second expansion
  - Again, if we expand $T(n/2^2)$ we get, $T(n/2^2)=1+T(n/2^3)$
  - So, $T(n) = 1+1+1+T(n/2^3)$ // third expansion
  - (Continued to the next slide …)

Get T(n/2):
Replace n
by n/2
in T(n)

Solving Recurrences: Iterative Method

- (Continued from the previous slide …)
- We continue k times until T(…) becomes $T(n/2^k)$, which is T(1), because $n = 2^k$
- That will be the terminating condition
- So, $T(n) = 1+1+1+…+1+T(n/2^k)$ // k-th expansion
- Observe that, after every expansion, 1 is added
- So there are k number of 1 before $T(n/2^k)$
- Therefore, $T(n) = k + T(n/2^k) = k + T(1)$
- As $T(1)=0$, we get $T(n) = k + 0 = k$
- As $k = \log_2 n$, $T(n) = \log_2 n$
- This is the final answer and the end of the solution

Try to find a series of summation

Solving Recurrences: Iterative Method

- **Example:** Solve the following recurrence by iterative method. Assume that n is power of 2.

$$S(n) = \begin{cases} S(n/2) + n, & \text{for } n > 1 \\ 0, & \text{for } n = 1 \end{cases}$$

- **Solution:** n is power of 2, so $n = 2^k$
  - $S(n) = n + S(n/2)$ // first/given expansion
  - If we replace n by n/2, we get $S(n/2) = n/2 + S(n/2^2)$
  - So, $S(n) = n + n/2 + S(n/2^2)))$ // second expansion
  - Again, if we expand $S(n/2^2)$ we get, $S(n/2^2) = n/2^2+S(n/2^3)$
  - So, $S(n) = n + n/2 + n/2^2 + S(n/2^3))$ // third expansion
  - (Continued to the next slide …)

Get S(n/2):
Replace n
by n/2
in S(n)

Solving Recurrences: Iterative Method

- (Continued from the previous slide …)
- We continue k times until S(…) becomes $S(n/2^k) = S(1)$, which is the terminating condition, because $n = 2^k$
- $S(n)=n+n/2+n/2^2+\ldots+n/2^{k-1}+S(n/2^k)$ // k-th expansion
- As $S(n/2^k)=S(1)=0$, we get $S(n)=n+n/2+n/2^2+\ldots+n/2^{k-1}+0$
- $S(n) = n(1+1/2+(1/2)^2+(1/2)^3+\ldots+(1/2)^{k-1})$
- Remember, $1+x+x^2+x^3+\ldots+x^r=\frac{x^{r+1}-1}{x-1}$
- With x=1/2 and r=k-1, we get $S(n)=n\frac{(\frac{1}{2})^{k-1+1}-1}{(\frac{1}{2})-1}$
- After simplification, $S(n) = 2n\,\frac{2^k-1}{2^k}$
- With $n=2^k$, we get $S(n) = 2n\,\frac{n-1}{n} = 2(n-1)$ (Answer)

Try to find a series of summation

Solving Recurrences: Iterative Method

- **Example:** Solve the following recurrence by iterative method. Assume that n is power of 2.

$$S(n) = \begin{cases} 2S(n/2) + n, & \text{for } n > 1 \\ 0, & \text{for } n = 1 \end{cases}$$

- **Solution:** n is power of 2, so $n = 2^k$. This gives $k = \log_2 n$
  - $S(n) = n + 2S(n/2)$
  - Replacing n by n/2, we get $S(n/2) = n/2 + 2S(n/2^2)$
  - So, $S(n) = n + 2(n/2 + 2S(n/2^2))) = 2n + 2^2S(n/2^2)$
  - Again, if we expand $S(n/2^2)$ we get, $S(n/2^2) = n/2^2+2S(n/2^3)$
  - So, $S(n) = 2n + 2^2(n/2^2 + 2ST(n/2^3)) = 3n+2^3S(n/2^3))$
  - (Continued to the next slide …)

Get S(n/2): Replace n by n/2 in S(n)

Solving Recurrences: Iterative Method

- (Continued from the previous slide …)
- Continue k times until S(…) becomes $S(n/2^k)=S(1)$, the terminating condition, because $n = 2^k$
- So, $S(n) = kn + 2^k S(n/2^k)$
- As $k = \log_2 n$, we get $S(n) = n\log_2 n + nS(1)$
- As $S(1) = 0$, we get $S(n) = n\log_2 n$
- This ends the solution

- **Exercise:** Solve the following recurrence by iterative method. Assume that n is even.

$$T(n) = \begin{cases} 1 + \mathrm{T}(\mathrm{n}-2), & \text{for } \mathrm{n} > 1 \\ 0, & \text{for } \mathrm{n} = 0 \end{cases}$$

Try to find a series of summation

Solving Recurrences: Iterative Method

- **Exercise:** Solve the following recurrence by iterative method. Assume that n is power of 2.
  - $\mathrm{S(n)} = \begin{cases} \mathrm{S(n/2) + n, for\ n > 1} \\ \mathrm{0, \qquad\qquad\quad for\ n = 1} \end{cases}$
  - $\mathrm{S(n)} = \begin{cases} \mathrm{2S(n/2) + 2, for\ n > 1} \\ \mathrm{0, \qquad\qquad\qquad for\ n = 1} \end{cases}$
- **Exercise:** Solve the following recurrence by iterative method. Assume that n is power of 3.
  - $\mathrm{S(n)} = \begin{cases} \mathrm{3S(n/3) + 1, for\ n > 1} \\ \mathrm{0, \qquad\qquad\qquad for\ n = 1} \end{cases}$

Iterative method:
Expand
+
Stop
+
Sum

Lecture 10
Counting

If you count the blessings of Allah, you can never enumerate them all … (Quran 16:18)

Motivation

- Probably you saw a number plate of a car in your country
- It is normally a combination of some letters from A to Z and some digits from 0 to 9
- Each number plate is unique for identification
- Suppose that in a small country the number plate of a car is simply some numbers, say 3 digits from 0 to 9
- If that country has 10,000 cars, then is it possible to give a unique number plate to each car with three digits?
- No, because, only 1,000 unique numbers possible by 3 digits. So, for 10,000 cars, 3 digits are not enough
- So, how many digits are required for that country?
- In this lecture we shall see topics related to this scenario

Motivation

- Probably you have opened accounts in some computer applications, such as email, university account, etc.
- When you set a password for your account, you will not give a very small password, such as one or two digits
- Because, such a password will be easy to break
- Someone can try all the numbers from 0 to 99 one by one, and one of those will be your password
- Perhaps you will set a long password in combination of letter, digits, special symbols (such as !, *, +, #, $, etc.)
- It will make the password difficult to guess
- Someone have to try many combinations to break it
- In this lecture we shall see topics related to this scenario

Common Rules for Counting

- **Counting** deals with this type of questions: “how many”, “how many ways”, “find all”, etc.
- Counting becomes easier when some rules are applied
- Some common rules used in counting are:
  - Product rule
  - Sum rule
  - Principle of inclusion exclusion
  - Pigeonhole principle
  - Permutation and Combination
- There are many other rules, but we see only the above
- Counting is very vast
- We only see some basic techniques and examples

Rules are important for counting

Product (Multiplication) Rule

- **Example:** How many different words can you make by two letters from a, b, c (you can repeat same letter)?
- **Solution:**
  - Two-letter words will be like these: ac, ba, aa, ca, …
  - Such a word has two positions, first and second
  - Any letter from a, b, c can be in the first position
  - Same for the second position (see here)
  - So, there are three choices for the first position
  - Similarly, there are three choices for 2nd position
  - Total choices: 3*3 = 9
- The **multiplication** (3*3) in the above line (it cannot be sum here like (3+3)) is called **product rule**

Pos 1	Pos 2
a	a
a	b
a	c
b	a
b	b
b	c
c	a
c	b
c	c

Total: 3*3=9

When is Product Rule Applied?

- Knowing when to apply product rule is conceptual
- From the previous example, we got some idea
- It is applied among size of some sets, and it is applied:
  - If a single count involves all sets (can be same set)
  - That means, when each count **depends** on all sets
- **Example:** There are 100 numbers with two digits
  - The numbers are 00, 01, 02, … 10, 11, …, 99
  - Each number (each count) is made up of two digits
  - Each digit comes from the set of 0-9 (set size 10)
  - So, two sets involved in each count, each of size 10
  - Total count = multiply size of two sets = 10*10= 100
- Some coming examples will highlight this concept

Product rule: each count depends on all sets

Product Rule

- **Example:** How many different two-letter words can you make from a to z so that the two letters are different?
- **Solution:**
  - Two letters are different. So, aa, bb, … not allowed
  - Any of 26 letters from a to z can be in position one
  - So, first position set size is 26
  - Once a letter is in position one, it cannot be in position two (see right-side example)
  - Any of the remaining 25 letters can be in position two, so the second position set size is 25
  - Total count: multiply set sizes = 26*25 = 650
- **Exercise:** Repeat by considering position two first

~~aa~~
ab
ac
…
az

25 choices

ba
~~bb~~
bc
…
bz

25 choices

…

za
zb
zc
…
~~zz~~

25 choices

Total: 26*25
=650

Product Rule

- **Example:** How many car number plates are possible with four capital letters first and three digits next?
- **Solution:**
  - Seven positions: L L L L N N N
  - Here, L for letter, N for digit
  - Each L position can have any one letter from A to Z, so 26 choices
  - Each N position can have 0 to 9, so 10 choices
  - Like this: (A-Z)(A-Z)(A-Z)(A-Z)(0-9)(0-9)(0-9)
  - So, total count: 26*26*26*26*10*10*10 (Answer)
- Sometimes, it is better understood if result is written as above in multiplicative format, instead of actual value

Product Rule

- **Exercise:** Repeat the previous example if all letters appear after all digits, like this N N N L L L L? Is the answer same? Why?
- **Example:** How many different passwords are possible with 10 characters, which are capital letters or digits?
- **Solution:**
  - Ten positions, and each position can be anything from A to Z or from 0 to 9
  - Each position has 26+10 = 36 choices (set size 36)
  - Total choices: 36*36*…*36 (ten times) = $(36)^{10}$
- **Exercise:** Repeat the above example where the letters can be small or capital

Product Rule

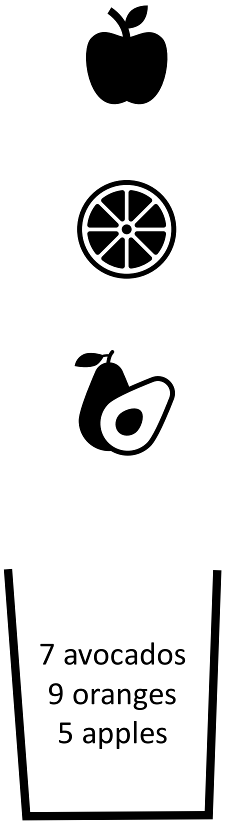
- **Exercise:** Repeat the above exercise if a character can also be any of these nine special symbols: **~**, **!**, **@**, **#**, **$**, **%**, **^**, **&**, *****
- **Example:** How many different binary numbers are possible with 5 binary digits? See example in the right-side picture →
- **Solution:** Five positions. Each position can be 0 or 1, so 2 choices. Total count: $2*2*2*2*2 = 2^5 = 32$
- **Example:** How many of them start with 0 and end with 1?
- **Solution:** See example in the right-side picture →
  - Start with 0 means, only one choice (0) for first position
  - End with 1 means, only one choice (1) for last position
  - Remaining positions have two choices each as before
  - So, total count: $1*2*2*2*1 = 2^3 = 8$

00000
00001
00010
...
11110
11111

00001
00011
00101
00111
01001
01011
01101
01111

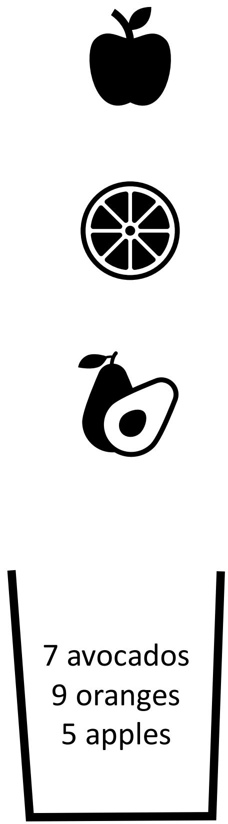
Sum Rule

- **Example:** Consider three trays, one with 5 apples, one with 9 oranges, and one with 7 avocados. In how many ways Muadh can pick one fruit from the trays?
- **Solution:**
  - Muadh can pick an apple in 5 ways or an orange in 9 ways or an avocado in 7 ways
  - Total number of choice for Muadh is 5+9+7 = 21
- In the above solution the choices are added (**sum**), not multiply, like 5*9*7 = 315. This is called **sum rule**
- Observe that, if it were multiplication, then 315 would be too many choices for Muadh. There is not that many fruits in total!



When is Sum Rule Applied?

- Knowing when to apply sum rule is conceptual
- It is applied when a choice (a count) depends on **only one set**
- For example, in the previous example, Muadh cannot pick two or more different fruits
- So, if he picks an orange, then it is **independent** of (it does not matter on) the number of apples or avocados
- It only depends on the number of orange, which is 9
- Same argument holds if he picks an apple or an avocado
- So, his total choices: choice for apple + choice for orange + choice for avocado = 5+9+7= 23



Sum Rule

- **Example:** In how many ways an IT company can hire one candidate for a job from the applicants of the following three disciplines (any discipline is fine for the job). Assume that there is no duplicate applicant among the disciplines.
  - Computer Science (CS): 19 applicants
  - Information System (IS): 13 applicants
  - Software Engineering (SE): 17 applicants
- **Solution:**
  - No candidate falls in more than one category
  - So, choices from each category are separate/ independent of other categories (continued …)

Sum rule: each count depends on one set

Sum Rule

- (Solution continued from the previous slide …)
- There are 19 choices for selecting an applicant from CS graduates, a **separate** 13 choices for selecting from IS graduates, and a **separate** 17 choices for selecting from SE graduates
- Since the choices are independent, sum rule is applied
- Total choice: 19+13+17 = 49

- **Exercise:** What will happen if there are duplicate applicants among the disciplines? Will the number of choices reduce or increase? Only think about it. We shall solve this type of cases in the coming slides?

Sum rule: each count depends on one set

Mix of Product and Sum Rules

- We may need to use both product rule and sum rule
- **Example:** Repeat the previous example, but this time choose two candidates. The order of choice is important. That means (candidate1, candidate2) $\neq$ (candidate2, canidate1)
- **Solution:**
  - First candidate can be chosen in 49 ways // last slide
  - Second candidate can be chosen in 48 ways from the remaining 48 applicants // sum rule
  - As (candidate1, candidate2) $\neq$ (candidate2, canidate1), it is like making a word of two different letters
  - So, we apply product rule. Total choices: 49*48

Mix of product rule and sum rule

Mix of Product and Sum Rules

- **Example:** How many passwords of length five to eight are possible with upper or lower case letters and digits?
- **Solution:**
  - Remember, there are 26 upper case letters, 26 lower case letters, and 10 digits
  - First, we find the number of possible passwords of length five
  - A password of length five has five positions
  - Each position can have an upper case letter, or a lower case letter, or a digit.
  - So, number of choices for each position is 26+26+10= 62 // sum rule

Mix of product rule and sum rule

Mix of Product and Sum Rules

- Total choice for all five positions: 62*62*62*62*62 = 62^5 // Product rule
- This is the number of possible password of length five
- Similarly, and separately, number of possible passwords of length six, seven, and eight are $(62)^6$, $(62)^7$, and $(62)^8$
- Solution for length five, six, seven and eight are separate
- So, by sum rule, total number of passwords of length five, six, seven and eight: $62^5+62^6+62^7+62^8$
- This is the answer

Mix of product rule and sum rule

Correct solution = All – Wrong solution

- Sometimes, it is easier to find correct solutions by computing wrong solutions first and then subtracting it from all solutions:

  correct solution = all solution – wrong solution
- This technique is used in other topics, such as in probability, which we shall see in future lectures
- **Example:** How many passwords of length five are there with upper case letters and with at least one digit?
- **Solution:** There will be letters as well as 1 to 5 digits
  - First, compute the number of **all** passwords without any restriction on letters or digits. That means, 0 or more letters with 0 or more digits. (Continue …)

Correct = all – wrong

Correct Solution = All – Wrong Solution

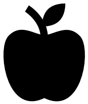
- Then, compute the number of password with no digit (this will be the **wrong** solution)
- Then subtract it from the number of all password (this will give the number of password with at least one digit, which will be the **correct** solution)
- All solutions (26 letters and 10 digits in each of five positions) = (26+10)*(26+10)*…five times = 36^5
- Wrong solutions (only 26 letters, no digit) = 26^5
- Correct solution (letters and at least one digit) = all – wrong solution = 36^5-26^5 = 48,584,800

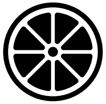
- **Exercise:** Solve the above example when the password length can be at least five and at most eight

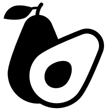
Correct = all – wrong

Principle of Inclusion-Exclusion

- Remember, in the sum rule examples in previous slides the sets were disjoint
- In one example, the sets of apple, orange and avocado were disjoint
- In another example, we assumed that there is no common applicants among the CS, IS and SE gradates
- What happens if there are common elements among the sets, that means, the sets intersect
- In that case, the sum rule needs to be adjusted
- Because, the common elements in the sets should be carefully added so that there is no repetition (see next example…)

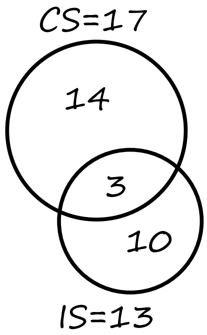






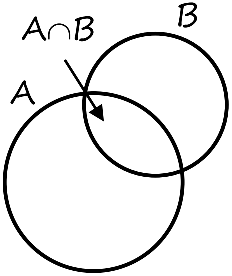
Principle of Inclusion-Exclusion

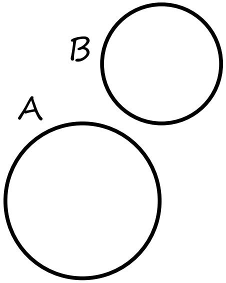
- **Example:** In how many ways we can choose a candidate from 17 CS graduates and 13 IS graduates where 3 of them have graduated in both CS and IS?
- **Answer:**
  - It will be wrong to simply add 17+13 = 30 by sum rule
  - Why? It is better understood by Venn diagram
  - Actually, there are (17-3) + (13-3) + 3 = 27 different persons
  - If we compute the answer as 17+13=30, then 3 is added twice, which is wrong
  - We need to deduct one “3” from 30 to make it correct. So, the correct answer is 27



Principle of Inclusion-Exclusion

- From the previous example, we get the idea that for finding the size of the union of two sets, the common elements should be deducted from their sum
- Mathematically, this principle is as follows:
  principle of inclusion-exclusion:
  $$|A \cup B| = |A| + |B| - |A \cap B|$$
- By words: Cardinality of the union of two sets is the sum of the cardinality of the two sets minus the cardinality of their intersection
- If two sets are disjoint, then $|A \cap B| = 0$
- In that case, the rule becomes: $\mathbf{|A \cup B| = |A|+|B|}$
- This is what we saw as the sum rule





Principle of Inclusion-Exclusion

- **Example:** In a food store there are 101 items in the list of sweet items and 87 items in the sour items. 23 items are marked as sweet and sour and are in both lists. In how many ways someone can choose one food item?
- **Solution:**
  - Suppose, A: sweet items, B: sour items
  - It is like choosing an item from **union** of all items
  - So, the number of ways of choosing is same as the number of different items (cardinality) in the union
  - We can find this by principle of inclusion-exclusion
  - $|A|=101, |B|=87, |A \cap B|=23$
  - Total choice: $|A|+|B|-|A \cap B| = 101 + 87 - 23 = 165$

$|A \cup B| =$
$|A|+|B|-|A \cap B|$

If A,B disjoint:
$|A \cup B|=|A|+|B|$

Principle of Inclusion-Exclusion

- **Example:** Repeat the previous example for choosing two different items, where the order of the two items chosen are important. That means, (item1, item2) is different than (item2, item1)?
- **Solution:**
  - The first item can be chosen in 165 ways // last slide
  - Second item can be any of the remaining 164 items
  - So, the number of choice for the second item is 164
  - As (item1, item2) $\neq$ (item2, item1), it is like making a word with two different letters
  - So, we need to apply product rule
  - Total choices: 165*164

$$|A \cup B| = |A| + |B| - |A \cap B|$$

If A,B disjoint:

$$|A \cup B| = |A| + |B|$$

Principle of Inclusion-Exclusion

- **Example:** How many binary numbers of length seven are there that start with 0 or end with 1?
- **Solution:** Suppose that set A = numbers that start with 0, and set B = numbers that end with 1
  - $A \cup B$ is the set of numbers that start with 1 **or** end with 0
  - We shall find: $|A \cup B| = |A| + |B| - |A \cap B|$
  - $|A \cap B|$ is the set of numbers that start with 0 **and** end with 1
  - $|A \cap B|$ is included both in set A and in set B
  - $|A| = 2^6$. Because the fist position is fixed to 1, so 1 choice. Other 6 positions can be 0 or 1, so 2 choices each. Total $1*2*2*2*2*2*2 = 2^6$ (continue…)

<u>A</u>

0000000

0000001

…

0111111

<u>B</u>

0000001

0000011

…

1111111

<u>$A \cap B$</u>

0000001

0000011

…

0111111

Principle of Inclusion-Exclusion

- (Continued from the previous slide …)
- Similarly, $|B| = 2^6$ // Why? Explain by yourself
- $|A \cap B| = 2^5$ // Why? Explain by yourself
- Now, $|A \cup B| = |A|+|B|-|A \cap B| = 2^6+2^6-2^5$ (Answer)

- **Exercise:** Solve this example by using the technique **correct = all – wrong.** Compute wrong solution as: find the numbers that do not start with 0 or end with 1.
- **Exercise:** There are total 100 people in a city. Among them, 50 people have a home and 60 people have a car. Among the people having a car or a home, 20 people have both a home and a car. How many people have neither a home nor a car?

<u>A</u>

0000000
0000001
…
0111111

<u>B</u>

0000001
0000011
…
1111111

<u>$A \cap B$</u>

0000001
0000011
…
0111111

Principle of Inclusion-Exclusion for Multiple Sets

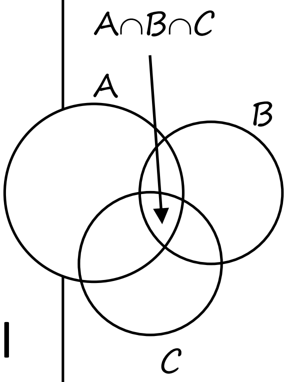
- Principle of inclusion-exclusion can be generalized for more than two sets
- It remains easy when the sets are all disjoint

$$|A1 \cup A2 \cup \ldots \cup An| = |A1|+|A2| + \ldots + |An|$$

- When the sets are not disjoint, it becomes more complicated
- For three sets A, B and C, it is as follows:

$$|A \cup B \cup C| =$$
$$|A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C|$$

- **Exercise:** Explain how the above rule is derived?
- **Exercise:** Rewrite the above rule if A and B are disjoint, but they both intersect C



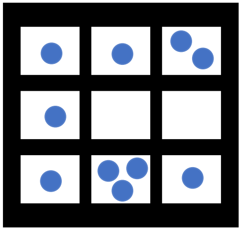
Pigeonhole Principle: Motivation

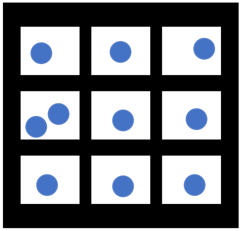
- Pigeonhole principle is simple but useful in counting
- It is used in many places in science and engineering
- Before we state the principle, we see some examples
- **Example:** Suppose that you are 14 friends. I do not know any of your month of birth. But I can tell these:
  - At least two of you have same month of birth
  - How? Because, I know the pigeonhole principle
  - I can tell the same thing even if you are 13 friends
  - But I can not tell it anymore if you are 12 or less!
- **Exercise:** Take any 13 or 14 dates of birth randomly as you like. Then verify the above example. See here →

1. 05-10-2000
2. 23-**11**-2001
3. 01-05-1999
4. 17-08-1997
5. 15-09-2001
6. 21-01-2001
7. 09-02-1998
8. 13-07-1996
9. 25-03-2003
10. 03-**11**-2005
11. 11-06-1993
12. 27-04-1992
13. 03-12-2002

Pigeonhole Principle: Motivation

- **Example:** Suppose that you have 9 pigeons and 9 boxes as their homes. Everyday they return during the sunset to their homes. But today 10 pigeons returned, may be the extra one came with them from another place. The following will be true:
  - At least one box will have two or more pigeons
  - Note that it is true no matter how the pigeons take their homes, separately or in common boxes
  - These are two (among many) possible examples
  - This will also be true for 11 or more pigeons
- **Exercise:** It is not true for 9 pigeons. Draw two pictures (like right-side)---one for true, one for false

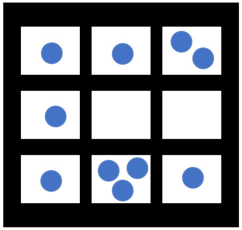


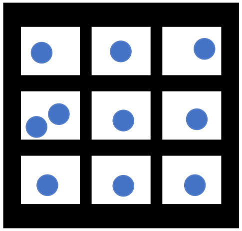


$n=10, m=9$

Pigeonhole Principle

- **Pigeonhole principle:** When n items are putted in m boxes, if n>m, then (for any distribution) at least one box will contain two or more objects (some boxes may be empty)
- **Example:**
  - In the previous example of birth date, n = number of friends = 14, and m = possible birth months= 12
  - As n>m, at least one month will be repeated
- **Example:**
  - In the previous example of pigeons, n = number of pigeon returned = 10, and m = number of boxes=9
  - As n>m, at least one box has two or more pigeons

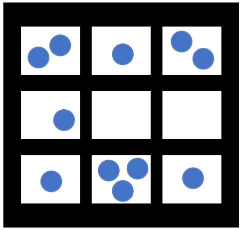


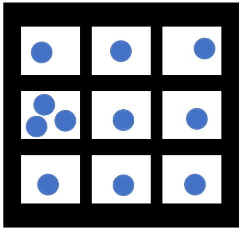


n=10, m=9

Pigeonhole Principle

- Three important things to notice in this principle (see the quoted text below):
- When n items are putted in m boxes, if “n>m”, then “at least one” box contains “two or more” items
- Example: **Importance of “at least one”:**
  - By “at least one” it means that if n>m, then there must be one box (may be more) that contains more than one item
  - It will be true for all possible distributions
  - For example, in the two right-side pictures, with n=11 and m=9, bottom distribution has one such box, and top distribution has three such boxes

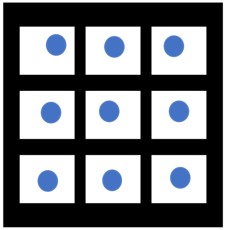




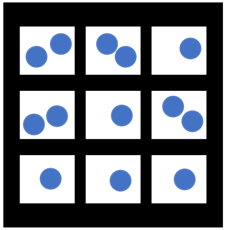
$n=11, m=9$

Pigeonhole Principle

- **Exercise:** In the previous example, find distributions (counterexamples) to show that it will not be correct if “at least one” is replaced by “zero” or by “at least two”
- **Example: Importance of “n>m”:**
  - The principle does not hold for n=m or n<m
  - Because, each item can go to a separate box. See
  - So, no box contains two or more elements
- **Example: Importance of “two or more”:**
  - It will be wrong if we replace “two or more” by something else, such as “one” or “three or more”
  - For example, here no box has “three or more”
  - **Exercise:** Find a similar counter-example for “one”



n=m=9



n=13, m=9

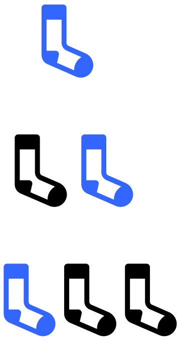
Pigeonhole Principle

- **Example:** To have at least one repeated birth date among a group of students, the number of students in the group must be at least 367
  - Because, by pigeonhole principle, m = possible birth dates
  - m = 366, including February 29-th // like boxes
  - n = number of students = ? // like items
  - By pigeonhole principle, n must be > m
  - So, n = 367 or higher
  - So, at least 367 students should be in the group
- **Exercise:** How many students must be there in a group to have a repetition in birth **day** (Friday, Saturday, …)?

$m = 366$
$n > m$
So, $n >= 367$

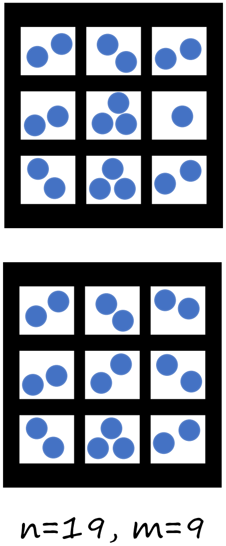
Pigeonhole Principle

- **Example:** Suppose a basket has socks of same size but of two colors, with each color having many socks. Minimum how many socks should you pick to get a pair of socks of same color so that you can wear them to go out?
  - Here, m = color (like boxes) = 2, n (like items) = ?
  - By pigeonhole principle, n>m
  - So, n = 3 or more socks should be picked (**Answer**)
  - If n = 2, then the two socks may be of different color
  - But for n $\geq$ 3, at least one color have two socks
- **Exercise:** If at least ten socks must be picked up to get a pair of same color socks, then how many colors of socks are there?



Generalized Pigeonhole Principle

- In the pigeonhole principle, some box gets **two** or more items, because n is bigger than m
- What if n is not only bigger, but much bigger, than m?
- Can we say that some box will get **three** or more items?
- Yes
- That is the **generalized pigeonhole principle**:
    - When n items are putted in m boxes, if n>m, then at least one box will get $\lceil n/m \rceil$ or more items
- **Example:** If 19 pigeons are putted in 9 boxes, then in any distribution, at least one box will get at least $\lceil 19/9 \rceil = 3$ pigeons (see right-side examples)
- **Exercise:** Repeat the above example for 28 pigeons



Generalized Pigeonhole Principle

- **Example:** Suppose that a basket has 100 socks of five colors, 20 of each color. You and your brother want to wear socks of same color to go out. At least how many socks you must pick?
- **Solution:**
  - This minimum number is n (like items) = ?
  - m = different colors (like colored boxes) = 5
  - You need at least 4 socks of same color (2 for you and 2 for your brother)
  - So, $\lceil n/5 \rceil \geq 4$. So, $n \geq 16$. So, 16 socks must be picked up
  - Note: $n \geq 20$ is wrong! Because, 16 is enough. See

$\lceil 15/5 \rceil = \lceil 3 \rceil = 3$

$\lceil 16/5 \rceil = \lceil 3.2 \rceil = 4$

$\lceil 17/5 \rceil = \lceil 3.4 \rceil = 4$

$\lceil 18/5 \rceil = \lceil 3.6 \rceil = 4$

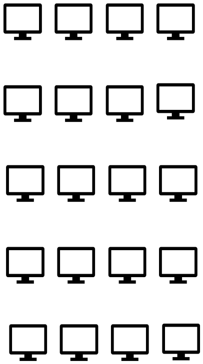
$\lceil 19/5 \rceil = \lceil 3.8 \rceil = 4$

$\lceil 20/5 \rceil = \lceil 4 \rceil = 4$

$\lceil 21/5 \rceil = \lceil 4.2 \rceil = 5$

Generalized Pigeonhole Principle

- **Exercise:** Repeat the previous example by replacing the values 100 and 20 by
  - (i) 50 and 10
  - (ii) 200 and 40
- **Example:** If you are 50 friends, then at least $\lceil 50/12 \rceil=5$ of you have same month in your birth date
- **Exercise:** What is wrong in the following statement:
  - When n items are putted in m boxes, if n>m, then at least two box will get one or more items
- **Exercise:** A computer lab has 20 computers. At a time, maximum how many students can use the lab so that no three students share a computer?



Motivation: Permutation and Combination

- Consider these two problems
  1. From 5 students (a,b,c,d,e), in how many ways 3 students can become 1st, 2nd, and 3rd?
  2. From 5 students (a,b,c,d,e), in how many ways 3 students can make a team for a competition?
- The above two problems look same
- Will their solutions be also same?
- No. Because, in the second problem, you just **choose** 3 students
- But, for the first problem, just choosing 3 students is not enough, they should be **arranged** as 1st, 2nd and 3rd too
- (Continue to the next slide …)

Permutation:
arrange/order

Combination:
collect/gather

Motivation: Permutation and Combination

- (Continued from the previous slide …)
- In the first problem, bce (b 1st, c 2nd, e 3rd) is different than cbe (c 1st, b 2nd, e 3rd)
- Whereas, in the second problem, bce, cbe, ecb, ... and many more are all same
- First problem is about ordering, and is called **permutation**
- Second problem is about selection, and is called **combination**
- **Exercise:** In the above example, who will have higher number of count? Permutation or combination? Why?
- **Exercise:** Write all assignments of b,c,e to 1st, 2nd, 3rd

Permutation:

arrange/order/

assign

Combination:

collect/gather/

choose/select

Permutation

- Product rule will help us understanding and defining permutation. Let us see an example
- **Example:** Given 10 letters, how many 3-letter (without repetition) words are there?
- **Solution:**
  - There are three positions for three letters
  - One position can take any of the 10 letters, so 10 choices
  - Another position can take any of the remaining 9 letters, so 9 choices
  - The remaining position has 8 letters to choose from, so 8 choices (continue to the next slide …)

….	….	….
10	9	8

Permutation

- (Continued from the previous slide …)
- Total choices by product rule: 10*9*8 (**Answer**)
- The above result is same as: 10*…*(10-3+1) = $\frac{10*9*8*7*6*5*4*3*2*1}{7*6*5*4*3*2*1} = \frac{10!}{7!} = \frac{10!}{(10-3)!}$
- Why are we writing this in a complicated way?
- Because, this example can be generalized as follows: given n elements, how many ways r elements can arrange
- The answer by product rule is: n(n-1)(n-2)…(n-r+1)
- Which is same as: $\frac{n!}{(n-r)!}$

* We are seeing all these to define permutation (next…)

….	….	….
10	9	8

Permutation Definition

- **Permutation** means arrangement where ordering of the items is important and counted
- Permutation is denoted as P(n,r), where $n \geq r$
- It means that the number of ways to permute/arrange/order r elements from n elements
- It is computed as: $P(n,r) = \frac{n!}{(n-r)!} = n(n-1)(n-2)\ldots(n-r+1)$
- **Exercise:** Verify that (i) P(n,n) = n!, (ii) P(n,0) = 1, (iii) P(n,1) = n
  - The second exercise above is little tricky
  - It means that choosing 0 item from n items is also a choice (1 choice). So, it is wrong to say P(n,0) = 0

$P(n,r) =$
$n!/(n-r)! =$
$n(n-1)\ldots(n-r+1)$

Permutation Examples

- **Example:** Suppose that there are five guests in your home. In how many ways (orders) you can shake hands with them one by one?
- **Solution 1:** By permutation formula, n=5, r=5, and

$$P(n,r) = P(5,5) = \frac{5!}{(5-5)!} = \frac{5!}{0!} = \frac{5!}{1} = 5! = 120$$

- **Solution 2:**
  - For product rule, five places for five guests
  - First place 5 choices, second place 4 choices, so on …
  - Total choices: 5*4*3*2*1 = 120
- **Exercise:** Repeat the above example if you shake hands with one particular guest twice in any order?

$P(n,r) =$

$n!/(n-r)! =$

$n(n-1)\ldots(n-r+1)$

Permutation Examples

- **Example:** In how many ways you can permute the five letters {q, i, u, e, o} so that "qu" always remain together
- **Solution:** "qu" can be considered as a single letter
  - So, total four letters can be considered (qu, i, e, o)
  - With n=4 and r=4, we can now arrange these four letters in P(n,r)=P(4,4) = $\frac{4!}{(4-4)!} = \frac{4!}{0!} = \frac{24}{1}$ = 24 ways
- **Exercise:** In the above example, in how many ways
  a. q and u remain together as "qu" or "uq"?
  b. q and u remain separated?
- **Exercise:** How many ways to arrange the letters of the word "neutral" so that three vowels remain together?

Example

qu i o e

i qu e o

o qu e i

e i o qu

…

Permutation Examples

- **Example:** Among your all 10 friends, Anas is your best friend. In how may ways (orders) can you visit six friends, but always visit Anas first?
- **Solution:**
  - In the ordering, Anas is always in the first position
  - So, choice and ordering is needed for the remaining five friends from the remaining nine friends
  - n=9, r=5, P(n,r) = P(9,5) = $\frac{9!}{(9-5)!} = \frac{9!}{4!}$ = 15120
- **Exercise:** How many words of 10 letters (no repetition) are there so that five odd positions are fixed with five vowels in this way a – e – i – o – u – ?

$P(n,r) =$

$n!/(n-r)! =$

$n(n-1)\ldots(n-r+1)$

Combination Definition

- **Combination** means collection/grouping/gathering where ordering of items is not important (not counted)
- Comparing with permutation, combination will be something smaller, because permutation is ordering in addition to collection
- Combination is denoted as C(n,r), where n ≥ r
- It means that the number of ways to collect/group/gather r elements from n elements
- It is computed as: $C(n,r) = \frac{n!}{(n-r)!r!} = \frac{n(n-1)(n-2)\ldots(n-r+1)}{r(r-1)(r-2)\ldots 3\cdot 2\cdot 1}$
- **Exercise:** Verify (i) C(n,n)=1, (ii) C(n,0)=1, (iii) C(n,1)=n
  - The first two exercises above say that there is only one way to take all elements or take no elements

$$C(n,r) = \frac{n!}{(n-r)!r!} = \frac{n(n-1)\ldots(n-r+1)}{r(r-1)\ldots 3\cdot 2\cdot 1}$$

Permutation or Combination?

- **Example:** From 20 students in a class, in how many ways 11 students can be selected for a football team?
- **Solution:**
  - First, we see whether it is a permutation problem or a combination problem
  - Forming a team is simply a collection of 11 players
  - It is not important to count who is selected first, who is second, or so on. So, ordering not important
  - So, it is a combination problem
  - We apply the combination formula with n=20, r=11
  - C(20,11) $=\frac{20!}{(20-11)!11!}=\frac{20(20-1)(20-2)\ldots(20-11+1)}{11\cdot 10\cdot 9\ldots 3\cdot 2\cdot 1}$ = 167960

$$C(n,r) = \frac{n!}{(n-r)!r!} = \frac{n(n-1)\ldots(n-r+1)}{r(r-1)\ldots 3\cdot 2\cdot 1}$$

Permutation or Combination?

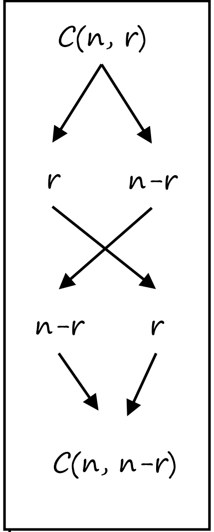
- **Example:** From 20 students, in how many ways 11 students can be selected for 11 prizes (1st to 11th)?
- **Solution:** This example is similar to the previous one
  - But this time, simply selecting 11 students is not enough. Ordering of the selected students is also important (who is 1st, who is 2nd, and so on …)
  - So, it is a permutation problem, with n=20, r=11
  - So, $P(20,11) = \frac{20!}{(20-11)!} = 20 \cdot 19 \cdot 18 \ldots 10$

    $= 6{,}704{,}425{,}728{,}000$
- **Exercise:** Among 11 men and 9 women, how many ways 7 men and 5 women can be selected for a committee?
- **Exercise:** How many ways they can be assigned 12 chairs?

$$C(n,r) = \frac{n!}{(n-r)!r!} = \frac{n(n-1)\ldots(n-r+1)}{r(r-1)\ldots 3 \cdot 2 \cdot 1}$$

C(n, r) = C(n, n-r)

- **Exercise:** Repeat the previous two examples for 9 prizes. Is any result same with 11 prizes? Why?
- Combination has this interesting property: C(n,r)=C(n,n-r)
- This can be proven both mathematically and logically
- **Example:** Prove that C(n, r) = C(n, n-r)
  - $C(n,r) = \frac{n!}{(n-r)!r!} = \frac{n!}{(n-r)!r!} = \frac{n!}{(n-r)!(n-(n-r))!} = C(n, n-r)$
- Logically, selecting r elements from n elements means making two partitions with number of elements r and n-r
- This is same as making two partitions with n-r and n-(n-r)=r elements, which is selecting (n-r) elements. See
- **Example:** $C(10,3)=\frac{10!}{(10-3)!3!} = \frac{10!}{7!3!} = \frac{10!}{3!7!} = \frac{10!}{(10-7)!7!} = C(10,7)$



P(n, r) = C(n, r)*r!

- **Exercise:** Show that C(n,0) = C(n,n)
- Permutation and combination are closely related
- Mathematically, P(n, r) = C(n, n-r)r!
- This can be proven both mathematically and logically
- **Example:** Prove that P(n, r) = C(n, n-r)r!
  - $P(n,r) = \frac{n!}{(n-r)!} = \frac{n!r!}{(n-r)!r!} = \frac{n!}{(n-r)!r!} r! = C(n,r)r!$
- Logically, permutation P(n,r) has two steps
  1. Select r elements from n elements // C(n,r)
  2. For each selection, arrange r elements // r!
  - Each selection in (1) has P(r,r)=r! arrangement in (2)
  - By product rule, multiply (1) and (2)
- **Exercise:** Show that P(n,n) = C(n,n)n!

Permutation:

- *Select (combination)*
- *Arrange*
- *Multiply*

Permutation: Select First, Then Arrange

- **Example:** How many words of 5 letters with no repetition are there?
- **Solution:**
  - Choose 5 letters from 26 letters in C(26, 5) ways
  - For each such choice of the 5 letters, there are P(5,5) = 5! arrangements of those 5 letters
  - So, total arrangement: C(26, 5)*5!
  - This is same as P(26, 5)
  - So, the answer is: C(26, 5)*5! = P(26, 5) = 26*25*24*23*22 = 7,893,600
- **Exercise:** How many words of 25 letters with no repetition are there? What about words of 26 letters?

Permutation:

- *Select (combination)*
- *Arrange*
- *Multiply*

Permutation: Select First, Then Arrange

- **Example:** How many words of 3 vowels (no repeat) and 5 consonants (no repeat) are there?
- **Solution:**
  - Choose 3 vowels from 5 vowels in C(5,3) ways
  - Choose 5 of 21 consonants in C(21,5) ways
  - Total choice for 3 vowels and 5 consonants: C(5,3)*C(21,5)
  - After choosing, arrange them in P(8,8) = 8! ways
  - Total arrangements: C(5,3)*C(21,5)*8! = 8,204,716,800
- **Exercise:** How many words of 5 vowels (no repeat) and 5 consonants (no repeat) are there?

Permutation:

- *Select (combination)*
- *Arrange*
- *Multiply*

Permutation: Select First, Then Arrange

- **Example:** How many words of 10 letters (no repetition) are there so that even positions are occupied by vowels and odd positions are by consonants
- **Solution:** We shall use the idea of choice then permute
    - **Choices for vowels:**
        - As no repetition is allowed, all five vowels (a, e, i, o, u) must be chosen for five even positions
        - There are C(5,5)=1 way to do that
        - Then arrange them in P(5,5) = 5! ways within even positions
        - So, total arrangements for vowels: 1*5! = 5!
    - (Continue to the next slide…)

Permutation:

- *Select (combination)*
- *Arrange*
- *Multiply*

Permutation: Select First, Then Arrange

Permutation:
- *Select (combination)*
- *Arrange*
- *Multiply*

- (Continued from the previous slide…)
- **Choices for consonants:**
  - Five consonants are to be chosen from 21 consonants for the five odd positions
  - There are C(21,5)=20,349 ways to do that
  - Arrange them in 5! ways within odd positions
  - So, total arrangement for consonants is 20,349*5!
- Finally, by product rule, total arrangements for 10 letters = choice for five vowels * choice for five consonants = 5!*20,349*5! = 293,025,600
- **Exercise:** Repeat the above example for eight letters

Permutation: Select First, Then Arrange

- **Example:** In how many ways 3 red and 5 white cars can park along a line so that no two red cars are adjacent?
- **Solution:**
  - Here the position of red and white cars will be relative, with no actual parking positions
  - Any two red cars should be separated by one or more white cars
  - If we place the white cars along a line, then there will be 6 positions in the left and right of 5 white cars
  - See the right-side picture
  - (Continued …)

-W-W-W-W-W-

⇩

-WRWRW-W-WR

(WRWRWWWR)

…

RW-W-WRW-WR

(RWWWRWWR)

…

Permutation: Select First, Then Arrange

  - (Continued from the previous slide…)
  - Red cars must choose 3 of those 6 positions
  - This has C(6,3) = 20 ways
  - Then arrange them within themselves in 3! ways
  - So, total arrangement for red cars: 20*3!= 120
  - There is only one choice for the relative positions of the white cars--just place them on a line
  - Then arrange them within themselves in 5! ways
  - Total arrangement for white cars: 1*5! = 120
  - Total arrangement for all 8 cars: 120*120 = 14400
- **Exercise:** How many 9-bit binary numbers have four 1s? (Hint: Choose 4 positions for 1s. That's enough. Why?)

-W-W-W-W-W-

⇩

-WRWRW-W-WR

(WRWRWWWR)

…

RW-W-WRW-WR

(RWWWRWWR)

…

Lecture 11
Introduction to Probability

…Indeed, Allah provides for whom He wills without account. (Quran 3:37)

Motivation

- **Example:** Suppose that you had a class exam today
  - The exam had 20 MCQs, 1 mark for each question
  - Pass mark is 10
  - Each question had 4 options, one of them is correct
  - You did not have any preparation for the exam
  - You answered all questions **randomly** (blindly)
  - What is your **chance** of correctly answering Q1, Q2, and so on …
  - What is your **chance** of marginally passing (getting exactly 10)?
  - What total marks can you **expect** in the exam?
- Answering these questions deal with **probability**

Class Exam
Q1: …
a: …
b: …
c: …
d: …
Q2: …
a: …
b: …
c: …
d: …
Q3: …

Motivation

- **Example:** Let us explore the previous example more
  - Suppose that the questions are not MCQs, but True/False
  - Will your chance of correctly answering each question increase or decrease? Why?
  - What about the expected marks now? Will your expectation increase or decrease? Why?
  - Also, how do you select your answer (a, b, c, d, T, F) for each question truly randomly?
    - That means, do not choose one of a, b, c, d (say c) or T, F (say T) more frequently than others?
- These are some of the things related to probability

Class Exam

Q1: … (T/F)

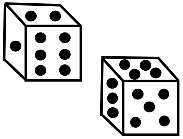
Q2: … (T/F)

Q3: … (T/F)

…

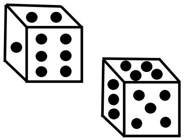
Definitions

- We shall investigate the previous two examples later
- For defining different terms related to probability, we shall use some other common examples
- **Example:**
  - Consider a coin with two **similar** sides, Head(H) and Tail(T)
  - You through it up in the air
  - When it falls down on the ground, it may be H or T
  - Chance of H is 50% and chance of T is 50%
  - This chance is called **probability**
  - It is written as Prob{H} = 1/2, Prob{T} = 1/2
  - Appearance of H and T are called two **outcomes**



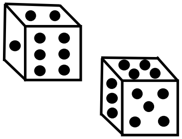
Definitions

- **Example:**
  - Consider a dice of six **similar** sides---1, 2, 3, 4, 5, 6
  - You through it over a surface
  - When it stops, possible outcome is 1, 2, 3, 4, 5 or 6
  - All possible outcomes is also called **sample space**
  - Prob{any one sample} = 1/6
  - Prob{1} = Prob{2} = … = Prob{6} = 1/6
- In general, **Probability of an outcome = 1/number of outcomes**
- A coin or dice with "similar sides" means that all outcomes/events are **equally likely** (have same chance)
- This type of coin or dice is called **fair**, or **unbiased**



Properties of Probability

- Probability of any event is ≤ 1 and ≥ 0
- Sum of probability of all events = 1
- **Example:** For troughing a coin
  - $0 \leq \text{Prob}\{H\} = \text{Prob}\{T\} = 1/2 \leq 1$
  - $\text{Prob}\{H\} + \text{Prob}\{T\} = 1/2 + 1/2 = 1$
- **Example:** For troughing a dice
  - $0 \leq \text{Prob}\{1\} = \text{Prob}\{2\} = \ldots = \text{Prob}\{6\} = 1/6 \leq 1$
  - $\text{Prob}\{1\}+\ldots+\text{Prob}\{6\} = 1/6+1/6+1/6+1/6+1/6+1/6 = 1$
- **Exercise:** If you look at a digital watch randomly, then what is the probability that its second value is odd (like 23, 47, etc.)? What is the sample space here? How do you verify sum of probability is one?



11:23:19

Properties of Probability

- Probability can be computed for more than one outcome
- **Example:** When you through a dice, what is the probability that it comes up with an even side?
- **Solution:** Among six sides of a dice, three sides are even. So, Prob{an even side} = 3/6 = 1/2
- In the above example, “even side” is called an **event**
- Generally, **Prob{an event} = event size/total outcome**
- **Example:** A basket contains 5 green balls and 3 blue balls. If you pick a ball randomly (blindly), then the probability of it is a blue ball is 3/8. Similarly, probability of it is a green ball is 5/8
- **Exercise:** What is the probability of it is not a blue ball?

Prob{event}
=
(event size)/
total outcome

Examples

- Probability can be computed over combined outcomes
- **Example:** Suppose that you through two coins together (or one coin twice). What is the probability that both of them are tail?

- **Solution 1:**
  - Four outcomes of two throws: {HH, HT, TH, TT}
  - Only one of them is both tails (TT)
  - So, Prob{both tails} = both tail/total outcome = 1/4
- **Solution 2:**
  - Prob{1st throw T} = 1/2, Prob{2nd throw T} = 1/2
  - By product rule, Prob{both tail (TT)}=(1/2)*(1/2)=1/4
- **Exercise:** What is the probability of exactly one is tail?

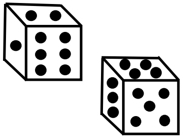
Examples

- **Example:** Suppose a computer program looks into the computer clock randomly again and again, and stops when it sees an even second. What is the probability that the program stops at its fifth look? (See here) →
- **Solution:** A clock has 30 odd and 30 even seconds
  - Suppose E means even and O means odd seconds
  - Output of the five looks should be like this OOOOE
  - In one look, Prob{O} = Prob{E} = 30/60 = 1/2
  - By product rule, Prob{OOOOE} = Prob{O}*Prob{O}*Prob{O}*Prob{O}*Prob{E} = (1/2)*(1/2)*(1/2)*(1/2)*(1/2) = $(1/2)^5$ = 0.03125
- **Exercise:** What if the computer stops at k-th look?

11:23:19
↓
11:23:47
↓
11:24:33
↓
11:24:59
↓
11:25:44

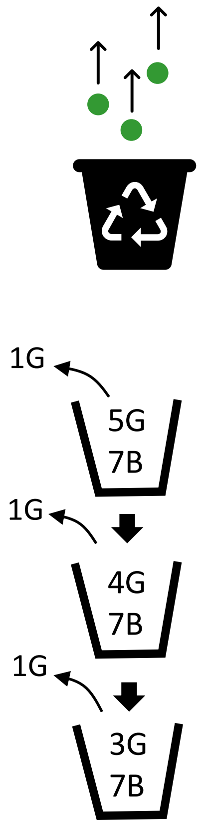
Examples

- **Example:** If you through one dice twice (or two dice once together), then what is the probability that the difference between the two outcomes is two?
- **Solution:**
  - Possible outcomes for two throws are 36: {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,1),(2,2),…,(6,6)}
  - 8 of them have difference two in the outcomes: {(1,3), (3,1), (2,4), (4,2), (3,5), (5,3), (4,6), (6,4)}
  - So, Prob{two outcomes differ by two} = 8/36 = 2/9
- **Exercise:** Write all possible outcomes for three throws
- **Exercise:** If you throw two dices, then what is the probability that the sum of their outcomes is nine?

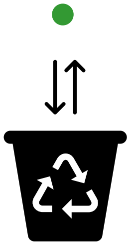


Sampling Without Replacement

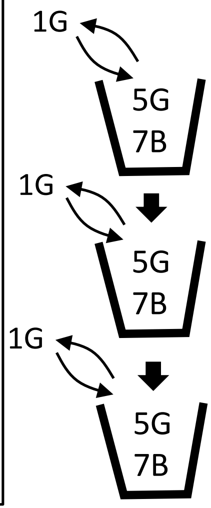
- **Example:** A basket contains 5 green and 7 blue balls. You pick three balls one by one. After picking, you do not put a ball back into the basket. What is the probability that all three balls are green?
- **Solution:** After picking a ball, it is not returned to the basket. This is called **sampling without replacement**
  - Prob{1st ball green} = green/all = 5/12
  - Remaining balls: 4 green, 7 blue
  - Prob{2nd ball green}=4/11. Remaining: 3 green, 7 blue
  - Prob{3rd ball green} = 3/10
  - By product rule, Prob{all three balls green} =(5/12)*(4/11)*(3/10) = 1/22 = 0.04545



Sampling With Replacement



- **Example:** Repeat the previous example by putting the ball back into the basket every time after picking
- **Solution:** After picking a ball, it is putted back into the basket. This is called **sampling with replacement**
  - Prob{1st ball green}=5/12
  - Remaining balls: 5 green, 7 blue
  - Prob{2nd ball green}=5/12
  - Remaining: 5 green, 7 blue
  - Prob{3rd ball green} = 5/12
  - Prob{all three balls green} = $(5/12)^3 = 0.07233$
- **Exercise:** Repeat the previous two examples if the three balls picked in sequence are green, blue, blue



Principle of Inclusion Exclusion

- Some rules on sets and counting that we saw before also apply to probability in similar ways
- One such rule is the principle of inclusion-exclusion
- **Principle of inclusion exclusion:** For two events A and B

  $$\text{Prob}\{A\cup B\} = \text{Prob}\{A\} + \text{Prob}\{B\} - \text{Prob}\{A\cap B\}$$
- This is same as:

  $$\text{Prob}\{A \text{ or } B\} = \text{Prob}\{A\} + \text{Prob}\{B\} - \text{Prob}\{A \text{ and } B\}$$
- It says that, when we count the probability of two events, we add their individual probabilities, but we should subtract the probability of their joint event to avoid repetition

For Sets:

$|A\cup B| =$

$|A|+|B|-|A\cap B|$

For Probability:

$\text{Prob}\{A\cup B\} =$

$\text{Prob}\{A\}+\text{Prob}\{B\}$

$-\ \text{Prob}\{A\cap B\}$

Principle of Inclusion Exclusion

- **Example:** Looking at a digital watch at random, what is the probability that the second is multiple of 15 or 20
- **Solution:** Assume that the events A, B are:
  - A: Seconds multiple of 15 are: 0, 15, 30, 45 (total 4)
  - B: Seconds multiple of 20 are: 0, 20, 40 (total 3)
  - So, $A \cap B$: Seconds multiple of 15 **and** 20 is: 0 (total 1)
  - Similarly, $A \cup B$: Seconds multiple of 15 **or** 20 = ?
  - $Prob\{A\} = 4/60$, $Prob\{B\} = 3/60$, $Prob\{A \cap B\} = 1/60$
  - $Prob\{A \cup B\} = Prob\{A\} + Prob\{B\} - Prob\{A \cap B\}$
    $= 4/60 + 3/60 - 1/60 = 6/60 = 0.1$
- **Exercise:** If a computer choses one number among 100 numbers from 1 to 100 at random, then what is the probability that the number is multiple of 30 **or** 40?

For Sets:

$|A \cup B| =$

$|A|+|B|-|A \cap B|$

For Probability:

$Prob\{A \cup B\} =$

$Prob\{A\}+Prob\{B\}$

$- Prob\{A \cap B\}$

Correct = All - Incorrect

- **Exercise:** Repeat the previous exercise if the number is multiple of **both** 30 **and** 40
- Remember, this technique: **correct = all - incorrect**
- This technique can be used for probability too
- **Example:** Suppose that you through a dice five times. What is the probability that 3 appears at least one time
- **Solution:** There are two possible events:
  - $E_{correct}$: 3 appears at least one time
  - E_{wrong}: 3 does not appear at all
  - $E_{correct}$ and E_{wrong} cover all possible outcomes
  - So, $Prob\{E_{correct}\} + Prob\{E_{wrong}\} = 1$
  - (Continued to the next slide …)

Correct = all – wrong

Correct = All - Incorrect

- (Continued from the previous slide …)
- We need to find Prob{$E_{correct}$}, which is 1-Prob{E_{wrong}}
- E_{wrong} means, in each throw, 3 does not appear. That means, only 1,2,4,5 or 6 appear (so, 5 valid outcomes)
- So, Prob{3 does not appear in 1st throw} = 5/6
- Similarly, Prob{3 does not appear in 2nd throw}=5/6
- So on for 3rd, 4th and 5th throws
- By product rule,
  Prob{E_{wrong} = 3 does not appear in all five throws}= $(5/6)^5$
- Prob{$E_{correct}$}= 1–Prob{E_{wrong}}= 1–$(5/6)^5$ = 0.5982

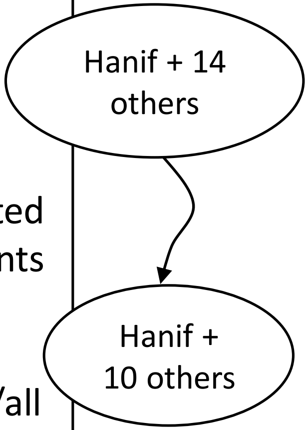
Correct = all – wrong

- **Exercise:** What is the probability that the sum of the five throws is smaller than 30? (Hint: Only one case has sum$\geq$30)

Probability by Counting

- **Example:** 11 out of 15 students is selected for a football team. What is the probability that Hanif is selected?
- **Solution:**
  - There are C(15,11) ways to select 11 students
  - How many of these selection include Hanif?
  - If Hanif is included, then only 10 should be selected (Hanif is another 1) from the remaining 14 students (14: Hanif is excluded, as he is already selected)
  - This can be done in C(14,10) ways
  - So, Prob{Hanif included in 11} = (Hanif included)/all

    $= C(14,10)/C(15,11) = \frac{14!}{4!10!} / \frac{15!}{4!11!} = 11/15 = 0.733$
- **Exercise:** Do this if Hares is selected but Hanif is not



Probability by Counting

- **Example:** There are five parking spaces for five people (A, B, C, D, E). What is the probability that two persons B and D always park side by side?
- **Solution:**
  - All possible ways to park by A,B,C,D,E is P(5,5) = 5!
  - B and D always park side by side
  - So, B and D are like a single person BD or DB
  - Number of ways to park by A, C, E, BD is P(4,4) = 4!
  - Similarly, number of ways to park by A, C, E, DB is 4!
  - Total ways to park by B and D together is: 4! + 4!
  - Prob{BD together}=(BD together)/all=(4!+4!)/5!=0.4
- **Exercise:** What if none of B, C, D park side by side?

A B C D E
A B C E D
A B D C E
…

A BD C E
A C E BD
…

A DB C E
A C E DB
…

Probability by Counting

- **Example:** A coin is thrown five times. What is the probability that exactly three of them are H?
- **Solution 1:** Five positions. Each has 2 choices (H or T)
  - So, H and T can appear in 5 throws (5 positions) in 2*2*2*2*2 = 2^5 ways (this is all possible outcome)
  - Among them, C(5,3) ways have exactly 3 H

  //It chooses 3 places for 3 H in C(5,3) ways. Once 3 H
  // chosen, 2 T can be placed in remaining 2 places in
  // C(2,2) = 1 ways. So, total C(5,3)*1 = C(5,3) ways
  - So, Prob{3 H in 5 throws} = (count for 3 H)/all
    = C(5,3)/2^5 = 10/32 = 0.3125
- We solve it in another way, which will be useful later …

Example:

H H H T T
H H T H T
T H TH H
H T T H H
T T H H H
…

Probability by Counting

- **Solution 2:** In each throw, Prob{H} = Prob{T} = 1/2
  - There are C(5,3) ways that have 3 H in 5 throws
  - For each way,
    Prob{exactly 3 H in 5 throws) = Prob{3 H and 2 T}
    = $(\text{Prob}\{H\})^3 * (\text{Prob}\{T\})^2 = (1/2)^3 * (1/2)^2 = (1/2)^5 = 1/32$
  - Observe that this probability is same for all C(5,3) ways (any arrangement) of 3H and 2T. See here
  - Total probability in C(5,3) ways: 1/32 + 1/32 + … + (5,3) times = 10*(1/32) = 0.3125
- **Exercise:** Repeat the example if at most 3 H are there
- **Exercise:** Repeat the example if a dice is thrown five times and exactly three "Side 2" are there

<u>Prob{Seq.}:</u>

Prob{HHTHT} =
$$\frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2}$$

Prob{HTTHH} =
$$\frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2}$$

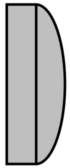
Prob{HHHTT} =
$$\frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2}$$

…

all same as 1/32

Ununiform Distribution

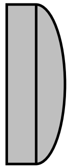
- So far, we have seen that the outcomes of a coin throw, or a dice throw, or looking at clock are equally likely
- Because, the coin, dice, or clock was fair or unbiased
- This equal distribution of probability among the outcomes is called **uniform distribution**
- However, a coin, dice, or clock may be **biased** or defective
- In that case, probability of outcomes may not be same
- For example, if we throw a biased coin again and again, then it may happen that H comes twice frequent than T
- This type of unequal probability among the outcomes is called **ununiform distribution**



A biased coin

Ununiform Distribution

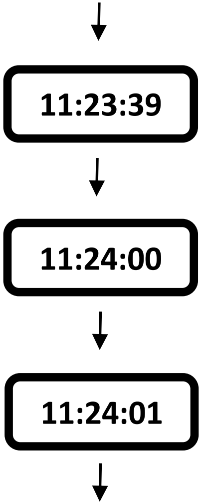
- **Example:** Consider a biased coin where H comes thrice as frequent than T. What is the probability (probability distribution) of H and T?
- **Solution:**
  - H is more frequent than T
  - So, probability of H will be higher than T
  - H is three times frequent than T, so Prob{H}=3*Prob{T}
  - Total Probability = Prob{H} + Prob{T} = 1
  - 3*Prob{T} + Prob{T} = 1
  - This gives, Prob{T} = 1/4 and Prob{H} = 3/4
- **Exercise:** Find the probability of 1, 2, 3, 4, 5, 6 of a biased dice if the even sides are twice as frequent as odd sides



A biased coin

Ununiform Distribution

- **Example:** Consider a partially defective digital clock
  - Its hours and minutes are correct, but seconds not
  - There are 40 seconds, instead of 60
  - Length of each even second (E) is 1.5 original second
  - Length of each odd second (O) is 1 original second
  - In total, 40 seconds give 20*1.5 + 20*1 = 60 seconds
  - If we look at this clock at random, then Prob{E} = 1.5*Prob{O}
  - Prob{E} + Prob{O} = 1.5*Prob{O} + Prob{O} = 1
  - This gives, Prob{O} = 0.4, Prob{E} = 0.6
- **Exercise:** Repeat the above example with 30 defective seconds in a minute, each of length of 2 original seconds



Binomial Distribution

- **Example:** Consider a biased coin with Prob{H} = 1/4 and Prob{T} = 3/4. What is the probability that exactly 3H come up from 5 throws?
- **Solution:** 5 throws are like 5 positions along a line
  - Exactly 3H from 5 throws is like choosing 3 positions for 3 H from 5 positions. This is C(5,3) ways
  - In each such way, Prob{exactly 3H} = Prob{3H and remaining 2T) is: $(1/4)^3(3/4)^2$
  - This value is same for any sequence of 3H and 2T
  - Over all C(5,3) ways, Prob{exactly 3H}: $C(5,3)*(1/4)^3*(3/4)^2 = 0.08789$
- This is an example of **Binomial distribution** (see next…)

<u>Prob{Seq.}:</u>

Prob{HHTHT} = $(\frac{1}{4})(\frac{1}{4})(\frac{3}{4})(\frac{1}{4})(\frac{3}{4}) = (\frac{1}{4})^3(\frac{3}{4})^2$

Prob{HTTHH} = $(\frac{1}{4})(\frac{3}{4})(\frac{3}{4})(\frac{1}{4})(\frac{1}{4}) = (\frac{1}{4})^3(\frac{3}{4})^2$

Prob{HHHTT} = $(\frac{1}{4})(\frac{1}{4})(\frac{1}{4})(\frac{3}{4})(\frac{3}{4}) = (\frac{1}{4})^3(\frac{3}{4})^2$

…

All same as $(\frac{1}{4})^3(\frac{3}{4})^2$

Binomial Distribution

- The previous example can be generalized as follows
- **Example (Bernoulli trial, Binomial distribution):**
  - In general, "a coin or dice throw", "looking at a clock randomly", "answering an MCQ randomly", etc. are called a **trial**
  - If for a trial, the outcomes are just two, success or failure, then it is called a **Bernoulli trial**
  - If Prob{success}=p and Prob{failure}=q, then p+q=1
  - Probability of exactly r success in n Bernoulli trails is: $C(n,r)p^rq^{n-r} = C(n,r)p^r(1-p)^{n-r}$ // See previous example
  - The probability computation is this way is called **Binomial distribution**

p:
Prob{success}

Prob.{r success in n trials}
=
$C(n,r)p^r(1-p)^r$

Binomial Distribution

p: Prob{success}

Prob.{r success in n trials} = $C(n,r)p^r(1-p)^r$

- Let us again see the very first example of this lecture
- **Example:**
  - There are 20 MCQs in your exam
  - You are answering MCQs randomly, where each MCQ has 4 options, with only one option being correct
  - For each question, probability of correct answer is 1/4, and probability of wrong answer is 3/4
  - Probability of exactly 10 correct answers from 20 MCQs by binomial distribution = Prob{10 correct, 10 wrong} = $C(20,10)(1/4)^{10}(3/4)^{10}$
- **Exercise:** Calculate the exact value of the above probability
- **Exercise:** Repeat if the questions are True/False

Binomial Distribution

- **Example:** In the previous example, what is the probability that **at least** 18 of your answers are correct?
- **Solution:**
  - At least 18 means 18, 19 or 20 can be correct
  - We shall use binomial distribution
  - Prob{exactly 18 correct} = $C(20,18)(1/4)^{18}(3/4)^2$
  - Prob{exactly 19 correct} = $C(20,19)(1/4)^{19}(3/4)^1$
  - Prob{exactly 20 correct} = $C(20,20)(1/4)^{20}(3/4)^0$
  - By sum rule, Prob{at least 18 correct}:

    $C(20,18)(1/4)^{18}(3/4)^2 + C(20,19)(1/4)^{19}(3/4) + C(20,20)(1/4)^{20}$
- **Exercise:** Compute the value of the above probability

p: *Prob{success}*

Prob.{r success in n trials} = $C(n,r)p^r(1-p)^r$

Expected Value: Motivation

- **Example:**
  - You throw a coin many many times, say 100 times
  - How many times you can **expect** H?
  - 50. Why?
  - Because, the chance (**probability**) of H is 1/2 (50%)
  - So, 100*(1/2) = 50
  - What about T?
  - Same. 50
- **Example:**
  - If you throw it 80 times, then you can expect H 40 times, and T 40 times. Because, 80*(1/2) = 40
- **Motivation:** Expectation is like “count*probability”

*Expectation is like “count*prob.”*

Expected Value: Motivation

- **Example:** Everyday Zami's father gives him some money before he goes to school. His father throws a dice and gives money equivalent to the output of the dice. How much money Zami can **expect** next day from his father?
- **Solution:**
  - Remember, a dice-throw has 6 outputs: 1,2,3,4,5,6
  - So, Zami'z father gives him 1, 2, 3, 4, 5, or 6 Riyals
  - Next day Zami cannot expect something small (say 1 Riyal), because dice-output can be more (like 5, 6)
  - Similarly, he cannot expect something very high
  - Zami's true expectation should be something in middle
  - Actually, it will be **average** value:(1+2+3+4+5+6)/6=3.5

Expectation is like average

Expected Value: Definition

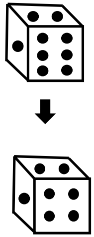
- Suppose X is a variable that counts some value in the outcomes of some trials
- For example, X can be the number of H in some coin throws, sum of the output of some dice-throws, etc.
- Such a variable X is called a **random variable**
- Random variables are helpful to find expected values
- **Expected value** of X is denoted as E(X) and is defined as

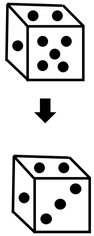
  E(X) = ∑(Prob{X}*Value(X)) over all outcomes
- **Example:** In the previous example, Zami's expected money is: (1/6)*1 + (1/6)*2 + (1/6)*3 + (1/6)*4 + (1/6)*5 + (1/6)*6 = (1+2+3+4+5+6)/6 = 3.5 Riyals
  - Because each side has probability 1/6

*Expectation = ∑(Prob.*value) over all outcome*

Expected Value: Example

- **Example:** Zami was very honest. He realized that something between 1 to 4 riyals is enough for him. So, one day he changed the face 5 of the dice as another face 3 and the face 6 as another face 4 without the knowledge of his father. Now, with this biased dice, how much money he can expect everyday?
- **Solution:** Now, the faces of the dice are: 1, 2, 3, 3, 4, 4
  - Prob{1}=1/6, Prob{2}=1/6, Prob{3}=2/6, Prob{4}=2/6
  - Now Zami's expectation is:
    (1/6)*1+(1/6)*2+(2/6)*3+(2/6)*4=2.83 Riyals
- **Exercise:** A biased coin has Prob{H}=1/3 and Prob{T}=2/3. What is the expected number of H in 100 throws?





Expected Value: Example

- **Example:** In a biased coin, Prob{H}=1/3 and Prob{T}=2/3. After expected how many throws the first H will appear?
- **Solution:**
  - Let the first H appears at the X-th throw
  - Before X-th throw, all throws are T
  - X may be 1, 2, 3, 4, 5, … α
  - If X=1, then the outcome of the only throw is {H}
  - Probability of such a throw is Prob{X=1}=Prob{H}=1/3
  - If X=2, then the outcomes of the two throws are {TH}
  - Probability of such case is Prob{X=2} = Prob{T}*Prob{H} = (2/3)(1/3)
  - (Continued to the next slide …)

*Expectation = Σ(Prob.*value) over all outcome*

Expected Value: Example

- (Continued from the previous slide …)
- If X=3, then the outcomes of the three throws: {TTH}
  - Probability of such case is Prob{X=3} = Prob{T}*Prob{T}*Prob{H} = (2/3)(2/3)(1/3)
- In general, for X=k,
  Prob{X=k} = $(\text{Prob}\{T\})^{k-1}$Prob{H} = $(2/3)^{k-1}(1/3)$
- So, $E(X)=\sum_{k=1}^{\infty}\left(k\left(\frac{2}{3}\right)^{k-1}\left(\frac{1}{3}\right)\right) = \left(\frac{1}{3}\right)\sum_{k=1}^{\infty}\left(k\left(\frac{2}{3}\right)^{k-1}\right)$
  $= \left(\frac{1}{3}\right)\frac{1}{\left(1-\frac{2}{3}\right)^2} = 3$ // use $\sum_{k=1}^{\infty}\left(kx^{k-1}\right) = \frac{1}{(1-x)^2}$
- **Exercise:** Proof this equality (Hint: start from right side)
- **Exercise:** Repeat this example with an unbiased coin

Expectation
=
*∑(Prob.*value)*
over all
outcome

Geometric Distribution

- The previous example can be generalized as follows, which is called **geometric distribution**
- **Geometric Distribution:** If a trial has Prob{success} = p and Prob{failure} = 1-p, then the expected number of trials at which the first success appears is 1/p.
- **Exercise:** Proof the above statement by following the previous example step by step.
- **Exercise:** Expected how many times a dice is to be thrown for the first appearance of side 5? Is it same for all sides? Why?
- **Exercise:** Expected how many times two dice should be thrown together so that their sum is 11?

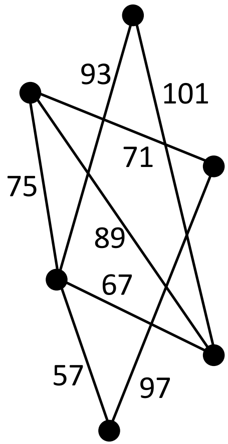
Geometric distribution:
fail
fail
fail
…
fail
success

Lecture 12
Graphs and Trees

…And indeed, the weakest of houses is the house of the spider, if they only knew.
(Quran 29:41)

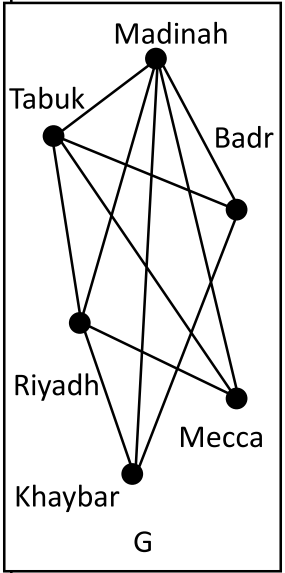
Motivation

- Graphs are used in many applications in mathematics, computer science, and similar other fields
- Many problems can be formulated by using graphs and then solved by graph algorithms and techniques
- **Example:**
  - Consider the road network of a country, where each city is a node (or a point), and the roads among them are lines. See right-side picture
  - Each line has labels corresponding to the distance
  - Suppose you want to find the minimum travelling distance among two cities
  - This can be solved by graph algorithms



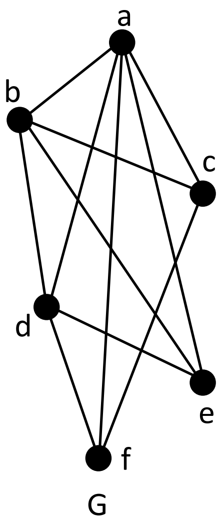
Definitions: Graph

- A **graph** consists of a set of **vertex** and a set of **edges**
- A graph G is written as G=(V,E), where V is the set of vertices and E is the set of edges
- An edge is a connection between two vertices
- An edge represents that the two vertices are related
- **Example:**
  - In this graph G, vertices are cities
  - An edge means that there is a road between two cities
  - If no road between two cities, then no edge
  - For example, a road exists from Madinah to Badr
  - Whereas, there is no road from Riyadh to Badr



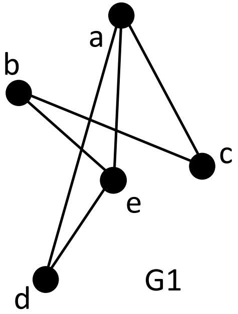
Definitions: Adjacency

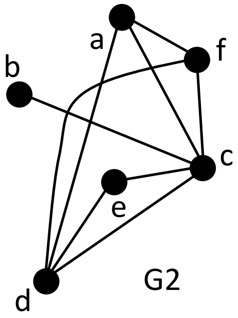
- An edge e=(u,v) **connects** two vertices u and v
- In that case, u and v are called **adjacent** to each other
- u and v are also called the **end points** of e
- e is also called **incident** to u and **incident** to v
- Adjacent vertices are also called **neighbors**
- **Example:** In the right-side graph G:
  - a and c are adjacent because of the edge (a, c)
  - c and e are not adjacent
  - d has four neighbors b, a, f, e
- **Exercise:** See a map of your country, draw the graph of road networks among major cities, find which cities are adjacent



Definitions: Degree

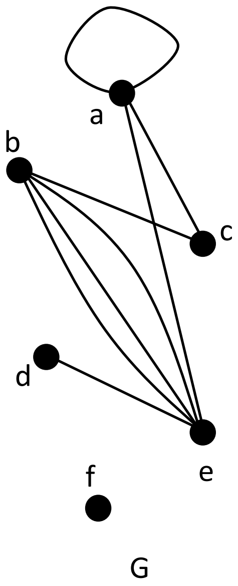
- **Degree** of a vertex x is the number of edges incident to x. It is written as **deg(x)**
- **Example:** In the right-side graph G1,
  - deg(a) = 3
  - deg(b) = 2
  - deg(c) = 2
  - deg(d) = 2
  - deg(e) = 3
- **Exercise:**
  - In this graph G2, find the degree of all vertices
  - Draw a graph with 4 vertices, each of odd degree
  - Draw a graph of six vertices each having degree 3





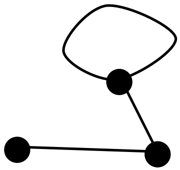
Definitions: Degree

- A **multi graph** has **multiple edges** among vertices
- In a multi graph, degree of a vertex counts all edges
- A vertex is called **isolated** if no edge is incident to it
- An isolated vertex has degree zero
- A **loop** is an edge if its two end points are the same
- A loop is counted twice as the degree of the vertex
- **Example:** The right-side graph G is a multi graph with
  - deg(a)=4, deg(b)=4, deg(c)=2, deg(d)=1, deg(e)=5, deg(f)=0
  - a has a loop and f is an isolated vertex
- **Exercise:** Draw a multi graph with two vertices and with loops such that each vertex has degree six

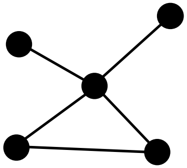


Handshaking Theorem

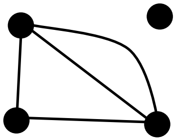
- Let us see a puzzle
- Look at these three graph G1, G2 and G3 in the right-side pictures
- They are arbitrarily taken
- For each of them, the sum of the degree is:
    - G1: 1+2+3 = 6
    - G2: 1+1+2+2+4 = 10
    - G3: 0+2+3+3 = 8
- Do you see any similarity among these sum values?
- Yes, they are all even!
- Is there any other similarities?
- Yes! Next slide …



G1



G2

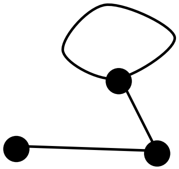


G3

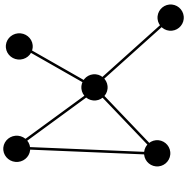
Handshaking Theorem

- For each of them, the sum of the degree is twice the number of edges:
  - G1: 1+2+3 = 6 = 2*3 (number of edges in G1 is 3)
  - G2: 1+1+2+2+4=10=2*5 (number of edges in G2 is 5)
  - G3: 0+2+3+3 = 8 = 2*4 (number of edges in G1 is 4)
- Is this true for any graph?
- Yes!
- This is called **handshaking theorem**:
  - For any graph, sum of degree of vertices are twice the number of edges
  - Mathematically, for a graph G = (V,E)

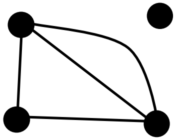
$$\sum_{\mathbf{v}\in\mathbf{V}} \mathbf{degree}(\mathbf{v}) = \mathbf{2}|\mathbf{E}|$$



G1



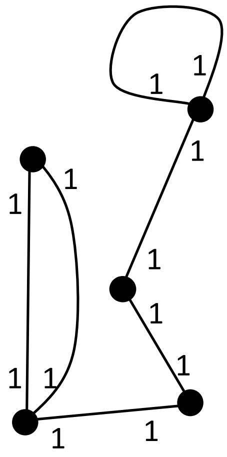
G2



G3

Proof of Handshaking Theorem

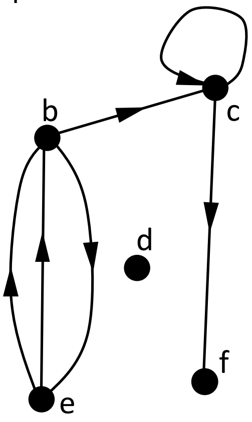
- Consider a graph G = (V,E) and an edge e = (u,v) of G
- e is counted as a degree two times for two vertices, once for u and once for v (even if u=v when e is a loop)
- So, e contributes 1 to the degree of u and 1 to the degree of v (see right-side picture)
- So, when the degree of all vertices are summed up (including the degree of u and v), e contributes 2 to that sum
- Similarly, every other edge contributes 2 to the sum
- Over all edges of E, total contribution is 2|E|
- There is no other contribution to the degree sum
- So, degree sum = 2 * number of edges



G

Directed Graphs

- In a **directed graph**, each edge e = (u,v) has a direction from u to v
- u is the **initial vertex** and v is the **terminal vertex**
- v is said to be **adjacent** to u
- There are two types of degree of a vertex in a directed graph: **indegree** (**indeg** for short) and **outdegree** (**outdeg** for short)
- **Indeg(v)** is the number of edges with terminal vertex v
- **Outdeg(v)** is the number of edges with initial vertex v
- **Example:** In the right-side figure, indeg(b) = indeg(c) = 2, indeg(e) = indeg(f) = 1, indeg(d) = 0, Outdeg(b) = outdeg(c) = outdeg(e) = 2, outdeg(d) = outdeg(f) = 0



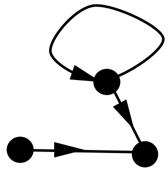
G

Handshaking Theorem

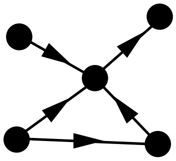
- Handshaking theorem holds for directed graphs too
- The theorem is expressed in terms of indegree and outdegree as follows:
  Sum of indegrees = sum of outdegrees = number of edges
- Mathematically, for a directed graph G = (V,E)

$$\sum_{\mathbf{v} \in \mathbf{V}} \mathbf{indeg}(\mathbf{v}) = \sum_{\mathbf{v} \in \mathbf{V}} \mathbf{outdeg}(\mathbf{v}) = |\mathbf{E}|$$

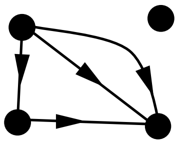
- For example, in G2 in the right-side picture
  - Sum of indeg = 0+0+1+1+3 = 5
  - Sum of outdeg = 0+1+1+1+2 = 5
  - Number of edges = 5
  - So, the theorem holds
- **Exercise:** Verify handshaking theorem for G1 and G3



G1



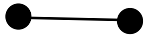
G2



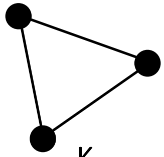
G3

Complete Graphs

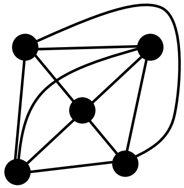
K_1



K_2



K_3

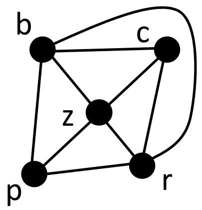


K_5

- A graph whose edges do not have any direction is called an **undirected graph**
- A graph without a loop or multiple edge is called **simple**
- A **complete graph** is a simple undirected graph where each pair of vertices has an edge
- In a complete graph, no more edges can be added without violating its simplicity
- A complete graph with $n \geq 1$ vertices is represented as K_n
- **Example:** Right-side pictures show K_1, K_2, K_3, K_5
- K_n has $C(n,2)=n(n-1)/2$ edges, as there are $C(n,2)$ ways to chose two vertex for an edge. Each vertex has degree $n-1$
- **Exercise:** Draw K_4 and K_6 and verify they have $C(n,2)$ edges

Walk, Path, Cycle

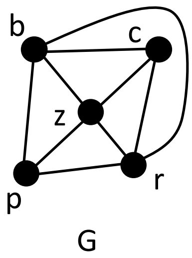
- A **walk** in a graph is a sequence of vertex so that the consecutive vertices in the sequence are adjacent
- A **path** is a walk where no two vertices are same, except may be the first and last vertices
- A **cycle** is a path when the first and last vertices are same
- **Example:** In the right-side picture,
  - (p, b, c, z, r, b, c, r) is a walk
  - (p, b, c, p, z, r, p) is not a walk, as (c,p) is not adjacent
  - (z, c, r, b) is a path
  - (z, c, r, b, c, r, z) is not a path as c and r are repeated
  - (b, z, c, b) and (b, c, z, p, r, b) are two cycles



G

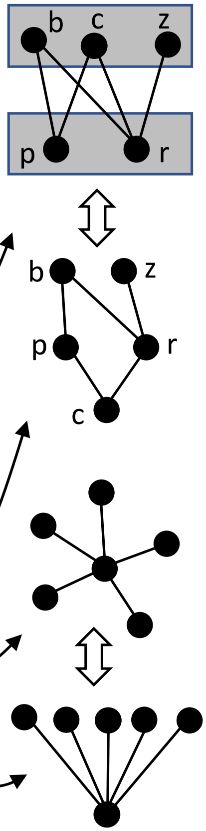
Walk, Path, Cycle

- **Length** of a walk, path or cycle is the number of edges
- Length of a walk can be infinite
- Whereas, length of paths and cycles are finite, because of avoiding vertex repetition
- **Example:** In the right-side graph G,
  - (b) is a walk as well as a path of length zero
  - (b, r) is a path of length one
  - (b, c, z, p, r, b) is a cycle of length five, and this is a maximum-length cycle in G
  - (b, c, b, c, b, c, …) is an infinite walk
- **Exercise:** Find all paths of length three in G
- **Exercise:** Find all cycles of length five in G



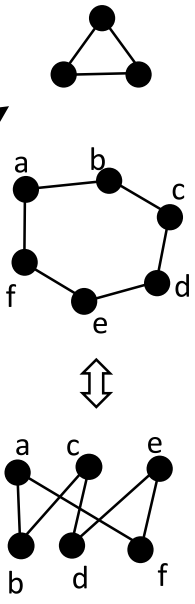
Bipartite Graphs

- A graph is **bipartite** if its vertices can be divided into two partitions such that there is no edge **within** a partition
- It means that all edges are **between** the two partitions
- **Example:** The top-right graph is a bipartite graph
    - One partition (shaded box) contains (b, c, z), and the other partition (shaded box) contains (p, r)
- Sometimes graphs are bipartite but are not drawn as bipartite. Such graphs can be redrawn as bipartite
- **Example:** This graph is same as the graph above it
- **Example:** This graph is a **star graph**, where a center vertex is connected to every other vertex, and there is no more edges. This graph is bipartite and is redrawn is here



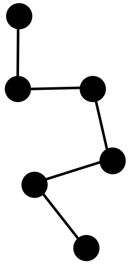
Bipartite Graphs

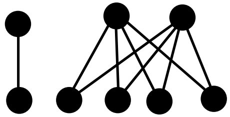
- **Example:** Odd length (3, 5, 7, …) cycles are not bipartite
  - Because its edges cannot be partitioned into two groups without having an edge within a partition
- **Example:** Drawing the cycle of length three as bipartite is not possible. Because, one partition will always have an edge within itself. See the top picture in the right-side
- **Exercise:** Try to draw cycles of length 5, 7, 9, 11, … as bipartite graphs. Why that would not be possible?
- **Example:** Even length (4, 6, 8, 10, …) cycles are bipartite
  - Because alternate vertices can be in same partition
- **Example:** A cycle of length 6 is redrawn as bipartite here
- **Exercise:** Draw cycles of length 8, 10, 12 as bipartite



Bipartite Graphs

- **Exercise:** Draw this path as bipartite
- **Exercise:** Explain why a path of length ≥ 1 which is not a cycle is bipartite (no matter whether the length of the path is even or odd)
- A bipartite graph is **complete** is every vertex in one partition is adjacent to every vertex in other partition
- A complete bipartite graph is represented as $K_{m,n}$
- m and n are the number of vertices in two partitions
- **Example:** $K_{1,1}$ and $K_{2,4}$ are drawn here
- Degree sum of $K_{m,n}$ is 2mn. Why? Think yourself!
- **Exercise:** Draw $K_{1,5}$, $K_{3,3}$, $K_{4,7}$. Verify that their degree sum is equal to 2mn

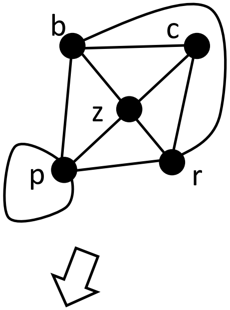




$K_{1,1}$ $K_{2,4}$

Graph Representation

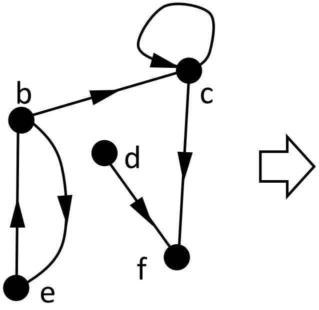
- So far, we have seen graphs by their pictures
- But graphs are efficiently represented to perform different operations and computations on them
- We shall see three useful representations of graphs:
  - Adjacency list
  - Adjacency matrix
  - Incidence matrix
- In an **adjacency list** of a graph, each vertex has a list of adjacent vertices (in any order)
- Adjacency list does not work for graphs with multiple edges
- **Example:** Right-side picture shows an example



Vertices	List of adjacent vertices
b	c, r, z, p
c	b, r, z
p	b, r, z, p
r	c, z, p, b
z	b, c, r, p

Adjacency List

- Adjacency lists work for directed graphs too
- **Example:** See below for a directed graph and its adjacent list



Vertices	List of adjacent vertices
b	c, e
c	c, f
d	f
e	b
f	

- **Exercise:** In the above example, reverse the direction of the edges of the graph and rewrite the adjacency list

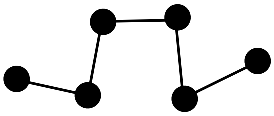
Adjacency list

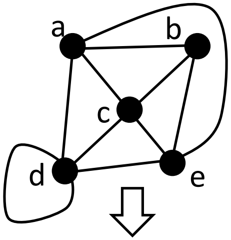
Adjacency matrix

Incidence matrix

Adjacency Matrix

- **Adjacency matrix** of a graph of n vertices is an $n \times n$ matrix M
- Each vertex is assigned to a unique row and column of M with same row and column number
- If (u,v) is an edge, then M[u,v] and M[v,u] is assigned to 1, otherwise they are assigned to 0
- **Example:** See the top-right corner
- **Exercise:** Draw the graph whose adjacency matrix is this matrix
- **Exercise**: Draw the adjacency matrix of the following graph





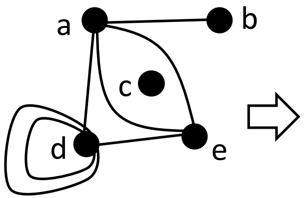
	a	b	c	d	e
a	0	1	1	1	1
b	1	0	1	0	1
c	1	1	0	1	1
d	1	0	1	1	1
e	1	1	1	1	0

M

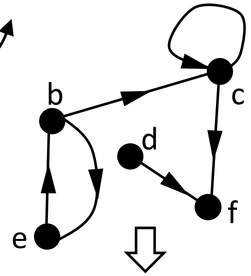
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	0	1	1	1
0	1	1	1	0

Adjacency Matrix

- For a multi graph, M[u,v] and M[v,u] get the value of the number of edges between u and v
- **Example:** A multi graph and its adjacency matrix is given in the top-right corner
- **Example:** For a directed graph, for an edge (u,v), only M[u,v] gets 1. See this example
- **Exercise:** Find an adjacency matrix in the previous example by reversing the direction of all edges
- **Exercise:** Why an adjacency matrix for an undirected graph is symmetric? That means, M[u,v] = M[v,u] for all u, v? Is it also true for a directed graph? (See the right-side examples)



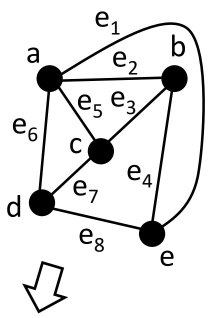
	a	b	c	d	e
a	0	1	0	1	2
b	1	0	0	0	0
c	0	0	0	0	0
d	1	0	0	2	1
e	2	0	0	1	0



	b	c	d	e	f
b	0	1	0	1	0
c	0	1	0	0	1
d	0	0	0	0	1
e	1	0	0	0	0
f	0	0	0	0	0

Incidence Matrix

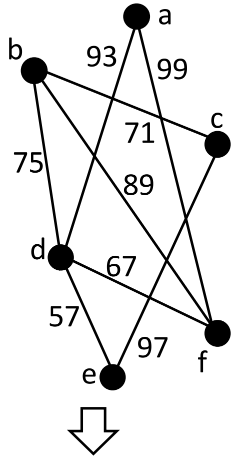
- **Incidence matrix** of a simple graph of n vertices and m edges is an n×m matrix M
- Each vertex is assigned to a unique row
- Each edge is assigned to a unique column
- For each edge $e_i=(u,v)$, $M[u,e_i] = M[v,e_i] = 1$
- All other cells of M are 0
- **Example:** See the right-side picture
- Each column in an incidence matrix has exactly two 1s
- **Exercise:** Incidence matrix for non-simple graphs can also be defined. But we do not see that here
- **Exercise:** Write incidence matrices for K_5 and $K_{3,4}$



	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8
a	1	1	0	0	1	1	0	0
b	0	1	1	1	0	0	0	0
c	0	0	1	0	1	0	1	0
d	0	0	0	0	0	1	1	1
e	1	0	0	1	0	0	0	1

Weighted Graphs

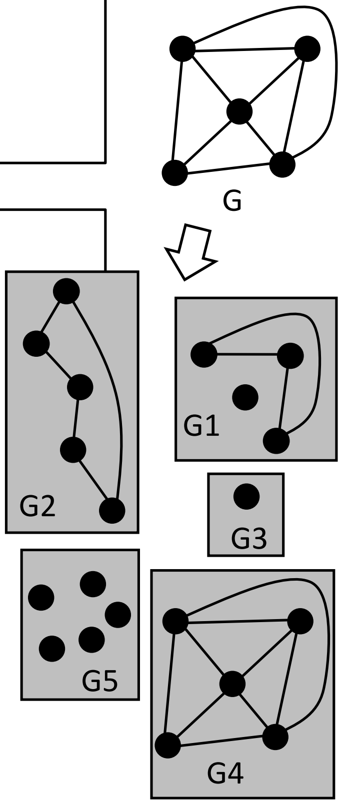
- A graph is called **weighted** when its edges have weights
- They can be represented by adjacency matrix
- If (u,v) is an edge, then M[u,v] and M[v,u] contains the weight of the edge (u,v)
- **Example:** See the right-side example
- Weight of an edge can be negative
- For example, in a graph of road network, a negative weight means you get some incentives if you use that road
- Weighted graphs arise in many applications, such as in shortest path computation



	a	b	c	d	e	f
a	0	0	0	93	0	99
b	0	0	71	75	0	89
c	0	71	0	0	97	0
d	93	75	0	0	57	67
e	0	0	97	57	0	0
f	99	89	0	67	0	0

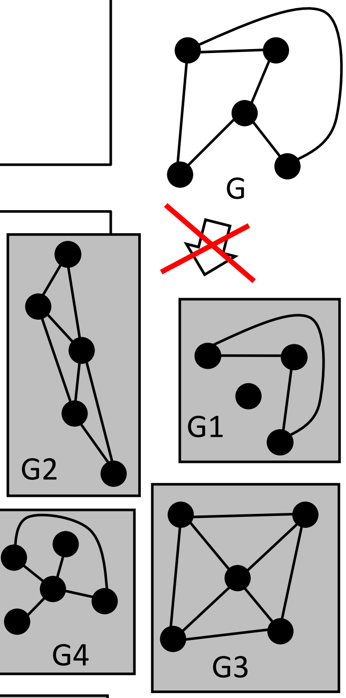
Subgraphs

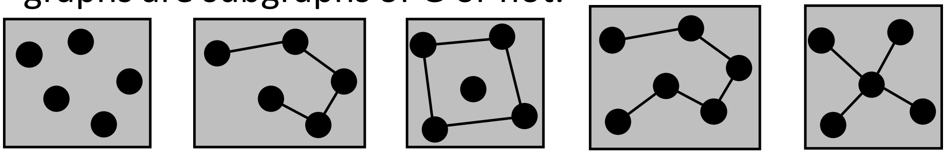
- A graph G’ is a **subgraph** of another graph G if the vertex and edge sets of G’ are subsets of the vertex and edge sets of G
- In another way to say, if G’ is available within G
- **Example:** In the right-side picture, G1, G2, G3, G4 and G5 are some subgraphs of G
  - A graph is a subgraph of itself, such as G4
  - G2 does not look like anything within G, but it is a cycle of length 5, and G has many cycles of length five (find yourself one such cycle in G)
  - G5 is a subgraph of G with all vertices of G but with no edge from G



Subgraphs

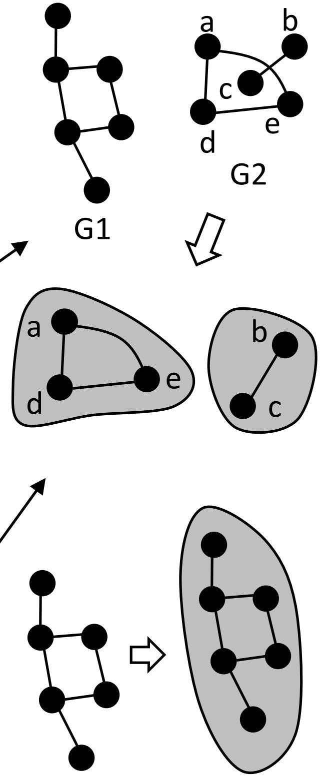
- **Example:** In the right-side picture, G1, G2, G3, and G4 are not subgraphs of G. Because,
  - G1 has a cycle of length 3, but G does not have any cycle of length 3 (verify yourself)
  - G2 has seven edges, but G has six edges
  - G3 is K_4, but G does not have any K_4
  - G4 has a vertex of degree 4, but G does not have any vertex with degree 4
- **Exercise:** Explain whether the following five graphs are subgraphs of G or not.





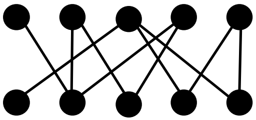
Connected Graphs

- A graph is **connected** if any two vertices has a path
- **Example:** In the top-right corner, G1 is connected, but G2 is not because many pairs of vertices have no path, such as there is no path from a to c
- **Connected components** of a graph G are the **maximal connected** subgraphs of G
- A maximal connected subgraph of G means no more vertex or edge from G can be added to the subgraph so that it remains connected
- **Example:** See two connected components of G2
- **Example:** A connected graph has itself as the only component. See here

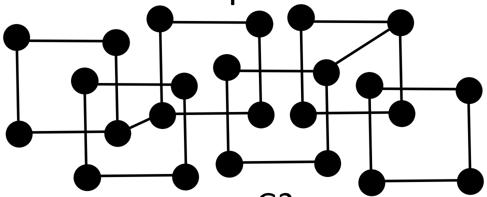


Connected Graphs

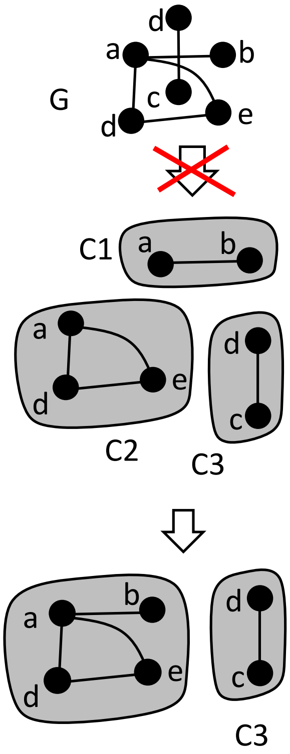
- **Example:** In the right-side example,
    - C3 is a connected component of G
    - C1 and C2 are not connected components of G
    - Because, C1 and C2 can be made bigger by adding more vertex and edge. For example, they can be merged together to get a bigger connected subgraph of G. This violates the condition of "maximal connected". See here
- **Exercise:** Find the connected components of the



G1

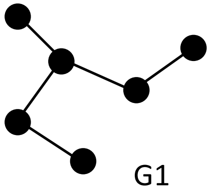


G2

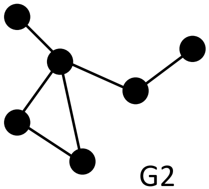


Trees

- A **tree** is a simple connected graph with no cycle
- **Example:** In the right-side figures:
  - G1 is a tree
  - G2 is not a tree because there is a cycle
  - G3 is a tree with only one vertex and no edge
  - G4 is not a tree, as it is not connected. However, it has two connected components, and each of them is a tree
- A disconnected graph whose connected components are trees is called a **forest**. For example, G4 is a forest
- **Exercise:** Draw a tree with 10 vertices and 9 edges
- **Exercise:** Draw a forest with 10 vertices and 7 edges

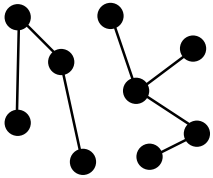


G1



G2

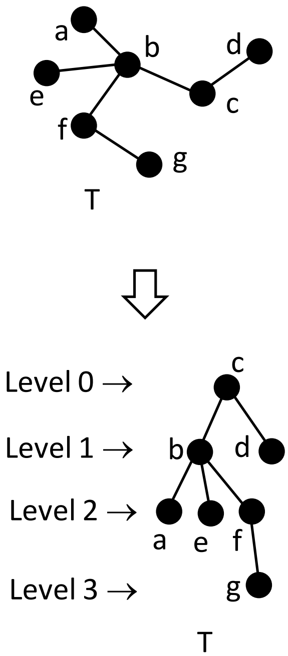
G3



G4

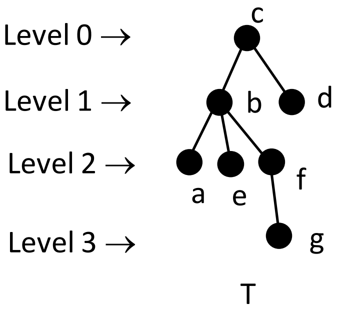
Rooted Tree

- A tree is called **rooted tree** if a specific vertex is assigned as a **root.** Other vertices are considered as gradually away from the root
- Rooted tree is better understood when it is drawn by **levels**
- Root is at the first level, which is level 0. Neighbors of the root are at the next level 1. Remaining neighbors of vertices of level 1 are at level 2. Remaining neighbors of level 2 vertices are in level 3. So on…
- **Example:** In the right-side picture T is redrawn as a rooted tree with root c. The levels are also shown



Height of a Tree

- **Height** of a rooted tree is the maximum level
- **Example:** Height of T in the previous example (again given below) is 3



Tree

Rooted tree

Root

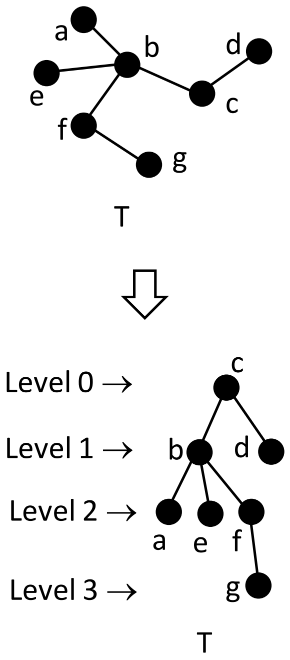
Level

Height

- **Exercise:** Redraw T with f as root. What is the height?
- **Exercise:** Draw a tree of 7 nodes of height (i) 1, (ii) 6

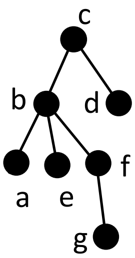
Parent, Child, Leaf, Internal Node

- In a rooted tree, a node v, which is not the root, has only one neighbor in the level above. It is called the **parent** of v. Root has no parent
- **Children** of v are the neighbors in one level below
- If v has no child, then v is called a **leaf**
- If v has child, then it is called an **internal** node
- **Example:** In the right-side picture,{a,e,f} are children of b. {c, b, f} are internal nodes and {a, e, g, d} are the leaves
- **Exercise:** Redraw T with a as root. How many internal nodes and leaves are there?
- **Exercise:** Redraw T with maximum possible height



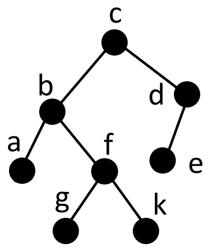
Siblings, Ancestors, Descendants

- In a rooted tree, nodes with same parent are called **siblings**
- A node v, other than the root, has a path from v to root. **Ancestors** of v are all the nodes that appear in that path
- Root is an ancestor of all remaining nodes in the tree
- **Descendants** of v are all nodes which have v as an ancestor
- Thus leaves have no descendants
- **Example:** In the right-side picture,
  - {a, e, f} are siblings
  - {c, b, f} are ancestors of g
  - {a, e, f, g} are the descendants of b
- **Exercise:** Find ancestors of a, e and d. Find descents of c, f and d

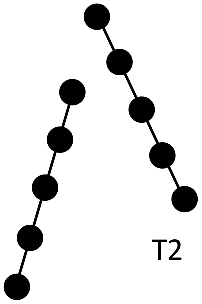


Binary Tree

- A rooted tree is called **ordered** if its children are ordered (with labels or identification) from left to right
- An ordered tree is called **binary** if its each internal node has at most two children, **left child** and **right child**
- **Example:** In the top-right corner, T is a binary tree, with:
    - Left child of b is a and right child of b is f
    - e is the left child of d
- **Example:** Some special binary trees:
    - T1 has no right child and T2 have no left child
- **Exercise:** What are the height T1 and T2?
- **Exercise:** What would be the height T1 and T2 if they have n nodes each?



T

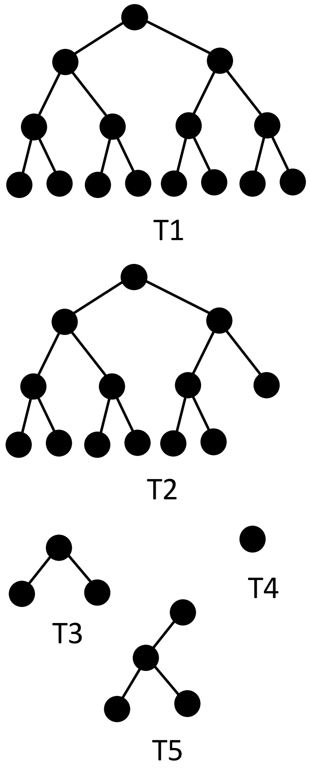


T2

T1

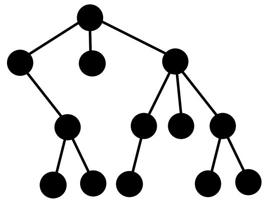
Complete Binary Tree

- A binary tree is **complete** if it contains maximum possible nodes in every level from first to last
- In another way, a complete binary tree has all its leaves in the last level and all internal nodes have two children
- **Example:** In the right-side pictures,
  - T1, T3, T4 are complete binary trees
  - T2 is not a complete binary tree, because one leaf is not in the last level
- **Exercise:** Why T5 is not complete?
- **Exercise:** Draw a complete binary tree with 31 nodes. Find its height and number of leaves

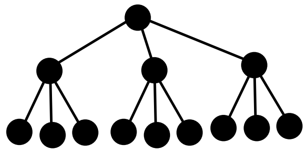


m-ary tree

- Binary tree can be generalized to **m-ary tree**
- An m-ary tree is an ordered rooted tree where each node has at most m children
- **Complete** m-ary tree, and height and levels of an m-ary tree are defined similar to binary tree
- **Example:** In the right-side pictures,
  - T1 is a 3-ary tree (also called **ternary** tree) of height three
  - T2 is a complete ternary tree
- **Exercise:** Draw a complete ternary tree of height three. How many nodes are there?
- **Exercise:** Draw a complete 4-ary tree of height 2



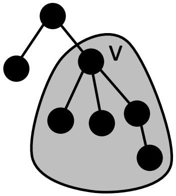
T1

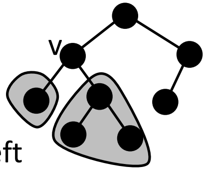


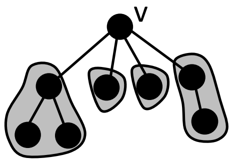
T2

Subtrees

- The tree rooted at an internal node of a tree T is called a **subtree** of T
- Example: In the top-right corner the shaded area represents a subtree rooted at v
- For a binary tree, for an internal node v, subtree rooted at the left child is called the **left subtree** of v and the subtree rooted at the right child is called the **right subtree** of v
- For an m-ary tree, for an internal node v, there are at most m subtrees rooted at the children of v
- Example: In this picture there are four subtrees rooted at the four children of v

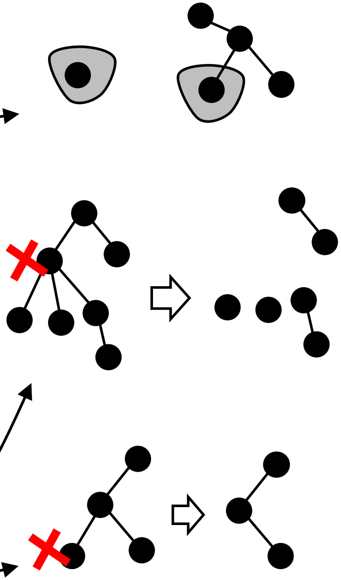






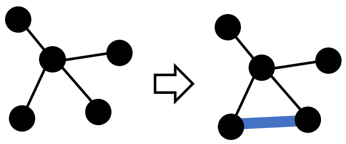
Properties of Tree

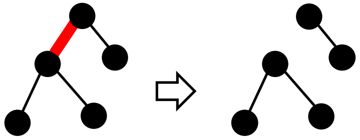
- There are many interesting properties of trees
- Any tree has at least one leaf (see shaded nodes in the right-side picture)
- If a tree has one node, then that node is the only leaf and there is no internal node
- **Removing a node** v from a tree removes v and its adjacent edges
- Removing an internal node v from a tree divides the tree into smaller trees
- In fact, it divided the tree into deg(v) smaller trees (see the right-side picture)
- Removing a leaf makes the tree a smaller tree

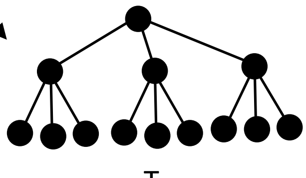


Properties of Tree

- **Adding an edge** between any two nodes of a tree makes a cycle, and the tree does not remain a tree
- **Example:** See the blue color edge here
- **Deleting an edge** (without deleting its two endpoints) divides the tree into two trees
- **Example:** See the red color edge in here
- **Exercise:** In the right-side tree T:
  - Delete minimum possible nodes to make the remaining nodes all separated
  - Add an edge to T to create a cycle of maximum possible length

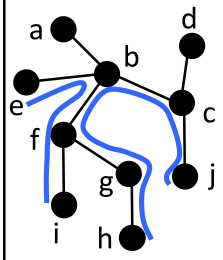






Tree: Any Two Nodes Have a Unique Path

- We now see some tree properties which need proofs
- **Theorem:** In a tree T, there is a **unique** path between any two vertices u and v
- Let us see some examples first (see right-side picture)
- Two unique paths between h and j is (h, g, f, b, c, j) and between e and i is (e, b, f, i) are shown in blue color
- **Proof:**
  - T is a connected graph, and by the definition of a connected graph, there is a path (say P1) from u to v
  - We prove that P1 is unique by proof by contradiction
  - For contradiction, assume that P1 is not unique
  - (Continued to the next slide …)

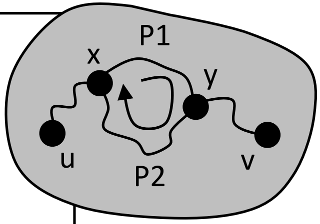


T

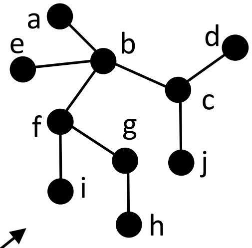
Tree: Any Two Nodes Have a Unique Path

- (Continued from the previous slide …)
- That means, there is another path (say P2) from u to v (see the right-side picture)
- Since both P1 and P2 start at u and end at v, and since p1≠P2, there is a vertex where P1 and P2 separate and then there is another vertex where this separation ends (P1 and P2 merge)
- Let x and y be those two vertices
- Then, the vertices of P1 from x to y and the vertices of P2 from y to x together make a cycle
- This contradicts that T is a tree and has no cycle

- **Exercise:** Find unique paths for all pair of vertices in T1



T

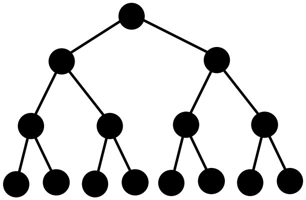


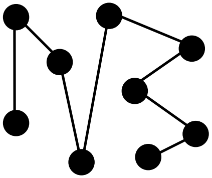
T1

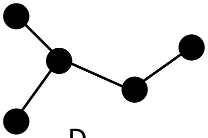
Tree of n Nodes Has n-1 Edges

- **Theorem:** A tree with n nodes has n-1 edges
- Before we prove this theorem, let us see some examples in the right-side pictures
  - A has 1 node and 0 edge
  - B has 15 nodes and 14 edges
  - C has 9 nodes and 8 edges
  - D has 5 nodes and 4 edges
- **Proof:** We use proof by induction
  - Let T_n denotes a tree with n nodes
  - **Base case:** A tree with n=1 node is this and has n-1 = 1-1 = 0 edge. So the base case is proved
  - (Continued to the next slide …)

A

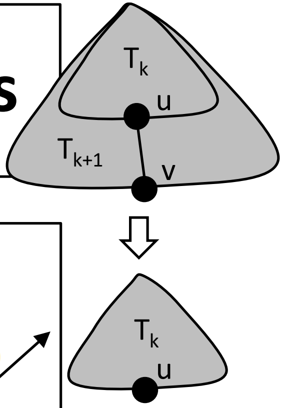


B


C

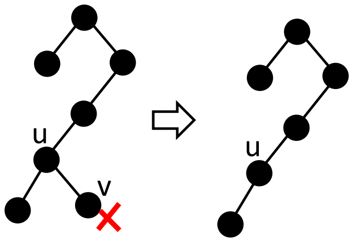

D

T_1


Tree of n Nodes Has n-1 Edges

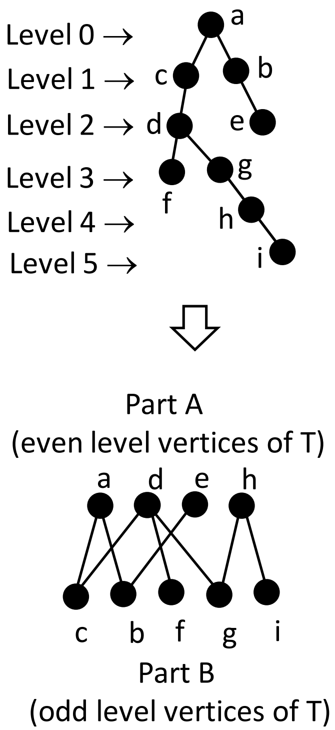


- (Continued from the previous slide…)
- **Induction step:** Assume T_k has k-1 edges (IHT)
  - Take T_{k+1}. We shall prove that T_{k+1} has k edges
  - Let v be a leaf of T_{k+1} and let u be its parent
  - Remove v and the edge (u,v), but keep u
  - This makes a smaller tree T_k with k nodes
  - By IHT, T_k has k-1 edges
  - So, T_{k+1} has (k-1) edges from T_k and the deleted edge (u,v)
  - So, total edge of T_{k+1} = (k-1)+1 = k
- **Example:** Here the tree has 7 vertices and 6 edges. Deleting v makes it a tree with 6 vertices and 5 edges



All Trees are Bipartite Graphs

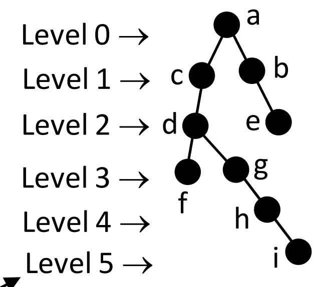
- **Theorem:** All trees are bipartite graphs
- **Proof:** We show that vertices of a tree T can be partitioned into two parts A and B such that all edges are between A and B (see right side)
  - Draw T as a rooted tree by taking a vertex, say v, as the root
  - Convert T to a bipartite graph as follows
  - Put the vertices of the even levels (level 0, 2, 4, …) in part A
  - Put the vertices of the odd levels (level 1, 3, 5, …) in part B
  - Then put the edges of T (continue …)

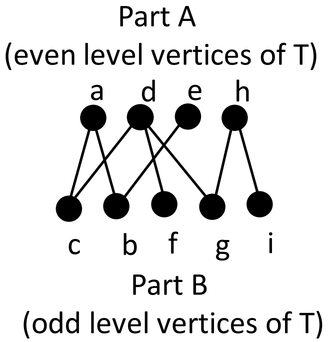


All Trees are Bipartite Graphs

- (Continued from the previous slide …)
- Every edge in T has one vertex in odd level and another vertex in even level (see here)
- No edge from odd level to odd level (part A to part A). Similarly, no edge from even level to even level (part B to part B)
- So, it is a bipartite graph (proof ends here)

- **Exercise:** Draw a complete binary tree of height five and then redraw it as a bipartite graph
- **Exercise:** Show by a counterexample that the opposite of the above theorem is not true: Not every bipartite graph is a tree





Leaves and Internal Nodes of Complete Binary Tree

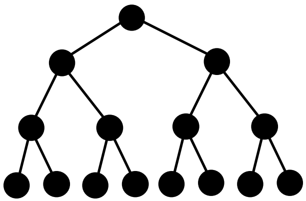
- **Theorem:** A complete binary tree T of height h has 2^h leaves and 2^h-1 internal nodes
- Before the proof, we see some examples
- In the following graph:
  - h = 3
  - Number of leaves is 8 = 2^3
  - Number of internal nodes is 7 = 2^3-1

Height = h

Leaves = 2^h

Internal nodes = 2^h-1

Total nodes = $2^{h+1}-1$



← Level 0, nodes 2^0

← Level 1, nodes 2^1

← Level 2, nodes 2^2

← Level 3, nodes 2^3

T

Leaves and Internal Nodes of Complete Binary Tree

- **Proof:** See the picture in the previous slide
  - The levels of T are 0, 1, 2, 3, 4, …, h-1, h
  - Maximum number of nodes in level 0 is 1 // the root
  - In subsequent levels, number of nodes in level l is the all possible children of the nodes in level l-1
  - Because T is a complete binary tree, every internal node has exactly two children
  - So, number of nodes in level l is twice the number of nodes in level l-1
  - So, number of nodes in level 1 = 2*1 = 2 = 2^1
  - Number of nodes in level 2 is $2*2^1 = 2^2$
  - So on … (Continued to the next slide …)

Level 0 nodes = 2^0

Level 1 nodes = 2^1

Level 2 nodes = 2^2

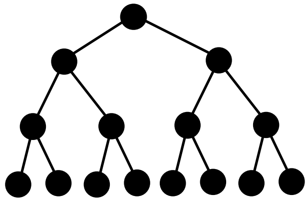
…

Level h nodes = 2^h

Leaves and Internal Nodes of Complete Binary Tree

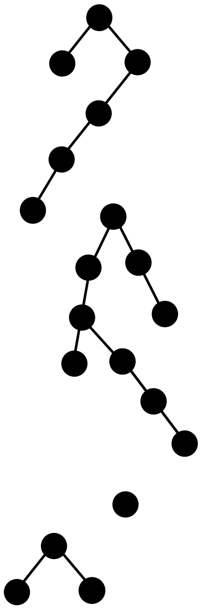
- (Continued from the previous slide …)
- In this way, number of nodes in level h-1 = 2^{h-1}
- Finally, number of nodes in level h is 2^h
- Among all these nodes, level h nodes are leaves, and all previous level nodes are internal nodes (see the picture again below)
- So, total leaves: 2^h
- Total internal nodes: $1+2^1+2^2+2^3+\ldots+2^{h-1}$

  $= \frac{2^{(h-1)+1}-1}{2-1} = 2^h-1$
- **Exercise:** Verify this theorem for trees with h = 0, 1, 2, 4, 5, 6, …



Binary Tree of Height h Has At Most 2^{h+1} -1 Nodes

- Previous theorem has some interesting consequences
- Consequence of a theorem is written as **corollary**
- **Corollary:** A binary tree of height h has at most 2^{h+1} -1 nodes
- **Proof:**
  - A binary tree has maximum possible nodes when it is complete, otherwise it has less number of nodes
  - From the previous theorem, a complete binary tree has: internal nodes + leaves = $2^h-1+2^h = 2*2^h-1 = 2^{h+1}-1$ nodes
  - So, maximum possible nodes in a tree is $2^{h+1}-1$
- **Exercise:** Verify this corollary for the right-side trees



Complete Binary Tree of n Nodes Has Height $\log_2(n+1)+1$

- **Exercise:** Write and prove the previous theorem for 3-ary trees
- **Corollary:** A complete binary tree of n nodes has height $\log_2(n+1)-1$
- **Proof:** By the previous corollary, $n = 2^{h+1}-1$
  - So, $2^{h+1} = n+1$, which gives $h+1 = \log_2(n+1)$ by taking log
  - So, $h = \log_2(n+1)-1$
- **Corollary:** A complete binary tree of l leaves has height $\log_2 l$
- **Proof:** By the previous theorem, $l = 2^h$. So, $h = \log_2 l$
- **Exercise:** Find the height of a complete binary tree in terms of number of internal nodes
- **Exercise:** Draw the complete binary trees of height 0, 1, 2, 3, 4, 5, 6 and verify the above corollaries

Remember:
$a^x = n$
$x = \log_a n$

References

1. Discrete Mathematics and Its Applications, by Kenneth Rosen, McGraw-Hill Education, 8th Edition, 2019
2. Discrete Mathematics in Computer Science, by Donald F. Stanat and David F. McAllister, Pearson, 1977
3. Discrete Mathematics: An Open Introduction, by Oscar Levin, 3rd Ed., 2015
4. Mathematics for Computer Scientists, by Gareth J. Janacek, Bookboon, 2009
5. Discrete Mathematics for Computer Scientists, by Clifford Stein, Robert L. Drysdale, and Kenneth Bogart, Addison-Wesley, 2011
6. Mathematics for Computer Science, by Eric Lehman, F. Thomson Leighton, and Albert R. Meyer, 2018
7. Concrete Mathematics, Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, Addison-Wesley, 2nd Edition, 1994
8. Webpage of this slidebook: https://sites.google.com/view/slidebook/home/discrete-mathematics

Acknowledgement

The author of this slidebook is grateful to many entities from many directions. The motivation behind writing this slidebook came while the author was teaching this course in Taibah University. During his teaching, it was realized that the students are reluctant to read the textbooks. At the same time, the traditional slides are not always having enough extra explanations and examples on the topics. Therefore, the author realized that something in between textbooks and traditional slides is necessary, and that made it possible to come up with this slidebook.

This slidebook has been followed by many respected colleagues in teaching in Taibah University and Al Jouf University. Several respected colleagues pointed out mistakes and typos as they found out during their teaching. The author would like to appreciatively mention their names as follows: Abdel Hamid Emara, Abdul Ahad Siddiqui, Hossam Diab, Mohammad Azad, Nada Salama, Omar Alhazmi, Rana Tarabishi, Redwan Nour, and Salwa AlSharif. May Almighty Allah give them the best reward for their good deeds.

The typesetting of this slidebook has been done with MS PowerPoint, which has been provided by the Taibah University.

About the Author

Masud Hasan completed his BSc. Engg. and MSc. Engg. in Computer Science and Engineering from Bangladesh University of Engineering and Technology (BUET) in 1998 and 2001, and PhD in Computer Science from the University of Waterloo, Canada in 2005. Since 2013, he is a professor in the College of Computer Science and Engineering in Taibah University, Madinah Al Munawara, Saudi Arabia. Before that, he had been a faculty member in the Department of Computer Science and Engineering in BUET since 1998 to 2013. In addition, he has experience in teaching at several other universities in Bangladesh as a guest instructor. His research interest includes Algorithms, Computational Geometry, and Theoretical Computer Science. He has jointly published more than seventy research articles in peer reviewed international journals and conference proceedings. He has served as a program committee member in some conferences and has worked as a reviewer for numerous peer reviewed conference proceedings and journals. He has given invited talks at some universities, including one in IUPUI, USA, and has given talks in several conferences and seminars, including one in Fields Institute, Toronto, Canada. In 2011 he was awarded a Young Scientist Award (Gold Medal) jointly by TWAS (Italy) and Bangladesh Academy of Sciences. Further information about him can be found in his homepage: https://sites.google.com/view/masudhasan