Algorithms
Chapter 1 Preliminaries

Associate Professor: Ching-Chi Lin
林清池 副教授
chingchi.lin@gmail.com

Department of Computer Science and Engineering
National Taiwan Ocean University

Outline

- **Mathematical Notions and Terminology**
- Definitions, Theorems, and Proofs
- Types of Proof

Sets$_{1/3}$

- A **set** is a group of objects represented as a unit.
- Sets may contain any type of object, including numbers, symbols, and even other sets.
- The objects in a set are called its **elements** or **members**.
- One way to describe sets formally is by listing its elements inside braces.
- Thus the set $\{7, 21, 57\}$ contains the elements 7, 21, and 57.

Sets$_{2/3}$

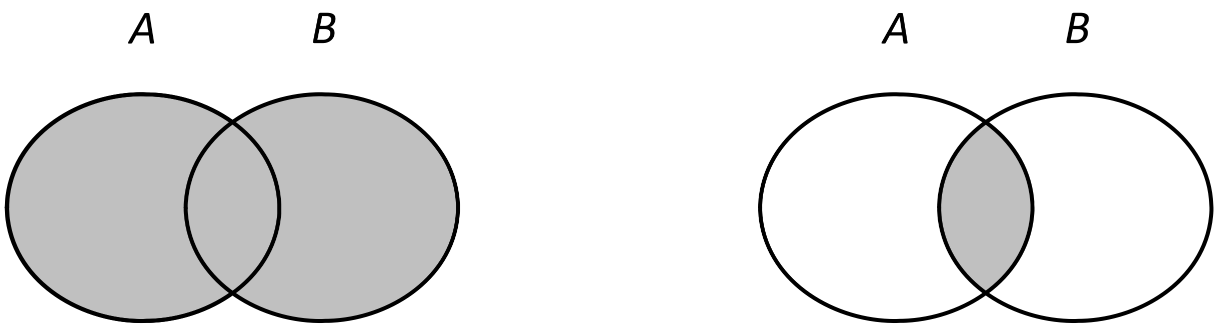
- The symbols $\in$ and $\notin$ denote set membership and non-membership, respectively.
- We write $7 \in \{7, 21, 57\}$ and $8 \notin \{7, 21, 57\}$.
- For two sets A and B, we say that A is a **subset** of B, written $A \subseteq B$, if every member of A is also a member of B.
- We say that A is a **proper subset** of B, written $A \subsetneq B$, if A is a subset of B and not equal to B.
- Let $A = \{7, 21\}$ and $B = \{7, 21, 57\}$. Then, we can write $A \subseteq B$ and $A \subsetneq B$.
- The set of **natural numbers** N is $\{1, 2, 3, \ldots\}$.

Sets$_{3/3}$

- The set with 0 members is called the **empty set** and is written ϕ.
- A set containing elements according some rule is denoted by $\{n \mid \text{rule about } n\}$.
  - $\{n \mid n = m^2 \text{ for some } m \in N\}$ ➔ the set of perfect squares.
- The **union** of A and B, written $A \cup B$, is the set we get by combining all the elements in A and B into a single set.
- The **intersection** of A and B, written $A \cap B$, is the set of elements that are in both A and B.
- The **complement** of A, written $\bar{A}$, is the set of all elements under consideration that are **not** in A.

Venn diagram

- The next two **Venn diagrams** depict the union and intersection of sets *A* and *B*.



(a) $A \cup B$ (b) $A \cap B$

Sequences

- A **sequence** of objects is a list of these objects in some order.
  - We usually designate a sequence by writing the list within parentheses.
  - In a set the order doesn’t matter, but in a sequence it does.
- For example:
  - The sequence 7, 21, 57 would be written (7, 21, 57).
  - Hence (7,21,57) is not the same as (57, 7, 21).
- Repetition does matter in a sequence, but it doesn't matter in a set.
  - Thus (7,7,21,57) is different from (7,21,57) and (57, 7, 21).
  - The set {7, 21, 57} is identical to the set {7, 7, 21, 57}.

Tuples and power sets

- Finite sequences often are called **tuples**.
  - A sequence with k elements is a k-tuple.
  - Thus (7,21,57) is a 3-tuple.
  - A 2-tuple is also called a **pair**.
- The **power set** of A is the set of all subsets of A.
- For example:
  - If A is the set {O, I}, the power set of A is the set {ϕ, {O}, {I}, {O, I}}.
  - The set of all pairs whose elements are Os and 1s is {(0, 0), (0, 1), (1, 0), (1, 1)}.

Cartesian product

- The **Cartesian product** of A and B, written A x B, is the set of all pairs wherein the first element is a member of A and the second element is a member of B.

- For example:
  - If $A = \{I, 2\}$ and $B = \{x, y, z\}$, then
    $A \times B = \{(I, x), (I, y), (I, z), (2, x), (2, y), (2, z)\}$.

- We can also take the Cartesian product of k sets, $A_I, A_2, \ldots, A_k$, written $A_I \times A_2 \times \ldots \times A_k$.

- For example:
  - If $A = \{I, 2\}$ and $B = \{x, y, z\}$, then
    $A \times B \times A = \{(1, x, 1), (1, x, 2), (1, y, 1), (1, y, 2), (1, z, 1), (1, z, 2),$
    $(2, x, 1), (2, x, 2), (2, y, 1), (2, y, 2), (2, z, 1), (2, z, 2)\}$.

Outline

- Mathematical Notions and Terminology
- **Definitions, Theorems, and Proofs**
- Types of Proof

Definitions, theorems, and proofs

- Theorems and proofs are the heart and soul of mathematics, and definitions are its spirits.

- These three entities are central to every mathematical subjects, including algorithms.

- In this class, you are expected to pick up the ability of reading and writing a concrete proof.

Definitions

- **Definitions** describe the objects and notions that we use.
  - Precision is essential to any mathematical definition.
  - When defining some object we must make clear what constitutes that object and what does not.

- For example:
  - A **set** is a group of objects represented as a unit.
  - The objects in a set are called its **elements** or **members**.
  - A **tree** graph is a connected graph without cycles.

Proofs

- After we have defined various objects and notions, we usually make **mathematical statements** about them.
  - A statement expresses that some object has a certain property.
  - The statement mayor may not be true.
  - The statements must be precise without any ambiguity.
- A **proof** is a convincing logical argument that a statement is true.
  - In mathematics an argument must be airtight, that is, convincing in an absolute sense.
  - A mathematician demands proof beyond any doubt.

Theorems, lemmas, and corollaries

- A **theorem** is a mathematical statement proved true. Generally we reserve the word for statements of special interest.
- **Lemmas** are the proved statements that are interesting only for their assistance in the proof of another statement.
- Occasionally a theorem or its proof may allow us to conclude easily that other, related statements are true. These statements are called **corollaries** of the theorem.

Finding Proofs

- The only way to determine the truth or falsity of a mathematical statement is with a mathematical proof.
- Unfortunately, finding proofs isn't always easy.
  - It can't be reduced to a simple set of rules or processes.
- However, some helpful general strategies are available.
  - Carefully read the statement you want to prove.
  - Make sure you understand all the notation.
  - Rewrite the statement in your own words.
  - Break it down and consider each part separately.
  - Experimenting with examples.
  - Try to find an object that fails to have the property, called a **counterexample**.

Multipart statements$_{1/2}$

- One frequently occurring type of **multipart statement** has the form "*P* if and only if *Q*", often written "*P* iff *Q*".
  - Both *P* and *Q* are mathematical statements.
  - The first part is "*P* only if *Q*," which means: If *P* is true, then *Q* is true, written $P \Rightarrow Q$.
  - The second is "*P* if *Q*," which means: If *Q* is true, then *P* is true, written $P \Leftarrow Q$.
  - We write "*P* if and only if Q" as $P \Leftrightarrow Q$.
  - To prove a statement of this form you must prove each of the two directions.

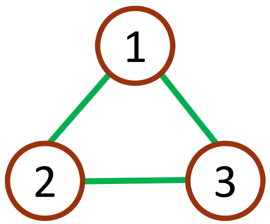
Multipart statements$_{2/2}$

- Another type of multipart statement states that two sets *A* and *B* are equal.
  - The first part states that *A* is a subset of *B*.
  - The second part states that *B* is a subset of *A*.
- To show that *A* = *B*, we must prove the following two statements.
  - Every member of *A* also is a member of *B*.
  - Every member of *B* also is a member of *A*.

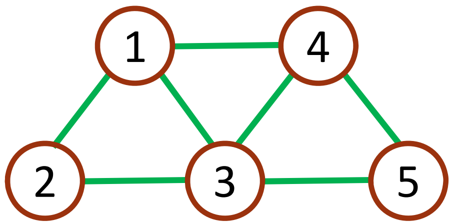
An example for finding Proofs$_{1/2}$

- Suppose that you want to prove the statement
  "**For every graph *G*, the sum of the degrees of all the nodes in *G* is an even number**".

- **First**, pick a few graphs and observe this statement.



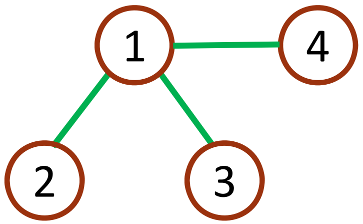
sum = 2 + 2 + 2
= 6



sum = 3 + 2 + 4 + 3 + 2
= 14

An example for finding Proofs$_{2/2}$

- **Next**, try to find a counterexample, that is, a graph in which the sum is an odd number.



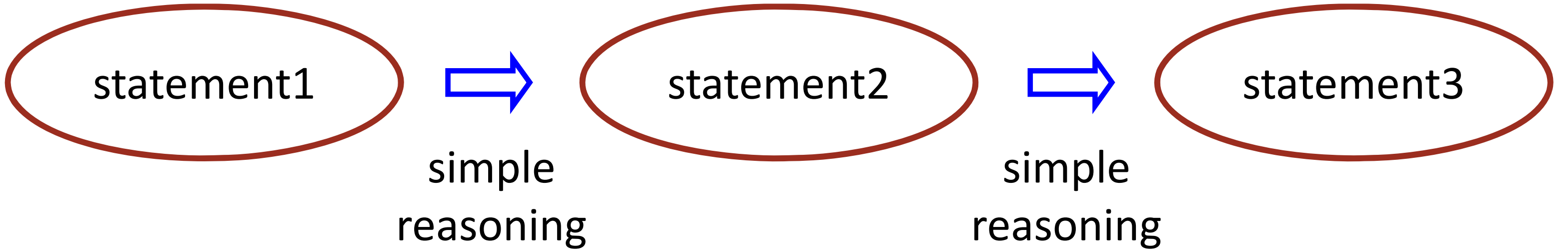
Every time an edge is added,
the sum increases by 2.

  - Can you now begin to see why the statement is true and how to prove it?

- If you are still stuck trying to prove the statement, try to prove a **special case** of the statement.
  - First try for $k = 1$, as well as $k = 2$, $k = 3$, $k = 4$ and so on.

Writing proofs

- A well-written proof is a sequence of statements, wherein each one follows by simple reasoning from previous statements in the sequence.



- Carefully writing a proof is important.
  - Enable a reader to understand it.
  - Make sure that it is free from errors.

Tips for producing a proof

- Be patient.
  - Researchers sometimes work for weeks or even years to find a single proof.
- Come back to it.
  - Look over the statement you want to prove, think about it a bit, leave it, and then return a few minutes or hours later.
- Be concise.
  - Good mathematical notation is useful for expressing ideas concisely.
  - But be sure to include enough of your reasoning when writing up a proof so that the reader can easily understand what you are trying to say.

An example for producing a proof

- Theorem : **For every graph *G*, the sum of the degrees of all the nodes in *G* is an even number**.
- Proof.
  - Every edge in *G* is connected to two nodes.
  - Each edge contributes 1 to the degree of each node to which it is connected.
  - Therefore each edge contributes 2 to the sum of the degrees of all the nodes.
  - Hence, if *G* contains *e* edges, then the sum of the degrees of all the nodes of *G* is 2*e*, which is an even number.

Outline

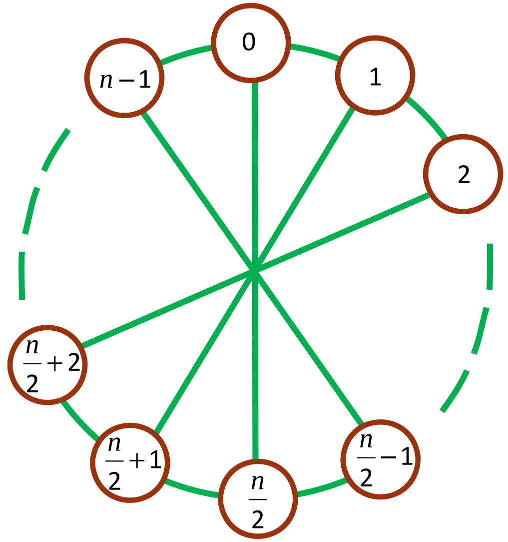
- Mathematical Notions and Terminology
- Definitions, Theorems, and Proofs
- **Types of Proof**

Types of proof

- Several types of arguments arise frequently in mathematical proofs.
  - Proof by construction.
  - Proof by contradiction.
  - Proof by induction.
- Note that a proof may contain more than one type of argument.
  - Because the proof may contain within it several different subproofs.

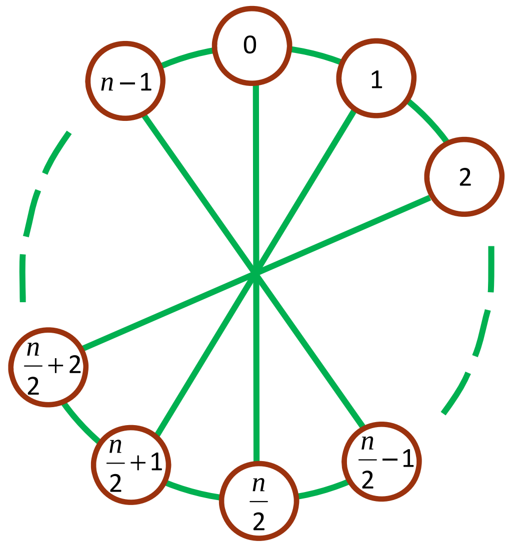
Proof by construction$_{1/2}$

- A graph is said to be ***k*-regular** if every node in the graph has degree k.
- Theorem : **For each even number n greater than 2, there exists a 3-regular graph $G(V, E)$ with n nodes.**
- Proof.
  - Let n be an even number greater than 2.
  - The set $V = \{0, 1, \ldots, n-1\}$.
  - The set $E = \{(i, i+1) \mid \text{for } 0 \le i \le n-2\}$
    $\cup \{(n-1, 0)\}$
    $\cup \{(i, i+n/2) \mid \text{for } 0 \le i \le n/2-1\}$.



Proof by construction$_{2/2}$

- The set $E = \{(i, i+1) \mid \text{for } 0 \le i \le n-2\}$
  $\cup \{(n-1, 0)\}$
  $\cup \{(i, i+n/2) \mid \text{for } 0 \le i \le n/2 - 1\}$.
- The edges described in the top and middle lines of E go between adjacent pairs around the circle.
- The edges described in the bottom line of E go between nodes on opposite sides of the circle.
- This mental picture clearly shows that every node in G has degree 3.



Proof by contradiction

- In this kind of arguments, we first **assume** that the theorem to prove is **false**.
- Then we show that this assumption leads to an obviously false consequence, called a **contradiction**.
- We use this type of reasoning frequently in everyday life.
  - Jack just came in from outdoors and he is completely dry.
  - We want to prove that It's not raining.
  - If it were raining, Jack would be wet.

    (assume false) **(contradiction)**
  - Therefore, it must not be raining.

An example for proof by contradiction

- A number is **rational** if it is a fraction m/n where m and n are integers.
- Theorem: $\sqrt{2}$ is **irrational**.
- Proof.
  - Assume for a contradiction that $\sqrt{2} = \frac{m}{n}$ is rational, where m and n are relatively prime integers.
  - $\sqrt{2} = \frac{m}{n} \quad => \quad n\sqrt{2} = m \quad => \quad 2n^2 = m^2.$
  - Since m^2 is even, m must be even as well.
  - Let $m = 2k$. Then we have $2n^2 = (2k)^2 = 4k^2$, which implies $n^2 = 2k^2$.
  - Since n^2 is even, n is even.
  - Both m and n are even, a **contradiction** to our assumption.

Proof by induction

- An advanced method to show that **all elements of an infinite set** have a specified property.
- Suppose that our goal is to prove that $P(k)$ is true for each natural number $k \in \{I, 2, 3, \ldots\}$.
- The format for writing down a proof by induction is as follows.
  - **Basis:** Prove that $P(1)$ is true.
  - **Induction step:** For each $i \geq 1$, assume that $P(i)$ is true and use this assumption to show that $P(i+1)$ is true.
- $P(1)$ is true: basis.
- $P(2)$ is true: $P(1)$ is true + induction step.
- $P(3)$ is true: $P(2)$ is true + induction step.

An example for proof by induction

- For each $n \geq 1$, we have

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}.$$

- Proof.
  - **The basis**: For n = 1, $1^2 = 1 = \dfrac{1\,(1+1)\,(2\times 1+1)}{6}$.
  - **Induction step**: For each $k \geq 1$, assume that the formula is true for $n = k$ and show that it is true for $n = k + 1$.

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = \frac{k\,(k+1)\,(2k+1)}{6} + (k+1)^2 = \frac{k\,(k+1)\,(2k+1) + 6(k+1)^2}{6}$$

$$= \frac{(k+1)\,(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)\,(2(k+1)+1)}{6}$$