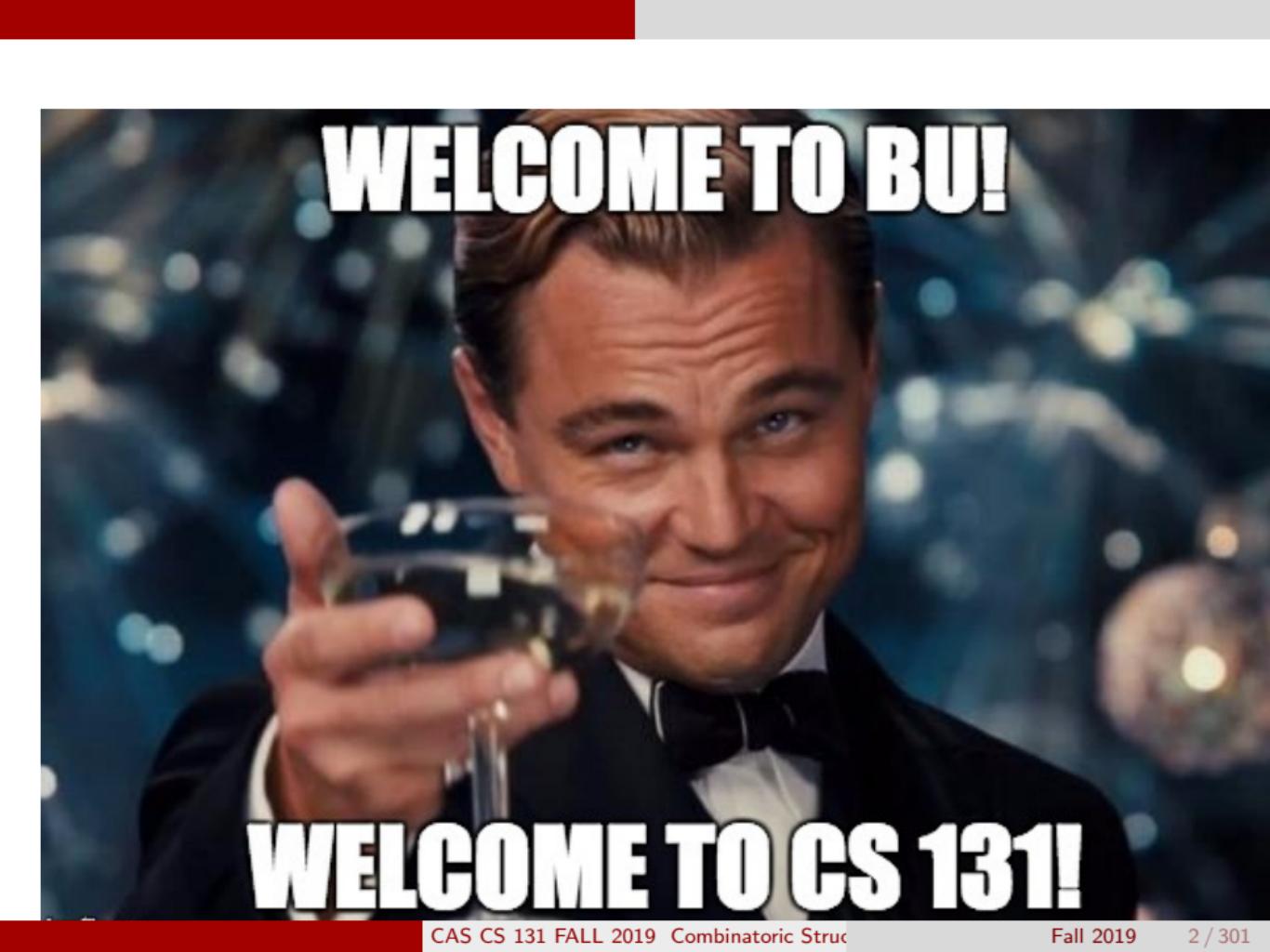


CAS CS 131  
FALL 2019  
Combinatoric Structures

Charalampos (Babis) Tsourakakis  
CS 131

Fall 2019



# WELCOME TO BU!

# WELCOME TO CS 131!

# Instructor – Professor



Babis Tsourakakis  
[tsourakakis.com](http://tsourakakis.com)

# Instructors – Teaching Fellows



Tolik  
Zinovyev  
tolik@bu.edu



Arsenii  
Mustafin  
aam@bu.edu



Hassan Saadi  
hsaadi13@bu.edu

**Great team of Teaching Fellows!**

# Discussion Labs

- On each Wednesday you will participate in a discussion lab.
- The TFs will hand out a set of problems related to the lectures, and you will solve it.
- Make sure you participate, ask your questions, share your ideas.
  - Participation is required
- Please attend the lab you have been assigned to.

# Class Web page

<https://tsourakakis.com/cs131-fall2019/>

The screenshot shows a Mac OS X desktop with a Chrome browser window open. The address bar displays the URL <https://tsourakakis.com/cs131-fall2019/>. The browser's top menu bar includes File, Edit, View, History, Bookmarks, People, Window, Help, and several system status icons. Below the address bar is a toolbar with various icons. The main content area of the browser shows the homepage of the CS131 Combinatorial Structures website. The page has a dark header with navigation links: HOME PAGE, PROJECTS, CV, GITHUB, PUBLICATIONS, PRESENTATIONS, TEACHING, GROUP, BLOG, MY LEARNING, and CONTACT. A horizontal line separates the header from the main content. The main content area features a section titled "CS131 COMBINATORIC STUCTURES — FALL 2019" and "Official Course description". It contains text about the course's focus on mathematical foundations and logical arguments. Below this is a "Info" section with links to the instructor's profile, Piazza page, and semester information. To the right of the main content, there is a "FOLLOW ME ON TWITTER" sidebar with a "Tweets by @Tsourakakis" feed. The feed shows a tweet from "Babis Tsourakakis Retweeted" (@MIT\_CSAIL) about the MIT supercomputer. Below the sidebar is a small image of server racks. At the bottom of the browser window, there is a "Waiting for syndication.twitter.com" message and a toolbar with various application icons.

# Piazza

<https://piazza.com/class/fall2019/cs131>

The screenshot shows a web browser window for the Piazza platform. The URL in the address bar is <https://piazza.com/class/fall2019/cs131>. The browser's toolbar includes icons for Home, History, Bookmarks, People, Window, Help, and several tabs related to the class. Below the toolbar is a bookmarks bar with links to various university resources like CS131 Combinatoric Structures, Algorithmic Data Structures, and timeseries. The main content area displays the course information for "CS 131: Combinatoric Structures" at Boston University - Fall 2019. The course description states: "Representation, analysis, techniques, and principles for manipulation of basic combinatorial data structures used in computer science. Rigorous reasoning is emphasized. (Counts as a Background Course for the CS concentration)." The general information section includes a link to the class website: <https://tsourakakis.com/cs131-fall2019/>. The announcements section has one entry: "Welcome to CS131" posted on 8/13/19 at 6:52 PM. The announcement text reads: "Hi All, and welcome to CS131! The class web site is up, and contains a tentative schedule for the class, and some important information. For convenience, the link is <https://tsourakakis.com/cs131-fall2019/>. First day of classes is Tuesday September 3rd. Looking forward to meeting you in a few weeks. Best wishes for the rest of your summer!" At the bottom of the page is a footer with the text "Copyright © 2017 Piazza Technologies, Inc. All Rights Reserved." and a toolbar with various application icons.

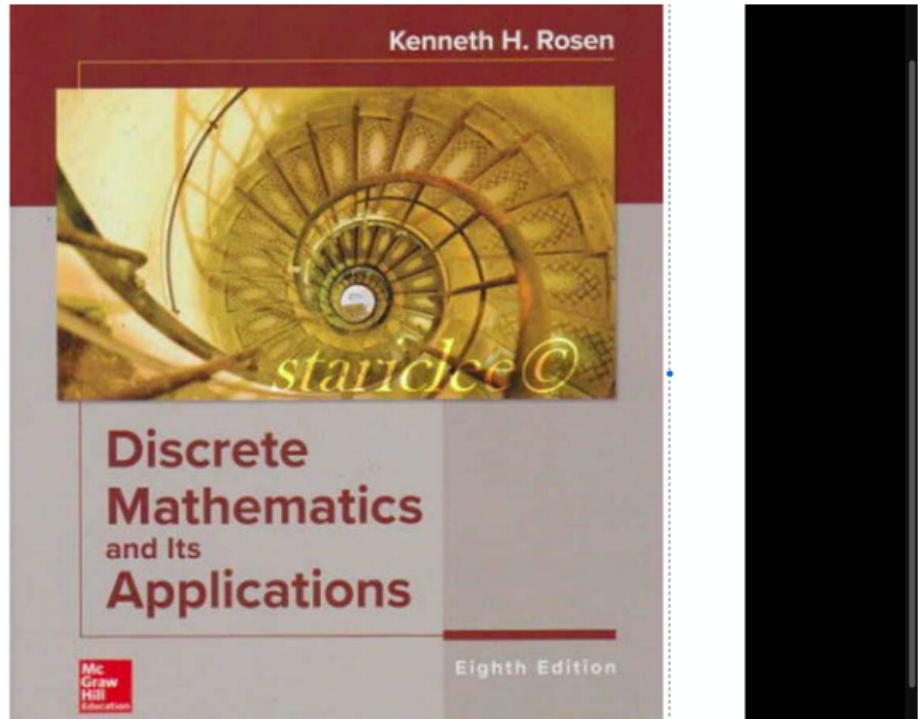
# Grading and Attendance

The course grade will break down as follows:

- Problem sets: 25%
- Two midterms: 40% (20+20%)
- Final exam: 30%
- Lab attendance and participation in lab, lecture, Piazza: 5%

Fun class but also **hard work!**

# Textbook



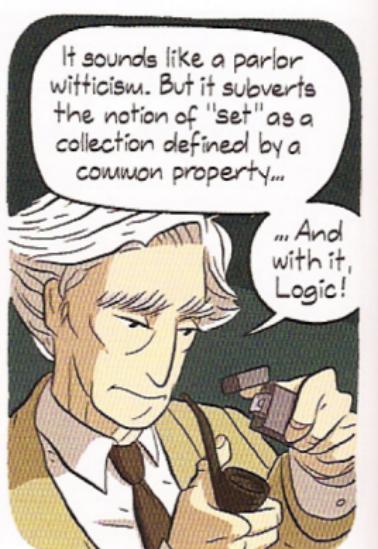
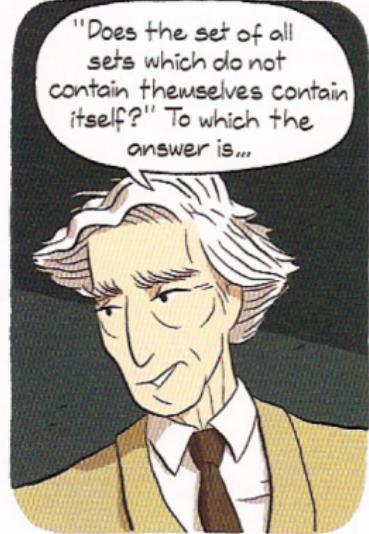
# Topics

CS 131 covers **fundamental** topics in Computer Science. The main goal is to introduce you to important proof techniques.

- ① Logic and proof
- ② Induction
- ③ Recursive algorithms, and recurrences
- ④ Number theory
- ⑤ Pigeonhole principle (aka box principle)
- ⑥ Basics of counting
- ⑦ Graph theory

You are building foundations in this class!

# These are Fun Topics ...



# Who is this guy?



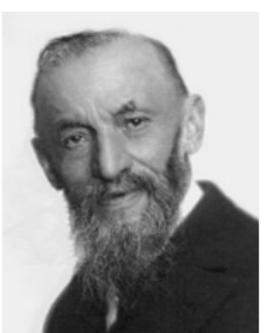
Bertrand Russell

*The whole problem with the world is that fools and fanatics are always so certain of themselves, but wiser people so full of doubts.*

that have lead to a lot of frustration too!



# Who are these guys?



**Giuseppe Peano** and **David Hilbert**

- Hilbert's problems are twenty-three problems in mathematics published by German mathematician David Hilbert in 1900. The problems were all unsolved at the time, and several of them were very influential for 20th-century mathematics.

# Paradox using inductive logic



## Sorites paradox

- A person with 0 hairs is bald.
- For any number  $n$ , if a person with  $n$  hairs is bald, then a person with  $n + 1$  hairs is also bald.

Therefore, we are all bald!

# Academic Conduct

- Academic standards and the code of academic conduct are taken very seriously by our university
- Bottom line:
  - Healthy collaboration for doing homeworks, is fine, and actually encouraged. You can learn from each other.
  - No collaboration during exams.
  - Do not cheat! Besides being a dishonest act, it may also have severe consequences on your academic trajectory.

# Office hours

- Prof. Tsourakakis: TR 8.30-10.00
- Arsenii: M 9:00-10.30, F 15.30:17.30
- Hassan: T 17:15 18:15, R 17:15 19:15
- Tolik: W 17:35 18:35, F 13:30 15:30

**This week:** Space 135 (lounge) at MCS.

# Lecture 1 (9/3)

# Propositional logic

We start our study of mathematical reasoning with **deductive reasoning**. Let's see few examples:

- ① It will either rain or snow tomorrow. Its too warm for snow. Therefore, it will rain.
  
- ② Either the butler is guilty or the maid is guilty. Either the maid is guilty or the cook is guilty. Therefore, either the butler is guilty or the cook is guilty.

# Logical form – Premises and conclusion

- ① It will either rain or snow tomorrow. Its too warm for snow.  
Therefore, it will rain.
- ② Either the butler is guilty or the maid is guilty. Either the maid is guilty or the cook is guilty. Therefore, either the butler is guilty or the cook is guilty.

**Valid argument:** The premises cannot all be true without the conclusion being true as well.

**Argument 1** is valid.

**Argument 2** is invalid (i.e., were the maid guilty, then both premises are true, but the conclusion is false).

# Propositional logic

By replacing statements by letters, we can study the logical structure of the arguments. These are called *propositions*.

## Logical form of valid arguments 1.

Premises:  $P$  or  $Q$ . Not  $Q$

Conclusion: Therefore  $P$ .

## Logical form of valid invalid argument 2.

Premises:  $P$  or  $Q$ .  $Q$  or  $S$

Conclusion: Therefore  $P$  or  $S$ .

# Propositional logic

- A proposition is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both.

Which ones are propositions?

- Boston is the capital of MA (**yes**)
- $1 + 1 = 2$  (**yes**)
- $x + 1 = 2$  (**no**)
- Read this carefully (**no**)
- Propositions are represented by propositional variables (or sentential variables), e.g.,  $P$  = it will rain.
- The value of a proposition is either true (T) or false (F)
- Compound propositions are composed by propositions using logical operators (e.g.,  $P$  **and**  $Q$ )

# Propositional logic

Symbol	Meaning
$\vee$	or
$\wedge$	and
$\neg$	not

- $P \vee Q$  stands for  $P$  **or**  $Q$
- $P \wedge Q$  stands for  $P$  **and**  $Q$
- $\neg P$  stands for **not**  $P$

**Important remark:** Logical **and**, **or**, **not** do not correspond to all uses of the words *and*, *or*, *not* in English.

- E.g., Tolik and Arsenii are friends (Here the word *and* does not connect two propositions as the logical **and**)
- Or in English can be used both as disjunctive or exclusive. In logic **or** is disjunctive, and we also have **xor** for exclusive or.

# Translating English sentences

Let's translate some English sentences into logic.

*Either Tolik went to the coffee shop, or Hassan ate noodles.*

- ① We introduce the necessary propositional variables
  - $P$  = Tolik went to the coffee shop
  - $Q$  = Hassan ate noodles.
- ② Now we express our compound statement using logical **or**
  - Our compound statement is  $P \vee Q$

# Translating English sentences

*Either Bill is at work and Jane isn't, or Jane is at work and Bill isn't.*

- ① We introduce the necessary propositional variables

- $B = \text{Bill is at work}$
- $J = \text{Jane is at work}$

- ② Now we express our compound statement step by step

- *Either Bill is at work and Jane isn't* translates to  $B \wedge \neg J$
- *Either Bill is not at work and Jane is* translates to  $\neg B \wedge J$
- The whole proposition is therefore

$$(B \wedge \neg J) \vee (\neg B \wedge J).$$

# Precedence of logical operators

Consider the proposition  $\neg p \wedge q$ . How should we interpret it?

- As  $\neg(p \wedge q)$ ...
- or  $(\neg p) \wedge q$ ?

Precedence of operators is as follows.

- ①  $\neg$
- ②  $\wedge$
- ③  $\vee$

Therefore, the correct way to interpret it as  $(\neg p) \wedge q$ .

**Remark:** For now, we will be using parentheses, but you should get familiar with the precedence of these three operators (more to follow).

# Translating Logic into English sentences

- ①  $((\neg S) \wedge L) \vee S$  where  $S$  stands “John is smart”, and  $L$  “John is lazy”.

Either John is smart, or John lazy and not smart

- ②  $(\neg(S \wedge L)) \vee S$

Either John is smart, or he is not both smart and lazy.

# Truth tables

- We wish to evaluate the true or falsity of a compound proposition.
- The first way we learn about doing this is through **truth tables**.

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

$p$	$\neg p$
T	F
F	T

# Truth tables

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

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

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

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

# Exclusive OR ( $\oplus$ )

**Definition:** The exclusive or of  $p$  and  $q$ , denoted by  $p \oplus q$  is the proposition that is true when exactly one of  $p$  and  $q$  is true and is false otherwise.

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

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

## Exclusive OR ( $\oplus$ )

**Example:** I will use all my savings to travel to Europe or to buy an electric car.

- $P =$  I will use all my savings to travel to Europe
- $Q =$  I will use all my savings to buy an electric car.

Our proposition *I will use all my savings to travel to Europe or to buy an electric car* can be expressed as  $P \oplus Q$

# Lecture 2 (9/5) Outline

- Truth tables (cont.)
- Conditional, biconditional
- Logical equivalence (truth tables and laws)
- Applications
  - Digital circuits
  - Logic puzzles and satisfiability

# Truth tables

**Practice:** Make a truth table for the formula  $\neg(P \wedge Q) \vee \neg R$ .

$P$	$Q$	$R$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg R$	$\neg(P \wedge Q) \vee \neg R$
F	F	F	F	T	T	T
F	F	T	F	T	F	T
F	T	F	F	T	T	T
F	T	T	F	T	F	T
T	F	F	F	T	T	T
T	F	T	F	T	F	T
T	T	F	T	F	T	T
T	T	T	T	F	F	F

# Truth tables

Let's create the **truth table** for two important compound propositions.

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

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

- These two propositions are **logically equivalent**, i.e., same truth values in all possible cases. We will get later to the formal definition, but we already know what this means:
  - Alice and Bob are both not in the room
  - Neither Alice nor Bob is in the room

# Conditional statement (aka implication)

**Definition:** Let  $p$  and  $q$  be propositions. The conditional statement  $p \rightarrow q$  is the proposition  
*if  $p$ , then  $q$ .*

$p$  is called the hypothesis (or antecedent or premise) and  $q$  is called the conclusion (or consequence).

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

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

# Conditional statement (aka implication)

Analyze the logical forms of the following statements.

- ① If at least ten people are there, then the lecture will be given.
  - ② The lecture will be given only if at least ten people are there.
  - ③ The lecture will be given if and only if at least ten people are there.
- $T$  = At least ten people are there
  - $L$  = The lecture will be given

# Conditional statement (aka implication)

- ① If at least ten people are there, then the lecture will be given.

$$T \rightarrow L$$

- ② The lecture will be given only if at least ten people are there.  
Equivalently, if there are not at least ten people, then the lecture won't be given.

$$\neg T \rightarrow \neg L \text{ or equivalently } L \rightarrow T \text{ (contrapositive)}$$

- ③ The lecture will be given if and only if at least ten people are there.

$$T \leftrightarrow L$$

# Conditional statement (aka implication)

There are many ways to express a conditional statement in English.

“if  $p$ , then  $q$ ”

“if  $p$ ,  $q$ ”

“ $p$  is sufficient for  $q$ ”

“ $q$  if  $p$ ”

“ $q$  when  $p$ ”

“a necessary condition for  $p$  is  $q$ ”

“ $q$  unless  $\neg p$ ”

“ $p$  implies  $q$ ”

“ $p$  only if  $q$ ”

“a sufficient condition for  $q$  is  $p$ ”

“ $q$  whenever  $p$ ”

“ $q$  is necessary for  $p$ ”

“ $q$  follows from  $p$ ”

“ $q$  provided that  $p$ ”

# Conditional statement (aka implication)

**Example:** Let  $p$  be the statement “Maria learns discrete mathematics” and  $q$  the statement “Maria will find a good job.” Express the statement  $p \rightarrow q$  as a statement in English.

# Conditional statement (aka implication)

**Example:** Let  $p$  be the statement “Maria learns discrete mathematics” and  $q$  the statement “Maria will find a good job.” Express the statement  $p \rightarrow q$  as a statement in English.

- If Maria learns discrete mathematics, then she will find a good job.
- Maria will find a good job when she learns discrete mathematics.
- Maria will find a good job unless she does not learn discrete mathematics.

# Converse, contrapositive, and inverse

Consider the implication  $p \rightarrow q$ .

- ① Converse of  $p \rightarrow q$ :  $q \rightarrow p$
- ② Contrapositive of  $p \rightarrow q$ :  $\neg q \rightarrow \neg p$
- ③ Inverse of  $p \rightarrow q$ :  $\neg p \rightarrow \neg q$

$$p \rightarrow q \text{ and } \neg q \rightarrow \neg p$$

- Implication  $p \rightarrow q$ : If John cashed the check I wrote then my bank account is overdrawn
- Contrapositive  $\neg q \rightarrow \neg p$  : If my bank account isn't overdrawn then John hasn't cashed the check I wrote

## Contrapositive law

$P \rightarrow Q$  is equivalent to  $\neg Q \rightarrow \neg P$ .

**Exercise:** Truth tables on blackboard!

# Converse, contrapositive, and inverse

**Proposition:** The home team wins whenever it is raining. Express the following in English.

- Converse  $q \rightarrow p$ : ??
- Inverse  $\neg p \rightarrow \neg q$ : ??
- Contrapositive  $\neg q \rightarrow \neg p$ : ??

# Converse, contrapositive, and inverse

**Proposition:** The home team wins whenever it is raining. Express the following in English.

- Converse  $q \rightarrow p$ : If the home team wins, then it is raining.
- Inverse  $\neg p \rightarrow \neg q$ : If it is not raining, then the home team does not win.
- Contrapositive  $\neg q \rightarrow \neg p$ : If the home team does not win, then it is not raining.

# Biconditional statement (bi-implications)

**Example:** Let  $p$  and  $q$  be propositions. The biconditional statement  $p \leftrightarrow q$  is the proposition

$p$  if and only if  $q$

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

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

**Example:** You can take the flight if and only if you buy a ticket.

$\underbrace{P}_{\leftrightarrow} \underbrace{\leftrightarrow}_{Q}$

# Precedence of logical operators

Precedence of operators is as follows.

- ①  $\neg$
- ②  $\wedge$
- ③  $\vee$
- ④  $\rightarrow$
- ⑤  $\leftrightarrow$

**Example:**  $\neg p \vee q \rightarrow r$  should be interpreted as  $((\neg p) \vee q) \rightarrow r$ .

# Bits (binary digits)

- Computers represent information using **bits**. A bit is a symbol with two possible values, namely, 0 (zero) and 1 (one).
- Our logical operations can be expressed using 0/1s in addition to T/F.

<i>Truth Value</i>	<i>Bit</i>
T	1
F	0

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

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

# Logic circuits – Gates

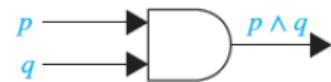
- Single output logic circuits receive binary input signals and output 0/1.
- Their basic components are the following three gates:



Inverter



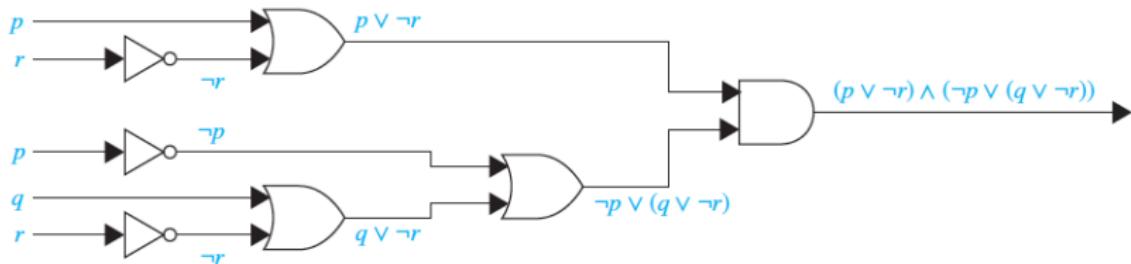
OR gate



AND gate

# Logic circuits – Example

- Using the basic gates we can produce combinatorial circuits for compound propositions.
- For now, parentheses will help you, but you should start getting familiar with the precedence of logical operators.



# Logical equivalence

Let's formalize the notion of logical equivalence that we saw earlier ( $\neg p \wedge \neg q$ ,  $\neg(p \vee q)$ ).

## Definitions:

- ① **tautology**: a compound proposition that is always true, e.g.  
 $p \vee \neg p$
- ② **contradiction**: a compound proposition that is always false,  
e.g.  $p \wedge \neg p$
- ③ **contingency**: a compound proposition that is neither a tautology nor a contradiction, e.g.  $p \wedge q$

# Logical equivalence

**Definition:** The compound propositions  $p$  and  $q$  are called logically equivalent if  $p \leftrightarrow q$  is a tautology. We also use the notation

$$p \equiv q$$

to denote logical equivalence.

**Important example:**

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

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

# Logical equivalence

- To prove that two propositions are logically equivalent, we may use the truth tables.
- Example:

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

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

## Logical equivalence – DeMorgan's laws

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

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

- DeMorgan's laws extend, e.g.,

$$\neg(p_1 \vee p_2 \vee \dots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n.$$

# Logical equivalence

TABLE 6 Logical Equivalences.

<i>Equivalence</i>	<i>Name</i>
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws

# Logical equivalence

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

# Logical equivalence

**Example:** Show that  $\neg(p \rightarrow q)$  and  $p \wedge \neg q$  are logically equivalent.

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

- The first equivalence is by the conditional-disjunction equivalence
- The second is by DeMorgan's law
- The last equivalence we use is by the double negation law

# Logical equivalence

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

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

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

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

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

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

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

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

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

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

**TABLE 8** Logical Equivalences Involving Biconditional Statements.

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

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

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

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

# Logical equivalence – Example

**Example:** Let's prove that  $p \wedge q \rightarrow p \vee q$  is a tautology.

$$\begin{aligned}(p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) && \text{by Example 3} \\ &\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{by the first De Morgan law} \\ &\equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{by the associative and commutative} \\ &&& \text{laws for disjunction} \\ &\equiv \mathbf{T} \vee \mathbf{T} && \text{by Example 1 and the commutative} \\ &&& \text{law for disjunction} \\ &\equiv \mathbf{T} && \text{by the domination law}\end{aligned}$$

# Logical puzzle and satisfiability

**Puzzle:** As a reward for saving his daughter from pirates, the King has given you the opportunity to win a treasure hidden inside one of three trunks. The two trunks that do not hold the treasure are empty. To win, you must select the correct trunk.

- Trunks 1 and 2 are each inscribed with the message “This trunk is empty”
- Trunk 3 is inscribed with the message “The treasure is in Trunk 2.”

The Queen, who never lies, tells you that only one of these inscriptions is true, while the other two are wrong. Which trunk should you select to win?

# Logical puzzle and satisfiability

- $p_i$ =treasure is in trunk  $i$ ,  $i = 1, 2, 3$
- The inscriptions of the three trunks are respectively  $\neg p_1, \neg p_2, p_2$
- According to the Queen

$$\underbrace{(\neg p_1 \wedge \neg(\neg p_1) \wedge \neg p_2)}_{\text{inscription 1 is the only true one}} \vee \underbrace{(\neg(\neg p_1) \wedge \neg p_2 \wedge \neg p_2)}_{\text{inscription 2 is the only true one}} \vee \\ \underbrace{(\neg(\neg p_1) \wedge \neg(\neg p_2) \wedge p_2)}_{\text{inscription 3 is the only true one}}.$$

Notice that only one of the terms of the disjunction can be true.

- By using equivalence laws, this is logically equivalent to  $p_1$
- Hence, the treasure is in trunk 1, and the inscription of trunk 2 is the only true one.

# Remark : Python and the *Truths* package

Creating truth tables in `python` is now a piece of cake thanks to  
<https://pypi.org/project/truths/>

```
from truths import Truths
print Truths(['a', 'b', 'cat', 'has_address'], ['(a and b)', 'a and b or cat', 'a and (b or cat) or has_address'])
```

a	b	cat	has_address	(a and b)	a and b or cat	a and (b or cat) or has_address
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	0
0	1	0	1	0	0	1
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	0	0
1	0	0	1	0	0	1
1	0	1	0	0	1	1
1	0	1	1	0	1	1
1	1	0	0	1	1	1
1	1	0	1	1	1	1
1	1	1	0	1	1	1
1	1	1	1	1	1	1

# Lectures 3 and 4 (9/10 and 9/12) Outline

- A quick remark
- Logic puzzles and satisfiability (from Lecture 2)
- Quantification logic (Rosen 1.4, 1.5)
  - Quantifiers
  - Equivalences involving quantifiers
- Rules of inference (Rosen 1.6)

# Quick remark

- Practice implications!
- Practice logical equivalencies!
- Produce table truths for them (good exercise).

Implication and its contrapositive:

- ① Statement: if  $xy$  is even, then  $x$  is even or  $y$  is even.
- ② Statement: If  $x$  is odd and  $y$  is odd, then  $xy$  is odd.

## Quick remark

- Let  $P$  is “ $xy$  is even”,  $Q$  is “ $x$  is even”, and  $R$  is “ $y$  is even”.
- Logical form of statement 1:  $P \rightarrow (Q \wedge R)$
- Contrapositive:

$$\neg(Q \wedge R) \rightarrow \neg P \equiv \neg Q \wedge \neg R \rightarrow \neg P.$$

- This is precisely statement 2!

# Logical puzzle and satisfiability

**Puzzle:** As a reward for saving his daughter from pirates, the King has given you the opportunity to win a treasure hidden inside one of three trunks. The two trunks that do not hold the treasure are empty. To win, you must select the correct trunk.

- Trunks 1 and 2 are each inscribed with the message “This trunk is empty”
- Trunk 3 is inscribed with the message “The treasure is in Trunk 2.”

The Queen, who never lies, tells you that only one of these inscriptions is true, while the other two are wrong. Which trunk should you select to win?

# Logical puzzle and satisfiability

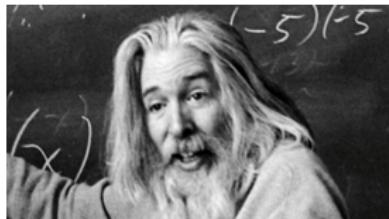
- $p_i$ =treasure is in trunk  $i$ ,  $i = 1, 2, 3$
- The inscriptions of the three trunks are respectively  $\neg p_1, \neg p_2, p_2$
- According to the Queen

$$\underbrace{(\neg p_1 \wedge \neg(\neg p_2) \wedge \neg p_2)}_{\text{inscription 1 is the only true one}} \vee \underbrace{(\neg(\neg p_1) \wedge \neg p_2 \wedge \neg p_2)}_{\text{inscription 2 is the only true one}} \vee \\ \underbrace{(\neg(\neg p_1) \wedge \neg(\neg p_2) \wedge p_2)}_{\text{inscription 3 is the only true one}}.$$

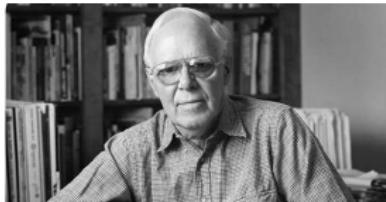
Notice that only one of the terms of the disjunction can be true.

- By using equivalence laws, this is logically equivalent to  $p_1$
- Hence, the treasure is in trunk 1, and the inscription of trunk 2 is the only true one.

## For those interested in puzzles..



Raymond Smullyan



Martin Gardner

- Many great books on puzzles for those who have fun with puzzles
- Raymond Smullyan and Martin Gardner are two important figures with many cool books

# Quantificational/First order logic/Predicate logic

- Propositional logic has its limitations. It deals with simple declarative propositions.
- First order logic (aka predicate or quantificational logic) covers predicates and quantification.
  - ① What is a predicate?
  - ② What is quantification?

# Predicate

- $P(x) = \underbrace{x}_{\text{variable}} \underbrace{\text{is greater than } 3}_{\text{predicate}}$
- $P(x)$  is a **propositional function** of  $x$ .
- Depending on  $x$ , the truth value of  $P(x)$  may change. For example:
  - $P(4)$  is true, since  $4 > 3$
  - but  $P(2)$  is false
- *Predicate* is a property that the subject of a statement may have.

# Predicate

- A predicate may be a function of two or more variables.
- E.g.,  $Q(x, y) = "x = y + 3"$ 
  - $Q(2, 2)$  is false since  $2 \neq 2 + 3$
  - $Q(3, 0)$  is true since  $3 = 0 + 3$ .
- $P(x_1, \dots, x_n)$  is a propositional function of  $n$  variables.

# Universal quantifier $\forall$

- Goal: Say that  $P(x)$  is true for every value of  $x$  in the universe of discourse
- “For all  $x$ ,  $P(x)$ ”
- We write  $\forall x P(x)$ .
- $\forall$  is called the universal quantifier since it states that  $P(x)$  is universally true.

# Universal quantifier $\forall$

Let's see some examples. Let's translate them in English and decide if they are true or false.

- ①  $\forall x(x^2 \geq 0)$  where the universe of discourse is the set of all real numbers
- ② Let  $M(x)$  be “ $x$  is a man”, and  $B(x)$  “ $x$  has blue eyes”. Let the universe of discourse be the set of all humans, i.e., domain of  $x$ .

$$\forall x(M(x) \rightarrow B(x)).$$

# Universal quantifier $\forall$

Let's see some examples. Let's translate them in English and decide if they are true or false.

- ①  $\forall x(x^2 \geq 0)$  where the universe of discourse is the set of all real numbers

This means that for every real number  $x$ ,  $x^2$  is non-negative.

This is true.

- ② Let  $M(x)$  be “ $x$  is a man”, and  $B(x)$  “ $x$  has blue eyes”.

$$\forall x(M(x) \rightarrow B(x)).$$

For every human  $x$ , if  $x$  is a man, then  $x$  has blue eyes. But  $M(\text{Prof. Tsourakakis}) = \text{true}$ ,  $B(\text{Prof. Tsourakakis}) = \text{false}$ . This immediately proves that not all men have blue eyes.  
(Counterexample)

## Remark

- A statement  $\forall x P(x)$  is false when there exists an  $x$  in the **domain** for which  $P(x)$  is false
- The domain is **very** important. Actually without being precise about the domain, asking the truth value of a universal statement does not make sense
- **Example:**  $\forall x (x^2 \geq x)$ 
  - if the domain are reals, then it is false.
  - If the domain is the set of integers, then it is true.
- If the domain is finite (e.g.,  $\{val_1, \dots, val_k\}$  for finite  $k$ ) then  $\forall x P(x)$  is equivalent to  $P(val_1) \wedge \dots \wedge P(val_k)$ .

# Existential quantifier $\exists$

- To write  $\exists x P(x)$  means that there is at least one value of  $x$  in the universe for which  $P(x)$  is true.
- $\exists$  is the existential quantifier
- Examples
  - $\exists(M(x) \wedge B(x))$ : there exists a blue-eyed man
  - $\exists x(x^2 - 2x + 5 = 0)$  with domain the real numbers
- If the domain is finite (e.g.,  $\{val_1, \dots, val_k\}$  for finite  $k$ ) then  $\exists x P(x)$  is equivalent to  $P(val_1) \vee \dots \vee P(val_k)$ .

# Important remarks

- **Precedence**  $\forall, \exists$ : The quantifiers  $\forall, \exists$  have higher precedence than all logical operators from propositional calculus
- E.g.,  $\forall xP(x) \vee Q(x)$  means  $(\forall xP(x)) \vee Q(x)$ .  
Contrast this to  $\forall x(P(x) \vee Q(x))$
- **Definition:** When a quantifier is used on the variable  $x$ , we say that this occurrence of the variable is **bound**. An occurrence of a variable that is not bound by a quantifier or set equal to a particular value is said to be **free**.
- **Examples:** Identify the free, and bound variables.
  - $\exists x(x + y = 1)$
  - Let  $L(x, y)$  be “ $x$  likes  $y$ ”, and the domain be the set of people.  
The statement is  $\forall xL(x, y)$ .

# Logical equivalence involving quantifiers

Statements involving predicates and quantifiers are *logically equivalent* if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions. We use the notation  $S \equiv T$  to indicate that two statements  $S$  and  $T$  involving predicates and quantifiers are logically equivalent.

You need to be very careful about distributing quantifiers over conjunctions and disjunctions:

- ① True or false:  $\forall x(P(x) \wedge Q(x)) \equiv \forall xP(x) \wedge \forall xQ(x)$ ?
- ② True or false  $\forall x(P(x) \vee Q(x)) \equiv \forall xP(x) \vee \forall xQ(x)$ ?
- ③ True or false:  $\exists x(P(x) \wedge Q(x)) \equiv \exists xP(x) \wedge \exists xQ(x)$ ?
- ④ True or false  $\exists x(P(x) \vee Q(x)) \equiv \exists xP(x) \vee \exists xQ(x)$ ?

# Logical equivalence involving quantifiers

- ①  $\forall x(P(x) \wedge Q(x)) \equiv \forall xP(x) \wedge \forall xQ(x)$  is **true**

To show that these statements are logically equivalent, we must show that they always take the same truth value, no matter what the predicates are, and no matter which domain of discourse is used.

We prove that if  $\forall x(P(x) \wedge Q(x))$  is true, then  $\forall xP(x) \wedge \forall xQ(x)$  is true, and **vice versa**.

Details on blackboard (see Rosen p.49)

# Logical equivalence involving quantifiers

②  $\forall x(P(x) \vee Q(x)) \equiv \forall xP(x) \vee \forall xQ(x)$  is **false**

Let's prove it by counterexample that illustrates that it is false.

- Let domain be the set of integers
- Let  $P(x) = x$  is even
- Let  $Q(x) = x$  is odd
- $\forall x(P(x) \vee Q(x))$  is true (every integer is either odd or even)
- $\forall xP(x) \vee \forall xQ(x)$  is false. (since  $\forall xP(x)$  is false as not all integers are even, and  $\forall xQ(x)$  is also false since not all integers are odd, hence disjunction is false)

# Logical equivalence involving quantifiers

③ :  $\exists x(P(x) \wedge Q(x)) \equiv \exists xP(x) \wedge \exists xQ(x)$ ? is **false**

Let's prove it by counterexample that illustrates that it is false.

- Let domain be the set of integers
- Let  $P(x) = x$  is even
- Let  $Q(x) = x$  is odd
- $\exists x(P(x) \wedge Q(x))$  is false (no integer can be both even and odd)
- $\exists xP(x) \wedge \exists xQ(x)$  is true. (2 is even, hence  $\exists xP(x)$  is true, and 3 is odd, hence  $\exists xQ(s)$  is also true. Therefore the conjunction is true.)

# Logical equivalence involving quantifiers

- ④ :  $\exists x(P(x) \vee Q(x)) \equiv \exists xP(x) \vee \exists xQ(x)$  is **true**

Homework/lab problem.

# Logical equivalence involving quantifiers – Negation of quantified expressions

Let's first see some sentences in English and their negation. Let's negate the following statements:

- Everybody is perfect (**universal quantifier**)
- Every student in CS131 has taken a course in calculus (**universal quantifier**)

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

# Logical equivalence involving quantifiers – Negation of quantified expressions

Let's again see some sentences in English and their negation. Let's negate the following statement:

- There does not exist a student in CS131 who meets the calculus prerequisites (**existential quantifier**)

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

# DeMorgan's laws for quantifiers

TABLE 2 De Morgan's Laws for Quantifiers.

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

# DeMorgan's laws for quantifiers – Examples

What are the negations of the statements ?

① There is an honest politician

②  $\forall x(x^2 > x)$

③  $\exists x(x^2 = 2)$

# DeMorgan's laws for quantifiers – Examples

What are the negations of the statements? We apply DeMorgan's laws everywhere!

- ① Let  $H(x)$  denote  $x$  is a mortal human being. The statement is  $\exists x H(x)$ . Its negation is:  
 $\neg \exists x H(x) \equiv \forall x \neg H(x)$ . In English, this simply means that every human being is immortal
- ② The negation of  $\forall x (x^2 > x)$  is as follows:  
 $\neg \forall x (x^2 > x) \equiv \exists x \neg (x^2 > x) \equiv \exists x (x^2 \leq x)$ .
- ③ The negation of  $\exists x (x^2 = 2)$  is:  
 $\neg \exists x (x^2 = 2) \equiv \forall x \neg (x^2 = 2) \equiv \forall x (x^2 \neq 2)$

# Practice

Analyze the logical forms for the following statements

- ① Someone did not do the homework.
- ② Nobody is perfect
- ③ Everything in that store is either overpriced or poorly made
- ④ Everybody in the dorm has a roommate he does not like.
- ⑤ All married couples have fights
- ⑥ John likes (*exactly*) one person.

Ideas?

# Practice (solutions)

- ① Someone did not do the homework.

Let  $H(x)$  stand for “ $x$  did the homework”. Then we can rewrite the statement as  $\exists x \neg H(x)$ . Equivalently,  $\neg \forall x H(x)$ .

- ② Nobody is perfect

Let  $P(x)$  stand for “ $x$  is perfect”. The statement is  $\neg \exists x P(x)$  or equivalently  $\forall x \neg P(x)$ .

# Practice (solutions)

- ③ Everything in that store is either overpriced or poorly made

We can rephrase this as “If something is in that store, then it is either overpriced or poorly made”.

Let  $S(x)$  stand for “ $x$  is in that store”

$O(x)$  stand for “ $x$  is overpriced”

$P(x)$  stand for “ $x$  is poorly made”.

$$\forall x(S(x) \rightarrow (O(x) \vee P(x))).$$

## Practice (solutions)

- ④ Everybody in the dorm has a roomate he does not like.

We wish to say  $\forall x$  (if  $x$  lives in the dorm, then  $x$  has a roomate he does not like)

Let  $D(x)$  stand for  $x$  lives in the dorm

Let  $L(x, y)$  stand for  $x$  likes  $y$

Let  $R(x, y)$  stand for  $x, y$  are roomates

$$\forall x(D(x) \rightarrow \exists y(R(x, y) \wedge \neg L(x, y))).$$

# Practice (solutions)

⑤ All married couples have fights.

- We need to define predicates that take two arguments  $x, y$ .
- Let  $M(x, y)$  mean “ $x$  and  $y$  are married to each other”.
- Let  $F(x, y)$  mean “ $x$  and  $y$  fight with each other”
- Then we can write

$$\forall x \forall y (M(x, y) \rightarrow F(x, y)).$$

# Practice (solutions)

- ⑥ **Remark:** John likes one person is not the same as John likes exactly one person

Let  $L(x, y)$  mean  $x$  likes  $y$

- ⑦ John likes one person means  $\exists x L(John, x)$ .
- ⑧ John likes exactly one person means that person is unique and this is expressed as

$$\exists x(L(John, x) \wedge \neg \exists y(L(John, y) \wedge y \neq x)).$$

- ⑨ We introduce a new quantifier to denote uniqueness of  $x$

$$\exists!x P(x)$$

# Nesting quantifiers

As we have seen already, we can use more than one quantifiers in one statement, or we can even *nest* them. Nesting order of the quantifiers **matters!**

**Exercise:** Decide if the following statements are true or false. We assume the domain is the set of natural numbers.

- ①  $\forall x \exists y (x < y)$
- ②  $\exists y \forall x (x < y)$
- ③  $\exists x \forall y (x < y)$
- ④  $\forall y \exists x (x < y)$
- ⑤  $\exists x \exists y (x < y)$
- ⑥  $\forall x \forall y (x < y)$

# Nesting quantifiers

①  $\forall x \exists y (x < y)$

True. Set  $y = x + 1$

②  $\exists y \forall x (x < y)$

False. No matter what  $y$  we pick, we can always find an  $x$  that is larger.

③  $\exists x \forall y (x < y)$

False. (why not  $x = 0$ ?)

④  $\forall y \exists x (x < y)$

False (for  $y = 0$  no such  $x$  exists)

⑤  $\exists x \exists y (x < y)$

True.

⑥  $\forall x \forall y (x < y)$

False. There is not even one value for  $x$  for which  $\forall y (x < y)$

# Negating nesting quantifiers

**Exercise:** Let's express the following negation so that no negation precedes a quantifier.

①  $\forall x \exists y (xy = 1)$

**Rule:** We apply successively the rules for negating statements involving a single quantifier.

② Therefore,

$$\neg \forall x \exists y (xy = 1) \equiv \exists x \neg \exists y (xy = 1) \equiv \exists x \forall y \neg (xy = 1) \equiv \exists x \forall y (xy \neq 1).$$

# Rules of inference

Some important tautologies give rise to some important rules of inference.

TABLE 1 Rules of Inference.

Rule of Inference	Tautology	Name
$\begin{array}{l} p \\ p \rightarrow q \\ \therefore q \end{array}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\begin{array}{l} \neg q \\ p \rightarrow q \\ \therefore \neg p \end{array}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \therefore p \rightarrow r \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\begin{array}{l} p \vee q \\ \neg p \\ \therefore q \end{array}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\begin{array}{l} p \\ \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \therefore \neg p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{l} p \\ q \\ \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \therefore q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

## Rules of inference – Remark

### Resolution.

- The resolution rule of inference relies on the tautology

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

- Plays an important role in programming languages based on logic, e.g., PROLOG
- **Example:** Let's apply the resolution rule on the hypotheses  
Jasmine is skiing or it is not snowing and It is snowing or Bart is playing hockey

# Rules of inference – Remark

## Example:

- Let  $p$  be the proposition “it is snowing”
- Let  $q$  be the proposition “Jasmine is skiing”
- Let  $r$  be the proposition “Bart is playing hockey”.
- Our hypothesis is  $((p \vee q) \wedge (\neg p \vee r))$
- Therefore, by the resolution rule we conclude  $(q \vee r)$  which means  
Jasmine is skiing or Bart is playing hockey

# Lectures 5 and 6 (9/17 and 9/19) Outline

- (Finish off) rules of inference (Rosen 1.6)
- Mathematical proofs (Rosen 1.7, 1.8)
  - How do we write proofs?
  - Direct
  - Contraposition
  - Counterexample
  - Contradiction
  - Proofs of equivalence

# Rules of inference

Consider the following argument. Is it valid?

- **Logical premise 1:** If  $\underbrace{\text{you have a current password}}_p$ , then  $\underbrace{\text{you can log onto the network}}_q$ .  
 $p \rightarrow q$
- **Logical premise 2:**  $\underbrace{\text{You have the current password}}_p$ .
- **Conclusion:** Therefore  $(\therefore), q$

## Rules of inference: *modus ponens*

- Yes, it is valid. The following tautology

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

leads to the this valid argument.

This rule of inference is called MODUS PONENS.

- **Remark:** If  $\sqrt{2} > \frac{3}{2}$  then  $(\sqrt{2})^2 > (\frac{3}{2})^2$ . We know that  $\sqrt{2} > \frac{3}{2}$ . Therefore,  $(\sqrt{2})^2 > (\frac{3}{2})^2$ , i.e.,  $2 > \frac{9}{4} = 2.25$ .
- **What is the issue here?**

# Rules of inference

- Some important tautologies give rise to some frequently used valid arguments/rules of inference.
- Addition
- “It is below freezing now, therefore it is below freezing or raining now”

$p$  therefore  $p \vee q$ .

The tautology  $p \rightarrow (p \vee q)$ .

# Rules of inference

- Some important tautologies give rise to some frequently used valid arguments/rules of inference.
- Simplification
- “It is below freezing and raining, therefore it raining”

The argument is of the form  $p$  therefore  $p \vee q$ .

The tautology  $p \rightarrow (p \vee q)$ .

# Rules of inference

TABLE 1 Rules of Inference.

Rule of Inference	Tautology	Name
$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

# Rules of inference – Resolution

## Resolution.

- The resolution rule of inference relies on the tautology

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

- Plays an important role in programming languages based on logic, e.g., PROLOG
- **Example:** Let's apply the resolution rule on the hypotheses  
Jasmine is skiing or it is not snowing and It is snowing or Bart is playing hockey

# Rules of inference – Resolution

## Example:

- Let  $p$  be the proposition “it is snowing”
- Let  $q$  be the proposition “Jasmine is skiing”
- Let  $r$  be the proposition “Bart is playing hockey”.
- Our hypothesis is  $((p \vee q) \wedge (\neg p \vee r))$
- Therefore, by the resolution rule we conclude  $(q \vee r)$  which means  
Jasmine is skiing or Bart is playing hockey

# Rules of inference – Fallacy

- If you do every problem in this book, then you will learn discrete mathematics.
- You learned discrete mathematics.
- Therefore, you did every problem in this book.

**Is this a valid argument?**

# Rules of inference – Fallacy

- If you do every problem in this book, then you will learn discrete mathematics.
- You learned discrete mathematics.
- Therefore, you did every problem in this book.

**No!**

- $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$  is not a tautology (set  $p = F, q = T$ )

# Rules of inference – Quantified statements

TABLE 2 Rules of Inference for Quantified Statements.

<i>Rule of Inference</i>	<i>Name</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalization
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

# Proofs

- **What is a proof?**
- A proof is a valid argument that establishes the truth of a mathematical statement, using the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems.
- Using these ingredients and rules of inference, the proof establishes the truth of the statement being proved.

# Direct proofs – Final version of a proof versus reasoning work

**Question:** How do we prove the following theorem?

**Theorem:** Suppose  $a, b$  are real numbers. If  $0 < a < b$  then  $a^2 < b^2$ .

- What is given to us as hypothesis?
- What is the conclusion?

# Direct proofs – Final version of a proof versus reasoning work

**Question:** How do we prove the following theorem?

**Theorem:** Suppose  $a, b$  are real numbers. If  $0 < a < b$  then  $a^2 < b^2$ .

- What is given to us as hypothesis?

**Givens:**  $a, b$  are real numbers

- What is the conclusion we want to prove?

**Goal:**  $P \rightarrow Q$  where  $P$  is  $0 < a < b$  and  $Q$  is  $a^2 < b^2$ .

# Direct proofs – Final version of a proof versus reasoning work

- **Direct proof** technique for  $P \rightarrow Q$ : Add  $P$  to the set of hypotheses. Then prove  $Q$ .
- **Let's apply it!** What is given to us as hypotheses now?
- **Givens:**  $a, b$  are real numbers,  $0 < a < b$
- **Goal:** Show that  $a^2 < b^2$

# Direct proofs – Final version of a proof versus reasoning work

Let's write the formal proof now.

- **Proof:** Suppose  $0 < a < b$ . Multiplying the inequality  $a < b$  by the positive number  $a$  we can conclude  $a^2 < ab$ , and similarly multiplying by  $b$  we get  $ab < b^2$ . Therefore,

$$a^2 < ab < b^2,$$

so,  $a^2 < b^2$  as required. **QED**<sup>1</sup>

---

<sup>1</sup> “quod erat demonstrandum”, literally meaning “what was to be shown”.

# Direct proofs

Prove the following theorems.

- ① If  $n$  is an odd integer, then  $n^2$  is odd.
- ② Suppose  $m, n$  are natural numbers. If  $m, n$  are both perfect squares, then  $nm$  is also a perfect square.

Solutions on blackboard

# Proof by contraposition

**Question:** How do we prove the following theorem?

**Theorem:** Suppose  $a, b, c$  are real numbers, and  $a > b$ . Prove that if  $ac \leq bc$  then  $c \leq 0$ .

- What is given to us as hypothesis?
- What is the conclusion?

# Proof by contraposition

**Question:** How do we prove the following theorem?

**Theorem:** Suppose  $a, b, c$  are real numbers, and  $a > b$ . Prove that if  $ac \leq bc$  then  $c \leq 0$ .

- What is given to us as hypothesis?

**Givens:**  $a, b, c$  are real numbers,  $a > b$

- What is the conclusion?

**Goal:**  $P \rightarrow Q$  where  $P$  is  $ac \leq bc$  and  $Q$  is  $c \leq 0$ .

# Proof by contraposition

- **Proof by contraposition** technique for  $P \rightarrow Q$ : Add  $\neg Q$  to the set of hypotheses. Then prove  $\neg P$ .
- What is given to us as hypothesis?

**Givens:**  $a, b, c$  are real numbers,  $a > b, c > 0$

**Goal:**  $ac > bc$

**So**, the proof structure using contraposition would look like this:

Suppose  $c > 0$

[Proof that  $ac > bc$  goes here]

Therefore, if  $ac \leq bc$  then  $c \leq 0$ .

# Proof by contraposition

This is how the final/formal proof by contrapositive would look like on the paper:

**Theorem:** Suppose  $a, b, c$  are real numbers, and  $a > b$ . Prove that if  $ac \leq bc$  then  $c \leq 0$ .

**Proof:** We will prove by contrapositive. Suppose  $c > 0$ . Then we can multiply both sides of the given inequality  $a > b$  by  $c$  and conclude that  $ac > bc$ . Therefore, if  $ac \leq bc$ , then  $c \leq 0$ .

## Important remark!

Even if we have used logic in the scratch work, we have not used them in the final form. While logic is essential to figure out a proof strategy, in the final write-up of the proof, mathematicians avoid using the notation and rules of logic.

# Direct vs contraposition

- **When do we use** a **direct** proof, and when a proof by **contraposition**?
- **Rule of thumb:** Evaluate first if a direct proof looks promising. If it does not seem to go anywhere, try alternative strategies, including proof by contraposition.
- **Example:** Prove that if  $n$  is an integer, and  $3n + 2$  is odd, then  $n$  is odd. (Blackboard)

# Proof by counterexample

## SHORTEST KNOWN PAPER PUBLISHED

March 22, 2017 - by randomprojection - in Think..., Uncategorized - Leave a comment

### COUNTEREXAMPLE TO EULER'S CONJECTURE ON SUMS OF LIKE POWERS

BY L. J. LANDER AND T. R. PARKIN

Communicated by J. D. Swift, June 27, 1966

A direct search on the CDC 6600 yielded

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

as the smallest instance in which four fifth powers sum to a fifth power. This is a counterexample to a conjecture by Euler [1] that at least  $n$   $n$ th powers are required to sum to an  $n$ th power,  $n > 2$ .

#### REFERENCE

1. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, p. 648.

I recently saw a post from OpenCulture, that I explored, and tweeted about: the shortest known paper published in a serious math journal.



Babis Tsourakakis  
@Tsourolampis



The Shortest-Known Paper Published in a Serious Math Journal:  
Two Succinct Sentences [goo.gl/x4seZE](http://goo.gl/x4seZE) via @openculture

# Remark

Nowadays computers give us a lot of power. A small piece of C++ code would be able to find the counterexample from that paper.

The screenshot shows a Mac OS X desktop with a browser window open to a GitHub Gist page containing C++ code. Below the browser are several application icons, including Finder, Mail, and various productivity tools. Two Twitter posts by Babine Tsourakakis are visible on the right side of the screen.

```
#include <iostream>
#include <cmath>
using namespace std;

// Disprove Euler conjecture
// Babine Tsourakakis (babine@seas.harvard.edu)
// March 22, 2017

long min(long x, long y){  
    if(x>y) return x;  
    else return y;  
}  
  
void dispove_eulerClng(No{  
    long target = 144;  
    long max_x = N-1; Floor( 0.25N ); x--);  
    for(Clng y = Floor(pow(target - pow(x,5), 0.25)) + min(y, 5);  
        for(Clng w = min(z, Floor(pow(target - pow(x,5)-pow(y,5), 0.25));  
            for(Clng v = min(z, Floor(pow(target - pow(x,5)-pow(y,5)-pow(w,5), 0.25));  
                count++;  
                if( pow(x,5)+pow(y,5)+pow(z,5)+pow(w,5) == target )  
                    cout << "Success! Euler disproved!"<<endl;  
            }  
        }  
    }  
}  
int main()  
{  
    dispove_euler(144);  
    return 0;  
}
```

Babine Tsourakakis (@tsourakakis)  
A Mathematical Model Unlocks the Secrets of Vision quantummagazine.org  
mathematical... via @QuantumMagazine

Babine Tsourakakis (@tsourakakis)  
Flipped classrooms fail to improve student performance  
livesinagraduation.com/news/flipped...  
... via @livesinagrad

<https://tsourakakis.com/2017/03/22/shortest-known-paper-published/>

# Lecture 7 (9/23)

## Outline

- Mathematical proofs (cont., Rosen 1.7, 1.8)
  - How do we write proofs?
  - Contradiction
  - Existence proofs
  - Proofs of equivalence
  - Exhaustive proofs (aka proofs by cases)
  - Uniqueness proofs
  - and...
    - Trivial proofs
    - WLOG
    - Forward/backward reasoning

# Proof by contradiction

**Exercise:** Prove that  $\sqrt{2}$  is irrational.

Ideas?

What does it mean to be rational to begin with?

## Proof by contradiction [Scratch work]

- *Irrational* means not rational, so our goal is a **negative** statement. This fact already suggests that a proof by contradiction might be the right choice.
- What would it mean for  $\sqrt{2}$  to be rational?  $\frac{p}{q} = \sqrt{2}$ , where  $p, q \neq 0$  are integers.
- *without loss of generality*, we may assume that  $p, q$  are both positive (since  $\sqrt{2} > 0$ ), and that the fraction is in lowest terms (i.e.,  $p, q$  have no common factors)
- What do we infer by squaring?

## Proof by contradiction [Scratch work]

- What do we infer by squaring? That both  $p, q$  are even!
- By squaring we obtain that  $p^2 = 2q^2$ .
- This means that  $p^2$  is even, and therefore  $p = 2a$  for some integer  $a$ , i.e.,  $p$  is even.
- By substituting  $p = 2a$  we obtain that  $q^2$  and hence  $q$  is also even since  $2q^2 = 4a^2 \rightarrow q^2 = 2a^2$ . Therefore  $q = 2b$  for some integer  $b$ .

# Proof by contradiction [Scratch work]

- So we have shown that  $p, q$  have to both be even.
- What does this mean?
  - That they share 2 as a common factor
- Therefore, our assumption that 2 is rational ( $\neg p$ ) leads to the contradiction that
  - ① 2 does not divide  $p, q$  (lower terms)
  - ②  $p, q$  are even, so 2 divides both of them
- Thus,  $\sqrt{2}$  is rational

## Proof by contradiction – $\sqrt{2}$ is irrational

Read carefully the way the proof is also written in Rosen, p. 90, 91

- **Remark:** Writing nice proofs requires practice
- Additional reading: Mathematical writing (sections 1,2,3)  
[http://jmlr.csail.mit.edu/reviewing-papers/knuth\\_mathematical\\_writing.pdf](http://jmlr.csail.mit.edu/reviewing-papers/knuth_mathematical_writing.pdf)

# Proof by contradiction – Technique

- Suppose we want to prove that  $p$  is true.
- For the sake of contradiction, let's assume  $\neg p$  is true.
- **Technique:** We prove that  $\neg p \rightarrow F$ .
  - This achieved by proving  $\neg p \rightarrow (r \wedge \neg r)$  for some proposition  $r$
- Practice, practice, practice!

# Proof by contradiction

- **Theorem:** If  $a, b$  are integers, then  $a^2 - 4b \neq 2$ .
- **Proof by contradiction (scratch work):** We wish to prove an implication  $p \rightarrow q \equiv \neg p \vee q$ . The negation is  $\neg(p \rightarrow q) \equiv p \wedge \neg q$ . In other words we need to assume that there exist two integers  $a, b$  such that  $a^2 - 4b = 2$ .
- That is how we need to start writing our proof.  
“Suppose for the sake of contradiction that there exist two integers  $a, b$  such that  $a^2 - 4b = 2$ .”
- The next step is to derive a contradiction based on this logical premise. What observations can we derive from  $a^2 - 4b = 2$ ?

## Proof by contradiction

**Proof:** Suppose for the sake of contradiction that there exist two integers  $a, b$  such that  $a^2 - 4b = 2$ . From this equation we get

$$a^2 = 2(1 + 2b) \tag{1}$$

so  $a^2$  is even, and therefore  $a$  is even. This means we can write  $a = 2c$  for some integer  $c$ . By plugging this expression in Equation 1 and dividing by 2, we obtain  $2(c^2 - b) = 1$ . Since  $c^2 - b$  is an integer, 1 is equal to an even number. Contradiction (i.e., 1 is odd  $\wedge$  1 is even). **QED**

# Proof by equivalence

- To prove a biconditional statement (if and only if)

$$p \leftrightarrow q$$

we need to prove  $p \rightarrow q$  and  $q \rightarrow p$ .

- Example:** Let  $n$  be an integer. Prove that  $n$  is odd if and only if (**iff**)  $n^2$  is odd.
  - One direction is ( $n$  is odd  $\rightarrow n^2$  is odd)
  - The other direction ( $n^2$  is odd  $\rightarrow n$  is odd)  
We have already proved both in class.
- How do we prove  $p_1 \leftrightarrow p_2 \leftrightarrow p_3$ ?

# Proof by equivalence

- How do we prove  $p_1 \leftrightarrow p_2 \leftrightarrow p_3$ ?
- **Idea 1:** Prove the following:
  - ①  $p_1 \rightarrow p_2$
  - ②  $p_2 \rightarrow p_1$
  - ③  $p_1 \rightarrow p_3$
  - ④  $p_3 \rightarrow p_1$
  - ⑤  $p_2 \rightarrow p_3$
  - ⑥  $p_3 \rightarrow p_2$
- **Better idea:** This is not necessary. It suffices to prove :
  - ①  $p_1 \rightarrow p_2$
  - ②  $p_2 \rightarrow p_3$
  - ③  $p_3 \rightarrow p_1$

# Proof by equivalence

- **Example :** Show that these statements about the integer  $n$  are equivalent:
  - ①  $p_1 : n$  is even
  - ②  $p_2 : n - 1$  is odd
  - ③  $p_3 : n^2$  is even

Details on blackboard (see also [Rosen, Example 14, p.92] )

- What is an efficient way to prove  $p_1 \leftrightarrow \dots \leftrightarrow p_n$  where  $n \geq 2$ ? (**generalize**)

**Intuition** (details in class): Ensure “strong connectivity” when we think of propositions as nodes, and conditionals as arcs

# Existence proofs

- **Claim:** Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

**Proof:**  $1729 = 10^3 + 9^3 = 12^3 + 1^3$  (computer search...)

- **Exercise:** Show that there exist irrational numbers  $x, y$  such that  $x^y$  is rational.

# Existence proofs

- **Exercise:** Show that there exist irrational numbers  $x, y$  such that  $x^y$  is rational.
- **Scratch work:** Well, the only irrational we have seen so far is  $\sqrt{2}$ , so let's consider  $\sqrt{2}^{\sqrt{2}}$ .
  - Well, it is hard to tell. But we know that one of the following two can be true:
    - ①  $\sqrt{2}^{\sqrt{2}}$  is rational, hence we are done.
    - ②  $\sqrt{2}^{\sqrt{2}}$  is irrational.
  - But in the latter case, notice that  $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ .
    - Therefore we have covered all cases.  
Either  $x = y = \sqrt{2}$  or  $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$  have the desired property.
- **Formal proof:** How to write it down? On blackboard and **pages 101, 102 Rosen**

# Proof by exhaustion (aka proof by cases)

- Tautology

$$[(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$$

- **Crucial first step:** Identify a **complete list** of possible cases (in principle, they need not be mutually exclusive, but in practice they usually are).

- **Exercises**

- ① Prove that if  $(n + 1)^3 \geq 3^n$  if  $n$  is a positive integer with  $n \leq 4$ .
- ② Prove that if  $n$  is an integer, then  $n^2 \geq n$
- ③ Let  $n$  be an integer. If 3 does not divide  $n$ , then 3 divides  $n^2 - 1$ .

Solutions on blackboard

# Without loss of generality (wlog)

- **Example:** If three objects are each painted either red or blue, then there must be at least two objects of the same color.

**Proof:** Assume without loss of generality that the first object is red. If either of the other two objects is red, we are finished; if not, the other two objects must both be blue and we are still finished.

- **Remarks**
  - ① The *wlog* allows us to cover the symmetric case where the first object is blue.
  - ② We will see this again later in class (pigeonhole principle)

# Vacuous and Trivial proofs

- Suppose we wish to prove that  $p \rightarrow q$ 
  - ① If  $p$  is always false, then the statement is always true (vacuous proof)
  - ② If  $q$  is always true, then the statement is again always true (trivial proof)
- Examples
  - ① Prove that if  $n$  is an integer with  $10 \leq n \leq 11$  which is a perfect square, then  $n$  is also a perfect cube.
  - ② Let  $P(n)$  be “if  $a,b$  are positive integers with  $a \geq b$  then  $a^n \geq b^n$ , where the domain consists of all nonnegative integers. Show that  $P(0)$  is true.
- Proofs on blackboard (see also [Rosen p.88,89])

# Uniqueness proofs

- $\exists!xP(x)$
- A uniqueness proof consists typically of two parts
  - ① Prove existence of  $x$  that has the desired property
  - ② Prove that if  $y$  has the desired property, then  $y = x$
- **Example:** There is a unique function  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that  $f'(x) = 2x$  and  $f(0) = 3$ .

Proof.

- ① Existence:  $f(x) = x^2 + 3$  (why?)
- ② Uniqueness: If  $f_0(x)$  and  $f_1(x)$  both satisfy these conditions, then  $f'_0(x) = 2x = f'_1(x)$ , so they differ by a constant, i.e., there is a  $C$  such that  $f_0(x) = f_1(x) + C$ . Hence,  $3 = f_0(0) = f_1(0) + C = 3 + C$ . This gives  $C = 0$  and so  $f_0(x) = f_1(x)$



# Forward/backward reasoning

- **AM-GM:** Let  $x, y$  be two non-negative real numbers. Prove that  $\frac{x+y}{2} \geq \sqrt{xy}$ .

## Backward reasoning.

$$\frac{x+y}{2} \geq \sqrt{xy} \leftrightarrow \left(\frac{x+y}{2}\right)^2 \geq (\sqrt{xy})^2 \leftrightarrow (x+y)^2 \geq 4xy \leftrightarrow (x^2 + 2xy + y^2) \geq 4xy \leftrightarrow (x^2 - 2xy + y^2) \geq 0 \leftrightarrow (x-y)^2 \geq 0.$$

- **Remark:** We can use backward reasoning to produce forward reasoning since we used *equivalent* inequalities.
- Details on the blackboard.

# Lecture 8, 9 (9/26, 10/1) Outline

- Sets and set operations [Rosen 2.1, 2.2]
- Sequences and summations [Rosen 2.4]

# Sets

- $\{0, 3, 1\}$  is a set
- $\{0, 1, 3\}$  is a set and it is the same as  $\{0, 3, 1\}$
- $(0, 1, 3)$  is not a set
- $\{a, b, c, d, \dots, z\}$  is a set
- $\{\{a, b\}, \{b, c\}\}$  is a set
- $\{a, b, b, c\}$  is **not** a set
- $\mathbb{N} = \{0, 1, 2, \dots\}$  is the set of naturals
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  is the set of integers
- $\mathbb{Z}^+ = \{1, 2, \dots\}$  is the set of positive integers
- $\mathbb{R}$  is the set of reals

**Question:** Can you define what a set is?

# Sets

**Definition:** A set is an **unordered collection of distinct objects**.

- Some remarks.
  - ① These objects are called elements or members of the set.
  - ② The elements could be sets themselves, or sets containing other sets etc.!
  - ③ We write  $a \in S$  to denote that  $a$  is a member of the set  $S$ .
  - ④ We write  $a \notin S$  to denote that  $a$  is not a member of the set  $S$ .
  - ⑤ It may be impractical to define a set by listing all its elements.
    - $P = \{2, 3, 5, 7, \dots\}$
    - Using dots is a common practice but requires the pattern to be clear.
    - A better practice:  $P = \{x | x \text{ is a prime number}\}$  (set builder)

**Exercise:** Rewrite the following sets using the set builder notation.

- $E = \{2, 4, 6, 8, 10, \dots\}$
- $A = \{\text{Brad Pitt, Matt Damon, Meryl Streep, ...}\}$

# Sets

**Exercise:** Rewrite the following sets using the set builder notation.

- $E = \{2, 4, 6, 8, 10, \dots\}$

$$E = \{n \mid n \text{ is a positive even integer}\}$$

- $A = \{\text{Brad Pitt, Matt Damon, Meryl Streep, ...}\}$

$$A = \{z \mid z \text{ is a Hollywood actor}\}$$

- The set of rationals

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0 \right\}$$

# Sets

## Three definitions and a question.

- ① **Subset/superset:** The set  $A$  is a subset of  $B$  (and  $B$  a superset of  $A$ ) if and only if every element of  $A$  is an element of  $B$ , i.e.,

$$\forall(x \in A \rightarrow x \in B).$$

To denote this, we write  $A \subseteq B$ .

- ② We say that  $A$  is a **proper subset** of  $B$  (we write  $A \subset B$ ) if

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A).$$

- ③ **Equal sets:** Two sets  $A, B$  are equal if and only

$$\forall x(x \in A \leftrightarrow x \in B).$$

We write  $A = B$ . Equivalently, this means  $A$  is a subset of  $B$  and  $B$  is a subset of  $A$

# Sets

- **Exercise:** Prove that for any subset  $S$ ,  $\emptyset \subseteq S$ . (blackboard)
  - Continuing with definitions...
  - **Size/cardinality of a set:** If there are exactly  $n$  distinct elements, we say that the set is finite and the cardinality is  $n$ . We write  $|S| = n$  to denote the size. When a set is not finite, it is infinite.
  - Can two sets be equal if they have different cardinalities? (blackboard)
  - **Power set:** Given a set  $S$ , the power set  $\mathcal{P}(S)$  is the set of all possible subsets of  $S$ .
- Example:** What is the power set of  $\{0, 1, 2\}$ ? (blackboard)

# Truth set

- A truth set is a special type of a set.
- **Definition:** The truth set of a statement  $P(x)$  is the set of all values of  $x$  that make the statement  $P(x)$  true, i.e.,

$$\text{Truth set of } P(x) := \{x | P(x)\}.$$

- **Example 1:**  $P(n) := n$  is an even prime number  
The truth set is  $\{2\}$ , since 2 is the only even prime number
- **Example 2:** Let  $Q(x)$  be  $x + 1 = 0$ 
  - If the domain of  $x$  is the set of naturals, the truth set is the empty set  $\{\}$  denoted as  $\emptyset$ .
  - If the domain is the set of integers, the truth set is  $\{-1\}$ .

# Operations on sets

- The intersection of two sets  $A, B$  is denoted  $A \cap B$  and is defined as follows:

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

- The union of  $A, B$  is the set of  $A \cup B$  and is defined as follows:

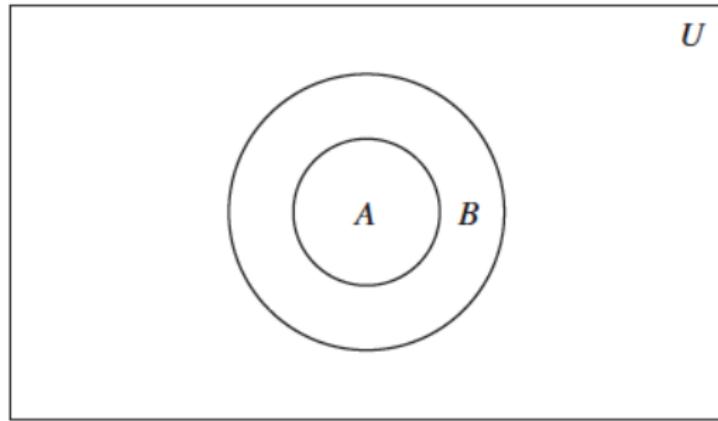
$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}.$$

- The difference of  $A, B$  is the set  $A \setminus B$  (also denoted as  $A - B$ ) defined as follows:

$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}.$$

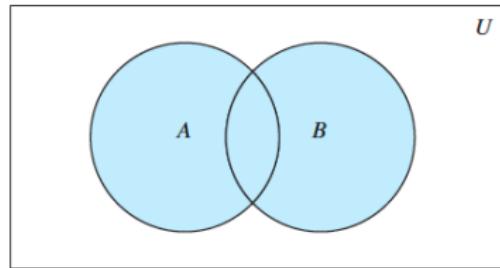
- The complement  $\bar{A}$  of a set  $A$  is defined as  $\bar{A} := \text{Domain} \setminus A$ . We refer to the domain frequently as *universe* and we denote it as  $U$ .

# Venn diagrams



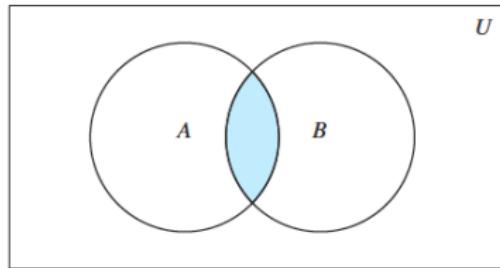
**FIGURE 2** Venn diagram showing that  $A$  is a subset of  $B$ .

# Venn diagrams



$A \cup B$  is shaded.

**FIGURE 1** Venn diagram of the union of  $A$  and  $B$ .



$A \cap B$  is shaded.

**FIGURE 2** Venn diagram of the intersection of  $A$  and  $B$ .

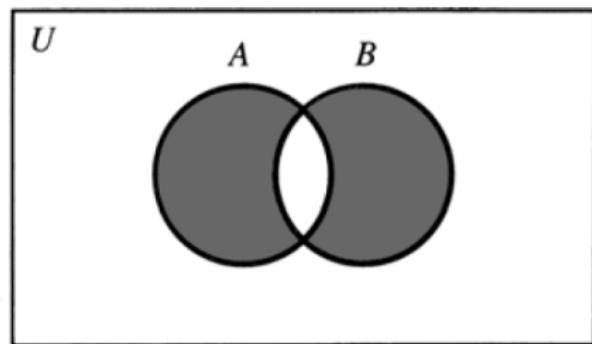
# Problems on sets – Exercise

- Suppose  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{2, 4, 6, 8, 10\}$ .
  - Visualize the sets using Venn diagrams
  - List the elements of the following sets
    - ①  $A \cap B$
    - ②  $A \cup B$
    - ③  $A \setminus B$
    - ④  $(A \setminus B) \cup (B \setminus A)$
    - ⑤  $(A \setminus B) \cap (B \setminus A)$
  - Prove that  $|A \cup B| = |A| + |B| - |A \cap B|$ . Generalize.

[Proof on blackboard]

# Symmetric difference

- The set  $(A \setminus B) \cup (B \setminus A)$  is an important set.
- The corresponding operation is also known as the symmetric difference of  $A, B$  and is denoted as  $A \triangle B$



$$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

## Problems on sets – Exercise

- Let  $A, B$  be sets such that  $A \cap B = A$ . Prove that  $A \subseteq B$ .

To prove this, we follow the steps we have seen in class

- ① Read carefully. What is given to you, and what is asked?

**Understand the problem!**

- ② Design a proof strategy.

- ③ Complete the proof.

- Ideas?

## Problems on sets – Exercise

Let's identify what is given, and what we are being asked to prove.

- **Givens:**  $A \cap B = A$
- **Goal:**  $\forall x(x \in A \rightarrow x \in B)$

Therefore, we may design a direct proof, where we consider an arbitrary  $x \in A$ , and prove  $x \in B$ .

- **Givens:**  $A \cap B = A$ , arbitrary  $x \in A$
- **Goal:**  $x \in B$

## Problems on sets – Exercise

Therefore a direct proof outline would like this:

- Suppose  $A \cap B = A$ .
- Choose an arbitrary  $x$
- Prove that if  $x \in A$  then  $x \in B$
- Since  $x$  was arbitrary we can conclude that  $A \subseteq B$ .
- Now that we have designed the proof, and filled all the details, we write it down nicely.

**Proof:** Suppose  $A \cap B = A$ , and  $x \in A$ . Since  $A = A \cap B = A$ ,  $x \in A \cap B$  and therefore  $x \in B$  as well. Therefore,  $A \subseteq B$ . **QED**

# Problems on sets – Exercise

- Prove that  $\overline{A \cap B} = \bar{A} \cup \bar{B}$  (first De Morgan law for sets.)

$$\begin{aligned}\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol} \\&= \{x \mid x \in \bar{A} \vee x \in \bar{B}\} && \text{by definition of complement} \\&= \{x \mid x \in \bar{A} \cup \bar{B}\} && \text{by definition of union} \\&= \bar{A} \cup \bar{B} && \text{by meaning of set builder notation}\end{aligned}$$

# Set identities

TABLE 1 Set Identities.

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

try proving a couple for practice, example on blackboard

# Sequence

- **Definition:** A sequence is a special type of a function....  
from a subset of the set of integers (usually either the set  $\{0, 1, 2, \dots\}$  or the set  $\{1, 2, 3, \dots\}$ )  
to a set  $S$ .  
We frequently denote the sequence as  $\{a_n\}$ .  
We use the notation  $a_n$  to denote the image of the integer  $n$ .
- $a_n$  is a term of the sequence.
- **Question:** what is the  $n$ -th term of a sequence?
  - **Answer:** Depends where the index starts from!
    - If the sequence is  $a_0, a_1, \dots$  the  $n$ -th term is  $a_{n-1}$
    - If the sequence is  $a_1, a_2, \dots$  the  $n$ -th term is  $a_n$

# Sequences

- $x_n = \frac{1}{n}, n \in \mathbb{Z}^+$
- $\{y_n\}_{n \geq 0}$  where  $y_n = 1 + 2n$ 
  - List the first 3 terms.
    - $y_0 = 1 + 2 * 0 = 1, y_1 = 1 + 2 = 3, y_2 = 1 + 2 * 2 = 5$
- $\{z_n\}_{n \geq 0}$  where  $z_n = 10^5 - 31n$ 
  - Arithmetic progression (AP):
$$x_0 = a, x_1 = a + d, x_2 = a + 2d, \dots, x_n = a + nd, \dots$$

$a$  initial term,  $d$  difference
- $\{a_n\}_{n \geq 0}$  where  $a_n = 3 * 7^n$ 
  - Geometric progression (GP):
$$x_0 = a, x_1 = ar, x_2 = ar^2, \dots, x_n = ar^n, \dots$$

$a$  initial term,  $r$  common ratio

# Sequences

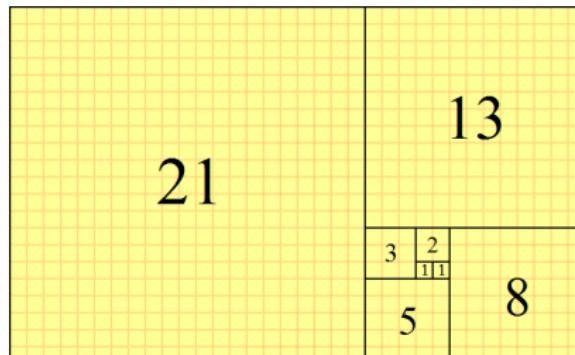
- A sequence can be specified via a **a recurrence relation**. We express  $a_n$  as a function of one or more previous terms of the sequence:

- $a_n = a_{n-1} + 3, a_1 = 20$ . List the first three terms of the sequence.

$$a_1 = 20, a_2 = a_{2-1} + 3 = a_1 + 3 = 23, a_3 = a_2 + 3 = 26$$

Can we get a **closed formula**? What kind of sequence is  $\{a_n\}$ ?

- Can you define a sequence after looking the next Figure?



# Fibonacci sequence



Italian mathematician (12th century)

**Definition:** The Fibonacci sequence  $f_0, f_1, f_2, \dots$  is defined by the initial conditions  $f_0 = 0, f_1 = 1$  and the recurrence

$$f_n = f_{n-1} + f_{n-2}, n = 2, 3, \dots$$

List the five first terms of the Fibonacci sequence. Blackboard

[https://www.youtube.com/watch?v=DRjFV\\_DETKQ](https://www.youtube.com/watch?v=DRjFV_DETKQ)

# Summations and multiplications

- To express the sum of  $a_m, a_{m+1}, \dots, a_n$  we write

$$\sum_{k=m}^n a_k,$$

or

$$\sum_{m \leq k \leq n} a_k,$$

or

$$\sum_{k=0}^{n-m} a_{m+k}.$$

- Variable  $k$  is index of summation. We could have used any other letter, namely  $\sum_{k=m}^n a_k = \sum_{i=m}^n a_i$ .

# Summations and multiplications

- Express the following sums and products using the  $\Sigma$ ,  $\prod$  notation:

①  $1 + 2 + 3 + \dots + 100$

②  $7 + 11 + 15 + 19 + 23$

③  $1 + 3 + 9 + 27 + 81$

and ... and “outlier” example

④  $100 + 150 + 219 + 220$

⑤  $1 * 3 * 5 * 7$

# Summations and multiplications

- Express the following sums using the  $\Sigma$  notation:

**Rule of thumb:** The key is to identify the sequence whose terms we are summing

$$① 1 + 2 + 3 + \dots + 100 = \sum_{i=1}^{100} i$$

$$② 7 + 11 + 15 + 19 + 23 = \sum_{k=0}^4 (7 + 4k)$$

$$③ 1 + 3 + 9 + 27 = \sum_{j=0}^3 3^j$$

and ... and “outlier” example where there is no clear sequence

$$④ 100 + 150 + 219 + 220 = \sum_{i \in \{100, 150, 219, 220\}} i$$

$$⑤ 1 * 3 * 5 * 7 = \prod_{i=1}^4 (2 * i - 1) = \prod_{i=0}^3 (2 * i + 1)$$

# Summations and multiplications

- To express the product of  $a_m, a_{m+1}, \dots, a_n$  we write

$$\prod_{k=m}^n a_k,$$

or

$$\prod_{m \leq k \leq n} a_k,$$

or

$$\prod_{k=0}^{n-m} a_{m+k}.$$

# Evaluating summations and multiplications

①  $\sum_{i=1}^{100} i$



Carl Friedrich Gauss (1777-1855)

1.  $1+100=101$

2.  $2+99=101$

⋮

49.  $49+52=101$

50.  $50+51 =101$

Therefore the sum is  $50 \times 101 = 5050$ .

# Evaluating summations and multiplications

- ① In general when we sum the  $n$  terms of an AP  $\{a_n\}$  with initial term  $a_1$  and difference  $d$  the sum is

$$\sum_{i=1}^n a_i = n \frac{a_1 + a_n}{2} = \frac{n}{2}(2a_1 + (n-1)d).$$

- ② Compute the sum  $\sum_{i=51}^{100} i$ :

- $\sum_{i=1}^{100} i - \sum_{i=1}^{50} i = 50 * 101 - 25 * 51 = 3775$   
or ... just
- $\sum_{i=51}^{100} i = \frac{50}{2}(51 + 100) = 25 * 151 = 3775$

- ③ For summing terms of a geometric series with initial term  $a$  and ratio  $r \neq 0, 1$  we have (proof [Rosen p. 174, and blackboard])

$$\sum_{j=0}^n ar^j = \frac{ar^{n+1} - a}{r - 1}.$$

# Higher order sums

- Double, triple and higher order summations appear in many contexts.
- One needs to be careful, i.e., understand what they are summing over.
- Example.

$$\begin{aligned}\sum_{i=1}^4 \sum_{j=1}^3 ij &= \sum_{i=1}^4 (i + 2i + 3i) = \\ \sum_{i=1}^4 (6i) &= 6 \sum_{i=1}^4 i = 6(1 + 2 + 3 + 4) = 60.\end{aligned}$$

## Another double summation

Evaluate  $\sum_{i=0}^2 \sum_{j=0}^3 (2i + 3j)$ .

- The inner sum is:

$$\begin{aligned}\sum_{j=0}^3 (2i + 3j) &= \sum_{j=0}^3 2i + \sum_{j=0}^3 3j \\&= 2i \sum_{j=0}^3 1 + 3 \sum_{j=0}^3 j \\&= 2i(4) + 3(0 + 1 + 2 + 3) \\&= 8i + 18.\end{aligned}$$

## Another double summation

Evaluate  $\sum_{i=0}^2 \sum_{j=0}^3 (2i + 3j)$ .

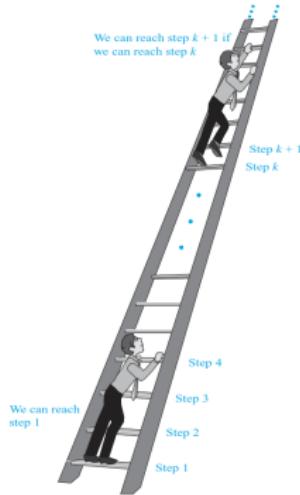
- The outer sum is therefore:

$$\begin{aligned}\sum_{i=0}^2 \left( \sum_{j=0}^3 (2i + 3j) \right) &= \sum_{i=0}^2 (8i + 18) = \sum_{i=0}^2 8i + \sum_{i=0}^2 18 \\ &= 8 \sum_{i=0}^2 i + 18 \sum_{i=0}^2 1 = 8(0 + 1 + 2) + 18(3) \\ &= 24 + 54 = 78.\end{aligned}$$

# Lecture 10 (10/3) Outline

- Mathematical induction [[Rosen 5.1](#)]
- **Remark** Everything up to this point (including 5.1) will be tested in midterm 1.

# Stairway to heaven



- ① We can reach the first rung of the ladder.
- ② If we can reach a particular rung of the ladder, then we can reach the next rung.

Can we reach every rung of this infinite ladder?

# Principle of mathematical induction

- **Goal:** The typical goal is to prove statements of the form “ $P(n)$  is true for all positive integers  $n$ ”.

- ① **Basis step:** We verify that  $P(1)$  is true.

**Analogy:** first rung of the ladder

- ② **Inductive step:** We show that the conditional statement  $P(k) \rightarrow P(k + 1)$  is true for all positive integers  $k$ .

**Analogy:** If we can reach a particular rung of the ladder, then we can reach the next rung.

As a rule of inference we can write:

$$P(1) \wedge \forall k (P(k) \rightarrow P(k + 1)) \rightarrow \forall n P(n).$$

# Practice problems

Use mathematical induction to prove the following statements.

- ①  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ .
- ② Conjecture a formula for the sum of the first  $n$  positive odd integers. Then prove your conjecture using mathematical induction
- ③  $2^n < n!$  for every integer  $n \geq 4$
- ④  $\sum_{j=0}^n ar^j = a\frac{r^{n+1}-1}{r-1}$ ,  $r \neq 1$
- ⑤  $\overline{\bigcap_{j=1}^n A_j} = \bigcup_{j=1}^n \overline{A_j}$  for  $n \geq 2$  (generalization of De Morgan's law)

# Lecture 11 (10/8) Outline

- Mathematical induction (cont.) [Rosen 5.1]
- Strong induction [Rosen 5.2]

## Practice problem

Let  $n \geq 0$  be an integer. Consider the following sum:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)}.$$

- ① Express the formula using the  $\sum$ ,  $\prod$  notation
- ② Conjecture a formula about this sum
- ③ Prove it use it induction

# Creative uses of mathematical induction

- **Theorem:** Let  $n$  be a positive integer. Show that every  $2^n \times 2^n$  checkerboard with one square removed can be tiled using right triominoes, where these pieces cover three squares at a time.



# Basis

- Let  $P(n)$  be the proposition that every  $2^n \times 2^n$  checkerboard with one square removed can be tiled using right triominoes.
- We will use induction.
- Basis  $n = 1$ :  $P(1)$  is true. There are four cases (i.e., defined by where is the missing square), and for each one we can tile the board with one right triomino.

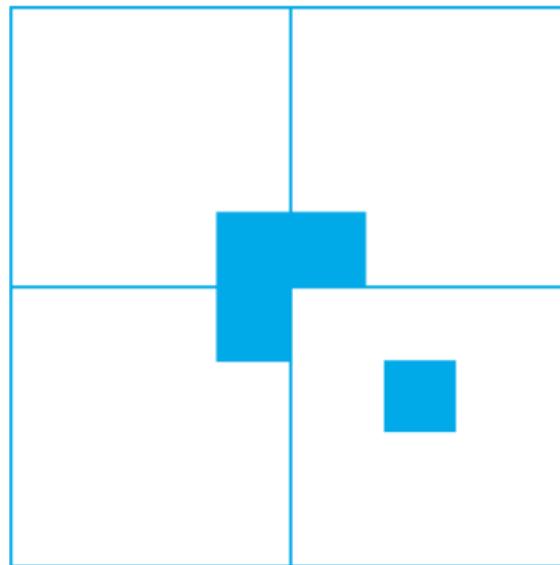


# Inductive step

- The inductive hypothesis is the assumption that  $P(k)$  is true for the positive integer  $k$
- It must be shown that under the assumption of the inductive hypothesis, that  $P(k + 1)$  must also be true
- **Question:** What is  $P(k + 1)$ ? (in English)

Ideas?

## Inductive step



**FIGURE 7** Tiling the  $2^{k+1} \times 2^{k+1}$  Checkerboard with One Square Removed.

# Principle of Strong induction

- **Goal:** The typical goal is to prove statements of the form “ $P(n)$  is true for all positive integers  $n$ ”.

- ① **Basis step:** We verify that  $P(1)$  is true.

**Analogy:** first rung of the ladder

- ② **Inductive step:** We show that the conditional statement  $P(1) \wedge P(2) \wedge \dots \wedge P(k) \rightarrow P(k + 1)$  is true for all positive integers  $k$ .

**Analogy:** If we can reach all the first  $k$  rungs, we can reach the  $(k + 1)$  rung.

## Practice problems

- Show that if  $n$  is an integer greater than 1, then  $n$  can be written as a product of primes. integer  $k$
- Every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.
- Let  $P(n)$  be the statement that a postage of  $n$  cents can be formed using 3-cent and 5-cent stamps. Prove that for all integers  $n \geq 8$ ,  $P(n)$  is true.

Proof on blackboard

# Geometry

- A polygon is a closed geometric figure consisting of a sequence of line segments  $s_1, \dots, s_n$  called **sides**.
- A polygon is **simple** if no two non-consecutive lines intersect.
- A **diagonal** of a simple polygon is a line segment connecting two non-consecutive vertices of the polygon, and a diagonal is called an **interior diagonal** if it lies entirely inside the polygon.

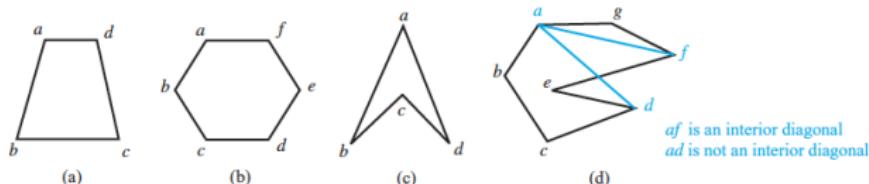


FIGURE 1 Convex and Nonconvex Polygons.

# Geometry

**Triangulation:** Division of a simple polygon into triangles by adding nonintersecting diagonals.



**Theorem :** A simple polygon with  $n$  sides, where  $n$  is an integer  $n \geq 4$  can be triangulated into  $n - 2$  triangles.

We will use the following fact without proof:

**Fact:** Every simple polygon with at least four sides has an interior diagonal.

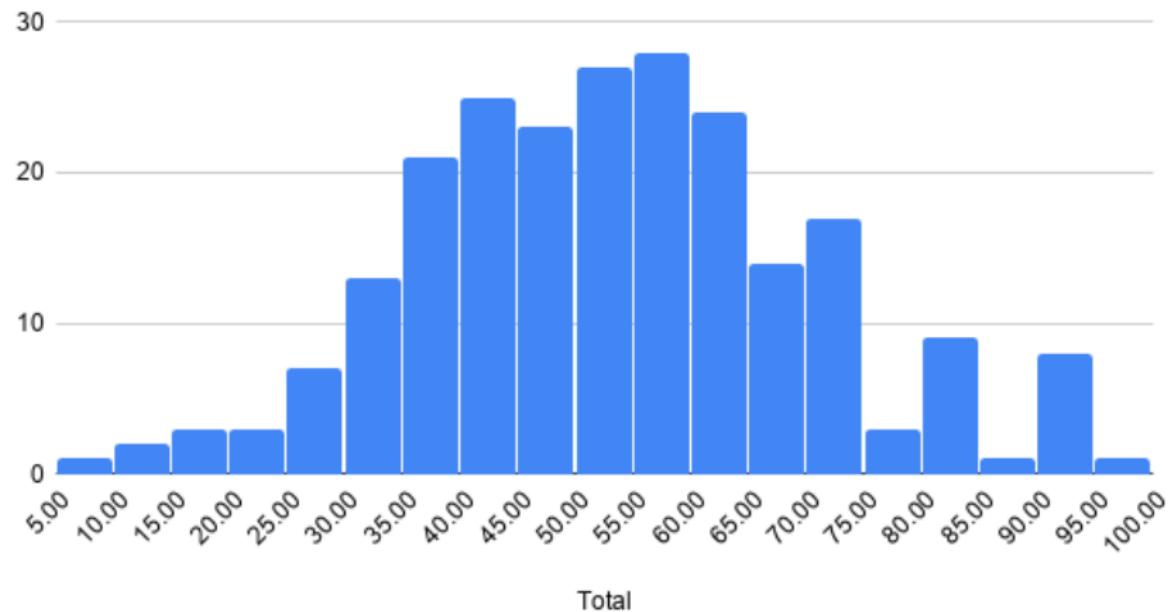
Proof on blackboard

# Lecture 12 (10/22) Outline

- Big- $O$ , big- $\Omega$  and big- $\Theta$  notation [Rosen 3.2]
- Master theorem for recurrences [Rosen 8.3.2]
- Recursive algorithms [Rosen 3.1, 5.4, 8.3.2] (to be continued)

# Midterm grades

Histogram of Total



## From last time (reminder)

**Theorem:** Prove that every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.

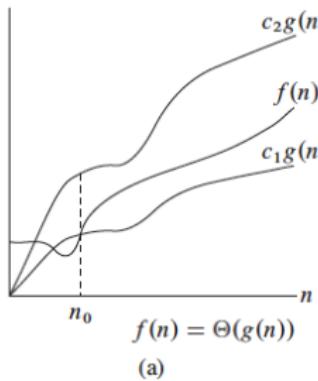
### Strong Induction

- Let  $P(n)$  be the statement that postage of  $n$  cents can be formed using 4-cent and 5-cent stamps.
- Basis.** We proved  $P(12)$ ,  $P(13)$ ,  $P(14)$ , and  $P(15)$  (i.e., that they are true) (why?)
- Inductive step.** We proved  $P(k - 3) \rightarrow P(k + 1)$  (how?)

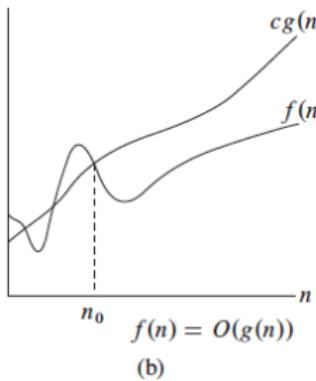
# Big $\mathcal{O}$ , $\Theta$ notation

- We will be interested in the worst-case **asymptotic** running time of an algorithm. This is a function  $T(n)$  which is a function whose domain is the set of natural numbers  $\mathbb{N}$  (integer input sizes).
- Big- $O$  notation provides a way to describe asymptotic **upper bounds**.
- Big- $\Omega$  notation provides a way to describe asymptotic **lower bounds**.
- Big- $\Theta$  notation provides a way to describe tight **asymptotic upper bounds**.

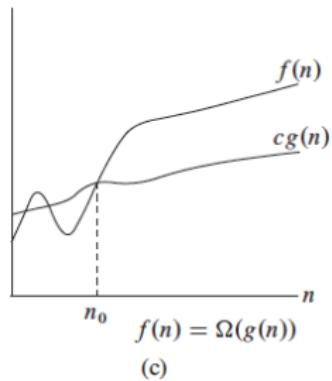
# Big $\mathcal{O}$ , $\Theta$ notation



(a)



(b)



(c)

**Question:** Can we attempt a definition for  $\mathcal{O}$ ,  $\Theta$ ,  $\Omega$  notation based on this figure?

# Big $\mathcal{O}$ notation –definition

## Definition:

- Let  $f$  and  $g$  be functions from  $\mathbb{Z}$  or  $\mathbb{R}$  to  $\mathbb{R}$ .
- We say  $f(n) \in O(g(n))$  (or just  $f(n)$  is  $O(g(n))$ ) if there are constants  $C$  and  $k$  such that

$$|f(n)| \leq C|g(n)|$$

whenever  $n > k$ .

**Remark:** This is read as “ $f(n)$  is big-oh of  $g(n)$ .”

## Big $\mathcal{O}$ notation –example

**Exercise:** Prove that  $f(x) = x^2 + 2x + 1$  is  $O(x^2)$ .

- Observe that when  $x > 1$  then  $x < x^2, 1 < x$
- Therefore  $f(x) = x^2 + 2x + 1 < 4x^2$  when  $x > 1$
- Hence by setting  $C = 4, k = 1$  we observe that  $|f(x)| \leq C|g(x)|$  when  $x > k$ .
- We conclude  $f(x) \in O(x^2)$ .

## Big $\mathcal{O}$ notation –remarks

- Notice we write  $f(n) \in O(n^2)$ .
- $O(n^2)$  is a **set** of functions!
- $O(n^2) = \{f(n) : \text{there exist positive constants } C, k \text{ such that } |f(n)| \leq Cn^2 \text{ for all } n > k\}$

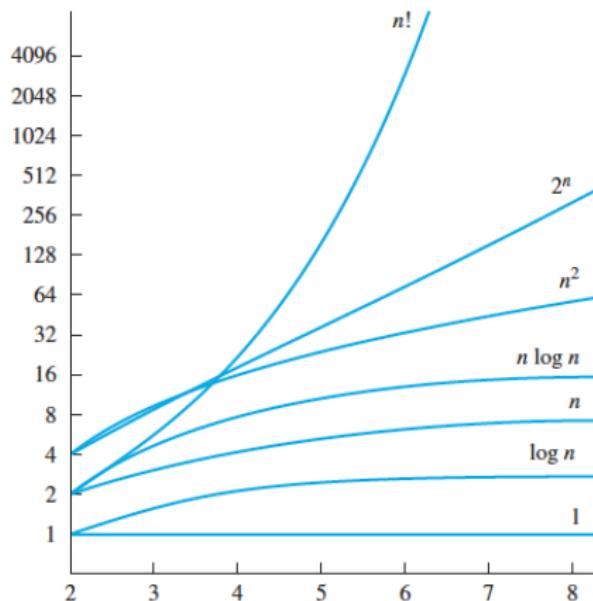
# Big $\mathcal{O}$ notation –remarks

## Theorem

Let  $f(x) = \sum_{i=0}^n a_i x^i$  where  $a_0, \dots, a_n$  are reals. Then  $f(x)$  is  $O(x^n)$ .

Proof details on blackboard

# Big $\mathcal{O}$ notation –remarks



**FIGURE 3** A Display of the Growth of Functions Commonly Used in Big- $O$  Estimates.

# Big $\Omega$ notation –definition

## Definition:

- Let  $f$  and  $g$  be functions from  $\mathbb{Z}$  or  $\mathbb{R}$  to  $\mathbb{R}$ .
- We say  $f(n) \in \Omega(g(n))$  (or just  $f(n)$  is  $\Omega(g(n))$ ) if there are constants  $C$  and  $k$  such that

$$|f(n)| \geq C|g(n)|$$

whenever  $n > k$ .

**Remark 1:** This is read as “ $f(n)$  is big-omega of  $g(n)$ .”

**Alternative definition:**  $f(n)$  is  $\Omega(g(n))$  if and only if  $g(n)$  is  $O(f(n))$

# Big Θ notation

## Definition.

- Let  $f$  and  $g$  be functions from  $\mathbb{Z}$  or  $\mathbb{R}$  to  $\mathbb{R}$ .
- We say  $f(n)$  is  $\Theta(g(n))$  if  $f(n)$  is  $O(g(n))$  and  $f(n)$  is  $\Omega(g(n))$ .

**Question:** Suppose someone tells you the worst-case running time is  $\Theta(n \log n)$ . What should you understand?

# Big Θ notation

- It is important to always keep in mind that  $\Theta(n \log n)$  is a set of functions. In the context of what you heard:
- $\Theta(n \log n) = \{f(n) : \text{there exist positive constants } c_1, c_2 \text{ and } k \text{ such that } 0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for all } n > k\}$
- Essentially we think of the running time as a function  $Cn \log n$  for some constant  $C$

# Master theorem

- Suppose we can break down a problem of size  $n$  into  $a$  subproblems of size  $n/b$ . The running time  $T(n)$  is naturally described as a recurrence.
- The next theorem provides a recipe to solve such recurrences that naturally occur when we design algorithms.

**MASTER THEOREM** Let  $f$  be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + cn^d$$

whenever  $n = b^k$ , where  $k$  is a positive integer,  $a \geq 1$ ,  $b$  is an integer greater than 1, and  $c$  and  $d$  are real numbers with  $c$  positive and  $d$  nonnegative. Then

$$f(n) \text{ is } \begin{cases} O(n^d) & \text{if } a < b^d, \\ O(n^d \log n) & \text{if } a = b^d, \\ O(n^{\log_b a}) & \text{if } a > b^d. \end{cases}$$

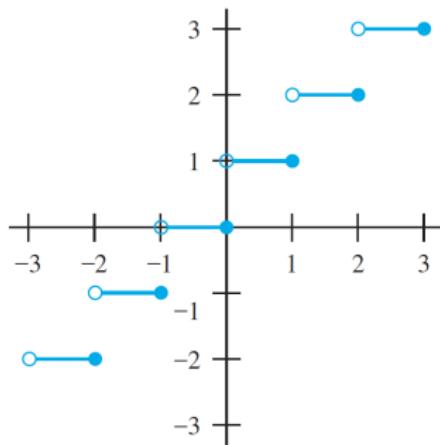
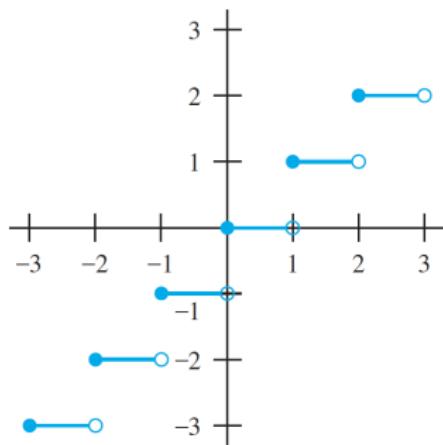
## Master theorem – some remarks

- Master theorem is true even when  $n$  is not a power of  $b$ . We will discuss this in the next lecture, when we will also see the functions of floors and ceilings.
- Not all recurrences are solved by the master theorem. However, it is a powerful tool to solve recurrences.
- **Example:** Let's solve this recurrence  $T(n) = T(n/2) + 5$  (more next time)

# Lecture 13 (10/24) Outline

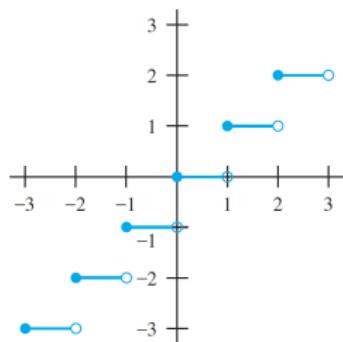
- Floors and ceilings [Rosen 2.3.5]
- Master theorem for recurrences [Rosen 8.3.2] (cont.)
- Recursive algorithms [Rosen 3.1, 5.4, 8.3.2] (to be continued)

# Floors and ceilings

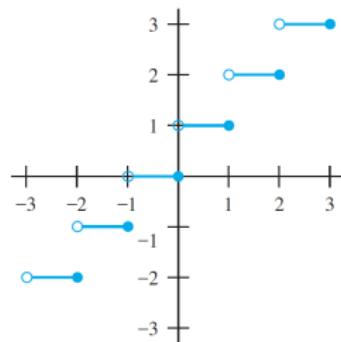


- Can you describe what these two functions do?

# Floors and ceilings



(a)  $y = [x]$



(b)  $y = [x]$

For any real number  $x$  we denote:

- ① using  $\lfloor x \rfloor$  the largest integer that is less than or equal to  $x$
- ② using  $\lceil x \rceil$  the smallest integer that is greater than or equal to  $x$

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1.$$

# Floors and ceilings

- $\lceil 3.5 \rceil = ?$
- $\lfloor 3.5 \rfloor = ?$
- $\lceil -0.1 \rceil = ?$
- $\lfloor -0.1 \rfloor = ?$
- Express the quotient and the remainder of  $a$  divided by  $n$  using floors/ceilings
- True or False:  $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = n$  for any integer  $n$
- True or False:  $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$  for all real numbers  $x, y$

# Floors and ceilings

[Explanation on the blackboard]

- $\lceil 3.5 \rceil = 4$
- $\lfloor 3.5 \rfloor = 3$
- $\lceil -0.1 \rceil = 0$
- $\lfloor -0.1 \rfloor = -1$
- $a - n \cdot \lfloor a/n \rfloor$
- True
- False

# Master theorem

**MASTER THEOREM** Let  $f$  be an increasing function that satisfies the recurrence relation

$$f(n) = af(n/b) + cn^d$$

whenever  $n = b^k$ , where  $k$  is a positive integer,  $a \geq 1$ ,  $b$  is an integer greater than 1, and  $c$  and  $d$  are real numbers with  $c$  positive and  $d$  nonnegative. Then

$$f(n) \text{ is } \begin{cases} O(n^d) & \text{if } a < b^d, \\ O(n^d \log n) & \text{if } a = b^d, \\ O(n^{\log_b a}) & \text{if } a > b^d. \end{cases}$$

- $a \geq 1, b > 1$  are constants

# Master theorem – important remark

**Question:** What happens when  $n$  is not a power of  $b$ ?

- Then at some level of the recursion the argument of  $f$  is no longer an integer. **problem, as we are dealing with integers**
- The master theorem remains valid as long as we interpret  $n/b$  as  $\lfloor n/b \rfloor$  or  $\lceil n/b \rceil$
- **Example:** The recurrence  $f(n) = f(\lfloor \frac{n}{2} \rfloor) + f(\lceil \frac{n}{2} \rceil) + cn^d$  has the same asymptotic behavior with  $f(n) = 2f(n/2) + cn^d$ .

$$T(n) = 2T(\lfloor \frac{n}{2} \rfloor) + n$$

- Let's apply the master theorem:
- $a = 2$
- $b = 2$
- $d = 1$
- We observe that  $b^d = 2^1 = 2 = a$ .

Therefore, by the master theorem  $T(n) = O(n \log n)$ .

$$T(n) = 9T\left(\frac{n}{3}\right) + n$$

- Let's apply the master theorem
- $a = 9$
- $b = 3$
- $d = 1$
- We observe that  $b^d = 3^1 = 3 < 9 = a$ .

Therefore, by the master theorem  $T(n) = O(n^{\log_b(a)}) = O(n^2)$

$$T(n) = 2T(\lfloor \sqrt{n} \rfloor) + \log n$$

Any ideas?

$$T(n) = 2T(\lfloor \sqrt{n} \rfloor) + \log n$$

## Change of variables

- Set  $m = \log n$
- Then we get  $T(2^m) = 2T(2^{m/2}) + m$
- Let  $S(m) = T(2^m)$ . Then  $S(m) = 2S(m/2) + m$ .
- Therefore  $S(m) = O(m \log m)$
- We conclude  $T(n) = S(m) = O(m \log m) = O(\log n \log \log n)$

$$T(n) = 2T(\lfloor \frac{n}{2} \rfloor) + n$$

We can also solve recurrences using induction! The approach I will sketch is known as the substitution method.

- ① Guess the form of the solution.

**Remark:** There is no general way to guess the correct solution.  
Requires experience and creativity.

- We guess  $T(n) = O(n \log n)$ .

- ② Use (strong) induction to prove that for all  $n \geq n_0$  ( $n_0$  also to be found)  $T(n) \leq cn \log n$  for some constant  $c$  ( $c$  to be found too).

# Algorithm design – Compute powers $a^n$

- Given a non-zero real number  $a$  and a non-negative integer  $n$ , design a recursive algorithm to compute  $a^n$

## Details on the blackboard

- Formalize the problem
- Design algorithm and prove its correctness
- Analyze the running time

# Lecture 14 (10/29) Outline

- Recursive algorithms [Rosen 3.1, 5.4, 8.3.2] (to be continued)
  - Binary search
  - Euclid's algorithm
- Introduction to number theorem [Rosen 4.1.1, 4.1.2, 4.13., 4.2.2]

# Algorithm design - binary search algorithm

- Given a sorted array of numbers, how fast can we decide if some number  $x$  is in our array?

Details on the blackboard

- Formalize the problem
- Design algorithm
- Running time analysis using the master theorem

# Algorithm design - how to compute the greatest common divisor (gcd)

- The greatest common divisor (gcd) of two (**or more integers**), which are not all zero, is the largest positive integer that divides each of the integers.
    - $\text{gcd}(100, 0) = 100$
    - $\text{gcd}(8, 4) = 4$
    - $\text{gcd}(8, 12) = 4$
    - $\text{gcd}(3, 10) = 1$
- We say that 3, 10 are relatively prime (or coprime)

**Problem:** How do we compute the gcd of two integers?

# Division – basics

- Let  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ . We say that  $a$  divides  $b$ , or that  $b$  is a multiple of  $a$  (**notation**  $a|b$ ) if there is an integer  $k$  such that  $b = k \cdot a$ .
- **Exercise:**
  - if  $a|b, a|c$  then  $a|(b + c)$
  - if  $a|b$  then  $a|bc$  for all integers  $c$
  - if  $a|b$  and  $b|c$ , then  $a|c$
- **Division algorithm:** Let  $a$  be an integer and  $d$  a positive integer. Then there are unique integers  $q, r$  with  $0 \leq r < d$  such that  $a = d \cdot q + r$ .
  - $q = \lfloor \frac{a}{d} \rfloor$  is the quotient. We also use the notation  $q := \text{adivd}$
  - $r = a - d \lfloor \frac{a}{d} \rfloor$  is the remainder. We also use the notation  $r := a \bmod d$

# Algorithm design - $gcd(a, b)$ Euclidean algorithm by subtraction

```
gcd(a, b)
if a = b then
    Return a
end if
if a > b then
    return gcd(a - b, b)
else
    return gcd(a, b - a)
end if
```

- Key fact for proving correctness.  $gcd(a, b) = gcd(a, b - a)$   
Let  $c = gcd(a, b)$ . To prove this we need to prove that  $c$  is a common divisor of  $a, b$  and it is the largest possible divisor.

# Algorithm design - $gcd(a, b)$ Euclidean algorithm by division

```
gcd(a, b)
if a mod b = 0 then
    Return b
else
    return gcd(b, a mod b)
end if
```

See homework 7

# Representations of integers

## Theorem

Let  $b$  be an integer greater than 1. Then if  $n$  is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0,$$

where:

- $k$  is a non-negative integer
- $a_0, \dots, a_k$  are non-negative integers less than  $b$
- $a_k \neq 0$ .

# Representations of integers

## Some important bases:

- When  $b = 10$ , the *base b expansion of n* is called **decimal**.
- When  $b = 2$ , the *base b expansion of n* is called **binary**.
- When  $b = 8$ , the *base b expansion of n* is called **octal**.
- When  $b = 16$ , the *base b expansion of n* is called **hexadecimal**.

## From $b = 2, 8, 16$ to decimal – Examples

**Question:** What is the decimal expansion of the integer that has  $(a_k a_{k-1} \dots a_0)_b$  as its base  $b$  expansion?

- $(10001)_2$
- $(111)_2$
- $(2341)_8$
- $(ABCD1EF9)_{16}$ 
  - Hex digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Blackboard

# From decimal to $b = 2, 8, 16$

**Question:** What is the binary/octal/hexadecimal expansion of the integer that has  $(a_k a_{k-1} \dots a_0)_{10}$  as its decimal expansion?

- Find the binary expansion of  $(2)_{10}, (17)_{10}, (241)_{10}$
- Find the octal expansion of  $(12345)_{10}$ .
- Find the hexadecimal expansion of  $(177130)_{10}$

**On the blackboard**

# Conversion between binary, octal, hexadecimal

## Observations

- ① Each octal digit corresponds to a block of three binary digits
- ② Each hexadecimal digit corresponds to a block of four binary digits

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

# Conversion between binary, octal, hexadecimal

## On the blackboard

- ① Find the octal and hexadecimal expansions of  
 $(11111010111100)_2$ .
  
  
  
  
  
  
  
  
- ② The binary expansions  $(765)_8$ ,  $(A8D)_{16}$ .

# Lecture 15 (10/31) Outline

- GCD, its properties, and the extended Euclidean algorithm  
[Rosen 4.3]

**Remark:** Everything up to here (including this lecture) can be tested in midterm 2.

# $\gcd(a, b)$ as linear combination of $a, b$

## Theorem

*The greatest common divisor of  $a$  and  $b$  is equal to the smallest positive linear combination of  $a$  and  $b$ .*

## Corollary

*An integer is linear combination of  $a$  and  $b$  iff it is a multiple of  $\gcd(a, b)$ .*

## Proof on blackboard

# Properties of the gcd

- ① Every common divisor of  $a, b$  divides  $\gcd(a, b)$
- ② Let  $k \in \mathbb{Z}^+$ . Then  $\gcd(ka, kb) = k\gcd(a, b)$
- ③ If  $\gcd(a, b) = 1$ , and  $\gcd(a, c) = 1$  then  $\gcd(a, bc) = 1$
- ④ If  $a|bc$  and  $\gcd(a, b) = 1$  then  $a|c$
- ⑤  $\gcd(a, b) = \gcd(b, a \bmod b)$

**Proof on blackboard**

# Euclidean algorithm

The Euclidean algorithm for computing the gcd of  $a, b$  is based on

$$gcd(a, b) = gcd(b, a \bmod b).$$

Let's compute the  $gcd(662, 414)$ .

$$662 = 1 \cdot 414 + 248$$

$$414 = 1 \cdot 248 + 166$$

$$248 = 1 \cdot 166 + 82$$

$$166 = 2 \cdot 82 + 2$$

$$82 = 41 \cdot 2 + 0$$

Therefore,  $gcd(662, 414) = 2$ .

# Extended Euclidean algorithm

- With some extra book keeping we can find the coefficients that give us the  $\gcd(a, b)$  as a linear combination of  $a, b$

$$\begin{aligned}2 &= 166 - 2 \cdot 82 = 166 - 2 \cdot (248 - 1 \cdot 166) \\&= 3 \cdot 166 - 2 \cdot 248 = 3 \cdot (414 - 1 \cdot 248) - 2 \cdot 248 \\&= 3 \cdot 414 - 5 \cdot 248 = 3 \cdot 414 - 5 \cdot (662 - 1 \cdot 414) \\&= 8 \cdot 414 - 5 \cdot 662\end{aligned}$$

# Lecture 16 (11/5) Outline

- Primes [Rosen 4.3]
- Euler  $\phi$ -function [Rosen 4.3 (exercises 21)]
- Modular arithmetic [Rosen 4.1.4, 4.1.5]

# Primes

Theorem (Fundamental theorem of arithmetic)

*Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.*

## Examples:

①  $100 = 2^2 5^2$

②  $13 = 13$

③  $999 = 3^3 37$

④  $1024 = 2^{10}$

# Prime factorization, gcd, and lcm

- **Definition.** The least common multiple of  $a, b$  denoted as  $\text{lcm}(a, b)$  is the smallest positive integer that is divisible by both  $a, b$ .
- Let  $a = \prod_{i=1}^n p_i^{a_i}$ ,  $b = \prod_{i=1}^n p_i^{b_i}$ .
- Then,

$$\gcd(a, b) = \prod_{i=1}^n p_i^{\min(a_i, b_i)},$$

$$\text{lcm}(a, b) = \prod_{i=1}^n p_i^{\max(a_i, b_i)}.$$

- **Question:** Why don't we use this algorithm in practice to compute the  $\gcd$  instead of Euclid's algorithm?

# Primes

## Theorem

*If  $n$  is a composite integer, then  $n$  has a prime divisor less than or equal to  $\sqrt{n}$ .*

## Theorem

*There are infinitely many primes.*

## Proof on blackboard

# Euler's $\phi$ -function



In 1763 Leonhard Euler introduced the function  $\phi(n)$ .

- $\phi(n)$  is equal to the number of remainders upon division by  $n$  that are relatively prime to  $n$
- Example:  $\phi(12) = 4$  since among the remainders 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11 the ones that are relatively prime to 12 are 1, 5, 7, 11.

# Euler's $\phi$ -function

- **Exercise:** Compute  $\phi(p)$  where  $p$  is a prime.
- **Exercise:** Compute  $\phi(p^m)$  where  $p$  is a prime, and  $m$  a natural number.

## Theorem

If  $m, n$  are relatively prime natural numbers, then

$$\phi(mn) = \phi(m)\phi(n).$$

**Corollary:** If  $n = p_1^{a_1} \dots p_s^{a_s}$  is the prime factorization of  $n$ , then

$$\phi(n) = \prod_{i=1}^s (p_i^{a_i} - p_i^{a_i-1}).$$

# Lecture 17 (11/12) Outline

- Exercises on GCD
- Modular arithmetic [Rosen 4.1.4, 4.1.5]

**Blackboard lecture**

# Lecture 18 (11/14) Outline

- Linear congruences [Rosen 4.4.2]
- Fermat's little theorem and applications [Rosen 4.4.5]

**Blackboard lecture**

# Lectures 19, 20, 21 (11/19, 21, 26) Outline

- Functions [Rosen 2.3 (one-to-one, onto)]
- Basics of counting [Rosen 6.1]
- Inclusion-exclusion rule [Rosen 8.5 (up to page 583)]
- Pigeonhole principle [Rosen 6.2]
- Permutations and combinations [Rosen 6.3]
  - Intro to graphs (basics) [Rosen 10.1, 10.2.4]
- Binomial theorem and combinatorial proofs [Rosen 6.3]
- Generalized permutations and combinations [Rosen 6.3]

# Exercise

- In any party of six people either at least three of them are (pairwise) mutual strangers or at least three of them are (pairwise) mutual acquaintances.

# Motivating questions

- ① John has five shirts, and three different pairs of jeans. In how many ways can he dress himself?
- ② Each student is assigned an id, that consists of one letter, and one number (e.g., A6). How many possible ids can we create?
- ③ How many strings of DNA of length 10 can one possibly create?
  - There exist 4 nucleobases: adenine (A), cytosine (C), guanine (G), and thymine (T).
  - **Remark:** bioinformatics and computational biology revolutionize personalized medicine among many other things, and are based on numerous ideas in combinatorics.



# Product rule

- Suppose that a procedure can be broken down into a **sequence** of two tasks.
  - If there are  $n_1$  ways to do the first task and for each of these ways of doing the first task
  - there are  $n_2$  ways to do the second task,
  - then there are  $n_1 n_2$  ways to do the procedure.
- For example: John has 5 different ways to choose his shirt first. Then for each shirt, he has 3 different ways to choose his jeans. Therefore, he can dress himself in 15 ways.

# Product rule - Problems

- How many functions are there from a set with  $m$  elements to a set with  $n$  elements?
- How many one-to-one functions are there from a set with  $m$  elements to one with  $n$  elements?
- The number of different subsets of a finite set  $S$  is  $2^{|S|}$ .

**Solutions on blackboard**

# Cartesian product

- **Definition:** The *ordered n-tuple*  $(a_1, \dots, a_n)$  is an ordered collection that has  $a_i$  as its  $i$ -th element for  $i = 1, \dots, n$ .
- Let  $A, B$  be sets. The Cartesian product  $A \times B$  is defined as the set of all ordered pairs  $(a, b)$ , where  $a \in A, b \in B$ ,

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

- Remarks
  - ①  $A \times B \neq B \times A$  (why?)
  - ②  $A_1 \times A_2 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_i \in A_i \text{ for all } i = 1, \dots, n\}$
- Question: If  
 $X = \{x : -1 \leq x \leq 1, x \in \mathbb{R}\}$ ,  $Y = \{y : -1 \leq y \leq 1, y \in \mathbb{R}\}$ , what is  $X \times Y$ ?

# Product rule - Cartesian product

- $A_1 \times A_2 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_i \in A_i \text{ for all } i = 1, \dots, n\}$
- $|A_1 \times A_2 \times \dots \times A_n| = \prod_{i=1}^n |A_i|$

To choose one of  $\underbrace{\{A, B, C\}}$  these AND one of  $\underbrace{\{X, Y\}}$  these  
is to choose one of these.

$$\overbrace{\{AX, AY, BX, BY, CX, CY\}}$$

[Source [https://en.wikipedia.org/wiki/Rule\\_of\\_product](https://en.wikipedia.org/wiki/Rule_of_product)]

# Sum rule – Problems

## Sum rule:

- If a task can be done either in one of  $n_1$  ways or in one of  $n_2$  ways,
- where none of the set of  $n_1$  ways is the same as any of the set of  $n_2$  ways,
- then there are  $n_1 + n_2$  ways to do the task.

**Question:** A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

# Subtraction rule

## Sum rule:

- If a task can be done either in one of  $n_1$  ways or in one of  $n_2$  ways,
- then there are  $n_1 + n_2$  minus the number of ways to do the task that are common to the two different ways.

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

# Inclusion exclusion rule

Theorem: Let  $A_1, A_2, \dots, A_n$  be finite subsets of a set  $X$ .

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap A_{i_2} \dots \cap A_{i_k}|.$$

Another way to see this equation is by expanding the “internal” sum term.

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

# Inclusion-exclusion rule

For example, when:

- $n = 2$ ,  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$
- $n = 3$ ,  $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$
- How many integers in  $\{1, \dots, 100\}$  are not divisible by 2, or 5?

# Inclusion-exclusion rule

- The key to applying the inclusion-exclusion rule is defining the sets  $A_i$  right.
- In our problem:
  - Let  $A_i$  be the set of numbers divisible by  $i = 2, 5$
  - $A_2 \cup A_5$  corresponds to which set?
  - $|A_2| = 50, |A_5| = 20$  (why?)
  - $|A_2 \cap A_5| = 10$  (why?)
  - $|A_2 \cup A_5| = 20 + 50 - 10$
  - So how many numbers are not divisible by either 2 or 5?

## Division rule

- **Division rule:** There are  $n/d$  ways to do a task if it can be done using a procedure that can be carried out in  $n$  ways, and for every way  $w$ , exactly  $d$  of the  $n$  ways correspond to  $w$ .
- **Example.** An automated system counts the legs of cows. Assuming all cows in a farm have four legs, and the system counts 44 legs, how many cows are there in the pasture?

By the division rule, there are  $\frac{44}{4} = 11$ .

# Some Counting Problems

- ① Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?
- ② How many bit strings of length eight either start with a 1 bit or end with the two bits 00?
- ③ A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?
- ④ How many different ways are there to seat four people around a circular table, where two seatings are considered the same when each person has the same left neighbor and the same right neighbor?

**Solutions on blackboard**

# The Generalized Pigeonhole Principle

**Theorem:** If  $N$  objects are placed into  $k$  boxes, then there is at least one box containing at least  $\lceil \frac{N}{k} \rceil$  objects.

- When  $N = k + 1$  we obtain the well-known (standard) pigeonhole principle.

If  $k$  is a positive integer, and  $k + 1$  or more objects are placed into  $k$  boxes, then there is (at least) one *box* containing two or more of the objects.

# Problems

To apply the pigeonhole principle, you need to decide **what are the objects and what are the boxes.**<sup>2</sup>

- ① Show that among 100 people, two have birthday on the same month. The same claim is true for 13 people, but not for 12.
- ② Show that if we take  $n + 1$  numbers from the set  $\{1, 2, \dots, 2n\}$ , then there exist two co-primes.
- ③ Every sequence of  $n^2 + 1$  distinct real numbers contains a subsequence of length  $n + 1$  that is either strictly increasing or strictly decreasing.
- ④ (From 11/19:) In any party of six people either at least three of them are (pairwise) mutual strangers or at least three of them are (pairwise) mutual acquaintances.

---

## Solutions on blackboard

<sup>2</sup>This is not an easy task in principle!

## Remark

The proof we did on blackboard is different from the one book.

- Again we want to prove that there exist two consecutive numbers. Their gcd will be one.
- To prove their existence, we proceed as follows:

### Proof.

Let our pigeonholes/boxes be the following sets

$\{1, 2\}$ ,  $\{3, 4\}$ ,  $\{2n - 1, 2n\}$ , and our pigeons/objects the  $n + 1$  numbers we choose from the set  $[2n] = \{1, 2, \dots, 2n\}$ . By the pigeonhole principle, two of the  $n + 1$  numbers will be in the same pigeonhole, and therefore they are consecutive since the pigeonhole sets were chosen to contain pairs of consecutive numbers. □

# Permutations

As we discussed during the previous lecture (11/19) a permutation of a set  $S$  is a bijective function on that set, i.e., a function  $f : S \rightarrow \text{to } S$  that 1-1 and onto.

- Equivalently, a permutation is an ordered arrangement of these objects.
- An  **$r$ -permutation** is an ordered permutation of  $r$  elements of a set.

**Example:** Let  $S = \{1, 2, 3\}$ . The ordered arrangement  $(3, 1, 2)$  is a permutation of  $S$ . The ordered arrangement  $3, 2$  is a 2-permutation.

# Permutations

- **Theorem:** Define  $P(n, r)$  to be the number of  $0 \leq r \leq n$   $r$ -permutations of a set  $S$  with  $n$  elements.

$$P(n, r) = \frac{n!}{(n - r)!}.$$

- ① How many possible routes does a salesman have that wants to travel eight different cities?
- ② Suppose there are eight runners in a race. How many different ways exist to award the three medals if all possible outcomes can occur, and there are no ties?
- ③ How many permutations of the letters  $ABCDEF$  contain the string  $ABC$ ?

## Proofs on blackboard

# Combinations

- An  $r$ -combination of elements of a set is an **unordered** selection of  $r$  elements from the set. Thus, an  $r$ -combination is simply a subset of the set with  $r$  elements.
- **Theorem:** Define  $C(n, r)$  to be the number of  $0 \leq r \leq n$   $r$ -combinations of a set  $S$  with  $n$  elements.

$$C(n, r) = \frac{n!}{r! \cdot (n - r)!} = \binom{n}{r}.$$

- $C(n, r) = \binom{n}{r}$  is also called binomial coefficient (we will see later why, when we see the binomial theorem).

# Combinations

- ① How many poker hands of five cards can be dealt from a standard deck of 52 cards?
- ② Let  $n, r$  be non-negative integers with  $r \leq n$ . Then

$$\binom{n}{r} = \binom{n}{n-r}.$$

A combinatorial proof of an identity is a proof that uses counting arguments (e.g., double counting, bijections) to the identity.

- ③ How many bit strings of length 10 contain
  - Exactly four 1s
  - at most four 1s
  - at least four 1s
  - an equal number of 0s and 1s

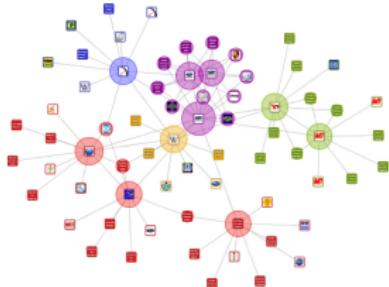
# Graphs

- **Definition:** A **graph**  $G(V, E)$  consists of  $V$ , a nonempty set of vertices (or nodes) and  $E$ , a set of edges. Each edge connects two nodes, that are called its endpoints.

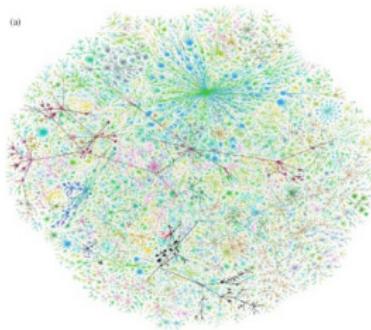
Some important remarks

- The **Facebook** social graph is undirected (i.e., edge is an unordered pair of nodes  $\{u, v\}$ )
- The **Twitter** follow graph is directed (i.e., edge is an ordered pair of nodes  $(u, v)$ )
- **Definition:** A graph is **bipartite** if and only if it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.
- Examples of graphs?

# Graphs are ubiquitous...



Computer network



Internet



Social network



Connectome



Airline network



Images

# Complete graph $K_n$

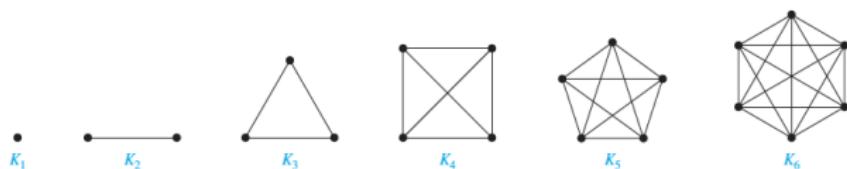
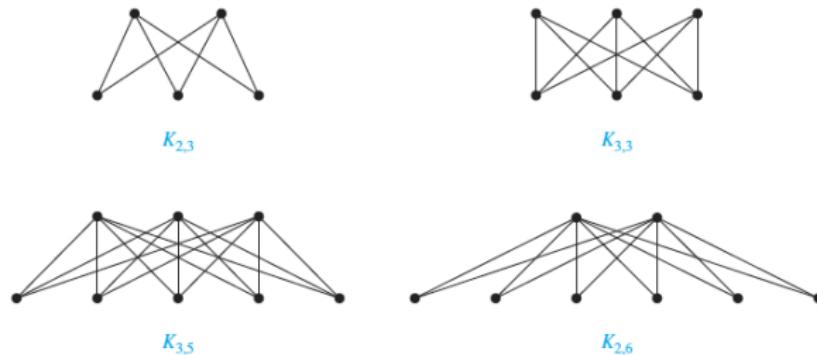


FIGURE 3 The Graphs  $K_n$  for  $1 \leq n \leq 6$ .

- The complete graph  $K_n$  (one edge between each possible pair of nodes)
  - How many edges does  $K_n$  have?

# Complete bipartite graph $K_{n,m}$



**FIGURE 9** Some Complete Bipartite Graphs.

- The complete bipartite graph  $K_{n,m}$ 
  - How many edges does  $K_{n,m}$  have?

# Permutations with repetitions

- **Question:** How many strings of length  $r$  can be formed from the uppercase letters of the English alphabet?
- **Answer:**  $26^r$

## Theorem

*The number of  $r$ -permutations of a set of  $n$  objects with repetition allowed is  $n^r$ .*

# Permutations with indistinguishable objects

## Theorem

*The number of different permutations of  $n$  objects where there are  $n_i$  indistinguishable objects of type  $i$  for  $i = 1, \dots, k$  is*

$$\frac{n!}{\prod_{i=1}^k n_i!}.$$

**Question:** How many different strings can be made by re-ordering the letters of the word SUCCESS?

## Proof on blackboard

Three derivations

- By the theorem  $\frac{7!}{3!1!2!1!}$ .
- By the product rule (procedure: choose the positions of Ss etc.)
- By the product and division rule (pretend Ss are different,  $S_1, S_2, S_3$  etc.)

# Combinations with repetitions

## Theorem

*The number of  $r$ -combinations from a set of  $n$  objects with repetition allowed in  $C(n + r - 1, r) = \binom{n+r-1}{r}$ .*

## Proof on blackboard

- **Question:** How many solutions does the equation  $x_1 + x_2 + x_3 = 11$  have where  $x_1, x_2, x_3$  are non-negative integers?

# Binomial theorem

## Theorem

Let  $x, y$  be variables,  $n$  a non-negative integer. Then,

$$(x + y)^n = \sum_{p=0}^n \binom{n}{p} x^p y^{n-p}.$$

- By setting  $x = y = 1$  we obtain  $2^n = \sum_{p=0}^n \binom{n}{p}$
- We can derive the same identity via a *combinatorial proof* by counting the number of subsets of a set with  $n$  elements in two different ways (double counting)
- By setting  $x = 1, y = -1$  we obtain  $\sum_{p=0}^n (-1)^p \binom{n}{p} = 0$

## Proof on blackboard

# Pascal's identity

By Pascal's identity:  
 $(\binom{4}{4}) + (\binom{5}{4}) = \binom{6}{5}$

...

...

## Theorem (Pascal's identity)

Let  $n, k$  be positive integers with  $n \geq k$ . Then,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

## Proof on blackboard

# Lectures 22, 23 (12/3, 12/5)

## Outline

- Some counting exercises
- Degree sequence, hand-shaking lemma, and other basic notions  
[Rosen 10.2, 10.3, 10.4]
- Trees [Rosen 11.1]
- Hall's theorem [Rosen 10.2]
- Euler and Hamilton cycles [Rosen 10.5]

Blackboard lecture

# Inclusion-Exclusion

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

## Problem :

- 1232 students have taken a course in Spanish.
- 879 have taken a course in French
- 114 have taken a course in Russian
- 103 have taken courses in both Spanish and French
- 23 have taken courses in both Spanish and Russian
- 14 have taken courses in both French and Russian
- 2092 students have taken at least one of Spanish, French, and Russian
- **Question:** How many students have taken a course in all three languages?

# Problems

- ① How many anagrams of the word BANANA exist?
  
- ② Assume that we have three different boxes and 7 pencils. In how many ways can we distribute the pencils in the boxes  
Remark: What is the number of solutions of  $x_1 + x_2 + x_3 = 7$ , where  $x_i \geq 0$  integers for  $i = 1, 2, 3$ ?

# Graphs

- **Definition:** A **graph**  $G(V, E)$  consists of  $V$ , a nonempty set of vertices (or nodes) and  $E$ , a set of edges. Each edge connects two nodes, that are called its endpoints.

Some important remarks

- The **Facebook** social graph is undirected (i.e., edge is an unordered pair of nodes  $\{u, v\}$ )
- The **Twitter** follow graph is directed (i.e., edge is an ordered pair of nodes  $(u, v)$ )
- **Definition:** A graph is **bipartite** if and only if it is possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.
- Examples of graphs?

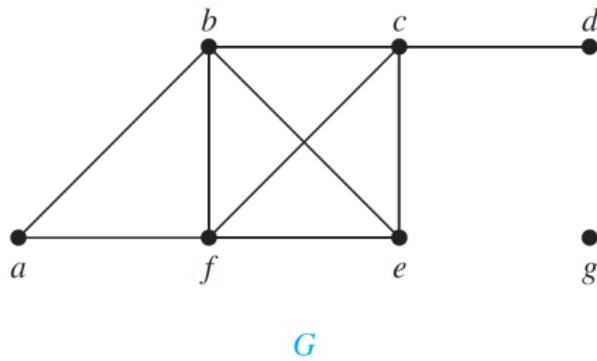
# Graphs – Basic definitions

## Definition

- ① Two nodes  $u, v$  in an undirected graph  $G(V, E)$  are called adjacent in  $G$  if  $\{u, v\} \in E(G)$ . Such an edge  $e = \{u, v\}$  is called incident with the vertices  $u, v$ , and is said to connect them.
- ② The degree of a vertex in an undirected graph is the number of edges incident with it. The degree of vertex  $v$  is denoted as  $\deg(v)$ .
- ③ A node with degree 0 is called isolated.

# Graphs – Degree sequence

Question: What are the degrees of the nodes in  $G$ ?



# Graphs – Degree sequence

Theorem (Handshake theorem)

Let  $G(V, E)$  be an undirected graph with  $m$  edges. Then,

$$2m = \sum_{v \in V} \deg(v).$$

Corollary

The number of nodes in  $G$  with odd degree is even.

Proofs on blackboard

# Graphs - Paths

## Definition

Let  $n$  be a non-negative integer and  $G$  an undirected graph. A **path** of length  $k$  from  $u$  to  $v$  in  $G$  is a sequence of  $n$  edges  $e_1, \dots, e_k$  of  $G$  for which there exists a sequence

$$u = x_0, x_1, \dots, x_{k-1}, x_k = v$$

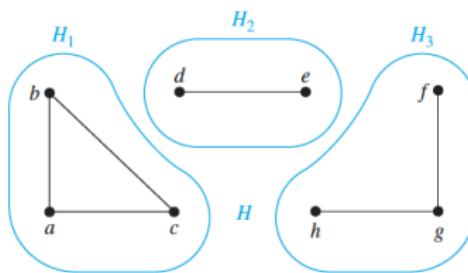
of vertices such that  $e_i = (x_i, x_{i-1})$  for  $i = 1, \dots, k$ .

The path is a **cycle/circuit** if  $u = v$  and has length greater than 0. A path or circuit is **simple** if it does not contain the same edge more than once.

# Graphs - Connectivity

## Definition

An undirected graph is called **connected** if there is a path between every pair of distinct vertices of the graph. An undirected graph that is not connected is called **disconnected**. We say that **we disconnect** a graph when we remove vertices or edges, or both, to produce a disconnected subgraph.



# Graphs - Isomorphism

## Definition

The simple graphs  $G_1 = (V_1, E_1)$ ,  $G_2 = (V_2, E_2)$  are **isomorphic** if there exists a one-to-one and onto function  $f : V_1 \rightarrow V_2$  with the property that

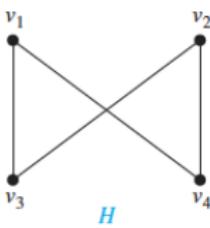
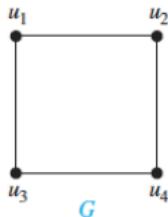
- $u$  and  $v$  are adjacency in  $G_1$  iff  $f(u)$  and  $f(v)$  are adjacent in  $G_2$  for all  $a, b \in V_1$

Such a function  $f$  is called an isomorphism.

## Remarks

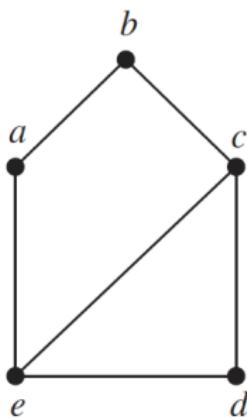
- If such a function  $f$  does not exist, i.e.,  $G_1, G_2$  are not isomorphic, they are called *non-isomorphic*.
- If two graphs have different number of edges, they are non-isomorphic (why?)

# Graphs - Isomorphism

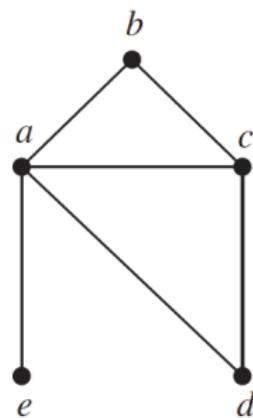


- $G, H$  are isomorphic. One isomorphism is  $f(u_1) = v_1, f(u_2) = v_4, f(u_3) = v_3, f(u_4) = v_2$  (why?)

# Graphs - Non-isomorphism



$G$



$H$

- It is easy to observe that  $G, H$  are non-isomorphic (why? hint: look at node  $e$  in  $H$ )

# Graphs - Problem

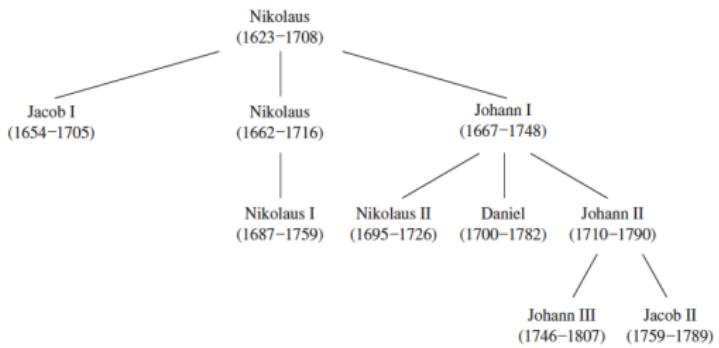
## Definition

- ① The **complementary graph**  $\bar{G}$  of a graph  $G$  has the same vertices as  $G$ . Two vertices are adjacent in  $G$  if and only if they are not adjacent in  $\bar{G}$ .
- ② A graph  $G$  is called self-complementary if  $G$  and its complement  $\bar{G}$  are isomorphic.

**Problem:** Show that if  $G$  is self-complementary graph with  $n$  vertices, then  $n \equiv 0 \pmod{4}$  or  $n \equiv 1 \pmod{4}$ .

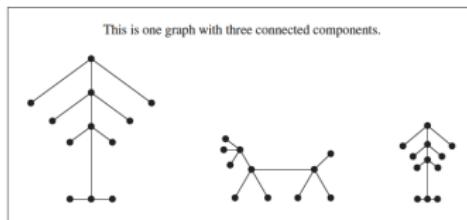
## Solution on blackboard

# Trees - Definition



The family **tree** of Bernoullis'.

# Trees - Definition



Example of a **forest**.

## Definition

A tree is a connected undirected graph with no simple circuits. A graph whose connected components are trees, is called a forest.

## Theorem

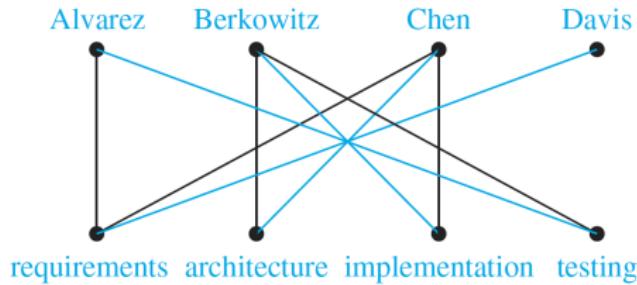
*An undirected graph is a tree if and only if there is a unique simple path between any two of its vertices.*

# Graph Matchings

- A set  $M$  of independent edges in a graph  $G(V, E)$  is called a **matching**.
- $M$  is a matching of  $U \subseteq V$  if every vertex in  $U$  is incident with an edge in  $M$ . The vertices in  $U$  are then called **matched** by  $M$ .
- Vertices not incident with any edge of  $M$  are *unmatched*.
- A **maximum matching** is a matching with the largest number of edges.
- A **perfect matching** of a graph is a matching in which every vertex of the graph is incident to exactly one edge of the matching.

# Graph Matchings – Hall's theorem

- We say that a matching  $M$  in a bipartite graph  $G(V, E)$  with bi-partition  $(V_1, V_2)$  is a complete matching from  $V_1$  to  $V_2$  if every vertex in  $V_1$  is the endpoint of an edge in a matching, i.e.,  $|M| = |V_1|$ .



- When can we find a complete matching from  $V_1$  to  $V_2$  in a bipartite graph?**

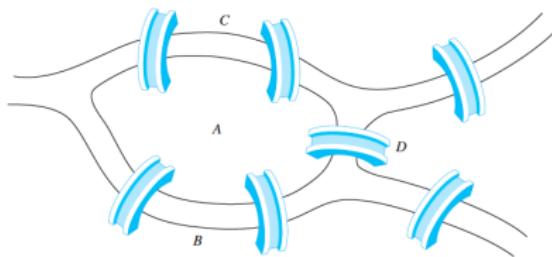
# Graph Matchings – Hall's theorem

## Theorem

*The bipartite graph  $G(V_1 \cup V_2, E)$  has a complete matching from  $V_1$  to  $V_2$  iff  $|N(A)| \geq |A|$  for all  $A \subseteq V_1$ . Here  $N(A) = \cup_{v \in A} N(v)$  where  $N(v)$  is the set of neighbors of  $v$ .*

**Constructive/algorithmic proof on blackboard using  
alternating paths**

# Eulerian cycles



The problem of the **seven bridges of Königsberg**.

- In Königsberg, locals took long walks through the town on Sundays.
- **Question:** Was it possible to start at some location in the town, travel across all the bridges once without crossing any bridge twice, and return to the starting point?

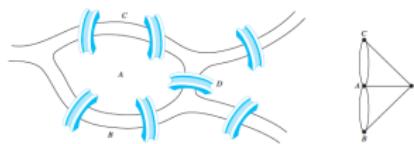
# Eulerian cycles



- “Its negative resolution by Leonhard Euler in 1736 laid the foundations of graph theory and prefigured the idea of topology.”
- His proof is considered to be the **first theorem** of graph theory.

# Eulerian cycles

- Euler reduced the problem to a graph problem.



- An Euler circuit in a (multi)graph  $G$  is a simple circuit containing every edge of  $G$ . An Euler path in  $G$  is a simple path containing every edge of  $G$ .

# Eulerian cycles

## Theorem

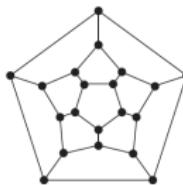
A connected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.



- Observation: there exist 4 vertices of odd degree.

# Hamilton cycles

- The icosian game is a mathematical game invented in 1856 by William Rowan Hamilton.

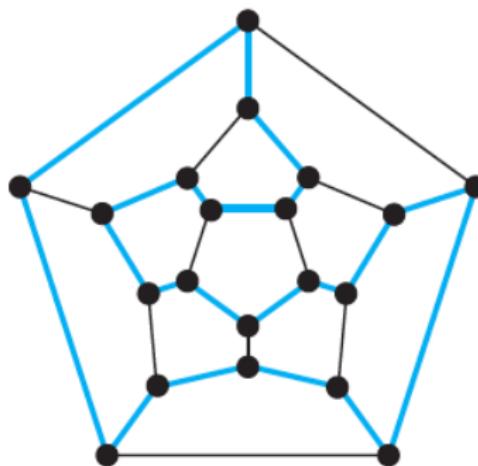


- Find a cycle along the edges such that every vertex is visited a single time, and the ending point is the same as the starting point.

# Hamilton cycles

## Definition

A simple path in a graph  $G$  that passes through every vertex exactly once is called a Hamilton path, and a simple circuit in a graph  $G$  that passes through every vertex exactly once is called a Hamilton circuit.



# Hamilton cycles - Ore's theorem

- In contrast to Eulerian cycles, Hamiltonian cycles are hard to find.  
By hard we mean that the *Hamiltonian Cycle Problem* is NP-complete
- However, we have certain results that provide sufficient conditions for Hamiltonicity.

## Theorem

*If  $G$  is a simple graph with  $n$  vertices where  $n \geq 3$  such that*

$$\deg(u) + \deg(v) \geq n$$

*for every pair of non-adjacent vertices  $u, v$ , then  $G$  has a Hamilton circuit.*

# Last lecture

## Lecture 24 Practicing problem solving (combinatorics)

**Blackboard lecture**

# Counting derangements

## Definition

A derangement is a permutation of the elements of a set, such that no element appears in its original position.

- Consider a set  $S$  of  $n$  items.
- **Question:** How many derangements of  $S$  exist?

# Inclusion exclusion rule

Theorem: Let  $A_1, A_2, \dots, A_n$  be finite subsets of a set  $X$ .

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap A_{i_2} \dots \cap A_{i_k}|.$$

Another way to see this equation is by expanding the “internal” sum term.

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

## Problem 2 - Counting perfect matchings

- ① Count the number of perfect matchings in  $C_n$
- ② Count the number of perfect matchings in  $K_n$
- ③ Remark: when  $n$  is odd, the number of such matchings is always 0 (why?).

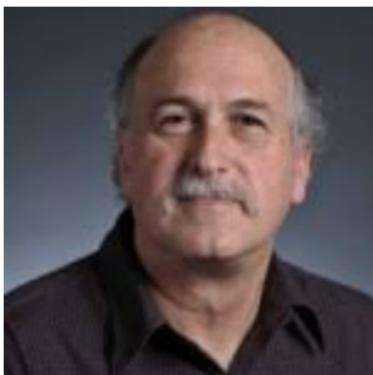
## Problem 3 - A graph theoretic problem

- Let  $G(V, E)$  be a graph,  $|V| = n$ . Suppose that for all non-adjacent pairs  $x, y$  of vertices, the sum of the nodes' degrees is at least  $n - 1$ , i.e.,

$$\deg(x) + \deg(y) \geq n - 1.$$

Prove that  $G$  is connected.

# Acknowledgements



Prof. Steve Homer (guest lecture)

For this deck of slides, the following sources were used:

- Discrete Mathematics and Its Applications by Rosen
- How to Prove It: A Structured Approach by Velleman
- Logicomix: An epic search for truth by Doxiadis, Papadimitriou
- Wikipedia

Hope you enjoyed CS131 with a child's curiosity!





*That's all Folks!*