Functions

Definition: Function

A function f from a set X to a set Y, denoted $f: X \to Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X, \exists y \in Y \ \ s.t. (x, y) \in f$

(F2) $\forall x \in X, \forall y_1, y_2 \in Y, \left((x, y_1) \in f \land (x, y_2) \in f\right) \to y_1 = y_2$

(That is, the y in (F1) is unique)

<u>Or alternatively</u>

Let f be a relation sets X and Y, i.e. $f \subseteq X \times Y$. Then f is a function from X to Y, denoted $f: X \to Y$, iff

$$\forall x \in X, \exists!\, y \in Y \ \ s.t. (x, y) \in f$$

<u>Informally</u>

A function from X to Y is an assignment to each element of X **exactly one element** of Y.

Arrow Diagrams

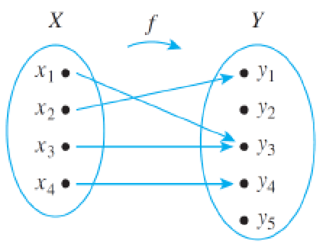


Figure 7.1.1

This arrow diagram defines a function because

1. Every element of X has an arrow coming out of it.
2. No element of X has two arrows coming out of it that point to two different elements of Y.

<u>Example</u>

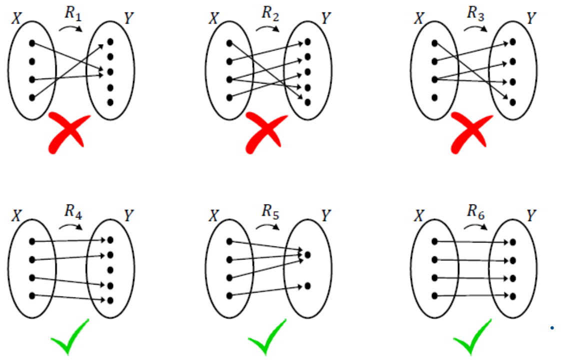
$f: \mathbb{R} \to \mathbb{R}$: $\forall x \in \mathbb{R}$, $f(x)$ is the real number s.t. $x^2 + y^2 = 1$

$f(x)$ is not a function.

(1) There is no y that satisfies the given equation (e.g. when $x = 2$)

(2) There are two different values of y that satisfies the eqn $(x = 0)$ $(y = \pm 1)$

<u>Example (Valid Functions)</u>



Definition: Argument, image, preimage, input, output

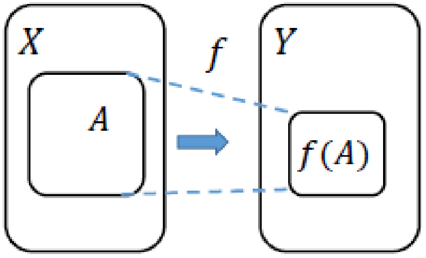
Let $f: X \to Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$.

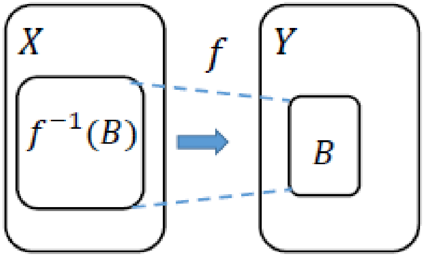
We say that "f sends/maps x to y" and we may also write $x \xrightarrow{f} y$ or $f: x \longmapsto y$. Also, x is called the **argument** of f.

$f(x)$ is read "f of x", or "the **output** of f for the **input** x", or "the value of f at x", or "the **image** of x under f".

If $f(x) = y$, then x is a **preimage** of y.

Definitions: Setwise image and preimage





Let $f: X \to Y$ be a function fromy set X to set Y.

- If $A \subseteq X$, then $f(A) = \{f(x) : \ x \in A\}$
- If $B \subseteq Y$, then $f^{-1}(B) = \{x \in X : f(x) \in B\}$

We call $f(A)$ the **(setwise) image** of A, and $f^{-1}(B)$ the **(setwise) preimage** of B under f.

Definitions: Domain, co-domain, range

Let $f: X \to Y$ be a function from set X to set Y.

- X is the **domain** of f and Y the **co-domain** of f
- The **range** of f is the (setwise) image of X under f
  $\{y \in Y : y = f(x) \ for \ some \ x \in X\}$

Definition: Sequence

A **sequence** $a_0, a_1, a_2, \cdots$ can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$.

<u>Example</u>

The sequence 2,3,5,9,17,33,... may be represented by the function $a: Z_{\geq 0} \to Z^+$ that satisfies for each $n \in Z_{\geq 0}, a(n) = 2^n + 1$

Definition: Fibonacci Sequence

The **Fibonacci sequence** $F_0, F_1, F_2, \cdots$ is defined by setting, for each $n \in Z_{\geq 0}$, $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

Definiton: String

Let A be a set. A **string** or a word over A is an expression of the form $a_0 a_1 a_2 \ldots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0 a_1 a_2 \ldots a_{l-1} \in A$. Here l is called the **length** of the string. The **empty string** ϵ is the string of length 0. Let A^* denote the set of all strings over A.

Equality of Sequences

Given two sequences $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$ defined by the functions $a(n) = a_n$ and $b(n) = b_n$ respectively for every $n \in Z_{\geq 0}$, we say that the two sequences are equal if and only if $a(n) = b(n)$ for every $n \in Z_{\geq 0}$.

Equality of Strings

Given two strings $s_1 = a_0 a_1 a_2 \ldots a_{l-1}$ and $s_2 = b_0 b_1 b_2 \ldots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that $s_1 = s_2$ iff $a_i = b_i$ for all $i \in \{0,1,2, \ldots, l-1\}$.

Theorem 7.1.1: Function Equality

Two functions $f: A \to B$ and $g: C \to D$ are equal, i.e. $f = g$, iff
(i) $A = C$ and $B = D$, and
(ii) $f(x) = g(x) \ \forall x \in A$.

Definitions: Bijections

A Function $f: X \to Y$ is:

Injective iff $\forall x_1, x_2 \in X(f(x_1) = f(x_2) \to x_1 = x_2)$

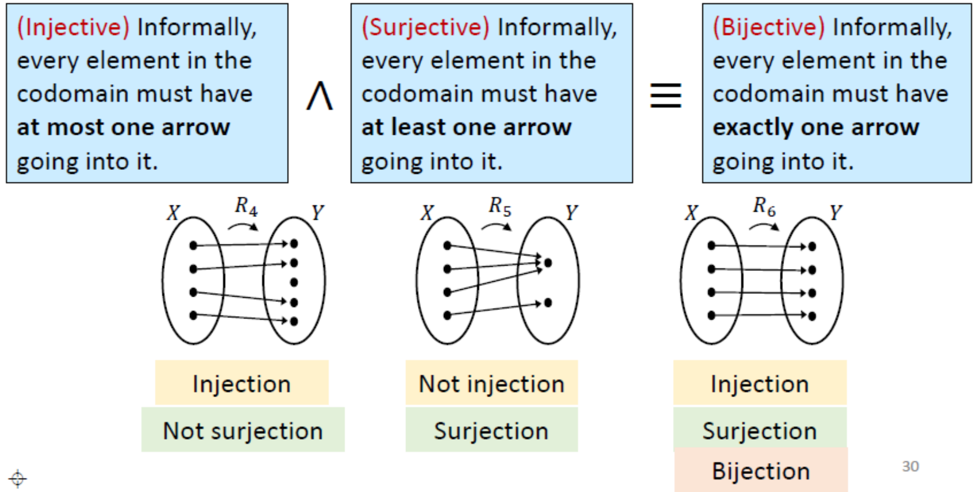
- or, equivalently $x_1 \neq x_2 \to f(x_1) \neq f(x_2)$
- f is <u>not</u> injective iff $\exists x_1, x_2 \in X \ (f(x_1) = f(x_2) \land x_1 \neq x_2)$

Surjective iff $\forall y \in Y \ \exists x \in X \ (y = f(x))$

- Every element in co-domain has a preimage. Range = Co-domain.
- f is <u>not</u> surjective iff $\exists y \in Y \ \forall x \in X \ \big(y \neq f(x)\big)$

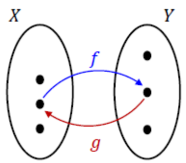
Bijective iff $\forall y \in Y \ \exists! \, x \in X \ (y = f(x))$

- f is bijective iff f is injective and surjective



Definition: Inverse Function

Let $f: X \to Y$. Then, $g: Y \to X$ is an **inverse** of f iff
$\forall x \in X \ \ \forall y \in Y \ \ \big(y = f(x) \Leftrightarrow x = g(y)\big)$.
We denote the inverse of f as f^{-1}.



Propopsition: Uniqueness of inverses
If g_1 and g_2 are inverses of $f: X \to Y$, then $g_1 = g_2$.

Theorem 7.2.3
If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection.
In other words, $f: X \to Y$ is bijective iff f has an inverse.

Proof: ($f: X \to Y$ is bijective iff f has an inverse)

1. ("if") Suppose f has an inverse, say $g: Y \to X$.
   1.1. We show injectivity of f.
      1.1.1. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.
      1.1.2. Define $y = f(x_1) = f(x_2)$.
      1.1.3. Then $x_1 = g(y)$ and $x_2 = g(y)$ as g is an inverse of f.
      1.1.4. Hence $x_1 = x_2$.
   1.2. We show surjectivity of f.
      1.2.1. Let $y \in Y$.
      1.2.2. Define $x = g(y)$.
      1.2.3. Then $y = f(x)$ as g is an inverse of f.
   1.3. Therefore f is bijective.

Proof: ($f: X \to Y$ is bijective iff f has an inverse)

1. ("if") Suppose f has an inverse, say $g: Y \to X$.
2. ("only if") Suppose f is bijective.
   2.1. Then $\forall y \in Y\ \exists!\, x \in X\ \big(y = f(x)\big)$ by the definition of bijection.
   2.2. Define the function $g: Y \to X$ by setting $g(y)$ to be the unique $x \in X$ such that $y = f(x)$ for all $y \in Y$.
   2.3. This g is well defined and is an inverse of f by the definition of inverse functions.
3. Therefore $f: X \to Y$ is bijective iff f has an inverse.

Definition: Composition of Functions
Let $f: X \to Y$ and $g: Y \to Z$ be functions.
Define a new function $g \circ f: X \to Z$ as follows: $(g \circ f)(x) = g\big(f(x)\big)\ \forall x \in X$.
where $g \circ f$ is read "g circle f" and $g(f(x))$ is read "g of f of x".
The function $g \circ f$ is called the **composition** of f and g.

Theorem 7.3.1 Composition with an Identity Function
If f is a function from a set X to a set Y, and id_X is the identity function on X, and id_Y is the identity function on Y, then $f \circ id_X = f$ and $id_Y \circ f = f$

Theorem 7.3.2 Composition of a Function with Its Inverse
If f:$X \to Y$ is a bijection with inverse function $f^{-1}: Y \to X$, then $f^{-1} \circ f = id_x$ and $f \circ f^{-1} = id_Y$

Theorem: Associative of Function Composition
Let f:$A \to B$, g:$B \to C$ and h:$C \to D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$.
Function composition is associative.

Theorem 7.3.3
If $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective.

Theorem 7.3.4
If $f: X \to Y$ and $g: Y \to Z$ are both surjective, then $g \circ f$ is surjective.

Definition: Addition and Multiplication on $\mathbb{Z}_n$

Define addition $+$ and multiplication $\cdot$ on $\mathbb{Z}_n$ as follows:
whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y]$$

Proposition: Addition on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2].$$

Proposition: Multiplication on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

Lemma Rel.1 Equivalence Classes

Let $\sim$ be an equivalence relation on a set A. The following are equivalent for all $x, y \in A$. (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

Mathematical Induction

Definitions: Sequence and Terms

A **sequence** is an ordered set with members called **terms**.
Usually, the terms are numbers. A sequence may have infinite terms.

Definition: Summation

If m and n are integers, $m \leq n$, the symbol

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

is the **sum** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We say that $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ is the **expanded form** of the sum, and we write

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

We call k the **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

Definition: Product

If m and n are integers, $m \leq n$, the symbol

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

is the **product** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We write

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \cdots \cdot a_n.$$

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

Theorem 5.1.1

If $a_m, a_{m+1}, a_{m+2}, \cdots$ and $b_m, b_{m+1}, b_{m+2}, \cdots$ are sequences of real numbers and c is any real number , then the following equations hold for any integer $n \geq m$:

1. $$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$$

2. $$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$$ (generalized distributive law)

3. $$\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \left(\prod_{k=m}^{n} (a_k \cdot b_k)\right)$$

Definition: Arithmetic Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called an **arithmetic sequence** (or **arithmetic progression**) iff there is a constant d such that

$$a_k = a_{k-1} + d \qquad \text{for all integers } k \geq 1.$$

If follows that,

$$a_n = a_0 + dn \qquad \text{for all integers } n \geq 0.$$

Definition: Geometric Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called a **geometric sequence** (or **geometric progression**) iff there is a constant r such that

$$a_k = r a_{k-1} \qquad \text{for all integers } k \geq 1.$$

If follows that,

$$a_n = a_0 r^n \qquad \text{for all integers } n \geq 0.$$

Principle of Mathematical Induction (PMI)

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following 2 statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a, P(n)$" is true.

Method of Proof by Mathematical Induction

Consider a statement of the form, "For all integers $n \geq a$, a property $P(n)$ is true." To prove such a statement, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true.

Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To perform this step,

suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

[This supposition is called the **inductive hypothesis.***]*

Then

show that $P(k+1)$ is true.

Theorem 5.2.2 (5th: 5.2.1) Sum of the First n Integers

For all integers $n \geq 1$,

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

Definition: Closed Form

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis (...) or a summation symbol (Σ), we say that it is written in **closed form**.

Proposition 5.3.1 (5th: 5.3.2)

For all integers $n \geq 0, 2^{2n} - 1$ is divisible by 3.

Theorem 5.2.3 (5th: 5.2.2) Sum of a Geometric Sequence

For any real number $r \neq 1$, and any integers $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proposition 5.3.2 (5th: 5.3.3)

For all integers $n \geq 3$, $\;2n + 1 < 2^n$.

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a)$, $P(a+1)$, . . . , and $P(b)$ are all true. **(basis step)**
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. **(inductive step)**

Then the statement

for all integers $n \geq a$, $P(n)$

is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis.** Another way to state the inductive hypothesis is to say that $P(a)$, $P(a+1)$, . . . , $P(k)$ are all true.)

Weak (regular) induction (or 1PI)

If

- $P(a)$ holds
- For every $k \geq a, P(k) \Rightarrow P(k+1)$

Then $P(n)$ holds for all $n \geq a$.

We may prove strong induction from weak and weak induction from strong (proofs omitted). This means both types of induction are equal in "power".

Hence, using more neutral terms, we can call the regular/strong versions the First Principle of Mathematical Induction (1PI) and Second Principle of Mathematical Induction (2PI) respectively.

Strong induction (or 2PI)

If

- $P(a)$ holds
- For every $k \geq a, \big(P(a) \wedge P(a+1) \wedge \cdots P(k)\big) \Rightarrow P(k+1)$

Then $P(n)$ holds for all $n \geq a$.

Strong induction (or 2PI) (variation – other variations possible)

If

- $P(a), P(a+1), \ldots, P(b)$ hold
- For every $k \geq a, P(k) \Rightarrow P(k+b-a+1)$

Then $P(n)$ holds for all $n \geq a$.

Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility

For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Example #15: Use 1PI to prove that any whole amount of $\geq \$12$ can be formed by a combination of \$4 and \$5 coins.

Proof (by *1PI*):

1. Let $P(n) \equiv$ (the amount of $\$n$ can be formed by \$4 and \$5 coins) for $n \geq 12$.
2. Basis step: $12 = 3 \times 4$, so three \$4 can be used. Therefore $P(12)$ is true.
3. Assume $P(k)$ is true for $k \geq 12$.
4. Inductive step: (To show $P(k+1)$ is true.)
   - 4.1. Case 1: If a \$4 coin is used for $\$k$ amount, replace it by a \$5 coin to make $\$(k+1)$.
   - 4.2. Case 2: If no \$4 coin is used for $\$k$ amount, then $k \geq 15$, so there must be at least three \$5 coins. We can then replace three \$5 coins with four \$4 coins to make $\$(k+1)$.
   - 4.3. In both cases, $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for $n \geq 12$.

Example #16: Use 2PI to prove that:

For all integers $n \geq 12, n = 4a + 5b$ for some $a, b \in \mathbb{N}$.

Proof (by *2PI*):

1. Let $P(n) \equiv (n = 4a + 5b)$, for some $a, b \in \mathbb{N}, n \geq 12$.
2. Basis step: Show that $P(12), P(13), P(14), P(15)$ hold.
   $12 = 4 \cdot 3 + 5 \cdot 0$; $13 = 4 \cdot 2 + 5 \cdot 1$; $14 = 4 \cdot 1 + 5 \cdot 2$; $15 = 4 \cdot 0 + 5 \cdot 3$;
3. Assume $P(i)$ holds for $12 \leq i < k$ given some $k > 15$.
4. Inductive step: (To show $P(k+1)$ is true.)
   - 4.1. $P(k-3)$ holds (by induction hypothesis), so, $k - 3 = 4a + 5b$ for some $a, b \in \mathbb{N}$
   - 4.2. $k + 1 = (k-3) + 4 = (4a + 5b) + 4 = 4(a+1) + 5b$
   - 4.3. Hence, $P(k+1)$ is true.
5. Therefore, $P(n)$ is true for $n \geq 12$.

Well-Ordering Principle for the Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Well-Ordering Principle for the Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Definition

A **recurrence relation** for a sequence $a_0, a_1, a_2, \cdots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \cdots, a_{k-i}$, where i is an integer with $k - i \geq 0$.

If i is a fixed integer , the **initial conditions** for such a recurrent relation specify the values of $a_0, a_1, a_2, \cdots, a_{i-1}$.

If i depends on k, the initial conditions specify the values of $a_0, a_1, a_2, \cdots, a_m$, where m is an integer with $m \geq 0$.

Definition

Let S be a finite set with at least one element. A **string over** S is a finite sequence of elements from S. The elements of S are called **characters** of the string, and the **length** of a string is the number of characters it contains. The **null string over** S is defined to be the "string" with no characters. It is usually denoted ϵ and is said to have length 0.

Recursive definition of of a set S.

(base clause) Specify that certain elements, called founders, are in S: if c is a founder, then $c \in S$.

(recursion clause) Specify certain functions, called constructors, under which the set S is closed: if f is a constructor and $x \in S$, then $f(x) \in S$.

(minimality clause) Membership for S can always be demonstrated by (infinitely many) successive applications of the clauses above.

Structural induction over S.

To prove that $\forall x \in S\ P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

(basis step) show that $P(c)$ is true for every founder c; and

(induction step) show that $\forall x \in S\left(P(x) \Rightarrow P(f(x))\right)$ is true for every constructor f.

In words, if all the founders satisfy a property P, and P is preserved by all constructors, then all elements of S satisfy P.

Example #21: Recursive definition of $\mathbb{Z}_{\geq 0}$.

$\mathbb{Z}_{\geq 0}$ is the unique set with the following properties:

(1. what the founders are) $0 \in \mathbb{Z}_{\geq 0}$. (base clause)

(2. what the constructors are) If $x \in \mathbb{Z}_{\geq 0}$, then $x + 1 \in \mathbb{Z}_{\geq 0}$. (recursion clause)

(3. nothing more) Membership for $\mathbb{Z}_{\geq 0}$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

Cardinality

Pigeonhole Principle

Let A and B be finite sets. If there is an injection $f: A \to B$, then $|A| \leq |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m > n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with (at least) two pigeons.

Dual Pigeonhole Principle

Let A and B be finite sets. If there is a surjection $f: A \to B$, then $|A| \geq |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m < n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with no pigeons.

Definitions: Finite set and Infinite set

Let $\mathbb{Z}_n = \{1,2,3, \dots, n\}$, the set of positive integers from 1 to n.

A set S is said to be **finite** iff S is empty, or there exists a bijection from S to $\mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$.

A set S is said to be **infinite** if it is not finite.

Definition: Cardinality

The **cardinality** of a finite set S, denoted $|S|$, is

(i) 0 if $S = \emptyset$, or

(ii) n if $f: S \to \mathbb{Z}_n$ is a bijection.

Theorem: Equality of Cardinality of Finite Sets

Let A and B be any finite sets.

$|A| = |B|$ iff there is a bijection $f: A \to B$.

Definition: Same Cardinality (Cantor)

Given any two sets A and B. A is said to have the **same cardinality** as B, written as $|A| = |B|$, iff there is a bijection $f: A \to B$.

Theorem 7.4.1 Properties of Cardinality

The cardinality relation is an equivalence relation.
For all sets A, B and C:

a. **Reflexive**: $|A| = |A|$.
b. **Symmetric**: $|A| = |B| \to |B| = |A|$.
c. **Transitive**: $(|A| = |B|) \wedge (|B| = |C|) \to |A| = |C|$.

Proof: $|2\mathbb{Z}| = |\mathbb{Z}|$

1. To show that H is injective:
   1.1 Suppose $H(n_1) = H(n_2)$ for some integers n_1, n_2.
   1.2 Then $2n_1 = 2n_2$ (by the definition of H), and hence $n_1 = n_2$.
   1.3 Therefore H is injective.
2. To show that H is surjective:
   2.1 Suppose $m \in 2\mathbb{Z}$.
   2.2 Then m is an even integer, so $m = 2k$ for some integer k (by the definition of even integer)
   2.3 But $H(k) = 2k = m$.
   2.4 Thus $\exists k \in \mathbb{Z}$ s.t. $H(k) = m$.
   2.5 Therefore H is surjective.
3. Therefore H is a bijection, and so $2\mathbb{Z}$ and $\mathbb{Z}$ have the same cardinality (by Cantor's definition of cardinality).

The set A having the same cardinality as $\mathbb{Z}^+$ is called countably infinite.

Definition: Cardinal numbers

Define $\aleph_0 = |\mathbb{Z}^+|$. (Some author use $\mathbb{N}$ instead of $\mathbb{Z}^+$.)

$\aleph$ is pronounced "aleph", the first letter of the Hebrew alphabet. This is the first cardinal number.

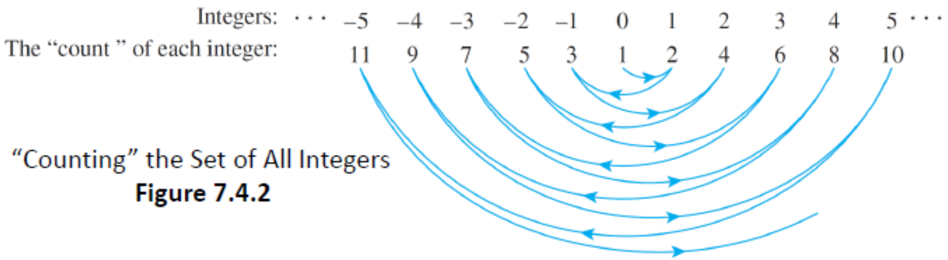
Definition: Countably infinite

A set S is said to be **countably infinite** (or, S has the cardinality of natural numbers) iff $|S| = \aleph_0$.

Definitions: Countable set and Uncountable set

A set is said to be **countable** iff it is finite or countably infinite.

A set is said to be **uncountable** if it is not countable



"Counting" the Set of All Integers
Figure 7.4.2

Every integer in $\mathbb{Z}$ is counted at most once (so the function is injective) and every integer in $\mathbb{Z}$ is counted at least once (so the function is surjective).

Therefore $\mathbb{Z}$ is countably infinite and hence countable.

9.2.3 $\mathbb{Q}^+$ is countable

Example #4: Show that $\mathbb{Q}^+$ (the set of all positive rational numbers) is countable.

Display the elements of $\mathbb{Q}^+$ in a grid as shown:

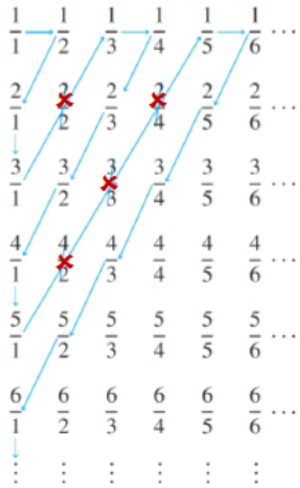


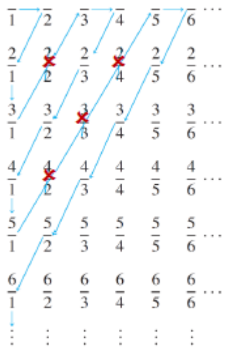
Figure 7.4.3

Define a function F from $\mathbb{Z}^+$ to $\mathbb{Q}^+$ by starting to count at $\frac{1}{1}$ and following the arrows as indicated, skipping over any number that has already been counted.

So, set $F(1) = \frac{1}{1}, F(2) = \frac{1}{2}, F(3) = \frac{2}{1}, F(4) = \frac{3}{1}$.

Then skip $\frac{2}{2}$ since $\frac{2}{2} = \frac{1}{1}$ which was counted.

Followed by $F(5) = \frac{1}{3}, F(6) = \frac{1}{4}, F(7) = \frac{2}{3}$, etc.



Note that every positive rational number appears somewhere in the grid, and the counting procedure is set up so that every point in the grid is reached eventually. Thus F is surjective.

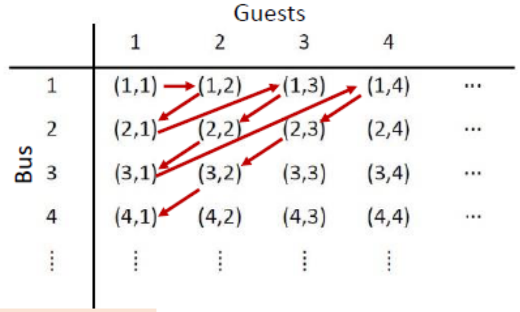
Skipping numbers that have already been counted ensures that no number is counted twice. Thus F is injective.

So F is a bijection from $\mathbb{Z}^+$ to $\mathbb{Q}^+$. Therefore $\mathbb{Q}^+$ is countably infinite and hence countable.

Theorem: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.

What if an infinite number of buses, each carrying an infinite number of guests, arrive at the Infinite Hotel? Is there room for all of them?

Display the elements of $\mathbb{Z}^+ \times \mathbb{Z}^+$ in a grid as shown:



The ordered pair (x, y) denotes bus x and guest y.

We then count the ordered paired in the following order according to this function $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ by:

$$f(x, y) = \frac{(x + y - 2)(x + y - 1)}{2} + x$$

9.2.5 Theorems

Theorem (Cartesian Product)

If sets A and B are both countably infinite, then so is $A \times B$.

(Proof omitted. Similar to diagonal counting method in example #4.)

Corollary (General Cartesian Product)

Given $n \geq 2$ countably infinite sets $A_1, A_2, \cdots, A_n$, the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is also countably infinite.

(Proof omitted. Proof by induction on n.)

Theorem (Unions)

The union of countably many countable sets is countable. That is, if $A_1, A_2, \cdots$ are all countable sets, then so is

$$\bigcup_{i=1}^{\infty} A_i$$

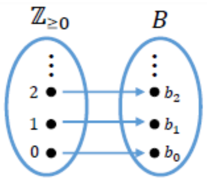
(Proof omitted. Similar to diagonal counting method in example #4.)

Definition: A set is said to be **countable** iff it is finite or countably infinite, that is, it has the same cardinality as $\mathbb{Z}_{\geq 0}$.

Proposition 9.1

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots \in B$ in which every element of B appears exactly once.

Justification:



function $f: \mathbb{Z}_{\geq 0} \to B$
$f(0), f(1), f(2), \cdots$
(surjectivity) $\forall b \in B\ \exists i \in \mathbb{Z}_{\geq 0}\ f(i) = b$
(injectivity) $\forall i, j \in \mathbb{Z}_{\geq 0}\ (f(i) = f(j) \Rightarrow i = j)$

sequence of elements of B
$b_0, b_1, b_2, \cdots$
Every $b \in B$ appears at least once.
Every $b \in B$ appears at most once.

Proposition 9.1

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots \in B$ in which every element of B appears exactly once.

Lemma 9.2: Countability via Sequence

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots$ in which every element of B appears.

Theorem: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable. (Revisit)

We will provide a proof sketch using sequence.

Proof sketch:

The figure below describes a sequence: (1,1),(1,2),(2,1),(1,3),(2,2),...
in which every element of $\mathbb{Z}^+ \times \mathbb{Z}^+$ appears.
So $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable by Lemma 9.2.

Bus \ Guests	1	2	3	4	
1	(1,1)	(1,2)	(1,3)	(1,4)	⋯
2	(2,1)	(2,2)	(2,3)	(2,4)	⋯
3	(3,1)	(3,2)	(3,3)	(3,4)	⋯
4	(4,1)	(4,2)	(4,3)	(4,4)	⋯
⋮	⋮	⋮	⋮	⋮	

Theorem 7.4.2 (Cantor)

The set of real numbers between 0 and 1,

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

is uncountable.

1. Suppose $(0,1)$ is countable.
2. Since it is not finite, it is countably infinite.
3. We list the elements x_i of $(0,1)$ in a sequence as follows:

$$\begin{aligned} x_1 &= 0.\, a_{11}\, a_{12} a_{13} \cdots a_{1n} \cdots \\ x_2 &= 0.\, a_{21}\, a_{22} a_{23} \cdots a_{2n} \cdots \\ x_3 &= 0.\, a_{31}\, a_{32} a_{33} \cdots a_{3n} \cdots \\ &\vdots \\ x_n &= 0.\, a_{n1}\, a_{n2} a_{n3} \cdots a_{nn} \cdots \\ &\vdots \end{aligned}$$

where each $a_{ij} \in \{0,1,\cdots,9\}$ is a digit.*

4. Now, construct a number $d = 0.\, d_1\, d_2 d_3 \cdots d_n \cdots$ s.t.

$$d_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1; \\ 2, & \text{if } a_{nn} = 1. \end{cases}$$

5. Note that $\forall n \in \mathbb{Z}^+, d_n \neq a_{nn}$. Thus, $d \neq x_n, \forall n \in \mathbb{Z}^+$.
6. But clearly, $d \in (0,1)$, hence a contradiction. Therefore $(0,1)$ is uncountable.

$$\boxed{\begin{aligned} x_1 &= 0.\, a_{11}\, a_{12} a_{13} \cdots a_{1n} \cdots \\ x_2 &= 0.\, a_{21}\, a_{22} a_{23} \cdots a_{2n} \cdots \\ x_3 &= 0.\, a_{31}\, a_{32} a_{33} \cdots a_{3n} \cdots \\ &\vdots \\ x_n &= 0.\, a_{n1}\, a_{n2} a_{n3} \cdots a_{nn} \cdots \end{aligned}}$$

Illustration:

0.20148802 ...	d_1 is 1 because $a_{11} = 2$
0.11666021 ...	d_2 is 2 because $a_{22} = 1$
0.03853320 ...	d_3 is 1 because $a_{33} = 8$
0.96776809 ...	d_4 is 1 because $a_{44} = 7$
0.00031002 ...	d_5 is 2 because $a_{55} = 1$

Hence $d = 0.12112$ ..., which is not in the list. So, the list is incomplete.
This is true regardless of how the elements in (0,1) are listed.

Theorem 7.4.3

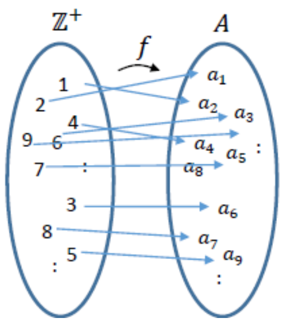
Any subset of any countable set is countable.

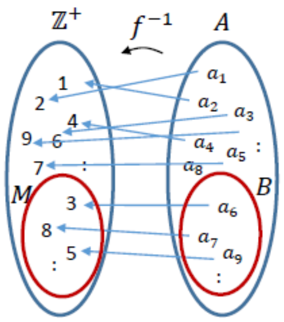
Proof:

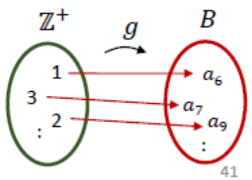
1. Let A be any countable set and B be any subset of A.
2. If A is finite then B must be finite and hence countable – done.
3. Suppose A is countably infinite. If B is finite, then B is countable – done.
4. Suppose B is infinite.
   - 4.1 Since A is countable, there is a bijection $f: \mathbb{Z}^+ \to A$.
   - 4.2 Let $M = f^{-1}(B)$ (note that f^{-1} is a bijection), and define a function $g: \mathbb{Z}^+ \to B$ inductively as follows:
     - S1. Let $g(1) = f(i_1)$, where i_1 is the minimum element in M.
     - S2. If $g(1), g(2), \cdots, g(k-1)$ have been defined, ...

4. Suppose B is infinite.
   - 4.1 Since A is countable, there is a bijection $f: \mathbb{Z}^+ \to A$.
   - 4.2 Let $M = f^{-1}(B)$ (note that f^{-1} is a bijection), and define a function $g: \mathbb{Z}^+ \to B$ inductively as follows :
     - S1. Let $g(1) = f(i_1)$, where i_1 is the minimum element in M.
     - S2. If $g(1), g(2), \cdots, g(k-1)$ have been defined, let

       $g(k) = f(i_k)$, where $i_k = \min\{m: m > i_{k-1}, m \in M\}$.
   - 4.3 g is a bijection (why?), hence B is countable.







Theorem 7.4.3

Any subset of any countable set is countable.

Corollary 7.4.4 (Contrapositive of Theorem 7.4.3)

Any set with an uncountable subset is uncountable.

Proposition 9.3

Every infinite set has a countably infinite subset.

Lemma 9.4: Union of Countably Infinite Sets.

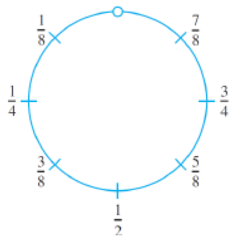
Let A and B be countably infinite sets. Then $A \cup B$ is countable.

9.4.2 Cardinality of $\mathbb{R}$

Example #5: Show that $|\mathbb{R}| = |(0,1)|$.

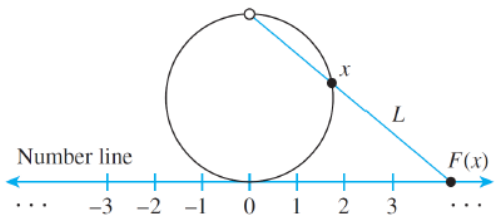
Let $S = (0,1)$, that is, $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

Imagine picking up S and bending it into a circle:



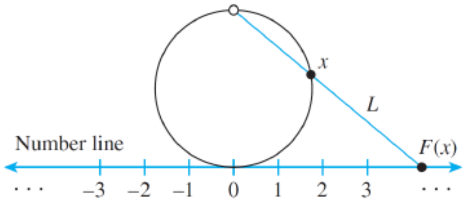
Define a function $F: S \to \mathbb{R}$ as follows:

Draw a number line and place the interval, S, bent into a circle as shown above, tangent to the line above the point 0, as shown below.



Larger Infinities: Cardinality of $\mathbb{R}$

For each point x on the circle representing S, draw a straight line L through the topmost point of the circle and x.



Let $F(x)$ be the point of intersection of L and the number line. ($F(x)$ is called the ***projection of*** x onto the number line.)

It can be seen that $F(x)$ is injective and surjective.
Hence S and $\mathbb{R}$ have the same cardinality, i.e. $|\mathbb{R}| = |(0,1)|$.

Counting & Probability

Definitions

- A **sample space** is the set of all possible outcomes of a random process or experiment.
- An **event** is a subset of a sample space.

Notation

For a finite set A, $|A|$ denotes the number of elements in A.

Equally Likely Probability Formula

If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability** of E, denoted P(E) is

$$P(E) = \frac{Number\ of\ outcomes\ in\ E}{Total\ number\ of\ outcomes\ in\ S} = \frac{|E|}{|S|}$$

Theorem 9.1.1: Number of Elements in a List

If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Theorem 9.2.1: Multiplication/Product Rule

If an operation consists of k steps,

The first step can be performed in n_1 ways,
The seconds steps can be performed in n_2 ways (regardless of how the first step was performed),
…
The kth step can be performed in n_k ways (regardless of how the preceding steps were performed)

Then the entire operation can be performed in

$$n_1 \times n_2 \times \ldots \times n_k \text{ ways.}$$

Example (Product Rule):

A typical PIN consists of four symbols chosen from the 26 letters in alphabet and 10 digits with repetition allowed.

Number of PINS possible: 36^4

Number of PINs possible w/o repetition: $\frac{36\times35\times34\times33}{36^4}$

Theorem 5.2.4 (Sets)

Suppose A is a finite set. Then $|\wp(A)| = 2^{|A|}$.
Since there are 2 choices (pick or drop) for every element a_i and there are n elements, by the multiplication rule, there are 2^n ways of forming subset.

Principle of Product (Multiplication Principle)

If there are m ways of doing something and n ways of doing another thing, then are are mn ways of performing both actions.

Principle of Sum (Addition Principle)

If we have m ways of doing something and n ways of doing another thing and we cannot do both at the same time, then there are m+n ways to choose one of these actions.

Permutations

A permutation of a set of objects is an ordering of the objects in a row. For example, the set of elements a,b,c has 6 permutations

abc acb cba bac bca cab

Theorem 9.2.2: Permutations

The number of permutations of a set with n $(n \geq 1)$ elements is $n!$
Note: $0! = 1$

Step 1: Choose an element to write first (n ways)
Step 2: Choose an element to write second (n-1 ways)
…
By multiplication rule: $n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1 = n!$

Example (Permutations):

How many ways can the letters in a word COMPUTER be arranged?

Since all letters are distinct, 8! permutations.

How many ways can the letters in the word *COMPUTER* be arranged if the letters *CO* must remain next to each other (in order) as a unit?

Treat 'CO' as one element. Then there are 7 total elements.
7! Permutations

If letters of the word *COMPUTER* are randomly arranged in a row, what is the probability that the letters *CO* remain next to each other (in order) as a unit?

$\frac{7!}{8!} = \frac{1}{8}$

Definition: r-permutation

An ***r*-permutation** of a set of ***n* elements** is an ordered selection of *r* elements taken from the set. The number of *r*-permutations of a set of *n* elements is denoted $P(n, r)$.

Given the set {a, b, c}, there are six ways to select two letters from the set and write them in order. [ab, ac, ba, bc, ca, cb].

Theorem 9.2.3: r-permutations from a set of n elements

If *n* and *r* are integers and $1 \leq r \leq n$, then the number of *r*-permutations of a set of *n* elements is given by the formula

$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1)$$

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

Theorem 9.3.1: Addition/Sum Rule

Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then $|A| = |A_1| + |A_2| + \cdots + |A_k|$.

Example (Addition Rule):

A password consists of one to three letters chosen from 26 letters with repetitions allowed. How many passwords are possible?

The set of all passwords can be partitioned into subsets consisting of those of length 1, length 2, and length 3. By addition rule, $N = 26 + 26^2 + 26^3$.

Theorem 9.3.2: Difference Rule:

If A is a finite set and $B \subseteq A$, then $|A \backslash B| = |A| - |B|$.

The difference rule holds as since $B \subseteq A$, $B \cup (A \backslash B) = \emptyset$ (the two sets are mutually disjoint), and $B \cup (A \backslash B) = A$ (the two sets union equals A). Hence by addition rule, $|B| + |A \backslash B| = |A|$. Subtracting $|B|$ from both sides gives

$$|A \backslash B| = |A| - |B|$$

Example (Difference Rule):

A PIN consists of four symbols chosen from 26 letters and 10 digits with repetition allowed. How many PINs contain repeated symbols?

There are 36^4 PINs when repetition is allowed (A). There are $36 \times 35 \times 34 \times 33$ PINs when repetition is not allowed (B). By difference rule, there are $36^4 - (36 \times 35 \times 34 \times 33)$ PINs that contains atleast one repeated symbol.

Probability of the Complement of an Event

If S is a finite sample space and A is an event in S, then

$$P(\bar{A}) = 1 - P(A)$$

Theorem 9.3.3: Inclusion/Exclusion Rule for 2 or 3 Sets

If A, B, and C are any finite sets, then

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

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

Pigeonhole Principle (PHP)

A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.

Generalized Pigeonhole Principle

For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $k < \frac{n}{m}$, then there is some $y \in Y$ such that y is the image of at least k+1 distinct elements of X.

Generalized Pigeonhole Principle (Contrapositive Form)

For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.

Counting & Probability II

Definition: r-combination

Let n and r be non-negative integers with $r \leq n$.

An r-combination of a set of n elements is a subset of r of the n elements

$\binom{n}{r}$ read "n choose r" denotes the number of subsets of size r (r-combinations) that can be chosen from a set of n elements

Theorem 9.5.1 Formula for $\binom{n}{r}$

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

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

Where n and r are non-negative integers

*Recall that $P(n,r) = \frac{n!}{(n-r)!}$

Theorem 9.5.2 Permutations with Sets of Indistinguishable Objects

Suppose a collection consists of n objects of which

n_1 are of type 1 and are indistinguishable from each other
n_2 are of type 2 and are indistinguishable from each other
:
n_k are of type k and are indistinguishable from each other

and suppose that $n_1 + n_2 + \ldots + n_k = n$. Then the number of distinguishable permutations of the n objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\cdots n_k!}$$

Summary

	Order Matters	Order Does Not Matter
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n,k)$	$\binom{n}{k}$

Pascal's Formula

Let n and r be positive integers, $r \le n$.

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Algebraic proof:

$$\text{R.H.S.} = \binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(n-r+1)!(r-1)!} + \frac{n!}{(n-r)!r!} = \frac{n!r}{(n-r+1)!r!} + \frac{n!(n-r+1)}{(n-r+1)!r!} = \frac{n!(n+1)}{(n-r+1)!r!}$$
$$= \frac{(n+1)!}{(n+1-r)!r!} = \binom{n+1}{r} = \text{L.H.S.}$$

Combinatorial proof:

1. $\binom{n+1}{r}$: choosing subsets of r elements from a set A of $n+1$ elements.
2. Let x be an element in A. A subset may or may not have x.
3. Case 1: If the subset has x, then there are $\binom{n}{r-1}$ ways of choosing these subsets.
4. Case 2: If the subset does not have x, then there are $\binom{n}{r}$ ways of choosing these subsets.
5. Therefore, there are $\binom{n}{r-1} + \binom{n}{r}$ ways of choosing subset of r elements from $n+1$ elements.

Theorem 6.3.1: Number of elements in a Power Set

If a set X has n $(n \ge 0)$ elements, then $\wp(X)$ has 2^n elements

Theorem 9.7.2: Binomial Theorem

Given any real numbers a and b and any non-negative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$
$$= a^n + \binom{n}{1} a^{n-1}b^1 + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n$$

$\binom{n}{r}$ is called binomial coefficient

$$(a+b)^5 = \sum_{k=0}^{5} \binom{5}{k} a^{5-k} b^k$$
$$= a^5 + \binom{5}{1}a^{5-1}b^1 + \binom{5}{2}a^{5-2}b^2 + \binom{5}{3}a^{5-3}b^3 + \binom{5}{4}a^{5-4}b^4 + b^5$$
$$= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Probability Axiom

Let S be a sample space. A probability function P from the set of all events in S to the set of real numbers satisfies the following axioms: For all events A and B in S,

1. $0 \le P(A) \le 1$
2. $P(\emptyset) = 0$ and $P(S) = 1$
3. If A and B are disjoint events $(A \cap B = \emptyset)$, then $P(A \cup B) = P(A) + P(B)$

Probability of the Complement of an Event

$P(\bar{A}) = 1 - P(A)$

Probability of a General Union of Two Events

If A and B are any events in a sample space S, then
$P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Definition: Expected Value

Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \dots, a_n$ which occur with probabilities $p_1, p_2, p_3, \dots, p_n$ respectively. The expected value of the process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n$$

Definition: Conditional Probability

Let A and B be events in a sample space S. If $P(A) \neq 0$, then the conditional probability of B given A denoted P(B|A) is

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

$$P(A \cap B) = P(B|A) \ \cdot P(A)$$

$$P(A) = \frac{P(A \cap B)}{P(B|A)}$$

Probability of a General Union of Two Events

If A and B are any events in a sample space S, then

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Theorem 9.9.1: Baye's Theorem

Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, \dots, B_n$

Suppose A is an event in S, and suppose A and all the B_i have non-zero probabilities. If k is an integer with $1 \le k \le n$, then

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + \cdots + P(A|B_n) \cdot P(B_n)}$$

Definition: Independent Events

If A and B are events in a sample space S, then A and B are independent iff

$P(A \cap B) = P(A) \cdot P(B)$

Definition: Pairwise Independent and Mutually Independent

Let A,B,C be events in a sample space S. A,B,C are **pairwise independent** iff they satistfy conditions 1-3 below. They are **mutually independent** iff they satisfy all four conditions below.

1. $P(A \cap B) = P(A) \cdot P(B)$
1. $P(A \cap C) = P(A) \cdot P(C)$
1. $P(B \cap C) = P(B) \cdot P(C)$
4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

Definition: Mutually Independent

Events $A_1, A_2, \dots, A_n$ in a sample space S are mutually independent iff the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset

$P(A_1 \cap A_2 \cap \dots \cap A_n) = P(A_1) \cdot P(A_2) \cdot \dots \cdot P(A_n)$

In general, the number of circular permutations of n objects is $(\boldsymbol{n-1})!$

Solutions of $\boldsymbol{x_1 + x_2 + x_3 + x_4 = 56}$ given that $\boldsymbol{x_i \ge 2^i + i}$ for $\boldsymbol{1 \le i \le 4}$

$x_1 \ge 3, x_2 \ge 6, x_3 \ge 11, x_4 \ge 20$

$3 + 6 + 11 + 20 = 40$

$y_i = x_i - (2^i + i),\ y_1 + y_2 + y_3 + y_4 = 16$

$\binom{16+4-1}{16} = 969$

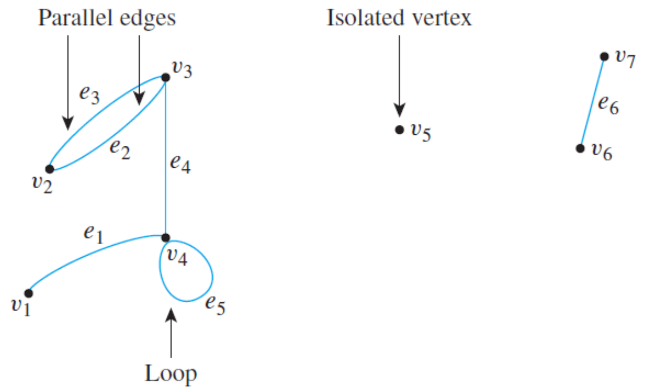
Graphs

An undirected graph is denoted by $G = (V, E)$ where

$V = \{v_1, v_2, \ldots, v_n\}$ is the set of vertices (or nodes) in G

$E = \{e_1, e_2, \ldots, e_k\}$ is the set of (undirected) edges in G

An (undirected) edge e connecting v_i and v_j is denoted as $e = \{v_i, v_j\}$



Example: $e_1 = \{v_1, v_4\}, e_5 = \{v_4, v_4\}$

Definition: Undirected Graph

An undirected graph G consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **edges**, where each (undirected) edge is associated with a set consisting of either one or two vertices called its **endpoints**.

An edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent vertices**; and a vertex that is an endpoint of a loop is said to be **adjacent to itself**.

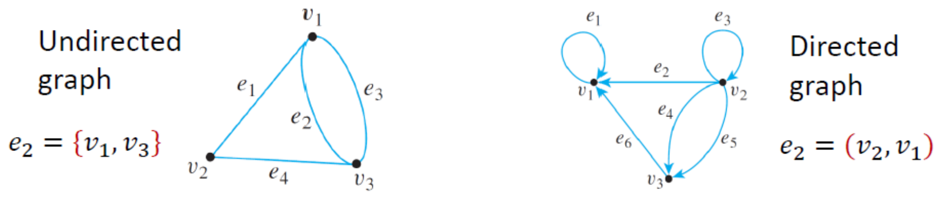
An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent edges**.

We write $e = \{v, w\}$ for an undirected edge e incident on vertices v and w.

Definition: Directed Graph

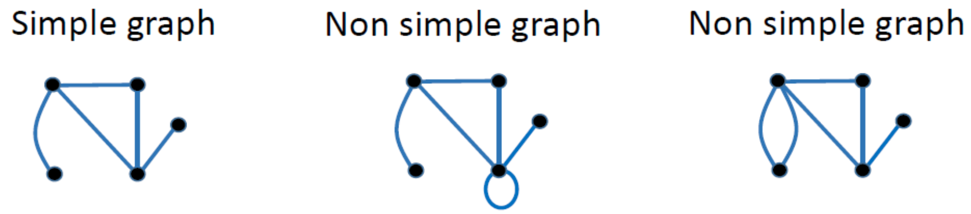
A directed graph, or **digraph**, G, consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **directed edges**, where each (directed) edge is associated with an ordered pair of vertices called its **endpoints**.

We write $e = (v, w)$ for a directed edge e from vertex v to vertex w.



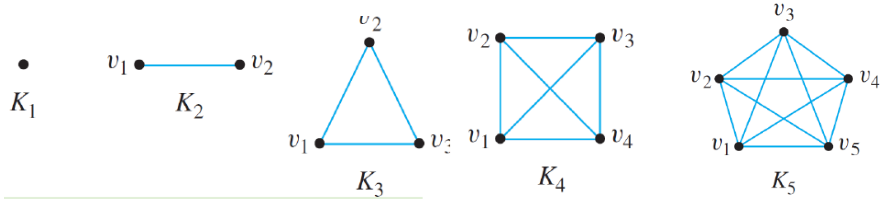
Definition: Simple Graph

A simple graph is an undirected graph that does not have any loops or parallel edges. (That is, there is at most one edge between each pair of distinct vertices.)



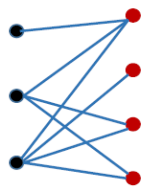
Definition: Complete Graph

A **complete graph** on ***n*** **vertices**, $n > 0$, denoted K_n, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.



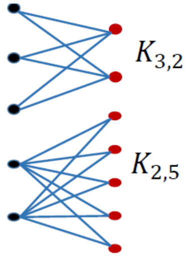
There are $\frac{n(n-1)}{2} = \binom{n}{2}$ edges in K_n.

Definition: Bipartite Graph
A **bipartite graph** (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V.



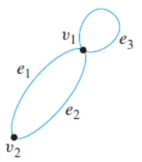
Bipartite graph

Definition: Complete Bipartite Graph
A **complete bipartite graph** is a bipartite graph on two disjoint sets U and V such that every vertex in U connects to every vertex in V.
If $|U| = m$ and $|V| = n$, the complete bipartite graph is denoted as $K_{m,n}$.

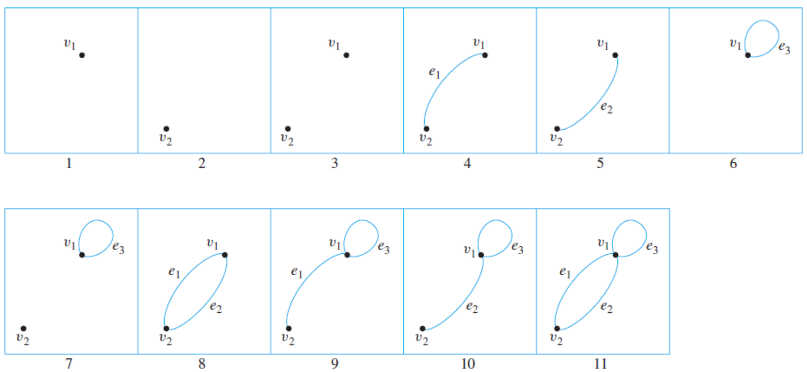


Definition: Subgraph
A graph H is said to be a **subgraph** of graph G if and only if every vertex in H is also a vertex in G, every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G.

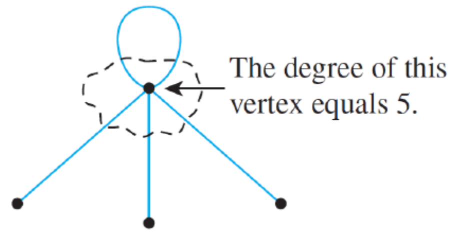
<u>Graph of G</u>



<u>Subgraphs of G</u>



Definition: Degree of a Vertex and Total Degree of an Undirected Graph
Let G be a undirected graph and v a vertex of G. The **degree** of v, denoted **deg(v)**, equals the number of edges that are incident on v, with an edge that is a loop counted twice.
The **total degree of G** is the sum of the degrees of all the vertices of G.



Theorem 10.1.1: The Handshake Theorem
If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G. Specifically, if the vertices of G are $v_1, v_2, \dots, v_n$ where $n \geq 0$, then

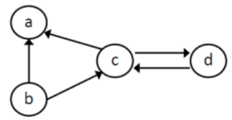
The **total degree of G** $= \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n)$
$$= \mathbf{2} \times (\boldsymbol{number\ of\ edges\ in\ G})$$

Corollary 10.1.2
The degree of a graph is even.

Proposition 10.1.3
In any graph there are an even number of vertices of odd degree.

Definition: Indegree and outdegree of a Vertex of a Directed Graph
Let $G = (V, E)$ be a directed graph and v a vertex of G. The **indegree** of v, denoted $\deg^-(v)$, is the number of directed edges that end at v. The **outdegree** of v, denoted $\deg^+(v)$, is the number of directed edges that originate from v.

$$\sum_{v\in V} \deg^-(v) = \sum_{v\in V} \deg^+(v) = |E|$$



$\deg^-(a) = 2$; $\deg^+(a) = 0$;
$\deg^-(b) = 0$; $\deg^+(b) = 2$;
$\deg^-(c) = 2$; $\deg^+(c) = 2$;
$\deg^-(d) = 1$; $\deg^+(d) = 1$.

Definitions

Let G be a graph, and let v and w be vertices of G.

A **walk from v to w** is a finite alternating sequence of adjacent vertices and edges of G. Thus a walk has the form: $v_0 e_1 v_1 e_2 \ldots v_{n-1} e_n v_n$

where the v's represent vertices, the e's represent edges, $v_0 = v$, $v_n = w$, and for all $i \in \{1,2,..,n\}$, v_{i-1} and v_i are the endpoints of e_i. The number of edges, n, is the **length** of the walk.

The **trivial walk** from v to v consists of the single vertex v.

A **trail from v to w** is a walk from v to w that does not contain a repeated edge.

A **path from v to w** is a trail that does not contain a repeated vertex.

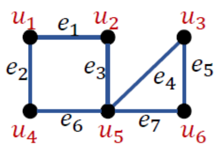
Definitions

A **closed walk** is a walk that starts and ends at the same vertex.

A **circuit** (or **cycle**) is a closed walk of length at least 3 that does not contain a repeated edge.

A **simple circuit** (or **simple cycle**) is a circuit that does not have any other repeated vertex except the first and last.

An undirected graph is **cyclic** if it contains a loop or a cycle; otherwise, it is **acyclic**.



Examples:

$u_1e_1u_2e_3u_5e_4u_3e_5u_6e_7u_5e_3u_2$ is a walk (may repeat edges and/or vertices).

$u_1e_1u_2e_3u_5e_4u_3e_5u_6e_7u_5e_6u_4$ is a trail (must not repeat edges).

$u_1e_1u_2e_3u_5e_4u_3e_5u_6$ is a path (must not repeat vertices and edges).

$u_5e_6u_4e_2u_1e_1u_2e_3u_5e_7u_6e_5u_3e_4u_5$ is a circuit.

$u_5e_6u_4e_2u_1e_1u_2e_3u_5$ is a simple circuit.

33

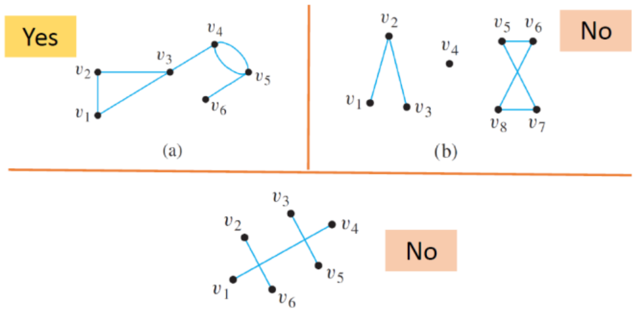
Definition: Connectedness

Two vertices v and w of a graph $G = (V, E)$ are **connected** if and only if there is a walk from v to w.

The graph G is connected if and only if given *any* two vertices v and w in G, there is a walk from v to w. Symbolically,

$$G \text{ is connected } iff\ \forall vertices\ v, w \in V, \exists\ a\ walk\ from\ v\ to\ w$$

Example: Connected



Lemma 10.2.1

Let G be a graph.

a. If G is connected, then any two distinct vertices of G can be connected by a path.

b. If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w in G.

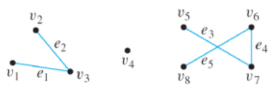
c. If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.

Definition: Connected Component

A graph H is a **connected component** of a graph G if and only if

1. The graph H is a subgraph of G;
2. The graph H is connected; and
3. No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.

Find all connected components of the following graph G.



G has 3 connected components H_1, H_2 and H_3 with vertex sets V_1, V_2 and V_3 and edge sets E_1, E_2 and E_3 , where

$V_1 = \{v_1, v_2, v_3\}$, $E_1 = \{e_1, e_2\}$

$V_2 = \{v_4\}$, $E_2 = \emptyset$

$V_3 = \{v_5, v_6, v_7, v_8\}$, $E_3 = \{e_3, e_4, e_5\}$

Definition: Euler Circuit
Let G be a graph. An **Euler circuit** for G is a circuit that contains every vertex and traverses every edge of G exactly once.

Definition: Eulerian Graph
An **Eulerian graph** is a graph that contains an Euler circuit.

Theorem 10.2.2
If a graph has an Euler circuit, then every vertex of the graph has positive even degree.

Contrapositive Version of Theorem 10.2.2
If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.

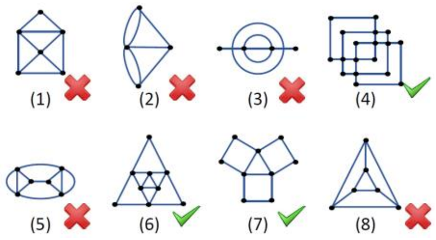
Theorem 10.2.3
If a graph G is connected and the degree of every vertex of G is a positive even integer, then G has an Euler circuit.

Theorem 10.2.4
A graph G has an Euler circuit if and only if G is connected and every vertex of G has positive even degree.

Definition: Euler Trail
Let G be a graph, and let v and w be two distinct vertices of G. An **Euler trail/path from v to w** is a sequence of adjacent edges and vertices that starts at v, ends at w, passes through every vertex of G at least once, and traverses every edge of G exactly once.

Corollary 10.2.5
Let G be a graph, and let v and w be two distinct vertices of G. There is an Euler trail from v to w if and only if G is connected, v and w have odd degree, and all other vertices of G have positive even degree.

Example: Euler Circuit



Definition: Hamiltonian Circuit
Given a graph G, a **Hamiltonian circuit** for G is a simple circuit that includes every vertex of G. (That is, every vertex appears exactly once, except for the first and the last, which are the same.)

Definition: Hamiltonian Graph
A **Hamiltonian graph** (also called **Hamilton graph**) is a graph that contains a Hamiltonian circuit.

Proposition 10.2.6
If a graph G has a Hamiltonian circuit, then G has a subgraph H with the following properties:
1. H contains every vertex of G.
2. H is connected.
3. H has the same number of edges as vertices.
4. Every vertex of H has degree 2.

The contrapositive of Proposition 10.2.6 says that if a graph G does *not* have a subgraph H with properties (1)–(4), then G does *not* have a Hamiltonian circuit.

Summary
An Eulerian circuit traverses every edge in a graph exactly once, but may repeat vertices, while a Hamiltonian circuit visits each vertex in a graph exactly once but may repeat edges.

	Repeated Edge?	Repeated Vertex?	Starts and Ends at Same Point?	Must Contain at Least One Edge?
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed walk	allowed	allowed	yes	no
Circuit	no	allowed	yes	yes
Simple circuit	no	first and last only	yes	yes

Definition: Matrix

An $m \times n$ (read "m by n") **matrix** A over a set S is a rectangular array of elements of S arranged into m rows and n columns.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix} \longleftarrow i\text{th row of } \mathbf{A}$$

jth column of **A**

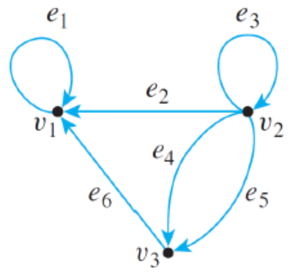
We write **A** = (a_{ij}).

If A and B are matrices, then A=B iff A and B have the same size and the corresponding entries of A and B are equal;
$a_{ij} = b_{ij} \;\; \forall i = 1,2, \dots, m$ and $j = 1,2, \dots, n$

A matrix for which the number of rows and columns are equal is called a **square matrix.**

If A is a square matrix of size $n \times n$, then the **main diagonal** of A consists of all the entries $a_{11}, a_{22}, \dots, a_{nn}$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1i} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2i} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{ni} & \cdots & a_{nn} \end{bmatrix} \longleftarrow \text{main diagonal of } \mathbf{A}$$



Directed Graph G

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Adjacency Matrix

A is called the adjacency matrix of G.

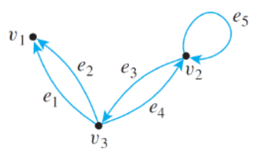
Definition: Adjacency Matrix of a Directed Graph

Let G be a directed graph with ordered vertices $v_1, v_2, \dots v_n$. The **adjacency matrix of G** is the $n \times n$ matrix **A** = (a_{ij}) over the set of non-negative integers such that

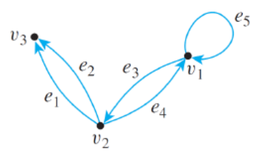
a_{ij} = the number of arrows from v_i to v_j for all $i, j = 1, 2, \dots, n$.

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{bmatrix} \end{array}$$

(a)



(a)



(b)

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

(b)

Definition: Adjacency Matrix of an Undirected Graph

Let G be an undirected graph with ordered vertices $v_1, v_2, \ldots v_n$. The **adjacency matrix of G** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of non-negative integers such that

a_{ij} = the number of edges connecting v_i and v_j for all $i, j = 1, 2, \ldots, n$.

Definition: Symmetric Matrix

An $n \times n$ square matrix A = (a_{ij}) is called **symmetric** if, and only if, $a_{ij} = a_{ji}$ for all $i, j = 1, 2, \ldots, n$.

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Note that the matrix is symmetric.

Definition: Scalar Product

Suppose that all entries in matrices **A** and **B** are real numbers. If the number of elements, n, in the ith row of **A** equals the number of elements in the jth column of **B**, then the **scalar product** or **dot product** of the ith row of **A** and the jth column of **B** is the real number obtained as follows:

$$[a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}] \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Definition: Matrix Multiplication

Let $\mathbf{A} = (a_{ij})$ be an $m \times k$ matrix and $\mathbf{B} = (b_{ij})$ an $k \times n$ matrix with real entries. The (matrix) product of **A** times **B**, denoted **AB**, is that matrix (c_{ij}) defined as follows:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & \boxed{c_{ij}} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \textstyle\sum_{r=1}^{k} a_{ir}b_{rj}.$$

for all $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Let $\mathbf{A} = \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix}$. Compute **AB**.

Solution:

$$\begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ c_{21} & c_{22} \end{bmatrix},$$

where

$$c_{11} = 2 \cdot 4 + 0 \cdot 2 + 3 \cdot (-2) = 2 \qquad \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix}$$

$$c_{12} = 2 \cdot 3 + 0 \cdot 2 + 3 \cdot (-1) = 3 \qquad \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix}$$

Multiplication of real numbers is commutative, but matrix multiplication is not.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}, \quad \text{but} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Identity Matrix

Definition: Identity Matrix

For each positive integer n, the $\boldsymbol{n \times n}$ **identity matrix**, denoted $I_n = (\delta_{ij})$ or just **I** (if the size of the matrix is obvious from context), is the $n \times n$ matrix in which all the entries in the main diagonal are 1's and all other entries are 0's. In other words,

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \qquad \text{for all } i, j = 1, 2, \ldots, n.$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

Definition: n^{th} Power of a Matrix

For any $n \times n$ matrix **A**, the **powers of A** are defined as follows:

$\mathbf{A}^0 = \mathbf{I}$ where **I** is the $n \times n$ identity matrix

$\mathbf{A}^n = \mathbf{A}\,\mathbf{A}^{n-1}$ for all integers $n \geq 1$

Let $\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$. Compute $\mathbf{A}^0$, $\mathbf{A}^1$, $\mathbf{A}^2$, and $\mathbf{A}^3$.

Solution:

$$\mathbf{A}^0 = \text{the } 2 \times 2 \text{ identity matrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\mathbf{A}^1 = \mathbf{A}\mathbf{A}^0 = \mathbf{A}\mathbf{I} = \mathbf{A}$$

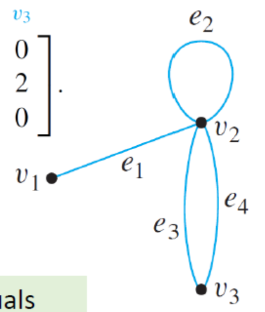
$$\mathbf{A}^2 = \mathbf{A}\mathbf{A}^1 = \mathbf{A}\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix}$$

$$\mathbf{A}^3 = \mathbf{A}\mathbf{A}^2 = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 9 & 10 \\ 10 & 4 \end{bmatrix}$$

The general question of finding the number of walks that have a given length and connect two particular vertices of a graph can easily be answered using matrix multiplication.

Consider the adjacency matrix **A** of the graph G.

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \!\!\begin{array}{c} \begin{matrix} v_1 & v_2 & v_3 \end{matrix} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}.$$



Compute $\mathbf{A}^2$:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 6 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$$

Note that the entry in row 2 and column 2 is 6, which equals the number of walks of length 2 from v_2 to v_2.

Theorem 10.3.2

If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and **A** is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \ldots, m$,

the ij-th entry of $\mathbf{A}^n$ = the number of walks of length n from v_i to v_j.

Definition: Isomorphic Graph

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.

***G* is isomorphic to *G*′**, denoted $G \cong G'$, if and only if there exist bijections $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ that preserve the edge-endpoint functions of G and G' in the sense that for all $v \in V_G$ and $e \in E_G$,

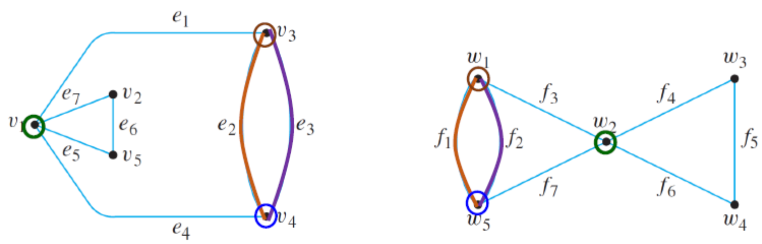
v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$.

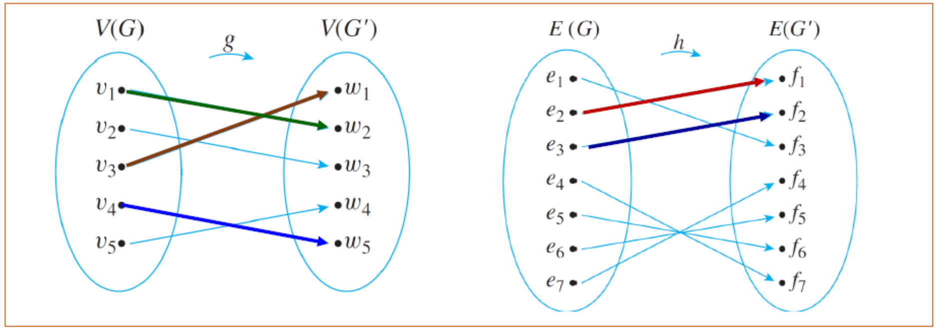
Alternative definition

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.

***G* is isomorphic to *G*′** if and only if there exists a permutation $\pi: V_G \to V_{G'}$ such that $\{u, v\} \in E_G \Leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$.

Example: Show that the following two graphs are isomorphic.





Theorem 10.4.1 Graph Isomorphism is an Equivalence Relation

Let S be a set of graphs and let $\cong$ be the relation of graph isomorphism on S. Then $\cong$ is an equivalence relation on S.

Definition: Planar Graph

A **planar graph** is a graph that can be drawn on a (two-dimensional) plane without edges crossing.

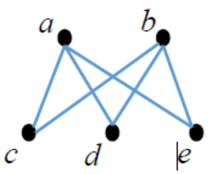
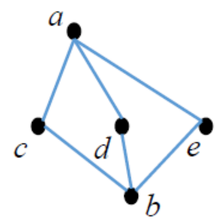
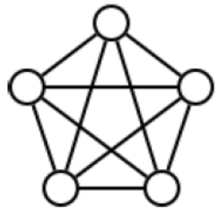


Figure 10.4.4

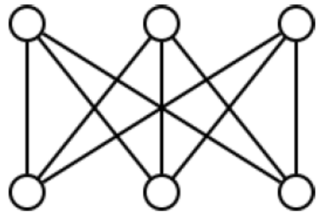
Non-planar representation of the graph



Planar representation of the graph



K_5



$K_{3,3}$

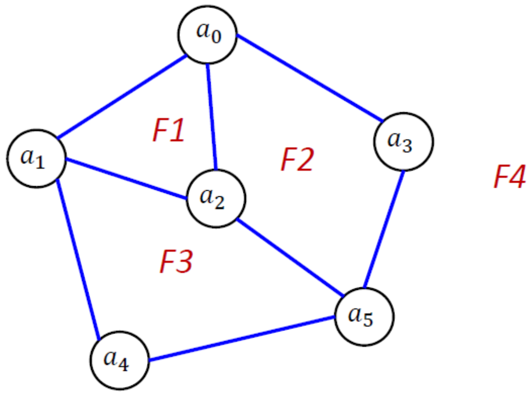
Kuratowski's Theorem:

A finite graph is planar if and only if it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.

Euler's Formula

For a connected planar simple graph $G = (V, E)$ with $e = |E|$ and $v = |V|$, if we let f be the number of faces, then

$$f = e - v + 2$$



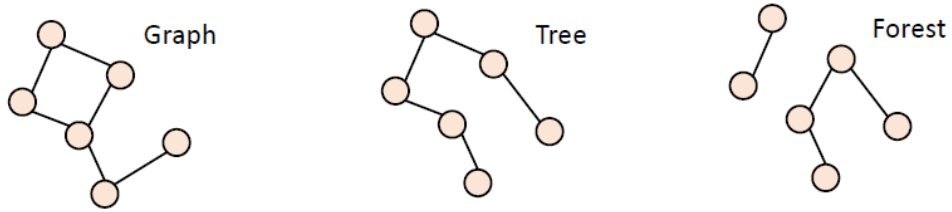
$e = 8$
$v = 6$
$f = 8 - 6 + 2 = 4$

Trees

Definition: Tree

(The graph is assumed to be undirected here)

A **graph** is said to be **circuit-free** iff it has no circuits.
A graph is called a **tree** iff it is circuit-free and connected.
A **trivial tree** is a graph that consists of a single vertex.
A graph is called a **forest** iff it is circuit-free and not connected.

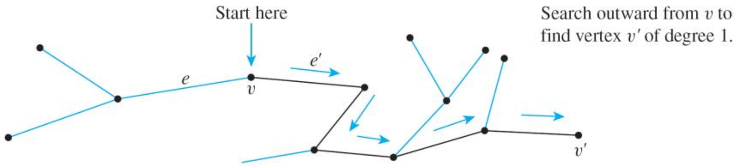


Lemma 10.5.1

Any non-trivial tree has at least one vertex of degree 1.

Proof: Let T be a particular but arbitrarily chosen non-trivial tree.
Step 1: Pick a vertex v of T and let e be an edge incident on v.
Step 2: While deg(v) > 1, repeat steps 2a, 2b and 2c:
2a: Choose e' to be an edge incident on v such that $e' \neq e$.
2b: Let v' be the vertex at the other end of e' from v.
2c: Let $e = e'$ and $v = v'$.

The algorithm must eventually terminate because the set of vertices of the tree T is finite and T is circuit-free. When it does, a vertex v of degree 1 will have been found.



Note: We can use another theorem to prove that a non-trial tree actually has at least two vertices of degree 1.

Definitions: Terminal vertex (leaf) and internal vertex

Let T be a tree.

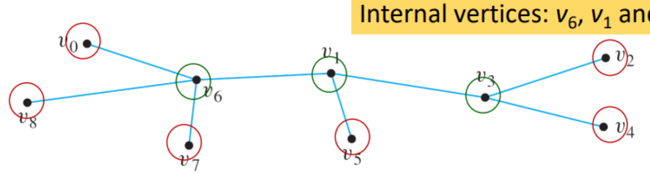
If T has only <u>one or two vertices</u>, then each is called a **terminal vertex** (or **leaf**).

If T has <u>at least three vertices</u>, then a <u>vertex of degree 1</u> in T is called a **terminal vertex** (or **leaf**), and a <u>vertex of degree greater than 1</u> in T is called an **internal vertex**.

Example: Find all terminal vertices (leaves) and all internal vertices in the following tree:

Leaves: v_0, v_2, v_4, v_5, v_7 and v_8.

Internal vertices: v_6, v_1 and v_3.



Theorem 10.5.2

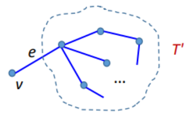
Any tree with n vertices (n > 0) has n – 1 edges.

Proof: By mathematical induction.
Let the property $P(n)$ be "any tree with n vertices has $n - 1$ edges".
$P(1)$: Let T be a tree with one vertex. Then T has no edges.
So $P(1)$ is true.

Show that for all integers $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true.

Suppose $P(k)$ is true.

1. Let T be a particular but arbitrarily chosen tree with $k + 1$ vertices.
2. Since k is positive, $(k + 1) \geq 2$, and so T has more than one vertex.
3. Hence, by Lemma 10.5.1, T has a vertex v of degree 1, and has at least another vertex in T besides v.
4. Thus, there is an edge e connecting v to the rest of T.
5. Define a subgraph T' of T so that $V_{T'} = V_T - \{v\}$ and $E_{T'} = E_T - \{e\}$.
   5.1 The number of vertices of T' is $(k + 1) - 1 = k$.
   5.2 T' is circuit-free.
   5.3 T' is connected.
6. Hence by definition, T' is a tree.
7. Since T' has k vertices, by inductive hypothesis, number of edges of T' = (number of vertices of T') – 1 = $k - 1$.
8. But number of edges of T = (number of edges of T') + 1 = k.
9. Hence $P(k+1)$ is true.

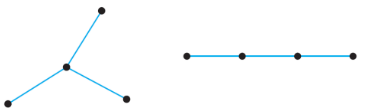


Theorem 10.1.1 The Handshake Theorem
Given a graph G=(V, E), the total degree of G = 2|E|.

Example:

- Every non-trivial tree has at least 2 vertices of degree of 1
- A tree with 4 vertices and 3 edges has total degree of 6
- For 4 vertices tree, the combinations of degree are:
  - 1,1,1,3 and 1,1,2,2

Therefore, there are two non-isomorphic trees with 4 vertices.



Lemma 10.5.3
If G is any connected graph, C is any circuit in G, and one of the edges of C is removed from G, then the graph that remains is still connected.

Reason: A circuit is connected by 2 distinct paths (clockwise and anticlockwise). Hence removing one edge means its not either clockwise/anticlockwise, and still connected.

Theorem 10.5.4
If G is a connected graph with n vertices and n – 1 edges, then G is a tree. (But not every graph with n vertices and n-1 edges is a tree. Must also be connected)

Proof:

1. Suppose G is a particular but arbitrarily chosen graph that is connected and has n vertices and $n-1$ edges.
2. Since G is connected, it suffices to show that G is circuit-free.
3. Suppose G is not circuit free
   3.1 Let C be the circuit in G.
   3.2 By Lemma 10.5.3, an edge of C can be removed from G to obtain a graph G' that is connected.
   3.3 If G' has a circuit, then repeat this process: Remove an edge of the circuit from G' to form a new connected graph.
   3.4 Continue the process of removing edges from the circuits until eventually a graph G'' is obtained that is connected and is circuit-free.
   3.5 By definition, G'' is a tree.
   3.6 Since no vertices were removed from G to form G'', G'' has n vertices.
   3.7 Thus, by Theorem 10.5.2, G'' has $n-1$ edges.
   3.8 But the supposition that G has a circuit implies that at least one edge of G is removed to form G''.
   3.9 Hence G'' has no more than $(n-1)-1 = n-2$ edges, which contradicts its having $n-1$ edges.
   3.10 So the supposition is false.
4. Hence G is circuit-free, and therefore G is a tree.

Assume G is not circuit-free. G has n vertices and $n-1$ edges.

G'' is the result of removing edges from circuits in G. At least 1 edge removed from G. G'' has n vertices and at most $n-2$ edges.

Definitions: Rooted Tree, Level, Height
A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the root.

The **level of a vertex** is the number of edges along the unique path between it and the root.

The **height of a rooted tree** is the maximum level of any vertex of the tree.

Definitions: Child, Parent, Sibling, Ancestor, Descendant
Given the root or any internal vertex v of a rooted tree, the **children** of v are all those vertices that are adjacent to v and are one level farther away from the root than v.

If w is a child of v, then v is called the **parent** of w, and two distinct vertices that are both children of the same parent are called **siblings**.

Given two distinct vertices v and w, if v lies on the unique path between w and the root, then v is an **ancestor** of w, and w is a **descendant** of v.

a. What is the level of v_5? 2

b. What is the level of v_0? 0

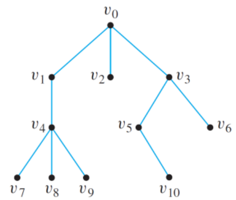
c. What is the height of this rooted tree? 3

d. What are the children of v_3? v_5 and v_6

e. What is the parent of v_2? v_0

f. What are the siblings of v_8? v_7 and v_9

g. What are the descendants of v_3? v_5, v_6 and v_{10}



Definitions: Binary Tree, Full Binary Tree

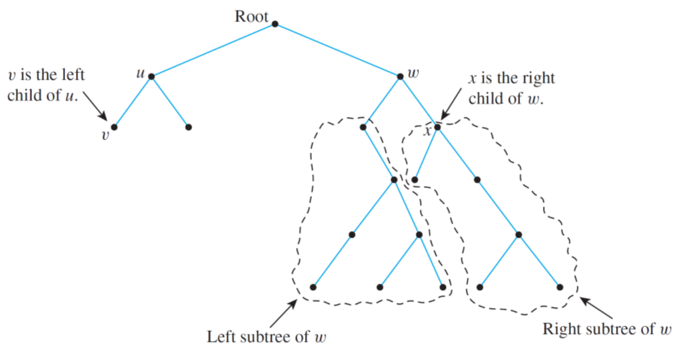
A **binary tree** is a rooted tree in which every parent has at most two children. Each child is designated either a left child or a right child (but not both), and every parent has at most one left child and one right child.

A **full binary tree** is a binary tree in which each parent has exactly two children.

Definitions: Left Subtree, Right Subtree

Given any parent v in a binary tree T, if v has a left child, then the **left subtree** of v is the binary tree whose root is the left child of v, whose vertices consist of the left child of v and all its descendants, and whose edges consist of all those edges of T that connect the vertices of the left subtree.

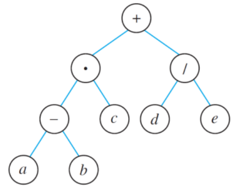
The **right subtree** of v is defined analogously.



Example:

Draw a binary tree to represent the expression

$((a - b) \cdot c) + (d/e)$



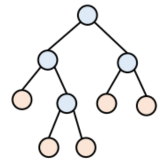
Theorem 10.6.1: Full Binary Tree Theorem

If T is a full binary tree with k internal vertices, then T has a total of 2k + 1 vertices and has k + 1 terminal vertices (leaves).

Proof:

1. Every vertex, except the root, has a parent.
2. Since every internal vertex of a full binary tree has exactly two children, the number of vertices that have a parent is twice the number of parents, or $2k$.

   #vertices of T = #vertices that have a parent + #vertices that do not have a parent = $2k + 1$



3. #terminal vertices = #vertices – #internal vertices = $2k + 1 - k = k + 1$
4. Therefore T has a total of **$2k + 1$ vertices** and has **$k + 1$ terminal vertices**.

Theorem 10.6.2

For non-negative integers h, if T is any binary tree with height h and t terminal vertices (leaves), then

$$t \leq 2^h$$

Equivalently,

$$\log_2 t \leq h$$

Depth-First Search

Pre-order (NLR)

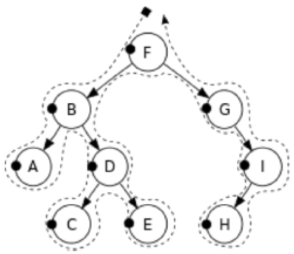
- Print the data of the root (or current vertex)
- Traverse the left subtree by recursively calling the pre-order function
- Traverse the right subtree by recursively calling the pre-order function

In-order (LNR)

- Traverse the left subtree by recursively calling the in-order function
- Print the data of the root (or current vertex)
- Traverse the right subtree by recursively calling the in-order function

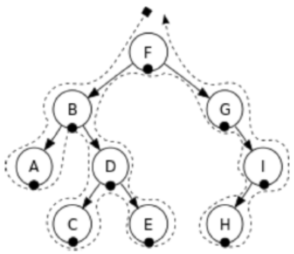
Post-order (LRN)

- Traverse the left subtree by recursively calling the post-order function
- Traverse the right subtree by recursively calling the post-order function
- Print the data of the root (or current vertex)



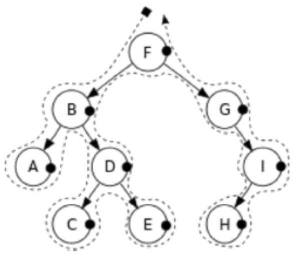
Pre-order:

F, B, A, D, C, E, G, I, H



In-order:

A, B, C, D, E, F, G, H, I



Post-order:

A, C, E, D, B, H, I, G, F

Definition: Spanning Tree

A spanning tree for a graph G is a subgraph of G that contains every vertex of G and is a tree

Proposition 10.7.1

1. Every connected graph has a spanning tree.
2. Any two spanning trees for a graph have the same number of edges.

Definitions: Weighted Graph, Minimum Spanning Tree

A **weighted graph** is a graph for which each edge has an associated positive real number **weight** . The sum of the weights of all the edges is the **total weight** of the graph.

A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.

If G is a weighted graph and e is an edge of G, then $\boldsymbol{w}(\boldsymbol{e})$ denotes the weight of e and $\boldsymbol{w}(\boldsymbol{G})$ denotes the total weight of G.

Algorithm 10.7.1 Kruskal

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Initialize T to have all the vertices of G and no edges.
2. Let E be the set of all edges of G, and let $m = 0$.
3. While ($m < n - 1$)
   - 3a. Find an edge e in E of least weight.
   - 3b. Delete e from E.
   - 3c. If addition of e to the edge set of T does not produce a circuit, then add e to the edge set of T and set $m = m + 1$

   End while

Output: T [T is a minimum spanning tree for G]

Algorithm 10.7.2 Prim

Input: G [a connected weighted graph with n vertices]

Algorithm:

1. Pick a vertex v of G and let T be the graph with this vertex only.
2. Let V be the set of all vertices of G except v.
3. For $i = 1$ to $n - 1$
    3a. Find an edge e of G such that (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V.
    3b. Add e and w to the edge and vertex sets of T, and delete w from V.

Output: T [T is a minimum spanning tree for G]

Tutorial Results

T6Q5 If $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective

T6Q6 If $f: X \to Y$ and $g: Y \to Z$ are both surjectiev, then $g \circ f$ is surjective

T6Q7 Order of a bijection $f: A \to A$ is defined to be smallest $n \in \mathbb{Z}^+$ s.t. $f \circ f \circ \ldots \circ f = id_A$

T8Q6

T8Q7 Set B is infinite iff there is $A \subseteq B$ s.t. $|A| = |B|$

T8Q9 Let A be a countably infinite set. $\wp(A)$ is uncountable.

T11Q5 Let $G = (V, E)$ be a simple, undirected graph. If G is connected, then $|E| \geqslant |V| - 1$.

T11Q6 Let $G = (V, E)$ be a simple, undirected graph. If G is acyclic, then $|E| \leqslant |V| - 1$.

T11Q7 Let $G = (V, E)$ be a simple, undirected graph. G is a tree if and only if there is exactly one path between every pair of vertices