INTRODUCTION TO SETS

SET THEORY

Def: Set - a collection of well defined objects.

Objects in the set are called elements or members, denoted by lower case letters.

a) $x \in A$, $x \notin A$

Ex: $P = \{1, 2, 3, \ldots\}$ positive integers

$N = \{0, 1, 2, 3, \ldots\}$ nonnegative integers → natural numbers

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ set of integers

$Q =$ rational numbers (m/n where m and $n \in Z$ and $n \neq 0$)

$\mathbb{R} =$ real numbers

Description of Sets

1. Describe the properties of members of the set

$A = \{x \mid x \in N \text{ and } x \leq 5\}$

(The set x, s.t. x is in N and $x \leq 5$)

2. List elements

$A = \{0, 1, 2, 3, 4, 5\}$ note: $\mathbb{R}$ cannot be listed.

3. Recursive Formula

$A = \{x_i \mid x_i = x_{i-1} + 1,\ i = 0, 1, 2, 3, 4, 5,\ x_0 = 0\}$

$x_0 = 0$

$i=1 \quad x_1 = x_0 + 1 = 0 + 1 = 1$

$i=2 \quad x_2 = x_1 + 1 = 1 + 1 = 2$

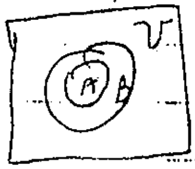
$i=3 \quad x_3 = x_2 + 1 = 2 + 1 = 3$

$i=4 \quad x_4 = x_3 + 1 = 3 + 1 = 4$

$i=5 \quad x_5 = x_4 + 1 = 4 + 1 = 5$

Def: The set A is said to be a subset of B, $A \subseteq B$, if every element of A is an element of B. A is a proper set of B, $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Venn Diagram:



weakness: can't show $A \subseteq B$ but can show $A \subset B$

use for pictures, counterexamples but not for

Properties of Sets (for all sets A, B, C)

use "elementwise approach"

$\square_1 \subseteq \square_2$

$x \in \square_1 \Rightarrow$ show $x \in \square_2$

1. $A \subseteq A$

$x \in A \Longrightarrow x \in A$

2. If $\underbrace{A \subseteq B \text{ and } B \subseteq C}_{\text{assumption}}$, then $\boxed{A \subseteq C}$

take $x \in A$ and show $x \in C$

$x \in A \xrightarrow{A \subseteq B} x \in B \xrightarrow{B \subseteq C} x \in C$

3. If $A \subseteq B$ and $B \subset C$, then $A \subset C$ note: to prove $A \subset C$: $\begin{matrix} A \subseteq C \\ A \neq C \end{matrix}$

$x \in A \xrightarrow{A \subseteq B} x \in B \xrightarrow{B \subset C} x \in C$

(for $A \neq C$, find a $y \in C$, $y \notin A$)

since $B \subset C$, $\exists\ y \in C$, $y \in B$

since $A \subseteq C$, $y \notin A$

4. If $A \subseteq B$ and $A \nsubseteq C$, then $B \nsubseteq C$.

note: to prove $B \nsubseteq C$, find a $y \in B$, $y \notin C$.

since $A \subseteq B$, $\exists y \in B$

since $A \nsubseteq C$, $\exists\ y \in A$, $y \notin C$

Def The universal set U is the set of all objects under consideration

Def The set of no elements is called the empty or null set and is denoted by $\emptyset$ or $\{\ \}$.

note: $\{\emptyset\}$ means $\emptyset \in \{\emptyset\}$ and is $\therefore$ not empty n: $\emptyset \subseteq A$ for all sets A

Pf. by contradiction (when ϕ is involved) → Assume opposite of desired conclusion and by logical steps come up w/ a contradiction.

Assume $\emptyset \nsubseteq A$ for some set A
There is $x \in \emptyset$, $x \notin A$
contradiction ∴ assumption is wrong

: If S is a set then $|S|$ is the cardinality of S and is the number of elements in the set

ei) $A = \{a, b, \ldots, z\}$, $|A| = 26$
ei) $|\emptyset| = 0$

F: Two sets are equal, $A = B$, iff $A \subseteq B$ and $B \subseteq A$.

note: $\{1,3,5\} = \{3,5,1\} = \{1,1,3,5,5,5\}$ (remember, order is not important in sets)

: Given a set S, the power set of S, denoted $P(S)$
$P(S) = \{A \mid A \subseteq S\}$ is the set of all subsets
→ has sets as elements

ie) $S = \{a, b, c\}$
$P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

ei) $P(\emptyset) = \{\emptyset\}$

ex) $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

note:

$\lvert A\rvert = n$	$\lvert P(A)\rvert = 2^n$
0 elements	1
1 element	2
3 elements	8

Cartesian Products

Def: The *ordered n-tuple* $(a_1, a_2, \ldots, a_n)$ is an *ordered* collection of elements where a_1 is the first element, a_2 is the second element and a_n is the n^{th} element.

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \text{ iff } a_1 = b_1,\ a_2 = b_2,\ \ldots,\ a_n = b_n$$

note: ordered pairs are 2-tuples

Def: Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of ordered pairs (a,b) where $a \in A$ and $b \in B$.

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

note: $|A| = 2$ $|B| = 3$
$|A \times B| = 2 \times 3$

ex) $A = \{1, 2\}$ $B = \{a, b, c\}$

$$A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$$
$$B \times A = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$$

note: The Cartesian product of $A \times B$ and $B \times A$ are not equal, unless $A = \phi$ or $B = \phi$ so that $A \times B = B \times A = \phi$ OR unless $A = B$.

Def: The Cartesian product of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is the set of ordered n-tuples.

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

$$\underbrace{A \times A \times \ldots \times A}_{n \text{ times}} = A^n$$

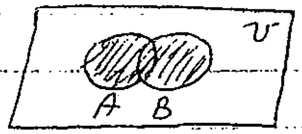
ex) $A = \{0,1\}$ $B = \{1,2\}$ $C = \{0,1,2\}$

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

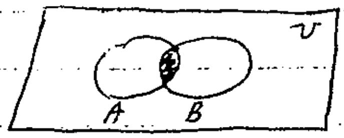
$|A \times B \times C| = |A| \cdot |B| \cdot |C| = 2 \times 2 \times 3 = 12$

1.5 SET OPERATIONS

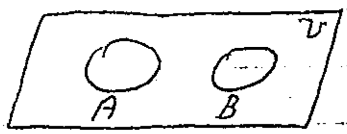
<u>Def</u>. The union of two sets A, B, denoted $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$



<u>Def</u>. The intersection of A, B, denoted $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$



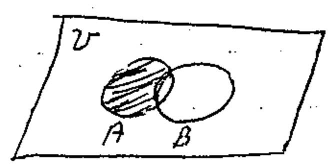
<u>Def</u>. Two sets are disjoint if $A \cap B = \emptyset$



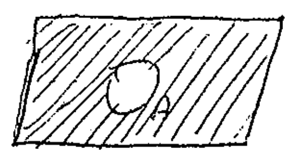
<u>Principle of inclusion - exclusion</u>

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

<u>Def</u> The difference of A, B, denoted $A - B$.
$A - B = \{x \mid x \in A \text{ and } x \notin B\}$



<u>Def.</u> The complement of A, denoted $\bar{A}$
$\bar{A} = \{x \mid x \in U \text{ and } x \notin A\} = \{x \mid x \notin A\}$



Theorem: $A-B = A \cap \overline{B}$

Pf: need to show $A-B \subseteq A \cap \overline{B}$ and $A \cap \overline{B} \subseteq A-B$

$$x \in A-B \overset{\text{Def} -}{\Longleftrightarrow} x \in A \text{ and } x \notin B \overset{\text{Def} \overline{A}}{\Longleftrightarrow} x \in A \text{ and } x \in \overline{B} \overset{\text{Def} \cap}{\Longleftrightarrow} x \in A \cap \overline{B}$$

Theorem: $\overline{\overline{A}} = A$

Pf: show $\overline{\overline{A}} \subseteq A$ and $A \subseteq \overline{\overline{A}}$

$$x \in \overline{\overline{A}} \overset{\text{Def} \overline{A}}{\Longleftrightarrow} x \notin \overline{A} \overset{\text{Def} \overline{A}}{\Longleftrightarrow} x \in A$$

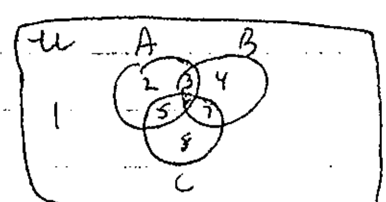
SET IDENTITIES (Theorems)

	Union	Intersection
Idempotent	$A \cup A = A$	$A \cap A = A$
Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$

Pf: $A \cup (B \cup C) = (A \cup B) \cup C$

$$x \in A \cup (B \cup C) \overset{\text{Def} \cup}{\Longleftrightarrow} x \in A \text{ or } x \in B \cup C \overset{\text{Def} \cup}{\Longleftrightarrow} x \in A \text{ or } (x \in B \text{ or } x \in C) \overset{\text{Logic}}{\Longleftrightarrow}$$
$$(x \in A \text{ or } x \in B) \text{ or } x \in C \overset{\text{Def} \cup}{\Longleftrightarrow} x \in (A \cup B) \cup C$$

Does $A \cup (B \cap C) = (A \cup B) \cap C$? No



$B \cap C = \{6, 7\}$
$A \cup (B \cap C) = \{2, 3, 5, 6, 7\}$
$A \cup B = \{2, 3, 4, 5, 6, 7\}$
$(A \cup B) \cap C = \{5, 6, 7\}$

∴ provides a counterexample

Distributive Laws for all sets A, B, C

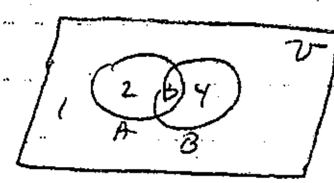
$$A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$$
$$A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$$

Pf: $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

$x\in A\cap(B\cup C) \xLeftrightarrow{\text{Def }\cap} x\in A \text{ and } x\in B\cup C \xLeftrightarrow{\text{Def }\cup} x\in A \text{ and } (x\in B \text{ or } x\in C) \xLeftrightarrow{\text{Logic}}$
$(x\in A \text{ and } x\in B) \text{ or } (x\in A \text{ and } x\in C) \xLeftrightarrow{\text{Def }\cap} x\in A\cap B \text{ or } x\in A\cap C \xLeftrightarrow{\text{Def }\cup} x\in(A\cap B)\cup(A\cap$

DeMorgans Law

$$\overline{A\cup B} = \bar{A}\cap\bar{B}$$
$$\overline{A\cap B} = \bar{A}\cup\bar{B}$$



$\overline{A\cup B} = \{1\}$ $\quad$ $\bar{A} = \{1,4\}$

$\overline{A\cap B} = \{1,2,4\}$ $\quad$ $\bar{B} = \{1,2\}$

Pf: $\overline{A\cap B} = \bar{A}\cup\bar{B}$

$x\in\overline{A\cap B} \xLeftrightarrow{\text{Def }\bar{A}} x\notin A\cap B \xLeftrightarrow{\text{Def }\cap} x\notin(A \text{ and } B) \xLeftrightarrow{\text{Logic}} x\notin A \text{ or } x\notin B \xLeftrightarrow{\text{Def }\bar{A}} x\in\bar{A} \text{ or } x\in\bar{B} \xLeftrightarrow{\text{Def }\cup} x\in\bar{A}\cup\bar{B}$

Lemmas:

$A\cup\bar{A} = U$
$A\cap\bar{A} = \phi$
$A\cup U = U$
$A\cap U = A$
$A\cup\phi = A$
$A\cap\phi = \phi$

Pf: $A\cap\bar{A}=\phi$
Assume $A\cap\bar{A}\neq\phi$
Then $x\in A\cap\bar{A}$
Def $\cap$ $x\in A$ and $x\in\bar{A}$
Def $\bar{A}$ $x\in A$ and $x\notin A$
contradiction

Pf: $A\cup\bar{A}=U$
$x\in A\cup\bar{A} \xLeftrightarrow{\text{Def }\cup} x\in A \text{ or } x\in\bar{A}$
$\xLeftrightarrow{\text{Def }\bar{A}} x\in A \text{ or } x\notin A \Longleftrightarrow x\in U$
(it really doesn't need to be pro
that something $\subseteq U$

Lemma: If $A\subseteq B$, then $A\cap B=A$

Pf:

$x\in A\cap B \xLeftrightarrow{\text{Def }A} x\in A \text{ and } x\in B \xLeftrightarrow{A\subseteq B} x\in A$

only needed when going $\Leftarrow$
not needed $\Rightarrow$

called Geometry style approach

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

$$\begin{aligned}
\overline{A\cup(B\cap C)} &= \bar{A}\cap\overline{(B\cap C)} && \text{DeMorgans} \\
&= \bar{A}\cap(\bar{B}\cup\bar{C}) && \text{DeMorgans} \\
&= (\bar{B}\cup\bar{C})\cap\bar{A} && \text{Commutative } (\cap) \\
&= (\bar{C}\cup\bar{B})\cap\bar{A} && \text{Commutative } (\cup)
\end{aligned}$$

Prove: $A-(A-B) = A\cap B$

$$\begin{aligned}
A-(A-B) &= A-(A\cap\bar{B}) && \text{Thm. } A-B = A\cap\bar{B} \\
&= A\cap(\overline{A\cap\bar{B}}) && \text{"} \\
&= A\cap(\bar{A}\cup\bar{\bar{B}}) && \text{DeMorgans} \\
&= A\cap(\bar{A}\cup B) && \text{Th. } \bar{\bar{A}} = A \\
&= (A\cap\bar{A})\cup(A\cap B) && \text{Distributive Law} \\
&= \phi\cup(A\cap B) && \text{Lemma } A\cap\bar{A} = \phi \\
&= A\cap B && \text{Lemma } A\cup\phi = A
\end{aligned}$$

"Generalized Unions and Intersections"

$$A_1\cap A_2\cap\dots\cap A_n = \bigcap_{i=1}^{n} A_i = \{x \mid x\in A_1 \text{ and } x\in A_2 \text{ and } \dots \text{ and } x\in A_n\}$$

$$A_1\cup A_2\cup\dots\cup A_n = \bigcup_{i=1}^{n} A_i = \{x \mid x\in A_1 \text{ or } x\in A_2 \text{ or } \dots \text{ or } x\in A_n\}$$

ex) Let $U = P = \{1,2,3,\dots\}$

let $A_i = \{i, i+1, i+2, \dots\}$ $i = 1,2,3,\dots$

$A_1 = P = \{1,2,3,\dots\}$

$A_2 = \{2,3,4,\dots\}$

$A_3 = \{3,4,5,\dots\}$

$\bigcup_{i=1}^{n} A_i = A_1 = P$ $\quad\quad$ $\bigcap_{i=1}^{n} A_i = A_n = \{n, n+1, n+2, \dots\}$

Given a finite universe
Computer Representation of Sets
Arbitrary ordering of $U = (a_1, a_2, a_3, \ldots, a_n)$

Def: A bit (binary digit) is either a 1 or 0
A bit string is a finite sequence of 1's + 0's

Represent a subset A of U w/ a bit string of length n where the i^{th} bit is 1 if $a_i \in A$, i^{th} bit is 0 if $a_i \notin A$

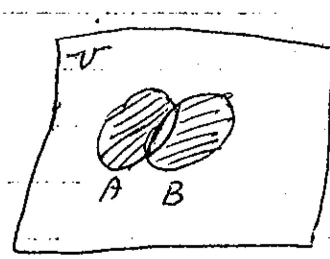
ex) $U = \{1, 2, 3, \ldots, 10\}$

$A = \{1, 2, 5, 8, 9\} = 1100100110$

$\bar{A} = 0011011001$

Def: The symmetric difference of A, B, denoted $A \oplus B$

$$A \oplus B = \{X \mid X \in A \text{ or } X \in B \text{ and } X \notin (A \text{ and } B)\}$$



Thm1: $A \oplus B = (A \cup B) - (A \cap B)$

Pf: $X \in A \oplus B \xLeftrightarrow{\text{Def } \oplus} X \in A \text{ or } X \in B \text{ and } X \notin (A \text{ and } B) \xLeftrightarrow{\text{Def } \cup, \cap} X \in A \cup B \text{ and } X \notin A \cap B \xLeftrightarrow{\text{Def } -} X \in (A \cup B) - (A \cap B)$

Thm2: $A \oplus B = (A - B) \cup (B - A)$

Pf: $X \in A \oplus B \xLeftrightarrow{\text{Def } \oplus} X \in A \text{ or } X \in B \text{ and } X \notin (A \text{ and } B) \xLeftrightarrow{\text{Logic}} (X \in A \text{ and } X \notin B) \text{ or } (X \in B \text{ and } X \notin A)$
$\xLeftrightarrow{\text{Def } -} X \in A - B \text{ or } X \in B - A \xLeftrightarrow{\text{Def } \cup} X \in (A - B) \cup (B - A)$

Ch. 6 Relations

Reuben Soto

6.1 Relations & Their Properties

<u>Def</u>: Let A and B be sets. A <u>binary relation from A to B</u> is a subset of $A \times B$.

(note: elements of relations are always ordered pairs)

If $(a,b) \in R$, we say that a is related to b, aRb.
If $(a,b) \notin R$, we say that a is not related to b, $a \not R b$

ex) Let A be the cities in the US and B be the states in the US. Define the relation R by aRb if a is in the state b

(Miami, FL) $\in R$
(San Fran, WY) $\notin R$

<u>Def</u>: A relation from A to A is called a <u>relation on A</u>. (subset of $A \times A$)

ex) Consider the following relations on $\mathbb{Z}$.

$R_1 = \{(a,b) \mid a \leq b\} = \{(1,1), (1,2), (-10,50), \ldots\}$
$R_2 = \{(a,b) \mid a = b \text{ or } a = -b\} = \{(1,1), (1,-1), (-1,1), (-1,-1), (0,0), \ldots\}$
$R_3 = \{(a,b) \mid a+b \leq 3\} = \{(1,2), (1,1), (-10,5), \ldots\}$

ex) How many relations are there on a set with n elements?

$|A| = n$
$|A \times A| = n^2$
$|P(A \times A)| = 2^{n^2}$

Properties of a Relation R on A

① <u>Reflexive</u>: $(a,a) \in R$ for all $a \in A$ (aRa)

② <u>Irreflexive</u>: $(a,a) \notin R \ \forall a \in A$ $(a \not R a)$

③ <u>Symmetric</u>: If $\underset{aRb}{(a,b) \in R}$ then $\underset{bRa}{(b,a) \in R}$ $\forall a,b \in A$

④ <u>Antisymmetric</u>: If $\underset{aRb}{(a,b) \in R}$ and $\underset{bRa}{(b,a) \in R}$ then $a=b$ $\forall a,b \in A$.

in other words → If $a \neq b$ and $(a,b) \in R$, then $(b,a) \notin R$
counterexample: $(a,b) \in R$ and $(b,a) \in R$, $a \neq b$

⑤ <u>Transitive</u>: If $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$ $\forall a,b,c \in A$
(note: a and c could be the same)
counterexample: $(a,b) \in R$ and $(b,c) \in R$ but $(a,c) \notin R$

(EX) ① $N = \{0,1,2,\ldots\}$
$R = \{(a,b) \mid a+b \text{ is even}\}$
$R = \{(0,2),(1,1),(1,3),(2,4),\ldots\}$

Reflexive: $(a,a) \in R \ \forall a \in N$
$a+a = 2a$ is even

Not Irreflexive: since $(1,1) \in R$

Symmetric: If $(a,b) \in R$, then $a+b$ is even and $\therefore$ $b+a$ is even so $(b,a) \in R$ $\forall a,b \in N$

Not Antisymmetric: since $(1,3) \in R$ and $(3,1) \in R$

Transitive: if $(a,b) \in R$ and $(b,c) \in R$, then $a+b$ is even and $b+c$ is even so either all a,b,c are even or all a,b,c are odd. Either way $a+c$ is even

② $A = \{1,2,3,4\}$
$R = \{(1,1),(1,3),(4,2),(2,4),(2,3),(3,1)\}$

Not Reflexive: since $(2,2) \notin R$

Not Irreflexive: since $(1,1) \in R$

Not Symmetric: since $(2,3) \in R$ but $(3,2) \notin R$

Not Antisymmetric: since $(1,3) \in R$ and $(3,1) \in R$

Not Transitive: since $(4,2) \in R$ and $(2,4) \in R$ but $(4,3) \notin R$ OR since $(4,2) \in R$ and $(2,4) \in R$ but $(4,4) \notin R$

(Ex 3) $A = \mathbb{Z}$

$R = \{(x,y) \mid x+y$ is a multiple of 3, $x+y \equiv 0 \mod 3\}$

(notation: $x \equiv y \mod p$, $x-y \equiv 0 \mod p$; $x-y$ is a multiple of p, $x-y = p \cdot z$ for some $z \in \mathbb{Z}$)

$R = \{(0,3), (-1,4), (-2,-4), (1,2), \ldots\}$

Not Reflexive: since $(1,1) \notin R$

Not Irreflexive: since $(3,3) \in R$

Symmetric: if $(a,b) \in R$, then $a+b = 3z$ for some $z \in \mathbb{Z}$, then $b+a = 3z$ $\therefore$ $(b,a) \in R$ $\forall a,b \in \mathbb{Z}$

Not Antisymmetric: since $(1,2) \in R$ and $(2,1) \in R$

Not Transitive: since $(1,2) \in R$ and $(2,1) \in R$ but $(1,1) \notin R$ or
since $(2,4) \in R$ and $(4,5) \in R$ but $(2,5) \notin R$

(4) $A = \mathbb{Z}$

$R = \{(x,y) \mid x < y\}$

$R = \{(-2,5), (3,6), \ldots\}$

Not Reflexive: since $(1,1) \notin R$

Irreflexive: $(a,a) \notin R$ $\forall a \in \mathbb{Z}$ since $a \not< a$

Not Symmetric: since $(1,3) \in R$ but $(3,1) \notin R$

Antisymmetric: If $(a,b) \in R$ and $(b,a) \in R$,
then $a<b$ and $b<a \to$ impossible
since $F \to T$, the property holds

Transitive: If $(a,b) \in R$ and $(b,c) \in R$, then
$a<b$ and $b<c$, then $a<c$
$\therefore$ $(a,c) \in R$ $\forall a,b,c \in \mathbb{Z}$

(5) $A = \mathbb{Z}$

$R = \{(x,y) \mid x \leq y\}$

$R = \{(-2,5), (3,6), (1,1), \ldots\}$

Reflexive: $(a,a) \in R$ $\forall a \in \mathbb{Z}$ since $a \leq a$

Not Irreflexive: since $(1,1) \in R$

Not Symmetric: since $(3,6) \in R$ but $(6,3) \notin R$

Antisymmetric: If $(a,b) \in R$ and $(b,a) \in R$, then
$a \leq b$ and $b \leq a$ $\therefore$ $a=b$
$\forall a,b \in \mathbb{Z}$

Transitive: If $(a,b) \in R$ and $(b,c) \in R$, then
$a \leq b$ and $b \leq c$, then $a \leq c$ $\therefore$
$(a,c) \in R$ $\forall a,b,c \in \mathbb{Z}$

EX

6a $A = P$ (positive integers)

$R = \{(x,y) \mid x \text{ divides } y,\ x/y,\ y = x \cdot z \text{ for some } z \in Z\}$

$R = \{(2,4), (3,6), (1,1), \ldots\}$

Reflexive: $(a,a) \in R\ \forall a \in P$
$a|a$ because $a = a(1)$

Not Irreflexive: since $(1,1) \in R$

Not Symmetric: since $(2,4) \in R$ but $(4,2) \notin R$

Antisymmetric: If $(a,b) \in R$ and $(b,a) \in R$, then
$b = a \cdot z_1$ and $a = b \cdot z_2$ $z_2 z_1 \in P$
$b = (b \cdot z_2) z_1$
$z_1 z_2 = 1 \Rightarrow z_1 z_2 = 1$ or $\cancel{z_1 z_2 = -1}$
since $a,b > 0$

$\therefore a = b$

Transitive: If $(a,b) \in R$ and $(b,c) \in R$, then
$b = a \cdot z_1$ and $c = b \cdot z_2$ $z_1, z_2 \in Z$
$c = (a \cdot z_1) z_2$ then $a|c$ and
$(a,c) \in R\ \forall a,b,c \in P$

6b $A = Z$

$R = \{(x,y) \mid x \text{ divides } y,\ x/y,\ y = x \cdot z \text{ for some } z \in Z\}$

$R = \{(2,4), (3,6), (1,1), (1,-1), (2,0), (-5,5), \ldots\}$

Not Reflexive: since $(0,0) \notin R$

Not Irreflexive: since $(1,1) \in R$

Not Symmetric: since $(2,4) \in R$ but $(4,2) \notin R$

Not Antisymmetric: since $(1,-1) \in R$ and $(-1,1) \in R$

Transitive: If $(a,b) \in R$ and $(b,c) \in R$, then
$b = a \cdot z_1$ and $c = b \cdot z_2$ $z_1 z_2 \in Z$
$c = (a \cdot z_1) z_2$ then $a|c$ and
$(a,c) \in R\ \forall a,b,c \in Z$

$A=\{1,2,3\}$
$R=\{(1,1),(2,2)(3,3)\}$

[Re]flexive : by inspection

[No]t Irreflexive : since $(1,1) \in R$

[S]ymmetric : by inspection

[A]ntisymmetric : by inspection

[Tr]ansitive : by inspection

$A=\phi$
$R=\phi$

[R]eflexive : Pf by contradiction, Assume R is not Reflexive. $\exists x \in A$ s.t. $(x,x) \notin R$. contradiction $\therefore$ assumption is wrong

Irreflexive : Pf by contradiction. Assume R is not irreflexive. $\exists a \in A$ where $(a,a) \in R$. contradiction $\therefore$ assumption was wrong

[S]ymmetric : by Inspection

[A]ntisymmetric : by inspection

[T]ransitive : by inspection

⑨ $A=\{1,2,3\}$
$R=\phi$

Not Reflexive : since $(1,1) \notin R$

Irreflexive : by inspection

Symmetric : by inspection

Antisymmetric : by inspection

Transitive : by inspection

⑩ A = people in the world
$R=\{(x,y) \mid x$ is the parent of $y\}$

Not Reflexive : John cannot be his own parent

Irreflexive : yes, because no person can be related to themselves

Not Symmetric : If Bob is the parent of John, then John can't be the parent of Bob

Antisymmetric : If Bob is the parent of Joe + Joe is the parent of Bob, then Joe = Bob
$F \Rightarrow ? \Rightarrow T$

Not Transitive : If x is the parent of y and y is the parent

Combining Relations

ex) $A = \{1,2,3\}$ $B = \{1,2,3,4\}$

$R_1 = \{(1,1),(2,2),(3,3)\}$ $R_2 = \{(1,1),(1,2),(1,3),(1,4)\}$

$R_1 \cup R_2 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(1,4)\}$

$R_1 \cap R_2 = \{(1,1)\}$

$R_1 - R_2 = \{(2,2),(3,3)\}$

$R_2 - R_1 = \{(1,2),(1,3),(1,4)\}$

<u>Def</u>: Let R be a relation from a set A to a set B. The inverse relation, $R^{-1} = \{(b,a) \mid (a,b) \in R\}$ (relation from B to A)
The complementary relation, $\bar{R} = \{(a,b) \mid (a,b) \notin R\}$

ex) $A = \mathbb{Z}$
$R = \{(a,b) \mid a < b\}$
$R^{-1} = \{(a,b) \mid a > b\}$
$\bar{R} = \{(a,b) \mid a \geq b\}$

ex) Say R is symmetric. $A = \{1,2,3\}$, if $R = \{(1,2),(2,1),(2,2),(2,3),(3,2)\}$ then
$R^{-1} = \{(2,1),(1,2),(2,2),(3,2),(2,3)\}$ (note $R = R^{-1}$)

Say $R = \{(1,1),(1,2),(2,1),(2,3),(3,2)\}$ then $R^{-1} = \{(1,1),(2,1),(1,2),(3,2),(2,3)\}$
note: If $R = R^{-1}$, then R is symmetric

<u>Theorem</u>: Let R be a relation on A. R is symmetric iff $R = R^{-1}$.

Pf: ① If R is symmetric, then $R=R^{-1}$ ② If $R=R^{-1}$, then R is symmetric

① $(x,y) \in R \underset{R \text{ is sym.}}{\overset{\text{Assume}}{\Longleftrightarrow}} (y,x) \in R \overset{\text{By } R^{-1}}{\Longleftrightarrow} (x,y) \in R^{-1} \Longleftrightarrow R \subseteq R^{-1} \therefore R = R^{-1}$

② $(x,y) \in R \underset{R=R^{-1}}{\overset{\text{Assume}}{\Longrightarrow}} (x,y) \in R^{-1} \overset{\text{Def } R^{-1}}{\Longrightarrow} (y,x) \in R$

5/ <u>EQUIVALENCE RELATIONS</u>

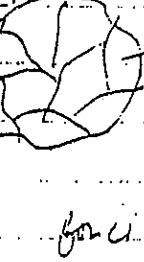
<u>Def</u>: An equivalence relation R on A is a relation which is reflexive, symmetric, and transitive.

Ex: ①. R is a relation on the set of strings of letters in English alphabet.
$w_1 R w_2$ iff $\text{length}(w_1) = \text{length}(w_2)$ w_1, w_2 strings
$\ell(w_1) = \ell(w_2)$

Reflexive: wRw $\forall$ strings w $\ell(w) = \ell(w)$
Symmetric: If $w_1 R w_2$ then $\ell(w_1) = \ell(w_2)$ then $\ell(w_2) = \ell(w_1)$ then $w_2 R w_1$ $\forall$ strings w_1, w_2
Transitive: If $w_1 R w_2$ and $w_2 R w_3$, then $\ell(w_1) = \ell(w_2)$ and $\ell(w_2) = \ell(w_3)$, then $\ell(w_1) = \ell(w_3)$ then $w_1 R w_3$ $\forall$ strings w_1, w_2, w_3

Def: Let R be an equivalence relation on set A. The equivalence class of $a \in A$ is the set of elements that are related to "a" written as $[a] = \{b \mid bRa\}$

A



equivalence classes

for ①) $[\Lambda] = \{\Lambda\}$
$[a] = \{a, b, c, \ldots, z\}$ $|[a]| = 26$
$[aa] = \{aa, ab, ac, \ldots, az, bb, \ldots, za, \ldots, zz\}$ $|[aa]| = 26^2$
$[aaa] = \{aaa, \ldots, zzz\}$ $|[aaa]| = 26^3$

ei2) R is a relation on the set of all real numbers
aRb iff $a-b \in \mathbb{Z}$ (ex) $2R1$, $\pi R \pi - 2$, $2.2 R 2.1$)
Reflexive: $(a,a) \in R \Rightarrow aRa$ $\forall$ real numbers a $a-a=0 \in \mathbb{Z}$
Symmetric: If aRb then $a-b=z$, $z \in \mathbb{Z}$, then
$b-a=-z \in \mathbb{Z}$ $\forall$ reals a,b
Transitive: If aRb, bRc, then $a-b=z_1$ and $b-c=z_2$ $z_1, z_2 \in \mathbb{Z}$
then $a-c=z_1+z_2 \in \mathbb{Z}$ then aRc $\forall$ reals a,b,c

$[0]=\mathbb{Z}$
$[2.1]=\{\ldots,-1.9,-.9,.1,1.1,2.1,3.1,\ldots\} = \{2.1+z \mid z \in \mathbb{Z}\}$
$[\pi]=\{\pi+z \mid z \in \mathbb{Z}\}$

ei3) $A=\mathbb{Z}$
$R=\{(a,b) \mid a \equiv b \bmod 2\}$ $\equiv (a-b=2 \cdot z, z \in \mathbb{Z})$
Reflexive: $(a,a) \in R$ $\forall a \in \mathbb{Z}$, $a-a=0=2 \cdot 0$
Symmetric: If $(a,b) \in R$ then $a-b=2 \cdot z$, $z \in \mathbb{Z}$, then $b-a=2(-z)$ then $(b,a) \in R$
$\forall a,b \in \mathbb{Z}$
Transitive: If $(a,b) \in R$ and $(b,c) \in R$, then $a-b=2z_1$ and $b-c=2z_2$, then
$a-c=2(z_1+z_2)$ then $(a,c) \in R$ $\forall a,b,c \in \mathbb{Z}$

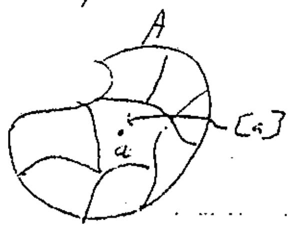
$[0]=\{\ldots,-4,-2,0,2,4,\ldots\}$
$[1]=\{\ldots,-3,-1,1,3,5,\ldots\}$) 2 classes → finite
$[5]=[1]$
$[-4]=[0]$

ei) $A=\mathbb{Z}$
$R=\{(x,y) \mid x \equiv y \bmod 4\}$

4 classes
$[0]=\{\ldots,-8,-4,0,4,8,12,16,\ldots\}$
$[1]=\{\ldots,-7,-3,1,5,9,13,17,\ldots\}$ (add 1 to above)
$[2]=\{\ldots,-6,-2,2,6,10,14,18,\ldots\}$ (add 1 to above or add 2 from original)
$[3]=\{\ldots,-5,-1,3,7,11,15,19,\ldots\}$ (add 1 to above or add 3 from original)

Partitions

Def: An equivalence relation R on A partitions the set A into equivalence classes. Every member of A is in one and only one class.



Theorem: Let R be an equivalence relation on A. The following statements are equivalent:

(i) aRb
(ii) $[a]=[b]$
(iii) $[a]\cap[b]\neq\phi$

$\Rightarrow$ ii) Pf: If aRb then $[a]=[b]$

"$\Rightarrow$" $x\in[a] \xRightarrow{\text{Def }[\,]} xRa$ and by assumption $aRb \xRightarrow{R \text{ transitive}} xRb \Rightarrow x\in[b]$ $\quad [a]\subseteq[b]$

"$\Leftarrow$" $x\in[b] \xRightarrow{\text{Def }[\,]} xRb$ and Assumption $\underset{R\text{ symmetric}}{bRa} \xRightarrow{R\text{ trans}} xRa \Rightarrow x\in[a]$ $\quad [b]\ [a]$

$\Rightarrow$ iii) If $[a]=[b]$ then $[a]\cap[b]\neq\phi$

$a\in[a]$ (because a is reflexive)

$a\in[a]\cap[b]\neq\phi$

$\Rightarrow$ i) If $[a]\cap[b]\neq\phi$, then aRb

Assume $\exists x\in A$ s.t. $x\in[a]\cap[b]$.

Since $x\in[a]$, then xRa

$x\in[b]$, then xRb

Also aRx (R symmetric)

Then aRb (R transitive + aRx and xRb.)

Theorem: $\bigcup_{a\in A}[a]=A$

"$\Rightarrow$" By def. $[a]\subseteq A$, $\bigcup_{a\in A}[a]\subseteq A$

"$\Leftarrow$" Take $a\in A \Rightarrow a\in[a]\in\bigcup[a]$, $A\subseteq\bigcup[a]$

1.6 Functions

Def : Let A and B be nonempty sets. A function denoted by f, from A to B is an assignment of a unique element of B to each element of A. We write $f(a)=b$ and $f: A \to B$.

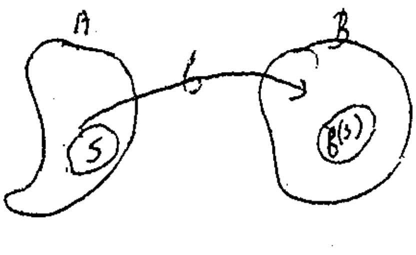
or $(a,b) \in f$ ← function is a special case of a Relation

Def : Let f be a function from A to B.
A is called the domain of f.
B is called the codomain of f.
If $f(a)=b$, we say b is the image of a, and a is the preimage of b.
The range of f is the set of all images of elements of A, $f(A)$.
f "maps" A to B.

ex). $A=\{a,b,c\}$ $B=\{1,2,3\}$

R_1	R_2	R_3	R_4
$a\to 1$	$a \to 1$	$a\to 1$	$a \to 1$
$a \to 2$	$b \to 2$	$b \to 1$	$b \to 2$
$b \to 3$		$c \to 1$	$c \to 3$
$c \to 3$			
not a function	not a function because c is not assigned	function from A to B	function from A to B

Def: Let f be a function from the set A to B. Let $S \subseteq A$. The image of S, denoted by $f(S)$ is the subset of B that consists of the images of the elements of S.



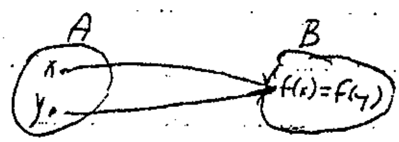
ei). $A=\{a,b,c,d,e\}$ $B=\{1,2,3,4\}$

$\underline{f}$

$a \to 2$ $S=\{b,c,d\}$
$b \to 1$
$c \to 4$ $f(S)=\{1,4\}$
$d \to 1$
$e \to 1$

f : Let $f: A \to B$ be a function, f is one-to-one, 1:1, or injective, if $x \neq y$ implies $f(x) \neq f(y)$ $\forall x,y \in A$

Counterexample:

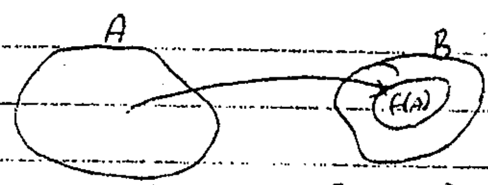


ei) $A=\{a,b,c,d\}$ $B=\{1,2,3,4\}$

a)
$a \to 1$
$b \to 1$
$c \to 2$
$d \to 3$
not 1:1

b)
$a \to 4$
$b \to 3$
$c \to 2$
$d \to 1$
is 1:1

E : Let $f: A \to B$ be a function f is onto or surjective if $f(A)=B$.



$f(A) \subseteq B$ for any function

To prove onto, need to prove $B \subseteq f(A)$: Given $b \in B$, find an $a \in A$ with $b=f(c$
Counterexample: find some $b \in B$ with no preimage.

Ex: ① $f: N \to N \quad f(x) = x^2$

$f = \{(0,0), (1,1), (2,4), (3,9), \ldots\}$

One-to-one: Assume $x \neq y \quad x, y \in N$

$x^2 \neq y^2 \quad x, y \in N$

$f(x) \neq f(y)$

Not onto: $3 \notin f(N)$

or

$2 \notin f(N)$

② $f: Z \to Z \quad f(x) = x^2$

$f = \{(0,0), (1,1), (-1,1), \ldots\}$

Not one-to-one since $(1,1) \in f$ and $(-1,1) \in f$

$f(1) = f(-1) = 1$

Not onto: $-2 \notin f(Z)$

OR

$2 \notin f(Z)$

③. $f: N \to N$ $\quad f(x) = x+1$

$f = \{(0,1), (1,2), (2,3), \ldots\}$

One to one: Assume $x \neq y$

$x+1 \neq y+1$

$f(x) \neq f(y) \quad \forall x,y \in N$

Not onto: ($\emptyset$ is not a preimage, not a 2nd value in f)

$\emptyset \notin f(N)$

since the natural numbers are $0, 1, 2, \ldots$ each one must exist as a second value in f

④. $f: Z \to Z$ $\quad f(x) = x+1$

$f = \{\ldots, (-1,0), (0,1), (1,2), \ldots\}$

One-to-one: Assume $x \neq y$

$x+1 \neq y+1$

$f(x) \neq f(y) \quad \forall x,y \in Z$

Onto: Take a $z \in Z$ (general element in the codomain (2nd $\exists$ $z \to \underline{z}$))

$z = f(\square)$ (fill in the square)

$z = f(z-1) \qquad f(z-1) = z-1+1 = z$

$z-1 \in Z$ (domain Z)

5. $f: N \to N_e \quad N_e = \{0, 2, 4, 6, \ldots\}$

$f(x) = 2x$

$f = \{(0,0), (1,2), (2,4), (3,6), \ldots\}$

One-to-One: if $x \neq y$

$2x \neq 2y$

$f(x) \neq f(y) \quad \forall x, y \in N$

Onto: Given $n_e \in N_e$

$n_e = f(\frac{n_e}{2}) \qquad \frac{n_e}{2} \in N \left(\text{because } \begin{matrix} n_e = 2n \\ n \in N \end{matrix} \right)$

6. $f: N \times N \to N$

$f((x,y)) = x \cdot y$

Not one-to-one since $f((2,5)) = 10 = f((5,2))$

Onto: Given $n \in N$

$n = f((1,n)) \qquad (1,n) \in N \times N \qquad$ [or $f((n,1))$]

Def: A function $f: \mathbb{R} \to \mathbb{R}$ is strictly increasing if $f(x) < f(y)$ whenever $x < y$ (strictly decreasing if $f(x) > f(y)$ whenever $x < y$)

If f is strictly increasing or decreasing, f is one-to-one because $x \neq y$ and then $f(x) < f(y)$ or $f(x) > f(y)$, $f(x) \neq f(y)$.

Def: A function f is called a bijection or a one-to-one correspondence if f is both one-to-one and onto.

xv). Let A be a set. The identity function on A is the function $i_A: A \to A$ with $i_A(x) = x$. The identity function is a bijection.

<u>One-to-One</u>

Assume $x \neq y$, $x, y \in A$

$i_A(x) \neq i_A(y)$

<u>Onto</u>

Given $a \in A$.

$a = i_A(a)$

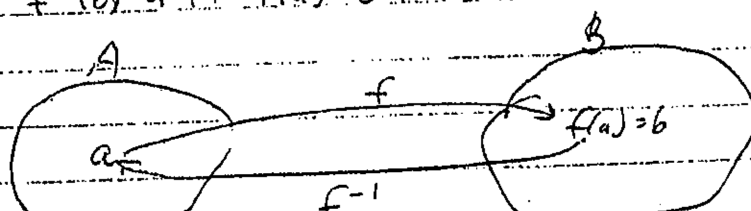
xi). $A = \{1,2,3\}$ $\quad B = \{a,b,c\}$

f	f^{-1}
$1 \to a$	$a \to 1$
$2 \to a$	$a \to 2$
$3 \to b$	$b \to 3$
not 1:1	not a function anymore because original function was not 1:1

xi). $A = \{1,2\}$ $\quad B = \{a,b,c\}$

f	f^{-1}
$1 \to a$	$a \to 1$
$2 \to b$	$b \to c$
(not onto)	not a function from B to A because c isn't mapped → original function needed to be onto for the inverse to be a function

<u>Def</u>: Let f be a bijection from A to B. The inverse function $f^{-1}: B \to A$ defined by $f^{-1}(b) = a$ if $f(a) = b$. f is called invertible. f^{-1} is a bijection as well.



P_6: <u>One-to-One</u>:

Assume $b_1 \neq b_2$

$f(a_1) \neq f(a_2)$ because f is onto

$a_1 \neq a_2$ (a_1 is preimage of b_1 and a_2 is a preimage of b_2) because ... is a fu

$f^{-1}(b_1) \neq f^{-1}(b_2)$ Def f^{-1}

<u>Onto</u>:

Given $a \in A$

$a = f^{-1}(\underline{f(a)})$

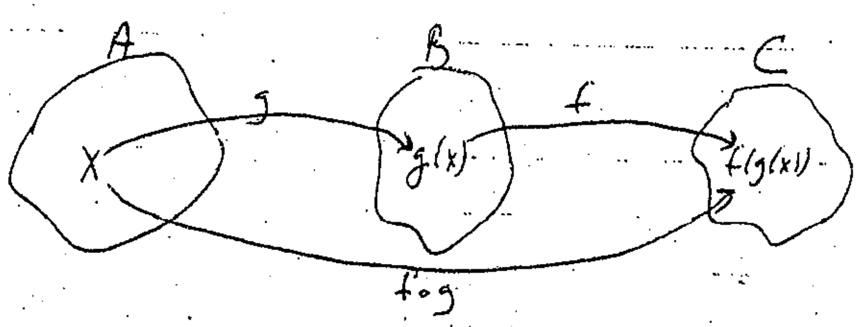
$f(a) \in B$ by def.

u) $f: Z \to Z$ $f(x) = x+1$

To find inverse let $y = f(x)$ and solve for x.

$y = x+1$	let $y = f(x)$
$x = y-1$	solve for (x)
$y = x-1$	switch x and y
$f: Z \to Z$ $f^{-1}(x) = x-1$	replace y with $f^{-1}(x)$

<u>Def</u>: Let $g: A \to B$ and $f: B \to C$ be functions. The composition of f with g, $f \circ g(x) = f(g(x))$.



$f \circ g: A \to C$

codomain

ii) $f: \mathbb{R} \to \mathbb{R}$ $f(x) = 2x+3$ $g(x) = x^2$ $g: \mathbb{R} \to \mathbb{R}$

$f \circ g(x) = f(g(x)) = f(x^2) = 2(x^2)+3 = 2x^2+3$

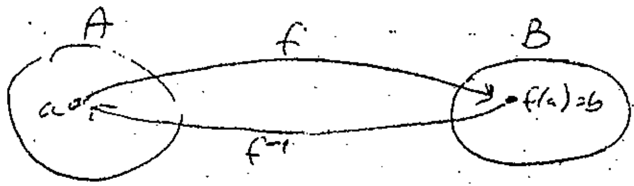
$g \circ f(x) = g(f(x)) = g(2x+3) = (2x+3)^2 = 4x^2+12x+9$

ii) $f: \mathbb{R} \to \mathbb{R}$ $\quad f(x) = 2x+3 \quad g(x) = x^2 \quad g: \mathbb{R} \to \mathbb{R}$

$$f \circ g(x) = f(g(x)) = f(x^2) = 2(x^2)+3 = 2x^2+3$$

$$g \circ f(x) = g(f(x)) = g(2x+3) = (2x+3)^2 = 4x^2+12x+9$$

iii) Say f is invertible, $f: A \to B$



$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a \qquad f^{-1} \circ f = i_A$

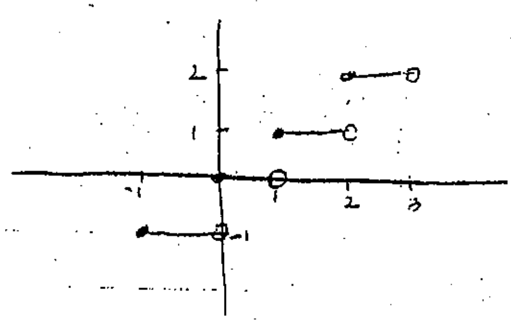
$(f \circ f^{-1})(b) = f(f^{-1}(b)) = b \qquad f \circ f^{-1} = i_B$

iv) $f: \mathbb{R} \to \mathbb{Z} \qquad f(x) = \lfloor x \rfloor = [x]$ (domain $= \mathbb{R}$, codomain $= \mathbb{Z}$)

called floor function or greatest integer function

$f(x) =$ greatest integer $\leq x$

$f(\pi) = 3$
$f(5) = 5$
$f(-1.3) = -2$
$f(-5) = -5$



note: not 1:1 but onto

1.7 SEQUENCES AND SUMMATIONS

Def: A sequence is a function whose domain is $N = \{0, 1, 2, \ldots\}$ OR $P = \{1, 2, \ldots\}$

$$a_1, a_2, a_3, \ldots, a_n, \ldots$$

$a_n = f(n)$ n^{th} term of sequence

ex) $a_n = \frac{1}{n}$ $f: P \to Q$

$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$

ex) $b_n = (-1)^n$ $f: N \to Z$

$1, -1, 1, -1, 1, \ldots$

SUMMATION NOTATION

$$\sum_{j=m}^{n} a_j = a_m + a_{m+1} + \ldots + a_n$$

$\boxed{\text{note: } a_j \text{ is like } f(j)}$

j = index of summation

n = upper limit

m = lower limit

$m, n \in Z$ $m \leq n$

ex) $\sum_{j=1}^{100} \frac{1}{j} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots \frac{1}{100}$

ex) $\sum_{j=1}^{10} 5 = \underbrace{5 + 5 + \ldots + 5}_{10} = 50$

CARDINALITY

DM 417B

FINITE SETS

$A = \{1,2,3,4\}$ $\quad B = \{a,b,c\}$

$|A| > |B|$

f

$1 \to a$

$2 \to b$

$3 \to c$

$4 \to a$

not 1:1

$A = \{1,2,3\}$ $\quad B = \{a,b,c,d\}$

$|A| < |B|$

f

$1 \to a$

$2 \to b$

$3 \to c$

1:1 but not onto

If $|A| = |B|$ then there is a bijection $f: A \to B$

$A = \{1,2,3,4\}$ $\quad B = \{a,b,c,d\}$

If $f: A \to B$ is a bijection, then $|A| = |B|$

Define a relation "$\cong$", "isomorphism" on the sets of all sets.

$A \cong B$ if there is a bijection $f: A \to B$

(A is isomorphic to B)

Theorem: "$\cong$" is an equivalence relation on the set of all sets.

Pf: Reflexive: $A \cong A$ for all sets A since $i_A: A \to A$ is a bijection

Symmetric: If $A \cong B$, then $B \cong A$ $\forall$ sets A, B

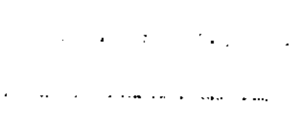
Since $A \cong B$, then there is an $f: A \to B$ which is a bijection,

then $f^{-1}: B \to A$ is a bijection then $B \cong A$.

Transitive: If $A \cong B$ and $B \cong C$, then $A \cong C$ $\forall$ sets A, B, C

Since $A \cong B$, there is an $f: A \to B$ which is a bijection

$B \cong C$, there is an $f: B \to C$ which is a bijection



④ If $f: A \to B$, $g: B \to C$, both 1:1, then $g \circ f: A \to C$ is 1:1

take $a_1 \neq a_2$, $a_1, a_2 \in A$

$f(a_1) \neq f(a_2)$, f is 1:1

⑥ If $f: A \to B$ is onto and $g: B \to C$ is onto, then $g \circ f: A \to C$ is onto

take $c \in C$, there is a $b \in B$ with $g(b) = c$. For that $b \in B$ there is an $a \in A$ with $f(a) = b$.

$g \circ f(a) = g(f(a)) = g(b) = c$

∴ Isomorphism is an equivalence relation on the set of all sets and ∴ the set of all sets can be partitioned into equivalence classes.

ei) $A = \{1, 2, 3\}$ $\quad |A| = 3$ $\quad$ (equivalent class is 3)
$B = \{a, b, c\}$ $\quad |B| = 3$

ei) $|\{x_1, x_2, \ldots, x_n\}| = n$ $\quad$ (equivalent class is n)
$A = \{a_1, \ldots, a_n\}$

Infinite Sets

Note: $P = \{1, 2, 3, \ldots\}$ $\quad |P| = \aleph_0$ aleph null $\quad$ (1st letter in Hebrew alph

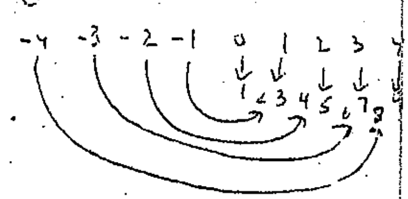
ei ① $N = \{0, 1, 2, \ldots\}$ $\quad |N| = \aleph_0$

$f: N \to P \quad f(n) = n + 1$

$$\begin{array}{lcccccc} (N) & 0 & 1 & 2 & 3 & 4 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ (P) & 1 & 2 & 3 & 4 & 5 & \ldots \end{array}$$

ei ② $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ $\quad |Z| = \aleph_0$

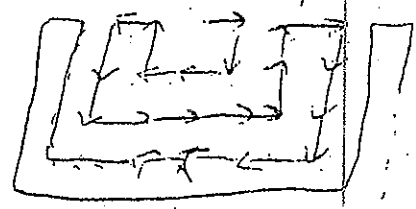
$f: Z \to P \quad f(z) = \begin{cases} 2z + 1 & \text{if } z \geq 0 \\ -2z & \text{if } z < 0 \end{cases}$



3

ii ③ $\mathbb{Q}$: $|\mathbb{Q}| = \aleph_0$

need to find pattern



(2) (divide by 2) (divide by 3) ... divide by n

$$\begin{array}{cccccccccc} \cdots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \\ \cdots & -\frac{3}{2} & -1 & -\frac{1}{2} & 0 & \frac{1}{2} & 1 & \frac{3}{2} & 2 & \cdots \\ \cdots & -1 & -\frac{2}{3} & -\frac{1}{3} & 0 & \frac{1}{3} & \frac{2}{3} & 1 & \frac{4}{3} & \cdots \\ & \vdots & & & & & & & & \end{array}$$

$P = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots)$
$Q = (0, 1, \frac{1}{2}, -\frac{1}{2}, -1, -2, -\frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, 2, 3, \frac{3}{2}, \ldots)$

$f: P \to Q$ bijection

ii) ④ $P \times P =$ $|P \times P| = \aleph_0$

$$\begin{array}{cccc} (1,1) \to & (1,2) & (1,3) & \cdots \\ (2,1) \leftarrow & (2,2) & (2,3) & \cdots \\ (3,1) \to & (3,2) \to & (3,3) & \cdots \\ \vdots & \vdots & \vdots & \end{array}$$

$P = (1, 2, 3, 4, 5, 6, \ldots)$
$P \times P = ((1,1), (1,2), (2,2), (2,1), (3,1), (3,2), \ldots)$

Def: A <u>countably infinite</u> set is a set with cardinality $\aleph_0$.
A <u>countable</u> set is a set that is finite or countably infinite.

Def: An <u>enumeration</u> of a set A, is a listing of A in the form $(a_1, a_2, \ldots, a_n)$ which lists A w/o repitition and has one a_n for each $n \in P$.

→ refers to only infinite sets

Theorems to prove infinite sets have cardinality $\aleph_0$.

If a set can be enumerated, it has cardinality $\aleph_0$ ...

$f: P \to A$ $\quad A = (a_1, a_2, \dots, a_n, \dots)$
$f(n) = a_n$

$A = (1, 4, 9, 16, 25, \dots)$
$|A| = \aleph_0$

$N_0 = \{1, 3, 5, 7, 9, \dots\}$
$|N_0| = \aleph_0$

if $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$
rewrite w/ a beginning value $Z = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ $\therefore |Z| = \aleph_0$

$A = \{100, 101, 102, \dots\}$
$|A| = \aleph_0$

$Z = \{-1, -2, -3, \dots\}$
$|Z| = \aleph_0$

Subsets of countable sets are countable
$\Rightarrow$ if original set is finite, any subset is finite and $\therefore$ countable.
$\Rightarrow$ if original set is infinite, then there is a bijection w/ P

We will prove all subsets of P are countable
Let $A \subseteq P$
$\Rightarrow$ if A is finite $\Rightarrow$ done
$\Rightarrow$ if A is infinite $\Rightarrow$ enumerate $A = (a_1, a_2, \dots, a_n, \dots)$ where
a_1 = smallest element of A
a_2 = smallest element of $A - \{a_1\}$
a_3 = smallest element of $A - \{a_1, a_2\}$

$\therefore$ by the 1st theorem, A is $\aleph_0$ and countable.

if your set is an infinite subset of a countable set, then your set is countable and $\therefore\ \aleph_0$

(i) $\mathbb{Q}^+ \subseteq \mathbb{Q}$ $\qquad |\mathbb{Q}^+| = \aleph_0$

(ii) $P \times \{1,2,3\} \subseteq P \times P$ $\qquad |P \times \{1,2,3\}| = \aleph_0$

Thm: The $\underbrace{\text{countable union}}_{a}$ of $\underbrace{\text{countable sets}}_{b}$ is countable

$\underbrace{\bigcup_{i \in I}}_{a} \underbrace{A_i}_{b}$

Let I = countable index set
either $I = \{1,2,\ldots,n\}$ or $I = P$

Pf: a) $I = \{1,2,\ldots,n\}$
Let a_{ij} = j^{th} element of the i^{th} set

(throw out repeats) $\bigcup_{i=1}^{n} A_i = \{a_{11}, a_{21}, \ldots, a_{n1}, a_{12}, a_{22}, \ldots, a_{n2}, a_{13}, a_{23}, \ldots, a_{n3}, \ldots\}$

either listing is finite or listing is an enumeration of the union.
$\therefore$ union is countable

b) $\bigcup_{i=1}^{\infty} A_i = (a_{11}, a_{12}, a_{22}, a_{21}, a_{31}, a_{32}, a_{33}, \ldots)$ (throw out repeats)

$A_1 \quad a_{11} \to a_{12} \quad a_{13}$
$A_2 \quad a_{21} \leftarrow a_{22} \quad a_{23}$ $\quad \therefore$ this is an enumeration of the union
$A_3 \quad a_{31} \to a_{32} \to a_{33}$

ii) Set of bit strings $= \bigcup_{n=0}^{\infty}$ bit strings of length n

|bit strings of length n| $= 2^n$ $\quad \therefore$ this is a countable union because $|\mathbb{N}| = \aleph_0$ of countable sets (2^n finite) is countable

ii) $N \times Z = \bigcup_{n=0}^{\infty} \{n\} \times Z$

$\{n\} \times Z$ is countable

$z \to (n, z)$

$f: Z \to \{n\} \times Z$

bijection

$\therefore$ is a countable union of countable sets which is countable.

Thm: If S and T are countable sets then $S \times T$ is a countable set.

ii) $N \times Z = \bigcup_{n=0}^{\infty} \{n\} \times Z$

N is countable and Z is countable $\therefore$ $N \times Z$ is countable set

Pf: Show that $S \times T$ is a countable union of countable sets

Since S is countable, $S \times \{t\}$ is countable.

$S \times T = \bigcup_{t \in T} S \times \{t\}$ is a countable union of countable set.

by theorem, $S \times T$ is countable

Def: An infinite set which does not have cardinality $\aleph_0$ is called uncountably infinite.

Thm: The real numbers are uncountably infinite. Cantor's diagonal argument.

Pf: Assume the real #'s are countably infinite and $\therefore$ can be enumerated.
(contradiction)

$\mathbb{R} = (r_1, r_2, r_3, \ldots, r_n, \ldots)$

$r_1 = a_1 . b_{11} b_{12} b_{13} b_{14}$

$r_2 = a_2 . b_{21} b_{22} b_{23} b_{24}$

$r_3 = a_3 . b_{31} b_{32} b_{33} b_{34}$

$\vdots$

$r_n = a_n . b_{n1} b_{n2} b_{n3} b_{n4} \cdots b_{nn} \cdots$

$\circledast$ a_i = integer position of r_i, $a_i \in Z$

b_{ij} = j^{th} decimal place of r_i

$b_{ij} \in \{0, 1, 2, \ldots, 9\}$

(cont) $\rightarrow$

Consider $b_{11}, b_{22}, b_{33}, \dots, b_{nn}, \dots$ is a sequence of 0's thru 9's.
We want to create $\overline{b_{11}}, \overline{b_{22}}, \overline{b_{33}}, \dots, \overline{b_{nn}}, \dots$

$$\overline{b_{ii}} = \begin{cases} 1 \text{ if } b_{ii} = 0 \\ 2 \text{ if } b_{ii} = 1 \\ 3 \text{ if } b_{ii} = 2 \\ \vdots \\ 9 \text{ if } b_{ii} = 8 \\ 0 \text{ if } b_{ii} = 9 \end{cases} \qquad i = 1, 2, 3, \dots \iff \overline{b_{ii}} = \begin{cases} b_{ii} + 1 \text{ if } b_{ii} = 0, \dots 8 \\ 0 \text{ if } b_{ii} = 9 \end{cases}$$

b_{11}	b_{22}	b_{33}	b_{44}	b_{55}
1	9	0	2	4
$\overline{b_{11}}$	$\overline{b_{22}}$	$\overline{b_{33}}$	$\overline{b_{44}}$	$\overline{b_{55}}$
2	0	1	3	5

Could define $\overline{b_{ii}} = \begin{cases} 0 \text{ if } b_{ii} \neq 0 \\ 1 \text{ if } b_{ii} = 0 \end{cases}$

(*) Define $b = .\overline{b_{11}}\,\overline{b_{22}}\,\overline{b_{33}} \cdots \overline{b_{nn}} \cdots$
b is a real number
but b is not on the enumeration $r_1, r_2, r_3, \dots, r_n, \dots$
$b \neq r_1$ because $\overline{b_{11}} \neq b_{11}$ (diff. at 1st decimal place)
$b \neq r_2$ because $\overline{b_{22}} \neq b_{22}$ (" " 2nd " ")

In general $b \neq r_n$ because $\overline{b_{nn}} \neq b_{nn}$ for $n = 1, 2, 3, \dots$ (diff. at nth decimal place)

Contradiction: The reals cannot be enumerated and are uncountably infinite.

ii) The set of real numbers r, $0 \le r < 1$ are uncountably infinite
(*) $\therefore a_1, a_2, \dots, a_n, \dots$ would be where $a_i = 0$

iii) The set of real numbers r, $0 \le r < 3$ are uncountably infinite
(*) $a_i = 0, 1, 2$

iv). The set of real numbers r, $1 \le r < 4$ are uncountably infinite
(*) $a_i = 1, 2, 3$
(**) $b = 1.\overline{b_{11}}\,\overline{b_{22}} \cdots \overline{b_{nn}} \cdots$ or $2. \dots$ or $3. \dots$
b must be an element that is on the list defined

ii) Prove that the set of all sequences of a's, b's, c's are uncountably infinite.

Note: $\begin{cases} S: a, a, b, b, c, c, a, b, b, c, \dots \\ \quad S(1), S(2), S(3), \dots \end{cases}$

Solution

Assume that the set of all sequences of a's, b's and c's is countably infinite and can be enumerated $S = (S_1, S_2, S_3, \dots, S_n, \dots)$

$$\begin{aligned} S_1 &= S_1(1), S_1(2), S_1(3), \dots \\ S_2 &= S_2(1), S_2(2), S_2(3), \dots \\ &\vdots \\ S_n &= S_n(1), S_n(2), S_n(3), \dots S_n(n), \dots \\ &\vdots \end{aligned}$$

S_{ij} = j^{th} value of i^{th} sequence
$i = 1, 2, \dots$
$j = 1, 2, \dots$

$S_i(j) \in \{a, b, c\}$

Define $\bar{S} = \bar{S}(1), \bar{S}(2), \bar{S}(3), \dots, \bar{S}(n), \dots$

by $\bar{S}(i) \begin{cases} a & \text{if } S_i(i) = b, c \\ b & \text{if } S_i(i) = a \end{cases}$ $\quad i = 1, 2, 3, \dots$

$\bar{S} \neq S_1$ because $\bar{S}(1) \neq S_1(1)$
$\bar{S} \neq S_2$ because $\bar{S}(2) \neq S_2(2)$
$\vdots$

In general, $\bar{S} \neq S(n)$, $n = 1, 2, 3, \dots$
because $\bar{S}(n) \neq S_n(n)$

$\therefore$ The set of sequences of a's, b's, c's cannot be enumerated and is uncountably infinite

Review: To prove an infinite set A has cardinality $\aleph_0$

1. Prove there is a bijection b/w A and P (or any other known $\aleph_0$ set).
2. Show that the set can be enumerated and state theorem.
3. Show A is a subset of a known $\aleph_0$ and state theorem.
4. Show A is a countable union of countable sets and state theorem.
5. Show $A = S \times T$ where S and T are countable and state theorem.

To prove an infinite set A is uncountably infinite

1. Use Cantor's Diagonal Argument (for $\mathbb{R}$'s or set of sequences)
2. Prove there is a bijection b/w A and $\mathbb{R}$
3. If A is uncountably infinite and $A \subseteq B$, then B is uncountably infinite (Pf in h.w. → use pf. by contradiction + theorem: subsets of countable sets are countable)

(where you would use #3) Prove $\mathbb{R} \times \mathbb{N}$ is uncountably infinite

$$\mathbb{R} \cong \overbrace{\mathbb{R} \times \{0\}}^{A} \subseteq \overbrace{\mathbb{R} \times \mathbb{N}}^{B}$$

$$r \to (r, 0)$$

if A is uncountably infinite (which it is because $A \cong \mathbb{R}$ which is uncountably infinite) and since $A \subseteq B$, then B is uncountably infinite.

Ch. 1. The Foundations: Logic, Sets, and Functions

6/9/97

1.1 Logic

Def: A proposition is a statement that is true or false but not both.

Letters to denote proposition $p, q, r, s, \ldots$.

Def: Truth value of proposition is either T (true) or F (false)

Def: Compound propositions are formed from existing propositions using logical operators.

logical operators

Def: Negation of p, $\neg p$

$$\neg : \{T, F\} \longrightarrow \{T, F\}$$

Def: A truth table displays the function values of operator

p	$\neg p$
T	F
F	T

Def: Conjunction of p and q, denoted $p \wedge q$, p "and" q

$$\wedge : \underbrace{\{T, F\} \times \{T, F\}}_{\text{binary}} \longrightarrow \{T, F\}$$

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

<u>Def</u>: <u>Disjunction</u> of p and q, $p \vee q$, p "or" q ("inclusive or")
$\vee : \{T,F\} \times \{T,F\} \to \{T,F\}$

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

<u>Def</u>: The <u>exclusive or</u> of p and q, $p \oplus q$ (p or exclusive q) read
$\oplus : \{T,F\} \times \{T,F\} \to \{T,F\}$

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

note: "p or q but not both"

<u>Def</u>: The <u>implication</u> of p and q, denoted $p \to q$
$\to : \{T,F\} \times \{T,F\} \to \{T,F\}$

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

if p, then q
p implies q
if p, q
(*) p only if q
p is sufficient for q
q if p
q whenever p
q is necessary for p

$\underset{\text{antecedent}}{p} \to \underset{\text{consequence}}{q}$

(*) iff
~~p if and only if q~~
$p \to q$ and $q \to p$
– p if q : $q \to p$
– p only if q : $p \to q$

<u>Def</u>: The <u>converse</u> of $p \to q$ is $q \to p$
The <u>contrapositive</u> of $p \to q$ is $\neg q \to \neg p$
The <u>inverse</u> of $p \to q$ is $\neg p \to \neg q$

p	q	$p \to q$	converse $q \to p$	contrapositive $\neg q \to \neg p$	inverse $\neg p \to \neg q$
T	T	T	T	T	T
T	F	F	T	F	T
F	T	T	F	T	F
F	F	T	T	T	T

logically equivalent ($p \to q$ and $\neg q \to \neg p$)
logically equivalent ($q \to p$ and $\neg p \to \neg q$)

<u>Def</u>: The <u>biconditional</u> of p and q, $p \leftrightarrow q$ (p "iff" q)
$\leftrightarrow : \{T,F\} \times \{T,F\} \to \{T,F\}$

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

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

$p \leftrightarrow q = \neg (p \oplus q)$

<u>BIT OPERATORS</u> (OR, AND, XOR → same as logical operators).
$\vee$ $\wedge$ $\oplus$

Bit = zero or one
Allow F=0, T=1

```
01101  10110
11000  11101
------------
11101  11111  OR
01000  10100  AND
10101  01011  XOR
```

1.2 Propositional Equivalences

<u>Def</u>: A <u>tautology</u> is a compound proposition that is always true.
ex) $p \vee \neg p$
A <u>contradiction</u> is a compound proposition that is always false.
ex) $p \wedge \neg p$
A <u>contingency</u> is a compound proposition that is neither a tautology nor a contingency

<u>Def</u>: Compound propositions that always have the same truth table are logically equivalent. $(P \Longleftrightarrow Q)$

ex) $p \to q \Longleftrightarrow \neg q \to \neg p$

ex DeMorgans Laws: $\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$
$\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$

ex) Distributive Laws: $p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$
$p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$

Pf: $p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$

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

logically equivalent

Note: A compound proposition w/ n propositions will have 2^n rows in the truth table

3.1 Rules of Inference

Draw conclusions or derive new assertions from old assertions.

<u>Def</u>: An <u>argument</u> is a set of premises followed by a conclusion

$$\begin{array}{l} P_1 \\ P_2 \\ \vdots \\ \underline{P_n} \\ \therefore C \end{array}$$

$P_1, P_2, \ldots, P_n, C$ are compound propositions

<u>Def</u>: An argument is valid if the conclusion is true whenever the premises are true
An argument is invalid if the conclusion can be false when the premises are true

consider $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow C$

→ to test the validity of an argument, construct a truth table of $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow C$, conjunction of the premises implying the conclusion.

→ if its a tautology, the argument is valid
→ if its not a tautology, the argument is invalid

The validity of an argument should not be confused w/ the truth or falsity of the premises and/or conclusion.

u) $$\begin{array}{l} p \rightarrow q \\ \underline{p} \\ \therefore q \end{array}$$

p	q	$[(p \rightarrow q) \wedge p] \rightarrow q$
T	T	T
T	F	T
F	T	T
F	F	T

Since truth table is a tautology, argument is <u>valid</u>

ii) $p \to q$
$q \to r$
$\therefore p \to r$

p	q	r	$[(p \to q) \land (q \to r)] \to (p \to r)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	
F	T	F	
F	F	T	
F	F	F	

* the only way to get an invalid table is when the conclusion is false, in other words, $p \to r = F$

$p = T$ and $r = F$

Invalid Arguments

① Affirming Consequent

$p \to q$
q
$\therefore p$

when would it be invalid

$p = F$
$q = T$

$p \to q$	T
q	T
p	F

② Denying Antecedent

$p \to q$
$\neg p$
$\therefore \neg q$

$p = F$
$q = T$

T
T
$\therefore$ F

③ Nonsequitor

p
$\therefore q$ $<$ $q = F$, $p = T$

ii) If the client was guilty, then he was at the scene of the crime. The client was not at the scene of the crime. Hence the client was not guilty.

p = client guilty
q = at scene

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

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

} conclusion = F
$\neg p = F$
$p = T$

ii) If David passes the final exam, then he will pass the course. David passes the course, hence he passed the final exam.

p = David passes final
q = passes the course

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

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

look at where p is false because this is only where a contradiction could occur

$\therefore$ INVALID

ii) The governor will call a special session if the Senate cannot reach a compromise. If a majority of the cabinet are in agreement, then the governor will not call a special session. The Senate can reach a compromise. Therefore the governor will not call a special session.

p = governor calls special session
q = Senate can reach compromise
r = majority of cabinet agree

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

p	q	r	$[(\neg q \to p) \wedge (r \to \neg p) \wedge q] \to \neg p$
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

shortcut → look for invalid only:
when conclusion is F &
premises are T:
$\neg p = F \therefore p = T$
premises = T
$q = T$ ... [illegible] look at 1st 2

Invalid

ii) ① $\neg r \rightarrow (s \rightarrow \neg t)$

② $\neg r \vee w$

③ $\neg p \rightarrow s$

④ $\underline{\neg w}$

⑤ $\therefore t \rightarrow p$

p	r	s	t	w	$(1 \wedge 2 \wedge 3 \wedge 4) \rightarrow 5$
F	F	T	T	F	$(F \wedge T \wedge T \wedge T) \rightarrow T$ $F \rightarrow T = T$

look at only values which make conclusion = F

$t \rightarrow p = F$

$t = T \quad p = F$

Make premises = T

$\neg w = T \rightarrow w = F$

$\neg p \rightarrow s = T,\ p = F \ \therefore s = T$

$\neg r \vee w,\ w = F \ \therefore \neg r = T \rightarrow r = F$

$\therefore$ VALID

NOTHER WAY

Direct Method of Proof (Formal Proof)

$\neg r \to (s \to \neg t)$	Assumption
$\neg r \vee w$	"
$\neg p \to s$	"
$\neg w$	"
$\neg r$	$(\neg w) \wedge (\neg r \vee w)$
$s \to \neg t$	$(\neg r) \wedge (\neg r \to (s \to \neg t))$
$\neg p \to \neg t$	$(\neg p \to s) \wedge (s \to \neg t)$
$t \to p$	contrapositive of $\neg p \to \neg t$

Indirect Method of Proof

If I study or if I am a genius, then I will pass the course. I will not be allowed to take the next course. If I pass the course, then I will be allowed to take the next course. Therefore I did not study.

p = study
q = genius
r = pass course
s = next course

$$\begin{array}{l} p \vee q \to r \\ \neg s \\ r \to s \\ \hline \therefore \neg p \end{array}$$

$p \vee q \to r$	Assumption
$\neg s$	"
$r \to s$	"
$\neg(\neg p)$	Negation of conclusion
p	Double negation
$p \to (p \vee q)$	Addition rule
$p \to r$	$(p \to (p \vee q)) \wedge ((p \vee q) \to r)$
r	$p \wedge p \to r$
s	$r \wedge r \to s$

13 Discrete

Predicates and Quantifiers

$P(x)$ propositional function

e.g. $x \geq 3$ $P(4)$ true $P(2)$ false.

In general $P(x_1, x_2, \ldots, x_n)$ propositional function of n variables

<u>Def</u> The universal quantification of $P(x)$
"$P(x)$ is true for all x in universe"
$\forall x\, P(x)$ (for every x)

<u>Ex.</u> Let $P(x)$ be "$x+1 > x$"
$\forall x\, P(x)$ is true
Let $Q(x)$ be "$x < 2$"
$\forall x\, Q(x)$ is false

<u>Def</u> the existential quantification of $P(x)$ is "There exists an element such that $P(x)$ is true"
$\exists x\, P(x)$
(There is an x, there is at least one x, for some x)

<u>Ex</u> $P(x)$ "$x > 3$"
$\exists x\, P(x)$ is true ($x = 4$)
$P(x)$ "$x = x+1$"
$\exists x\, P(x)$ is false.

Ex. $\forall x \forall y\ (x+y = y+x)$ Commutative

$\forall x \exists y\ (x+y=0)$ Inverse.

$\forall x \forall y \forall z\ (x+(y+z) = (x+y)+z)$

Translating Sentences into Logical Expressions

Ex "Some student in this class has visited Mexico"

"Every student in this class has visited either Canada or Mexico"

$M(x)$ x visited Mexico

$C(x)$ x visited Canada

$\exists x\, M(x)$

$\forall x\, (C(x) \vee M(x))$

Negations.

	Equivalent Statement
$\neg \exists x\, P(x)$	$\forall x\, \neg P(x)$ ($P(x)$ false for every x)
$\neg \forall x\, P(x)$	$\exists x\, \neg P(x)$ (There is an x for which $P(x)$ is false)

p 33 1, 3, 5, 9, 21 a–h, 25 a–c, 35

3.2

Mathematical Induction

To prove a statement $P(n)$ is true for $n = 1, 2, \ldots$:

(1) Basis step: $P(1)$ is shown to be true.
(2) Inductive step: $P(k) \to P(k+1)$ is shown to be true for $k = 1, 2, 3, \ldots$

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

Basis step: $n = 1$ $\quad 1 = \frac{1(1+1)}{2} = 1$ ✓
$n = 2$ $\quad 1 + 2 = \frac{2(2+1)}{2} = 3$ ✓

} really only need to do when $n = 1$

Inductive step: Assume $n = k$ $\quad k = 1, 2, \ldots$

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

Prove $n = k+1$

$$1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2} \checkmark$$

∴ Add $k+1$ to both sides of k^{th} case

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

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2} \checkmark$$

6) Prove $1^3+2^3+\cdots+n^3=\left(\frac{n(n+1)}{2}\right)^2$ $n=1,2,\ldots$

Basis step: $n=1$ $1^3=\left(\frac{1(2)}{2}\right)^2=1$

Inductive step: Assume $n=k$

$$1^3+2^3+\cdots+k^3=\left(\frac{k(k+1)}{2}\right)^2$$

Prove $n=k+1$

$$1^3+2^3+\cdots+(k+1)^3=\left(\frac{(k+1)(k+2)}{2}\right)^2$$

Add $k+1$ to both side of the k^{th} case

$$1^3+2^3+\cdots+k^3+(k+1)^3=\left(\frac{k(k+1)}{2}\right)^2+(k+1)^3$$

$$=\frac{(k(k+1))^2+4(k+1)^3}{4}$$

$$=\frac{(k+1)^2\left[k^2+4(k+1)\right]}{4}$$

$$=\frac{(k+1)^2\left[k^2+4k+4\right]}{4}$$

$$=\frac{(k+1)^2(k+2)^2}{4}$$

$$=\left(\frac{(k+1)(k+2)}{2}\right)^2$$

6/17/17 ③ Prove $n < 2^n$: $n = 1, 2, 3, \dots$

Basis Step: $n = 1$ $\quad 1 < 2^1$ ✓

Inductive Step: Assume $n = k$ $\quad k < 2^k$

Prove $n = k+1$ $\quad k+1 < 2^{k+1}$

Start w/ $(k+1)$ and - - - - - - get to 2^{k+1}

steps ① ③ ⑤ ④ ②

$$(k+1) \underset{\substack{\uparrow \\ \text{Assumption} \\ k<2^k}}{<} 2^k + 1 \underset{\substack{\downarrow \\ 1<2^k}}{<} \qquad 2^k + 2^k = 2^k \cdot 2 < 2^{k+1}$$

rewrite: $(k+1) < 2^k + 1 < 2^k + 2^k < 2^k \cdot 2 < 2^{k+1}$ ✓

④ Prove $n^3 - n$ is divisible by 3 $\quad n = 0, 1, 2, \dots$

Basis Step: $n = 0$ $\quad 0^3 - 0 = 0 = 3 \cdot 0$ ✓

Inductive Step: Assume $n = k$ $\quad k^3 - k$ is divisible by 3

Prove $n = k+1$ $\quad (k+1)^3 - (k+1)$ is divisible by 3

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = k^3 - k + 3k^2 + 3k$$

$$= \underset{\substack{\uparrow \\ \text{div. by 3} \\ \text{by assumption}}}{(k^3 - k)} + \underset{\substack{\uparrow \\ \text{div. by 3}}}{3(k^2 + k)}$$ ✓

note: with divisible problems, start w/ left side of $k+1$ and get k^{th} case + 3(something) which is obviously divisible by 3.

Geometric Progression

⑤ Prove $1+2+2^2+\cdots+2^n=2^{n+1}-1$ $\quad n=0,1,2,\ldots\ldots$

$2^0+2^1+2^2+\cdots+2^n$

Basis Step: $n=0$ $\quad 1=2^1-1=1$ ✓

$n=1$ $\quad 1+2=2^2-1=3$

$n=2$ $\quad 1+2+2^2=2^3-1=7$

Inductive Step: Assume $n=k$.

$1+2+2^2+\cdots+2^k=2^{k+1}-1$

Prove $n=k+1$

$1+2+2^2+\cdots+2^k+2^{k+1}=2^{k+2}-1$

Add 2^{k+1} to both sides of k^{th} case

$$\begin{aligned}1+2+\cdots+2^k+2^{k+1}&=2^{k+1}-1+2^{k+1}\\&=2\cdot2^{k+1}-1\\&=2^{k+2}-1\end{aligned}$$ ✓

⑥ Sums from Geometric Progression

$$\sum_{j=0}^{n}ar^j=a+ar+ar^2+\cdots+ar^n=\frac{ar^{n+1}-a}{r-1} \qquad n=0,1,2,\ldots$$

Basis Step: $n=0$ $\quad a=\frac{ar-a}{r-1}=\frac{a(r-1)}{r-1}=a$ ✓

Inductive Step: Assume $n=k$ $\quad a+ar+ar^2+\cdots ar^k=\frac{ar^{k+1}-a}{r-1}$

Prove $n=k+1$ $\quad a+ar+ar^2+\cdots ar^{k+1}=\frac{ar^{k+2}-a}{r-1}$

ar^{k+1} to both sides of k^{th} case: $\quad a+ar+ar^2+\cdots ar^k+ar^{k+1}=\frac{ar^{k+1}-a}{r-1}+ar^{k+1}$

$$=\frac{ar^{k+1}-a+ar^{k+2}-ar^{k+1}}{r-1}$$

⑦ Prove that a finite set with n elements has 2^n subsets $n=0,1,2,\ldots$

Basis Step: $n=0$: A set w/ 0 elements has $2^0=1$ subset $\emptyset \subseteq \emptyset$ ✓

Inductive Step: Assume $n=k$: A set w/ k elements has 2^k subsets.
Prove $n=k+1$: A set w/ $k+1$ elements has 2^{k+1} subsets.

Say $|S|=k+1$
take $x \in S$
$T = S - \{x\}$
$|T| = k$

Since T has k elements, it has 2^k subsets
Say $A \subseteq T$ $\quad A \subseteq S \quad \leftarrow 2^k$
$A \cup \{x\} \subseteq S \quad \leftarrow 2^k$

$2^k + 2^k$ subsets of S
$2 \cdot 2^k$ subsets of S
2^{k+1} subsets of S ✓

⑧ Use mathematical induction to prove $2^n < n!$ $n=4,5,6,\ldots$

Basis Step: $n=4$ $\quad 2^4 < 4!$ $\quad 16 < 24$ ✓

Inductive Step: Assume $n=k$ $\quad 2^k < k!$
Prove $n=k+1$ $\quad 2^{k+1} < (k+1)!$

$$2^{k+1} = 2^k \cdot 2 \underset{2^k < k!}{<} (k!)2 \underset{\substack{2<k+1 \\ k=4,5,\ldots}}{<} (k+1)k! = (k+1)!$$

note
$\boxed{5! \cdot 6 = 6!}$

$$2^{k+1} = 2^k \cdot 2 < (k!)2 < (k+1)k! = (k+1)!$$ ✓

(9) Prove the generalization of De Morgan's laws: $\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$ $\quad n=2,3,\ldots$

Basis Step: $n=2$ $\quad \overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$ $\quad$ De Morgans law ✓

Inductive Step: Assume $n=k$

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_k} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_k}$$

Prove $n=k+1$

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_{k+1}} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k+1}}$$

$$\begin{aligned}
\overline{A_1 \cap A_2 \cap \cdots \cap A_k \cap A_{k+1}} &= \overline{(A_1 \cap A_2 \cap \cdots \cap A_k) \cap A_{k+1}} && \text{Assoc.}\\
&= \overline{(A_1 \cap A_2 \cap \cdots \cap A_k)} \cup \overline{A_{k+1}} && \text{De Morgans}\\
&= (\overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_k}) \cup \overline{A_{k+1}} && \text{Assumption}\\
&= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_k} \cup \overline{A_{k+1}} && \text{Assoc.}
\end{aligned}$$

(10) Prove $6^{n+2} + 7^{2n+1}$ is divisible by 43 $\quad n=0,1,2,\ldots$

Basis Step: $n=0$: $6^2 + 7^1 = 36+7 = 43 = 43(1)$ ✓

Inductive Step: Assume $n=k$ $\quad 6^{k+2} + 7^{2k+1}$ is divisible by 43

Prove $n=k+1$ $\quad 6^{k+3} + 7^{2k+3}$ is divisible by 43

$$\begin{aligned}
6^{k+3} + 7^{2k+3} &= \boxed{}\,\overbrace{(6^{k+2} + 7^{2k+1})}^{\text{assumption}} + \boxed{\phantom{7^{2k+1}(-6)}}\\
&= 6(6^{k+2} + 7^{2k+1}) + 7^{2k+1}(-6)\\
&= \underbrace{6(6^{k+2} + 7^{2k+1})}_{\substack{\text{div. by}\\ \text{assumption}}} + 7^{2k+1}\underbrace{(-6+7^2)}_{\substack{43\\ \text{factor of } 43}}
\end{aligned}$$

✓

(11) Post Office prints only 5¢ and 9¢ stamps. Prove any postage can be made $n = 35¢, 36¢, 37¢, \ldots$

Basis Step: $n = 35¢$ $7 \cdot 5¢$ ✓

Inductive Step: Assume $n = k \rightarrow$ you can make $k¢$ w/ 5¢ and 9¢ stamps

• Prove $n = k+1 \rightarrow$ you can make $(k+1)¢$ w/ 5¢ and 9¢ stamps

In the $k¢$ of 5¢ and 9¢ stamps either

a) have a 9¢ stamp
replace 9¢ by $2 \cdot 5¢$
$(k+1)¢$ of postage

53-56

b) no 9¢ stamps
we have at least $7 - 5¢$ stamps
replace by $4 \cdot 9¢$ stamps
$(k+1)¢$ of postage

2/23/97

Recursively Defined Functions

Def: A recursive or inductive definition of a function w/ the set of nonnegative integers as its domain is given by:
(i) specifying the value at 0
(ii) giving a rule for finding its value at an integer from its values at smaller integers.

ex) $f(0) = 3$
$f(n+1) = 2f(n) + 3 \quad n \geq 0$
$n = 0$: $f(1) = 2f(0) + 3 = 2 \cdot 3 + 3 = 9$
$n = 1$: $f(2) = 2f(1) + 3 = 2 \cdot 9 + 3 = 21$
$n = 2$: $f(3) = 2f(2) + 3 = 2 \cdot 21 + 3 = 45$

ii) Give a recursive definition of the factorial function $F(n) = n!$

$F(0) = 1$

$F(n+1) = (n+1)F(n) \quad n \geq 0$

$n=0: F(1) = (1)F(0) = 1(1) = 1$

$n=1: F(2) = (2)F(1) = 2(1) = 2$

$n=2: F(3) = (3)F(2) = 3(2) = 6$

iii) The Fibonacci sequence of numbers $f_0, f_1, f_2, \ldots\ldots$ are defined by the equations:

$f_0 = 0$

$f_1 = 1$

$f_n = f_{n-1} + f_{n-2} \quad n \geq 2$

$n=2: f_2 = f_1 + f_0 = 1 + 0 = 1$

$n=3: f_3 = f_2 + f_1 = 1 + 1 = 2$

$n=4: f_4 = f_3 + f_2 = 2 + 1 = 3$

$f_0, f_1, f_2, \ldots$

$0, 1, 1, 2, 3, 5, 8, 13, \ldots$

<u>other application</u>

$f_0 = 1$

$f_1 = 1$

$f_n = f_{n-1} + f_{n-2} \quad n \geq 2$

$f_0, f_1, f_2, \ldots$

$1, 1, 2, 3, 5, \ldots$

The Second Principle of Mathematical Induction

Basis cases: $p(0), p(1), \ldots, p(q)$

Inductive Step: Show $p(0) \wedge p(1) \wedge \ldots \wedge p(k) \Longrightarrow p(k+1)$ holds (implication is true) $k \geq q$

$p(0)$

$\vdots$

$p(q)$

$p(q+1)$

$p(q+2)$

$\vdots$

a) $f_0 = 0$
$f_1 = 1$
$f_n = f_{n-1} + f_{n-2} \quad n \geq 2$

f_0	f_1	f_2	f_3	f_4
0	1	1	2	3

Prove $f_n > \alpha^{n-2} \quad n = 3, 4, \ldots$ where $\alpha = \frac{1+\sqrt{5}}{2}$

Basis cases: $n=3$: $f_3 > \alpha^1 \quad 2 > \frac{1+\sqrt{5}}{2}$ ✓
$n=4$: $f_4 > \alpha^2 \quad 3 > \left(\frac{1+\sqrt{5}}{2}\right)^2$ ✓

Inductive step: Assume $f_i > \alpha^{i-2} \quad i = 3, 4, \ldots, k$
Prove: $f_{k+1} > \alpha^{k-1}$

$$f_{k+1} = f_k + f_{k-1} \underset{\text{Assumption}}{>} \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1} \checkmark$$

Note: $x^2 - x - 1 = 0$
$x = \frac{1 \pm \sqrt{1-4(1)(-1)}}{2} = \frac{1 \pm \sqrt{5}}{2}$

$\alpha^2 - \alpha - 1 = 0$
$\alpha^2 = \alpha + 1$
$\alpha^{k-1} = \alpha^{k-3}(\alpha^2)$
$= \alpha^{k-3}(\alpha + 1)$
$= \alpha^{k-2} + \alpha^{k-3}$

b) Recursively define $a_0 = 1,\ a_1 = 3,\ a_n = 2a_{n-1} - a_{n-2},\ n \geq 2$

$n=2$: $a_2 = 2a_1 - a_0 = 2(3) - 1 = 5$
$n=3$: $a_3 = 2a_2 - a_1 = 2(5) - 3 = 7$
$n=4$: $a_4 = 2a_3 - a_2 = 2(7) - 5 = 9$

Guess explicit formula: $a_{n_{exp}} \stackrel{?}{=} 2n+1$

Prove $a_{n_{rec}} = a_{n_{exp}} \quad n = 0, 1, 2, \ldots$

Basis cases: $n=0$: $a_{0_{rec}} = 1 \qquad a_{0_{exp}} = 2(0)+1 = 1$
$n=1$: $a_{1_{rec}} = 3 \qquad a_{1_{exp}} = 2(1)+1 = 3$ ✓

Inductive Step: Assume $a_{0_{rec}} = a_{0_{exp}}$, $a_{1_{rec}} = a_{1_{exp}}$, $\ldots$, $a_{k_{rec}} = a_{k_{exp}}$ or Assume $a_{i_{rec}} = a_{i_{exp}} \quad i = 0, 1, 2, \ldots, k$

Prove $a_{k+1_{rec}} = a_{k+1_{exp}}$

$$a_{k+1_{rec}} = 2a_{k_{rec}} - a_{k-1_{rec}} \stackrel{\text{Assumption}}{=} 2a_{k_{exp}} - a_{k-1_{exp}} = 2(2k+1) - (2(k-1)+1) = 4k+2-(2k-2+1)$$
$$= 4k+2-2k+1 = 2k+3 = 2(k+1)+1 = a_{k+1_{exp}}$$

ii). Recursively define $b_0 = b_1 = b_2 = 1$, $b_n = b_{n-1} + b_{n-3}$ for $n \geq 3$

$n=3: b_3 = b_2 + b_0 = 1+1 = 2$

$n=4: b_4 = b_3 + b_1 = 2+1 = 3$

$n=5: b_5 = b_4 + b_2 = 3+1 = 4$

$n=6: b_6 = b_5 + b_3 = 4+2 = 6$

Prove $b_n \geq 2b_{n-2}$ $n = 3, 4, 5, \ldots$

Basis cases: $n=3$: $b_3 \geq 2b_1$ $2 \geq 2(1)$ ✓

$n=4$: $b_4 \geq 2b_2$ $3 \geq 2(1)$ ✓

$n=5$: $b_5 \geq 2b_3$ $4 \geq 2(2)$ ✓

Inductive Step: Assume $b_i \geq 2b_{i-2}$ $i = 3, 4, 5, \ldots,$

Prove $b_{k+1} \geq 2b_{k-1}$

$b_{k+1} = b_k + b_{k-2} \geq 2b_{k-2} + 2b_{k-4} = 2(b_{k-2} + b_{k-4}) = 2b_{k-1}$

$b_{k+1} \geq 2b_{k-1}$ ✓

197
4.1

COMBINATORICS

Techniques for counting large finite sets w/o listing elements

Travelling salesman problem ∴ visit 50 cities
How many ways to visit 50 cities?
$\underset{1^{st}\text{ city}}{\underline{50}} \times \underset{2^{nd}\text{ city}}{\underline{49}} \times \underline{48} \times \underline{47} \times \_\ \_\ \_ \times \underline{2} \times \underset{50^{th}\text{ city}}{\underline{1}} = 50!$

The Sum Rule

If a first task can be done in n_1 ways and a second task can be done in n_2 ways, and if these tasks cannot be done at the same time, then there are $n_1 + n_2$ ways to do either task.

"or" $\rightarrow$ +

if X is the disjoint union of $A_1, A_2, \ldots, A_n$, then $|X| = |A_1| + |A_2| + \cdots + |A_n|$

ex) Cards: 52 4 Suits: Hearts, Clubs, Spades, Diamonds
13 kinds within each suit: A, 2, ..., 10, J, Q, K

Q: In how many ways can we draw a heart and a spade? $13+13=26$
(can you draw a heart & spade at the same time → no ∴ use sum rule)

Q: A heart or an ace? $13+3$ or $12+4=16$

Q: An ace or a king? $4+4=8$

Q: A card numbered 2 through 10? $4+4+4+4+4+4+4+4+4 = 9(4) = 36$

ex) Dice 2 Dice
1–6 2–12

Q: How many ways to get a 7 or 11 w/ 2 dice? $6+2=8$

The Product Rule

Suppose that a procedure can be broken down into two tasks. If there are n_1 ways to do the first task and n_2 ways to do the second task after the first task has been done, then there are $n_1 n_2$ ways to do the procedure.

S_1 then S_2 then ... then S_n $\qquad |S_1 \times S_2 \times \cdots \times S_n| = \prod_{i=1}^{n} |S_i|$

u) Q: The chairs of an auditorium are to be labeled w/a letter and a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

$$\underset{L}{26} \times \underset{P.I.}{100} = 2600$$

Q: How many bit strings of length n?

$$\underset{1}{2}\ \underset{2}{2}\ \underset{3}{2} \times \cdots \times \underset{n}{2} = 2^n$$

Q: How many different license plates have 3 letters followed by 4 digits?

a) repetition allowed (always assumed unless stated else)

$$\underset{L}{26} \times \underset{L}{26} \times \underset{L}{26} \times \underset{D}{10} \times \underset{D}{10} \times \underset{D}{10} \times \underset{D}{10} = \underline{26^3 \times 10^4}$$

b) only letters are repeated: $26 \times 26 \times 26 \times 10 \times 9 \times 8 \times 7 = 26^3 \times 10 \times 9 \times 8 \times 7$

c) no repetition: $26 \times 25 \times 24 \times 10 \times 9 \times 8 \times 7$

Q: Telephone Numbering Plan

Old Plan: NYX NNX XXXX where X: 0-9, N: 2-9, Y: 0,1

New Plan: NXX NXX XXXX

old plan: $8 \times 2 \times 10 \times 8^2 \times 10^5 = 1{,}024{,}000{,}000$

new plan: $8 \times 10^2 \times 8 \times 10^6 = 6{,}400{,}000{,}000$

Q: Computer password 6-8 characters → letter or digit.

a) How many passwords?

length 6 $= 36^6$
or 7 $= 36^7$
or 8 $= 36^8$

$\left.\begin{array}{l} \\ \\ \end{array}\right\}$ mutually exclusive: $36^6+36^7+36^8$

b) How many passwords if each password must have <u>at least one</u> digit?

(at least one + none = TOTAL)

TOTAL passwords − passwords w/ no digits

$$36^6+36^7+36^8-(26^6+26^7+26^8) = 2{,}684{,}483{,}063{,}360$$

heorem: <u>The Pigeonhole Principle</u>

If $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Pf: (Contradiction): Suppose none of the boxes has more than one object. Then the total number of objects would be at most k.

ei) Among any group of 367 people, there must be at least 2 people w/ the same birthday.

ei) Among 102 students taking an exam (0-100), there are at least 2 students w/ the same grade.

heorem: <u>The Generalization Pigeonhole Principle</u>

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

$\lceil x \rceil$ − smallest integer $\geq x$

ei) $\lceil 5.4 \rceil = 6$ $\qquad$ $\lceil 5.4 \rceil = 6 < 5.4+1$

$\lceil 8 \rceil = 8$ $\qquad$ $\lceil 8 \rceil = 8 < 8+1$ $\qquad$ $\lceil \frac{N}{k} \rceil < \frac{N}{k}+1$

$\lceil -2.2 \rceil = -2$ $\qquad$ $\lceil -2.2 \rceil = -2 < -2.2+1$

(Contradiction)

Suppose none of the boxes contain more than $\lceil \frac{N}{K} \rceil - 1$ objects. Then the total number of objects is at most $\underbrace{K(\lceil \frac{N}{K} \rceil - 1) < K(\frac{N}{K}+1)-1}_{\text{contradiction}} = N$.

i). Among 100 people, there are at least how many born in the same month?

$\lceil \frac{100}{12} \rceil = 9$

ii). What is the minimum # of students in a class, to be sure at least 6 will receive the same grade? (A, B, C, D, F)

$\lceil \frac{N}{5} \rceil = 6$

$$\boxed{\begin{gathered}\lceil \tfrac{N}{K} \rceil = P \\ N = K(P-1)+1\end{gathered}}$$

$N = 5(6-1)+1 = 26$

iii). What is the least number of area codes needed to guarantee that 25 million phones in a state have distinct 10 digit telephone numbers?

$\text{NXX-}\underbrace{\text{NXX-XXXX}}_{\substack{\text{how many times} \\ \text{will I need to} \\ \text{repeat each \#} \\ \text{w/a diff. area code}}}$, N: 2-9 , X: 0-9

$\left\lceil \frac{25 \times 10^6}{8 \times 10^6} \right\rceil = 4$

need 4 area codes

4.3 PERMUTATIONS

Def: A permutation of r objects is an ordered arrangement of these objects.

i) $S = \{a, b, c\}$

\# of r=3 permutations

$$\left.\begin{array}{c} abc \\ acb \\ bac \\ bca \\ cab \\ aba \end{array}\right\} \text{6 permutations of 3 letters}$$

ii) $S = \{a, b, c\}$

\# of r=2 permutations

$$\left.\begin{array}{c} ab \\ ba \\ ac \\ ca \\ bc \\ cb \end{array}\right\} \text{6 permutations of } r=2$$

...orem: The number of r-permutations of a set w/ n distinct elements is $P(n,r)$.

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)\boxed{\frac{(n-r)(n-r-1)\cdots}{(n-r)(n-r-1)\cdots}} = \frac{n!}{(n-r)!}$$

$$\frac{(n)}{1} * \frac{(n-1)}{2} * \frac{(n-2)}{3} * \cdots * \frac{n-r+1}{r}$$

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

→ in particular if $r=n$, there are $n!$ permutations of n objects

e) Suppose there are eight runners in a race. Winner receives the gold medal, 2nd place receives silver, 3rd place receives the bronze. How many different ways to award metals if all outcomes are possible?

$$P(8,3) = \frac{8!}{5!} = 8 \times 7 \times 6 = \underline{336}$$

ii) In how many ways can 7 women and 3 men

a) be arranged in a row? $P(10,10) = 10!$

b) so that women are together and men are grouped together?

$\boxed{\text{men}}\boxed{\text{women}}$

$\boxed{\text{women}}\boxed{\text{men}}$

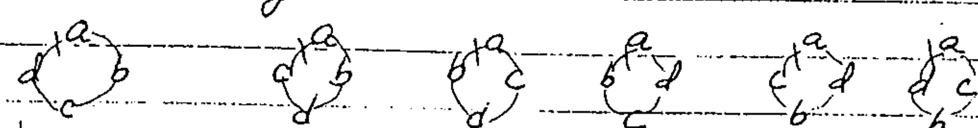
$$2! * 3! * 7!$$

c) so that the 3 men are together?

$\overset{1}{\boxed{\text{men}}}\ \overset{2}{w_1},\ \overset{3}{w_2} - - - - \overset{8)}{w_7}$

$3! * 8!$

Circular arrangements



abcd
abdc
acdb
adcb
adbc
acbd

Theorem: There are $(n-1)!$ circular arrangements of n objects.

note: if it ways keys on a keyring - since there is no top or bottom, you would divide by 2 : $\frac{(n-1)!}{2}$

Pf: There is a bijection b/w circular arrangements of n objects and linear arrangements of $(n-1)$ objects.
Fix one element of circular arrangement. Cut counterclockwise to this element. Form a linear arrangement. Drop the fixed element.

1:1 because diff. circular arrangements will result in diff. linear arrangements.

ONTO: Take a linear arrangement. Put back fixed element and form into a circular arrangement.

COMBINATIONS

Def: An r-combination of elements of a set is an unordered selection of r elements from the set. (r-subset)

ii) $S=\{a,b,c,d\}$ Form $r=3$ combinations
$\{a,b,c\}$ $\{a,c,d\}$ $\{a,b,d\}$ $\{b,c,d\}$

Theorem: The number of r-combinations of a set w/ n elements is $C(n,r)$.

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

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

i) How many 5 card hands?
→ order does not matter $\quad C(52,5) = \frac{52!}{5!\,47!} = \frac{52\times51\times50\times49\times48}{5\times4\times3\times2}$

i) How many 5 card hands of hearts? $C(13,5)$

i) How many 5 card hands of a single suit? $C(4,1)\,C(13,5)$ or $4 \cdot C(13,5)$

i) How many 5 card hands have 2 aces, 3 kings? $C(4,2) \cdot C(4,3)$

i) How many 5 card hands have 2 of one kind and 3 of another kind?

$P(13,2)\,C(4,2)\,C(4,3) = \underline{13} \cdot \underline{12} \cdot C(4,2)\,C(4,3) = 2\times C(13,2) \pm C(4,2)\,C(4,3)$

aces kings
J's 5's } example

i) There are 21 consonants and 5 vowels in English alphabet $\{a, e, i, o, u\}$.
Consider 8 letter strings w/ no repetition.

1) How many strings? $P(26,8)$

2) How many strings w/ 3 vowels and 5 consonants?
$C(5,3)\,C(21,5) \cdot 8!$

3) How many strings w/ 3 vowels and 5 consonants contain 'a'?
$C(21,5)\,C(4,2) \cdot 8!$

4) How many strings w/ 3 vowels and 5 consonants contain "a and b"?
$C(20,4)\,C(4,2) \cdot 8!$

5) How many strings w/ 3 vowels and 5 consonants contain "b and c"?
$C(19,3)\,C(5,3) \cdot 8!$

6) How many strings w/ 3 vowels and 5 consonants exclude "a and b"?
$C(20,5)\,C(4,3) \cdot 8!$

7) How many strings w/ 3 vowels and 5 consonants begin w/ "a" and end w/ "b"?
$C(20,4)\,C(4,2) \cdot 6!$

8) How many strings w/ 3 vowels and 5 consonants begin w/ "b" and end w/ "c"?

ii) Prove $2^n = \sum_{k=0}^{n} C(n,k)$

$$\begin{matrix} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & = 2^2 \\ & 1 & & 3 & & 3 & & 1 & = 2^3 \\ 1 & & 4 & & 6 & & 4 & & 1 = 2^4 \end{matrix}$$

$$(x+y)^n = \sum_{k=0}^{n} C(n,k) x^{n-k} y^k$$

$x=1$ and $y=1$

$$(1+1)^n = 2^n = \sum_{k=0}^{n} C(n,k) 1^{n-k} 1^k = \sum_{k=0}^{n} C(n,k)$$

Pf: of Binomial Theorem

$$(x+y)^n = C(n,0)x^n + C(n,1)x^{n-1}y + \cdots + C(n,n-1)xy^{n-1} + C(n,n)y^n \qquad n = 1, 2, \ldots$$

Basis Step: $n=1$: $(x+y)^1 = C(1,0)x^1 + C(1,1)y^1 = x+y$

Inductive Step: Assume $n=k$

$$(x+y)^k = C(k,0)x^k + C(k,1)x^{k-1}y + \cdots + C(k,k-1)xy^{k-1} + C(k,k)y^k$$

Prove $n=k+1$: $(x+y)^{k+1} = C(k+1,0)x^{k+1} + C(k+1,1)x^k y + \cdots + C(k+1,k)xy^k + C(k+1,k+1)y^{k+1}$

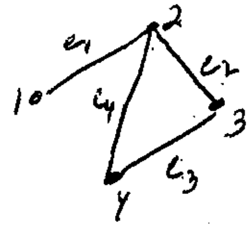
Take k^{th} case and multiply both sides by $(x+y)$:

$$(x+y)^k(x+y) = C(k,0)x^{k+1} + C(k,0)x^k y + C(k,1)x^k y + C(k,1)x^{k-1}y^2 + \cdots + C(k,k-1)x^2y^{k-1} + C(k,k-1)xy^k + C(k,k)xy^k + C(k,k)y^{k+1}$$

$$(x+y)^{k+1} = C(k+1,0)x^{k+1} + \underbrace{(C(k,0)+C(k,1))}_{C(k+1,1)}x^k y + \underbrace{(C(k,1)+C(k,2))}_{C(k+1,2)}x^{k-1}y^2 + \cdots + \underbrace{(C(k,k-1)+C(k,k))}_{C(k+1,k)}xy^k + C(k+1,k+1)y^{k+1}$$

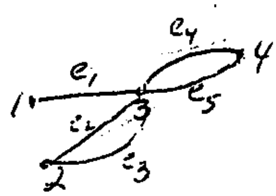
<u>Def</u>: A <u>simple graph</u> $G=(V,E)$ consists of V, a nonempty set of vertices, and E, a set of unordered pairs of distinct elements of V, called edges.

$V=\{1,2,3,4\}$
$E=\{e_1,e_2,e_3,e_4\}$



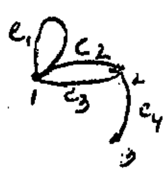
where $e_1=\{1,2\}$
$e_2=\{2,3\}$
$e_3=\{3,4\}$
$e_4=\{2,4\}$

<u>Def</u>: A <u>multigraph</u> $G=(V,E)$ consists of a nonempty set of vertices, V, and a set of unordered pairs of vertices, edges, E and a function: $f: E \to \{\{u,v\} \mid u,v \in V,\ u \neq v\}$. The edges e_1 and e_2 are called multiple or parallel edges if $f(e_1)=f(e_2)$.



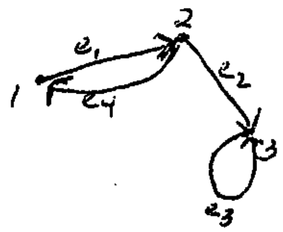
$f(e_2)=f(e_3)=\{2,3\}$
$f(e_4)=f(e_5)=\{3,4\}$

<u>Def</u>: A <u>pseudograph</u> $G=(V,E)$ consists of a nonempty set of vertices V, a set of unordered pairs of vertices, edges, E and a function: $f: E \to \{\{u,v\} \mid u,v \in V\}$. If $f(e)=\{u\}$, then edge e is called a loop.



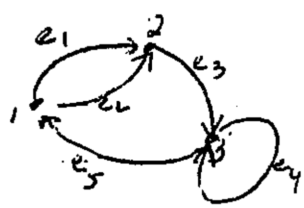
$f(e_1)=\{1\}$

Def : A directed graph $G=(V,E)$ consists of a nonempty set of vertices, V, and a set of edges, E, where $E \subseteq V \times V$ (ordered pairs of vertices).



$e_1 = (1,2)$
$e_2 = (2,3)$
$e_3 = (3,3)$
$e_4 = (2,1)$

Def : A directed multigraph $G=(V,E)$ consists of a set of nonempty vertices, V, a set of edges, $E \subseteq V \times V$, and a function:
$f: E \to \{(u,v) \mid u,v \in V\}$. The edges e_1 and e_2 are multiple edges if $f(e_1) = f(e_2)$



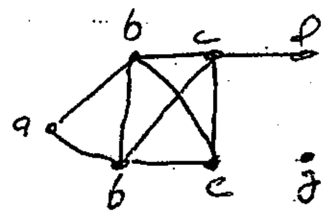
$f(e_1) = f(e_2) = (1,2)$

digraph → short version of directed graph.

Def: Two vertices u and v in an undirected graph G are called <u>adjacent</u> (or neighbors) in G if $\{u,v\}$ is an edge of G. If $e=\{u,v\}$, the edge e is called <u>incident</u> w/ the vertices u and v. The vertices u and v are called <u>endpoints</u> of the edge $e=\{u,v\}$.

Def: The <u>degree</u> of a vertex in an undirected graph is the number of edges incident w/ it. (Note: A loop contributes 2 to the degree of that vertex).

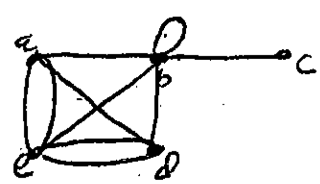
NOTATION: degree of $v = \deg(v)$.



$\deg(a) = 2$
$\deg(b) = 4$
$\deg(c) = 4$
$\deg(d) = 1$
$\deg(e) = 3$
$\deg(f) = 4$
$\deg(g) = 0$
$\overline{18}$

9 edges

Vertex of degree 0 is called <u>isolated</u>.
Vertex of degree 1 is called <u>pendant</u>.

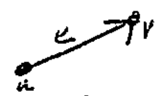


$\deg(a) = 4$
$\deg(b) = 6$
$\deg(c) = 1$
$\deg(d) = 5$
$\deg(e) = 4$
$\overline{20}$

10 edges

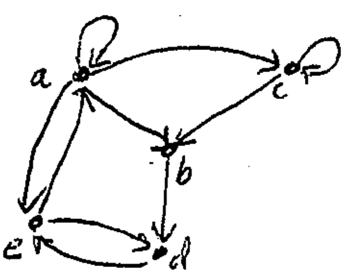
Theorem: $\sum_{v \in V} \deg(v) = 2|E|$ ($|E|$ = cardinality of E)

Pf: Every edge contributes "two" to the sum of the degrees rem: An undirected graph has an even number of odd degree vertices.



ef: When (u,v) is an edge of the directed graph G, u is said to be adjacent to v, and v is adjacent from u. The vertex u is called the initil vertex of (u,v) and v is called the terminal or end vertex of (u,v). In a loop, the initil and terminal vertex are the same.

ef: In-degree of v, $deg^-(v)$, is the number of edges w/ v as their terminal vertex.
Out-degree of v, $deg^+(v)$, is the number of edges w/ v as their initil vertex.



	in	out
a	2	4
b	2	1
c	2	2
d	2	1
e	2	2

oren: Let $G=(V,E)$ be a digraph, then $\sum_{v\in V} deg^-(v) = \sum_{v\in V} deg^+(v) = |E|$

Pf: Every edge contributes "one" to the in-degree and "one" to the out-degree.

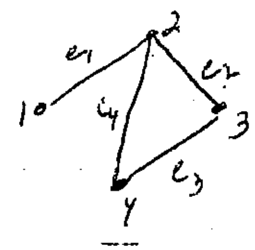
GRAPH THEORY

Repeat

7/9/97

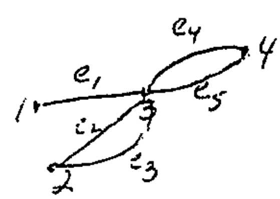
<u>Def</u>: A <u>simple graph</u> $G=(V,E)$ consists of V, a nonempty set of vertices, and E, a set of unordered pairs of distinct elements of V, called edges.

$V=\{1,2,3,4\}$
$E=\{e_1,e_2,e_3,e_4\}$



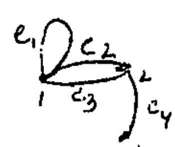
where $e_1=\{1,2\}$
$e_2=\{2,3\}$
$e_3=\{3,4\}$
$e_4=\{2,4\}$

<u>Def</u>: A <u>multigraph</u> $G=(V,E)$ consists of a nonempty set of vertices, V, and a set of unordered pairs of vertices, edges, E and a function: $f: E \to \{\{u,v\} \mid u,v \in V,\ u \neq v\}$. The edges e_1 and e_2 are called multiple or parallel edges if $f(e_1)=f(e_2)$.



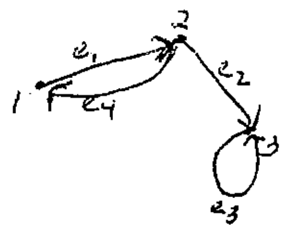
$f(e_2)=f(e_3)=\{2,3\}$
$f(e_4)=f(e_5)=\{3,4\}$

<u>Def</u>: A <u>pseudograph</u> $G=(V,E)$ consists of a nonempty set of vertices V, a set of unordered pairs of vertices, edges, E and a function:
$f: E \to \{\{u,v\} \mid u,v \in V\}$. If $f(e)=\{u\}$, then edge e is called a loop.



$f(e_1)=\{1\}$

Def: A <u>directed graph</u> $G=(V,E)$ consists of a nonempty set of vertices, V, and a set of edges, E, where $E \subseteq V \times V$ (<u>ordered</u> pairs of vertices).

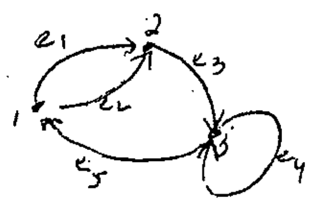


$e_1 = (1,2)$
$e_2 = (2,3)$
$e_3 = (3,3)$
$e_4 = (2,1)$

Def: A <u>directed multigraph</u> $G=(V,E)$ consists of a set of non-empty vertices, V, a set of edges, $E \subseteq V \times V$, and a function:

$$f: E \to \{(u,v) \mid u,v \in V\}.$$

The edges e_1 and e_2 are multiple edges if $f(e_1)=f(e_2)$



$f(e_1)=f(e_2)=(1,2)$

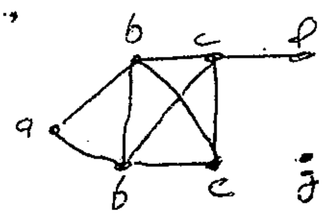
<u>digraph</u> $\to$ short version of directed graph.

Adjacent

Def: Two vertices u and v in an undirected graph G are called <u>adjacent</u> (or neighbors) in G if $\{u,v\}$ is an edge of G. If $e=\{u,v\}$, the edge e is called <u>incident</u> w/ the vertices u and v. The vertices u and v are called <u>endpoints</u> of the edge $e=\{u,v\}$.

Def: The <u>degree</u> of a vertex in an undirected graph is the number of edges incident w/ it. (Note: A loop contributes 2 to the degree of that vertex).

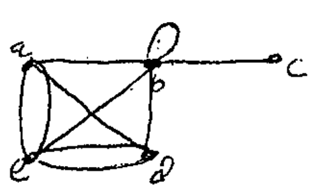
NOTATION: degree of $v = \deg(v)$.



$\deg(a)=2$
$\deg(b)=4$
$\deg(c)=4$
$\deg(d)=1$
$\deg(e)=3$
$\deg(f)=4$
$\deg(g)=0$
$\overline{18}$

9 edges

Vertex of degree 0 is called <u>isolated</u>.
Vertex of degree 1 is called <u>pendant</u>.



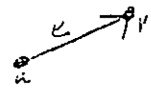
$\deg(a)=4$
$\deg(b)=6$
$\deg(c)=1$
$\deg(d)=5$
$\deg(e)=4$
$\overline{20}$

10 edges

Theorem: $\sum_{v\in V} \deg(v) = 2|E|$ $\quad$ ($|E|$ = cardinality of E)

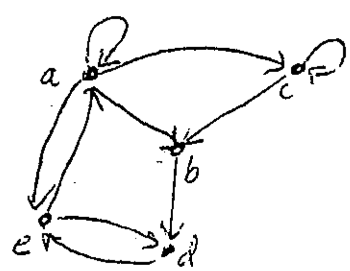
Pf: Every edge contributes "two" to the sum of the degrees

Theorem: An undirected graph has an even number of odd degree vertices.



Def: When (u,v) is an edge of the directed graph G, u is said to be adjacent to v, and v is adjacent from u. The vertex u is called the initial vertex of (u,v) and v is called the terminal or end vertex of (u,v). In a loop, the initial and terminal vertex are the same.

Def: In-degree of v, $\deg^-(v)$, is the number of edges w/ v as their terminal vertex.
Out-degree of v, $\deg^+(v)$, is the number of edges w/ v as their initial vertex.



	IN	OUT
a	2	4
b	2	1
c	2	2
d	2	1
e	2	2

Theorem: Let $G=(V,E)$ be a digraph, then $\sum_{v\in V} \deg^-(v) = \sum_{v\in V} \deg^+(v) = |E|$

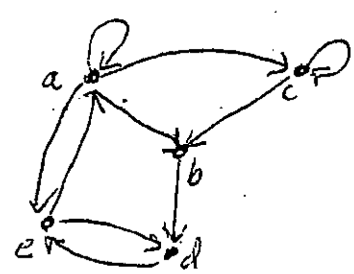
Pf: Every edge contributes "one" to the in-degree and "one" to the out-degree.

Lcture(?) until special types of graph

Theorem: An undirected graph has an even number of odd degree vertices.

Def: When (u,v) is an edge of the directed graph G, u is said to be adjacent to v, and v is adjacent from u. The vertex u is called the initial vertex of (u,v) and v is called the terminal or end vertex of (u,v). In a loop, the initial and terminal vertex are the same.

Def: In-degree of v, $deg^-(v)$, is the number of edges w/ v as their terminal vertex.
Out-degree of v, $deg^+(v)$, is the number of edges w/ v as their initial vertex.



	IN	OUT
a	2	4
b	2	1
c	2	2
d	2	1
e	2	2

Theorem: Let $G=(V,E)$ be a digraph, then $\sum_{v\in V} deg^-(v) = \sum_{v\in V} deg^+(v) = |E|$

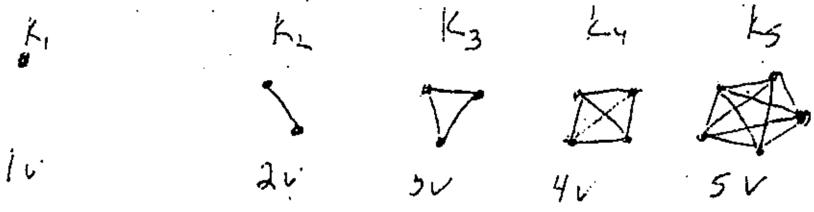
Pf: Every edge contributes "one" to the in-degree and "one" to the out-degree.

NEW

6/97

SPECIAL TYPES OF GRAPHS

→ A complete graph of n vertices, K_n, $n\in P$ is a simple graph containing exactly one edge b/w each pair of distinct vertices.

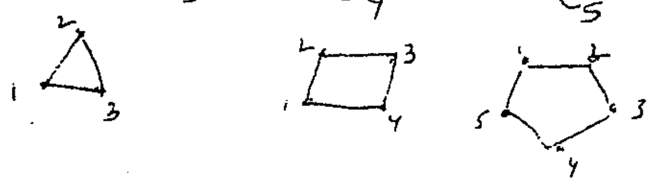


How many edges in K_n?

$$C(n,2) = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$$

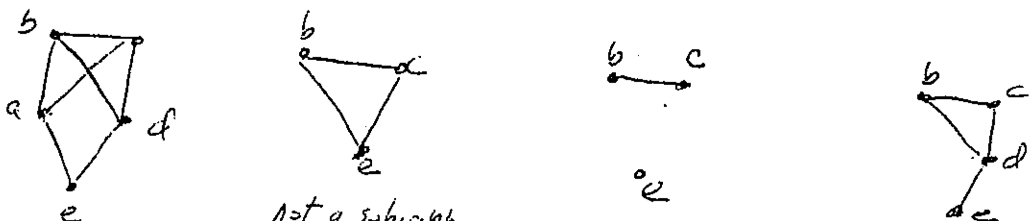
→ The <u>cycle</u>, C_n, $n \geq 3$, $n \in P$, consists of n vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1 v_2\}, \{v_2 v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}$.

$C_3 \cong K_3$ $\qquad$ C_4 $\qquad$ C_5



How many edges in a C_n? $\qquad n$

A <u>subgraph</u> of a graph $G=(V,E)$ is a graph $H=(W,F)$ where $W \subseteq V$ and $F \subseteq E$



G $\qquad$ Not a subgraph $\qquad$ subgraph $\qquad$ subgraph

<u>MATRICES</u>

A <u>matrix</u> is a rectangular array of numbers.
A matrix w/ m rows and n columns is called an $m \times n$ matrix.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad m \times n \qquad A = (a_{ij}) \ m \times n$$

Def: Let $A = (a_{ij})$ $B = (b_{ij})$ both $m \times n$ matrices

→ $A + B = (a_{ij} + b_{ij})$ $(m \times n)$

ex) $\begin{pmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{pmatrix} + \begin{pmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{pmatrix}$

$(3 \times 3) \quad + \quad (3 \times 3) \quad = \quad (3 \times 3)$

→ multiplication

$$\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{ik} \end{bmatrix} \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{kj} \end{bmatrix} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{ik} b_{kj}$$

Def: $\underset{m \times k}{(a_{ij})} \cdot \underset{k \times n}{(b_{ij})} = \underset{m \times n}{(c_{ij})}$ $\quad c_{ij} = a_{i1} b_{1j} + \cdots + a_{ik} b_{kj}$

ex) $\begin{pmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{pmatrix}$

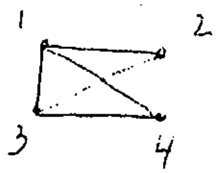
$4 \times 3 \quad 3 \times 2 \quad 4 \times 2$

REPRESENTING GRAPHS w/ ADJACENCY MATRICES

Def: Suppose $G = (V, E)$ is an undirected graph w/ $|V| = n$. The adjacency matrix A of G is the $n \times n$ matrix w/ a_{ij} = the number of edges from v_i to v_j

Note: $a_{ij} = a_{ji}$

If simple then $a_{ij} = 0$ or 1

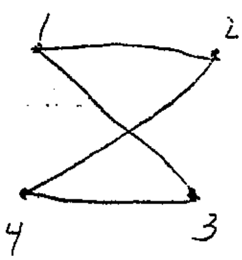
ii) 

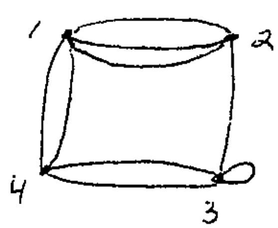
$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

4×4 because $\exists$ 4 vertices

ii) Draw a graph w/ adjacency matrix

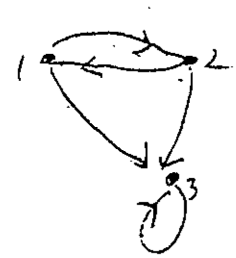
$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$



a) 

$$A = \begin{pmatrix} 0 & 2 & 0 & 2 \\ 3 & 0 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 2 & 0 & 2 & 0 \end{pmatrix}$$

Let $G = (V, E)$ be a directed graph (or multigraph) w/ $|V| = n$. The adjacency matrix A of G is the $n \times n$ matrix w/ a_{ij} = the number of edges $(v_i, v_j) \in E$.



$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

<u>No symmetry</u>

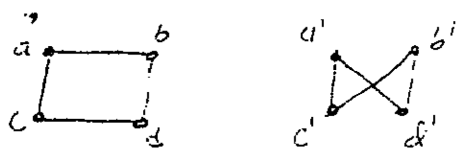
Isomorphism of Graphs

Is it possible to reorder the vertices of 2 graphs so that they are the same?

Def : The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a bijection $f: V_1 \to V_2$ that preserves adjacency: for every $\{v_1, v_2\} \in E_1$, then $\{f(v_1), f(v_2)\} \in E_2$

for digraphs: for every $(v_1, v_2) \in E_1$, then $(f(v_1), f(v_2)) \in E_2$

ex)



bijection	from 1st	from bijection	is an edge in graph 2
$a \to a'$	$\{a,b\} \to$	$\{a', d'\}$	✓
$b \to d'$	$\{a,c\} \to$	$\{a', c'\}$	✓
$c \to c'$	$\{b,d\} \to$	$\{d', b'\}$	✓
$d \to b'$	$\{c,d\} \to$	$\{c', b'\}$	✓

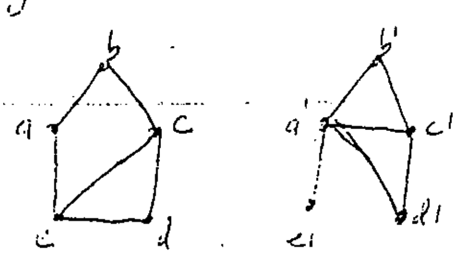
$\therefore$ two graphs are isomorphic

USE THIS AFTER YOUR PRETTY SURE ITS isomorphic

Invariants Under Isomorphism

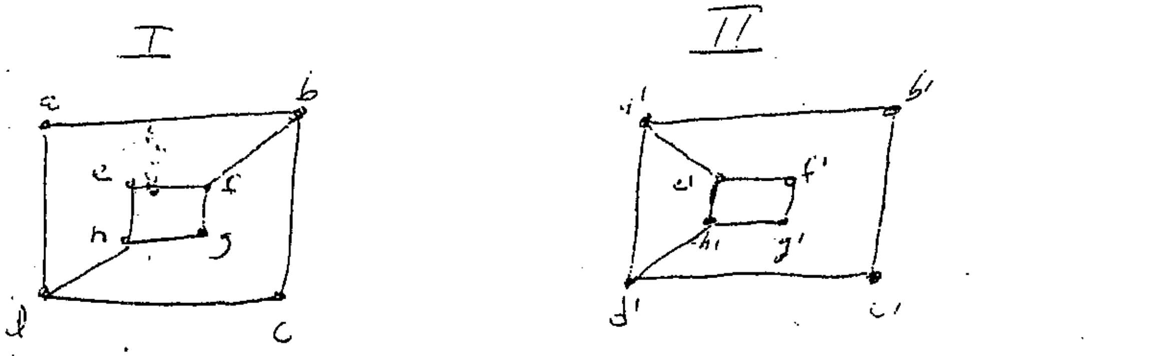
1. Same number of vertices
2. Same number of edges
3. Degree structure must be same

ex)



both have same # of vertices & edges however degree structure is different and $\therefore$ not isomorphic

4. Pattern of degree structure must be the same.
5. Corresponding subgraphs of graphs must be isomorphic.



→ both graphs have 8 V, 10 e, 4 vertices of degree 2 and 4 vertices of degree 3

→ pattern of degree structure differs:

in G I: vertices of degree 2 are nonadjacent.
G II: vertices of degree 2 are adjacent in pairs

in G I: vertices of degree 2 are adjacent to vertices of degree 3
G II: vertices of degree 2 are adjacent to one vertex of degree 3 and one vertex of degree 2.

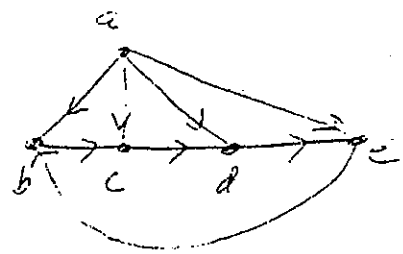
in G I: vertices of degree 3 are adjacent to one vertex of degree 3 and 2 of degree 2
G II: vertices of degree 3 are adjacent to two vertices of degree 3 and 1 of degree 2.

→ corresponding subgraphs are not isomorphic
in G II: vertices of degree 3 form a C_4 but not so in G I.
in G II: there are 3 C_4's but in G I there are only 2 C_4's.

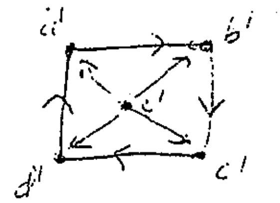
81

I

(i)



II



both have 5V, 8e

	in	out
1	0	4
4	2	1

→ can't find diff. patterns so ∴ find a bijection

start w/ definite ones ∴

$a \to e'$
$b \to \underline{a'}$ choose most confining
$c \to \underline{b'}$ determined: if $(b,c) \in I$, then $(a',\_) \in II$
$d \to c'$
$e \to d'$

List edges of G I

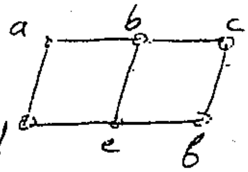
$(a,b) \to (e',a')$ ✓
$(a,c) \to (e',b')$ ✓
$(a,d) \to (e',c')$ ✓
$(a,e) \to (e',a')$ ✓
$(b,c) \to (a',b')$ ✓
$(c,d) \to (b',c')$ ✓
$(d,e) \to (c',d')$ ✓
$(e,b) \to (d',a')$ ✓

Connectivity and Paths

Def: A path of length n from x_0 to x_n, $n \in N$ in an undirected graph is a sequence of edges $e_1, e_2, \ldots, e_n$ s.t. $f(e_1) = \{x_0, x_1\}$, $f(e_2) = \{x_1, x_2\}$, $\ldots$, $f(e_n) = \{x_{n-1}, x_n\}$.

If simple graph, we denote path by vertex sequence $x_0 x_1 x_2 \cdots x_n$
(can draw entire graph w/o picking up your pencil)

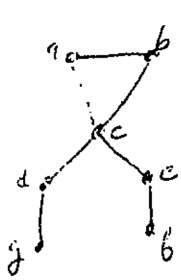
Def: A path is a circuit if it begins and ends at the same vertex ($x_0 = x_n$).
A path is simple if it does not contain the same edge more than once.
A simple circuit is a cycle.



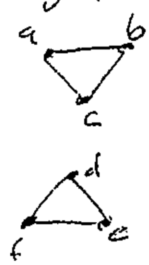
abcfeba — circuit of L6
abcfed — simple of L5
abeda — cycle of L4

Def: A path of length n, $n \in N$, from x_0 to x_n in a digraph is a sequence of edges $e_1, e_2, \ldots, e_n$ s.t. $f(e_1) = (x_0, x_1)$, $f(e_2) = (x_1, x_2) \cdots f(e_n) = (x_{n-1}, x_n)$.
We denote the path by vertex sequence $x_0 x_1 \ldots x_n$ if no multiple edges.
(Same definition for circuit, simple path, cycle as w/ undirected graph.)

Def. An undirected graph is called connected if there is a path b/w every pair of distinct vertices of the graph.

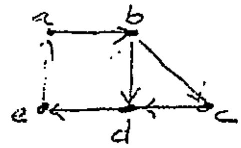


connected



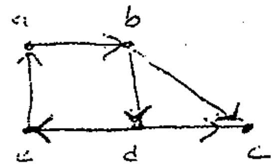
not connected

Def: A digraph is strongly connected if there is a path from v_i to v_j and from v_j to v_i for every pair of vertices v_i, v_j in the digraph.

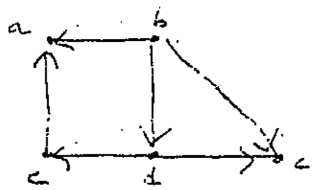


from textbook

Def: A digraph is weakly connected if there is a path from v_i to v_j or from v_j to v_i for every pair of vertices v_i, v_j in the digraph.



Weakly connected (one way path to c)

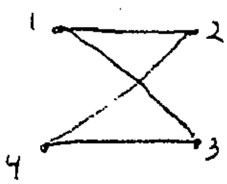


not connected because there is no path from a to c or c to a

Theorem: Let G be a graph w/ adjacency matrix A, $|V|=n$ (may be digraph, graph, multiple edges, loops allowed).

The number of paths of length r, $r \geq 0$ from v_i to v_j is the (i,j) entry of A^r.

2i)



$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad A^3 = \begin{pmatrix} 0 & 4 & 4 & 0 \\ 4 & 0 & 0 & 4 \\ 4 & 0 & 0 & 4 \\ 0 & 4 & 4 & 0 \end{pmatrix}$$

There are 4 paths of L3 from v_2 to v_4

2134

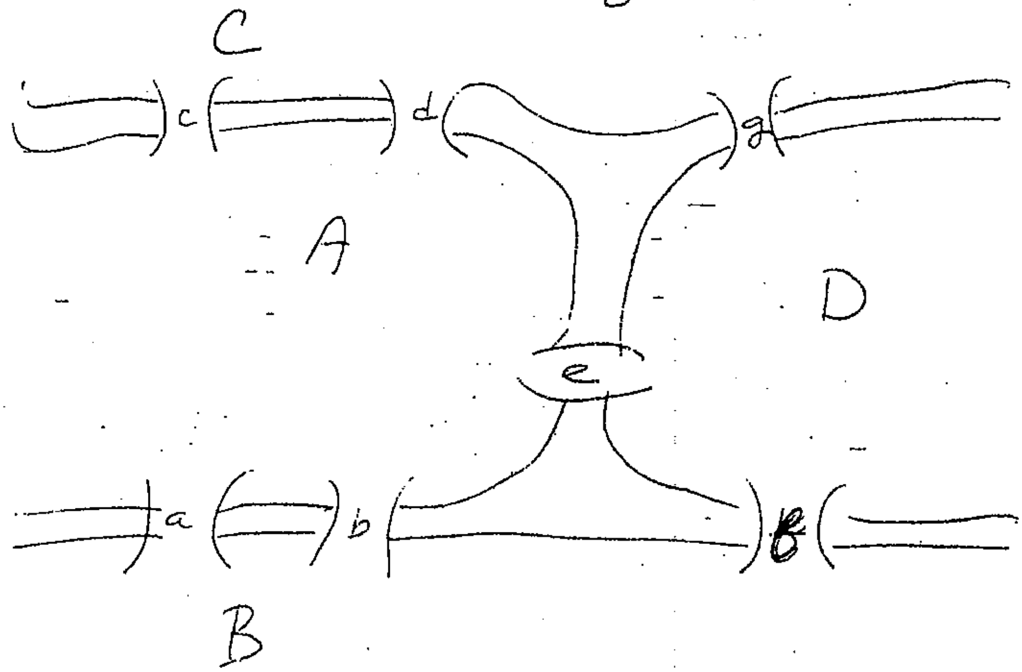
2124

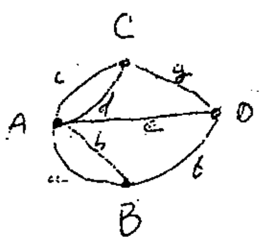
2424

2434

Special Types of Graphs

① The Seven Bridges of Konigsberg (Euler, 1736)





Def: An <u>Euler path</u> in G is a simple path containing every edge of G.
An <u>Euler circuit</u> in G is a simple circuit(cycle) containing every edge of G.

→ Say there is an Euler path. Start at odd degree vertex and you can't end at that odd degree vertex

→ if you don't start at odd degree vertex, must end at an odd degree.

start

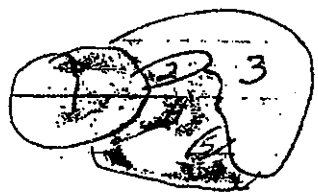
→ if you start at an even degree, you must end there.

→ if you don't start at ...

<u>ler's Theorem</u>: Let G be a connected graph. Then G has an Euler path iff every vertex has an even degree (circuit **AS** well) or exactly two vertices of odd degree.

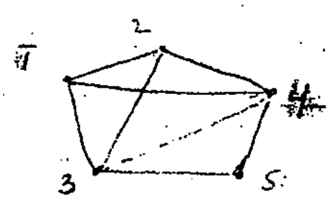
② <u>Four Color Problem</u>

Look at any <u>map</u> and try to color it so bordering countries never have the same color. (Using minimum # of colors)



You need at least 4 colors.

→ change countries into vertices + put an edge b/w vertices if the two countries share a common border.

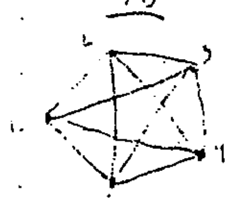


<u>Chromatic number = 4</u>

A coloring of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color.

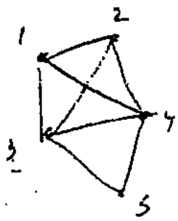
<u>Def</u>: The <u>chromatic number</u> of a graph is the least number of colors needed for a coloring of this graph.

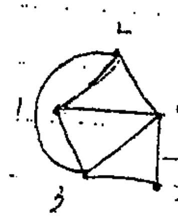
<u>K_5</u>



graphs chromatic # can be > 4.
The theorem states a graph from a map. ...

Def: A graph is called planar if it can be drawn w/o any edges crossing (called planar representation of the graph).





nonplanar: K_5 and $K_{3,3}$ or if a K_5 or $K_{3,3}$ is in its subgraph.

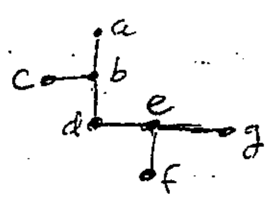
chromatic # is 2

eorem: Four color theorem asserts that the chromatic number of a planar graph is no larger than 4.

Note: this theorem does not apply to nonplanar graphs.

TREES

Def: A tree is an undirected graph w/ a unique path b/w each pair of vertices of G.



ef: A rooted tree is a tree w/ one designated vertex called the root.

f: A directed tree is a rooted tree w/ a unique directed path to each vertex from the root.

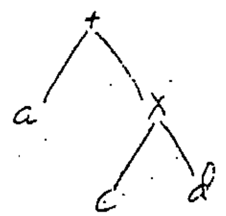
a (ROOT) → always at top

{because it always goes down you can

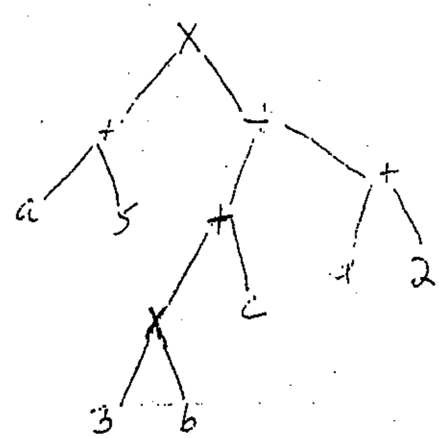
Computer scientists describe Algebraic and Logical Expressions as Directed Tree Structures

$a+b$:

$a+(c \times d)$;



$(a+5) \times [(3 \times b + c)/(d+2)]$



---

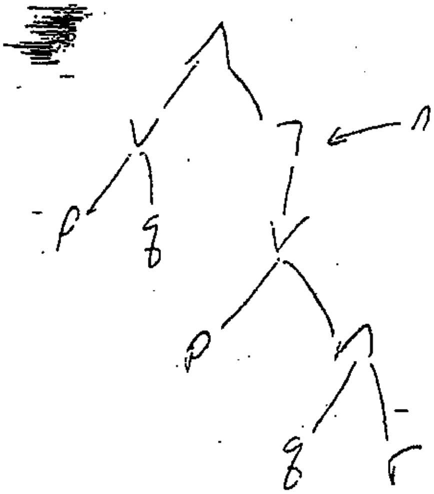
ef: Operator prefix notation (polish notation)
→ put operators before operands — unambiguous w/o use of parenthesis

$a+b \rightarrow +ab$
$a+(c \times d) \rightarrow +a \times cd$

$(a+5) \times [(3 \times b + c)/(d+2)]$:

start at root	X
go to left	X+a
hit operand go right	X+a5
	X+a5÷+X3bc+d2

e.) $\wedge \vee p q \neg \vee p \wedge q r$



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

Notebook Starts

Def: Polish postfix notation (AKA reverse polish notation) where the operators come after the operands.

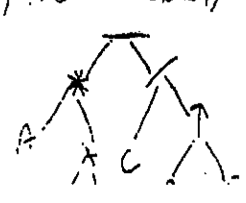
$a+b \rightarrow ab+$
$a+(c \times d) \rightarrow acd\times+$

$(p \vee q) \wedge (\neg(p \vee (q \wedge r)))$ (see tree above)   do from right to left but still start at root + go right

$p q \vee p q r \wedge \vee \neg \wedge$
↑ started here

* for multiplication
↑ for exponentiation

ei) ABC+*CDE↑/-   postfix



$A(B+C) - (C \div D^E)$

Thms: For Undirected Trees

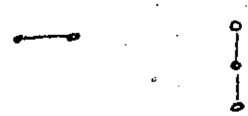
Thm: A simple graph is a tree iff G is connected and contains no cycles.

Pf: Tree $\Rightarrow$ connected
$\Rightarrow$ no cycles (or path would not be unique)

Connected, no cycles $\}$ $\Rightarrow$ unique path $\therefore$ a tree

Thm: In every nontrivial tree, there is at least one vertex of degree 1.

note: • trivial tree



Pf: # of vertices are finite. Start at any vertex. Move along to next adjacent vertex until you find a vertex of degree 1 because there are no cycles.

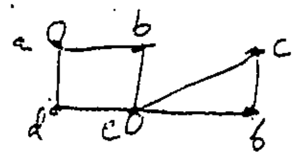
Thm: A tree w/ n vertices has $n-1$ edges, $n=1,2,3,\ldots$

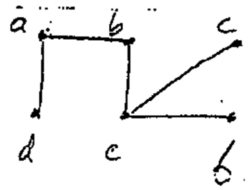
Pf: Basis case: A tree w/ 1 vertex has 0 edges. ✓
Inductive step: Assume a tree w/ k vertices has $k-1$ edges.
Prove that a tree w/ $k+1$ vertices has k edges

Say we have a tree w/ $k+1$ vertices.
One vertex has degree 1 (by Thm. above)

remove 1st vertex of degree + edge $\therefore$
k vertices, no cycles, connected
By assumption a tree w/ k vertices has $k-1$ edges, then
add 1 edge we took out and $\therefore$ the total

Theorem: A graph G is a tree if G has no cycles and $|E| = |V| - 1$

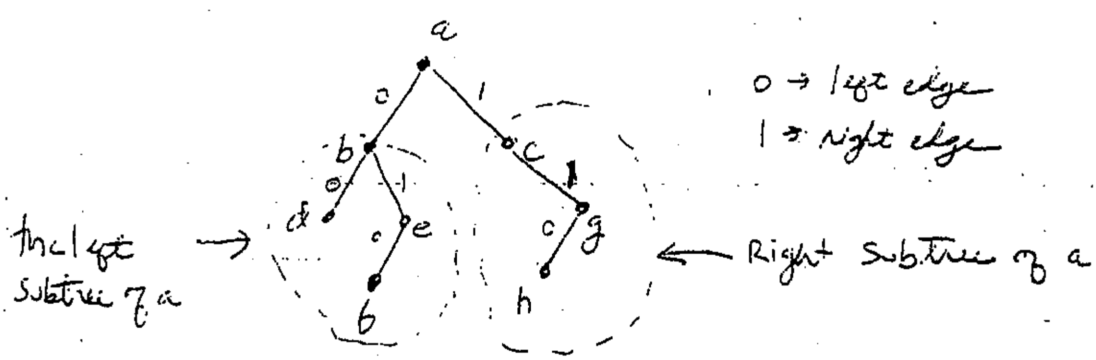




form. subgraph using all vertices that is a tree

Binary Trees

Def: A binary tree is a directed tree $T = (V, E)$ w/ an edge labeling $f: E \to \{0,1\}$ s.t. every vertex has at most one edge incident from it labeled w/ a 1 and/or 0.



Traversal of Binary Trees

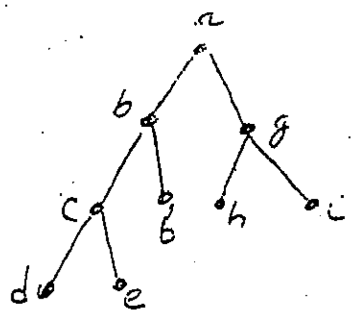
Def: A traversal of a binary tree is a process that enumerates each of the vertices in the tree exactly once.

① Preorder traversal

(a) For any subtree, first visit root

(b) Then perform preorder traversal on the entire left subtree from that root

(c) Then perform preorder traversal on the entire right subtree from that root



(just like Polish prefix)

Preorder traversal : $a\, T_b\, T_g$

$a\, b\, T_c\, T_f\, g\, T_h\, T_i$

$a\, b\, c\, T_d\, T_e\, f\, g\, h\, i$

abcdefghi

② Postorder traversal

(a) Perform postorder traversal on the roots' entire left subtree

(b) Then perform postorder traversal on the roots' entire right subtree

(c) Visit Root

Using example above

$T_b\, T_g\, a$

$T_c\, T_f\, b\;\; T_h\, T_i\, g\;\; a$

(just like Polish postfix notation)

$T_d\, T_e\, c\, f\, b\, h\, i\, g\, a$

decfbhiga

③ Inorder traversal

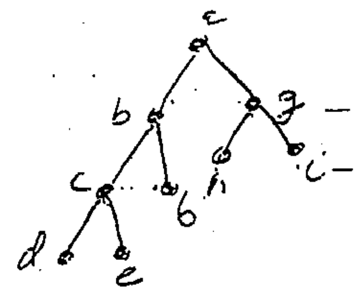
(a) Perform inorder traversal on the root's entire left subtree
(b) Visit root
(c) Perform inorder traversal on the root's entire right subtree

$$T_b\, a\, T_g$$

$$T_c\, b\, T_f\, a\, T_h\, g\, T_i$$

$$T_d\, c\, T_e\, b\, f\, a\, h\, g\, i$$

$$d\,c\,e\,b\,f\,a\,h\,g\,i$$



7/28/97

BOOLEAN ALGEBRA

Def: A Boolean algebra $(\beta, +, \cdot, -, 0, 1)$ is a set, β, with two binary operators, $+$, $\cdot$, one unary operator, $-$, and two elements $0, 1 \in \beta$ w/ the following properties:

1. There exists at least two elements $a, b \in \beta$ w/ $a \neq b$
2. $\forall\, a, b \in \beta$, $a+b \in \beta$ and $a \cdot b \in \beta$ (closure)
3. $\forall\, a, b \in \beta$, $a+b = b+a$, $a \cdot b = b \cdot a$ (commutative)
4. $\forall\, a \in \beta$, $a+0 = a$, $a \cdot 1 = a$ (identity)
5. $\forall\, a, b, c \in \beta$, $a \cdot (b+c) = a \cdot b + a \cdot c$; $a + (b \cdot c) = (a+b)(a+c)$ (distributive)

*

6. $\forall\, a \in \beta$, $\exists\, \bar{a} \in \beta$ w/ $a + \bar{a} = 1$, $a \cdot \bar{a} = 0$ (Complement)
7. $\forall\, a, b, c \in \beta$, $a + (b+c) = (a+b)+c$; $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associative)

other types of Boolean Algebras

$\mathcal{B}$	$\{T,F\}$	$\mathcal{P}(X)$
$+$	$\vee$	$\cup$
$\cdot$	$\wedge$	$\cap$
$\bar{\ }$	$\neg$	$\overline{(\ )}$
0	F	ϕ
1	T	$\mathcal{U}=X$

<u>Theorem</u>: $\forall a \in \mathcal{B}\quad a+a=a$ (Principle of Duality: $a \cdot a = a$)

→ to prove $a \cdot a = a$, just switch all $+$ to $\cdot$ and swap 0's and 1's but steps + reasons stay the same

Pf:
$$\begin{aligned} a+a &= (a+a)\cdot 1 && \text{Identity}\\ &= (a+a)\cdot(a+\bar{a}) && \text{Complement}\\ &= a + a\cdot\bar{a} && \text{Distributive}\\ &= a+0 && \text{Complement}\\ &= a && \text{Identity}\end{aligned}$$

<u>Theorem</u>: $\forall a \in \mathcal{B}$: $a+1=1$ (Dual: $a \cdot 0 = 0$)

Pf:
$$\begin{aligned} a+1 &= (a+1)\cdot 1 && \text{Identity}\\ &= (a+1)\cdot(a+\bar{a}) && \text{Complement}\\ &= a+1\cdot\bar{a} && \text{Distributive}\\ &= a+\bar{a} && \underline{\text{Identity}}\\ &= 1 && \text{Complement}\end{aligned}$$

<u>Theorem</u>: $\forall a,b \in \mathcal{B}\quad a+ab=a$ (Dual: $(a(a+b))=a$)

Pf:
$$\begin{aligned} a+a\cdot b &= a\cdot 1 + a\cdot b && \text{Identity}\\ &= a\cdot(1+b) && \text{Distributive}\\ &= a\cdot 1 && \text{Thm } \underline{a+1=1}\\ &= a && \text{Identity}\end{aligned}$$

<u>Theorem</u>: $\forall a,b \in \mathcal{B}\quad a+\bar{a}b=a+b$ (Dual: $a\cdot(\bar{a}+b)=a\cdot b$)

Pf:
$$\begin{aligned} a+\bar{a}b &= (a+\bar{a})\cdot(a+b) && \text{Distributive}\\ &= 1\cdot(a+b) && \text{Complement}\\ &= a+b && \text{Identity}\end{aligned}$$

Boolean Functions

Consider Boolean Algebra $(\{T,F\}, \vee, \wedge, \neg, T, F)$
however use notation $(\{1,0\}, +, \cdot, \bar{\ }, 1, 0)$ $\therefore$ $\underline{\beta} = \{1,0\}$

Def: A Boolean function of n variables is a function $f: \beta^n \to \beta$ where $\beta = \{1,0\}$

$$\beta^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \beta \quad 1 \le i \le n\}$$

ex) $f: \beta^3 \to \beta$ $\quad f((x,y,z)) = x \cdot y + \bar{z}$

x	y	z	f
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

Different Boolean expressions determine the same Boolean functions

ex) $f((x_1,x_2,x_3)) = x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$

ex) $f((x_1,x_2)) = \overline{x_1 \cdot x_2} = \bar{x}_1 + \bar{x}_2$

Standardized form for a Boolean function

Def: A literal is a Boolean variable or its complement. ex) $y = x$ or $y = \bar{x}$

Def: A minterm of the Boolean variables $x_1, x_2, \ldots, x_n$ is a Boolean product of literals $y_1 y_2 \ldots y_n$

ex) Two variables x_1, x_2

$y_1 y_2$ (where y_1 is a literal x_1 and y_2 is a literal x_2)

literals: $x \cdot x$ $\quad \bar{x} \cdot x$

→ In general, there are 2^n minterms for n variables

There is a bijection b/w n-tuples and minterms of n variables.

$(j_1, j_2, \ldots, j_n) \rightarrow y_1 y_2 \cdots y_n$

if $j_i = 1$ then $y_i = x_i$
$j_i = 0$ then $y_i = \overline{x_i}$

ex) $(1, 0, 0, 1) \rightarrow x_1 \cdot \overline{x_2} \cdot \overline{x_3} \cdot x_4$

ex) $\overline{x_1} \cdot \overline{x_2} \cdot x_3 \cdot x_4 \cdot \overline{x_5} \rightarrow (0, 0, 1, 1, 0)$

Def: Standardized Form for Boolean functions is called Disjunctive Normal Form or Sum of Products Form and is the representation of the function as a sum of minterms. (unique up to the ordering of the minterms)

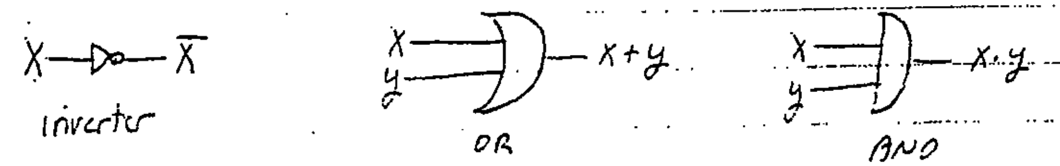
ex) Find the DNF for $F(x, y, z) = (x + y) \cdot \overline{z}$

Step 1: Calculate truth table

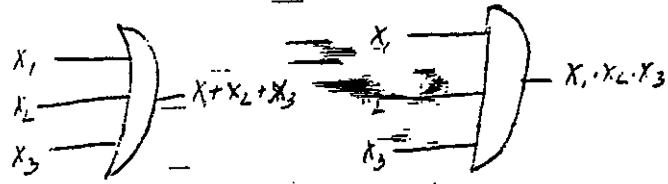
x	y	z	$(x+y)\cdot\overline{z}$	
1	1	1	0	
1	1	0	1	←
1	0	1	0	
1	0	0	1	←
0	1	1	0	
0	1	0	1	←
0	0	1	0	
0	0	0	0	

Step 2: Identify the n-tuples at which the function is 1 (←)
Step 3: Form the minterms corresponding to these n-tuples and add.

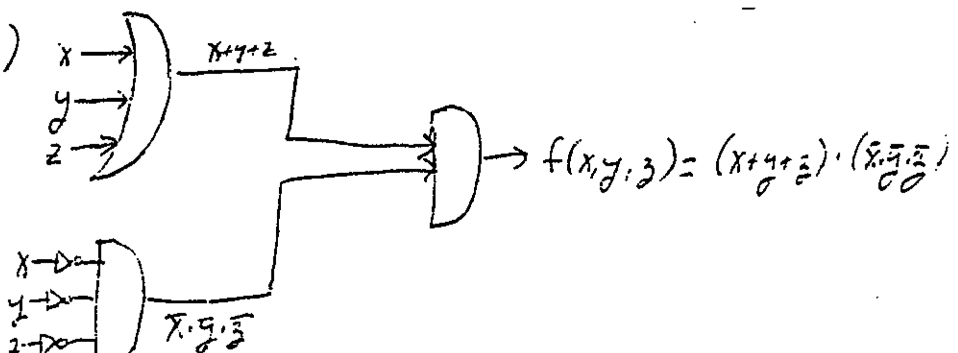
Gates:



Allow in design:



ex)



Minimization of Circuits

After representing a circuit by a Boolean function, you get an equivalent Boolean function g w/ a minimal number of terms in a Sum of products expression.

$$f((x_1,x_2,x_3)) = \overline{x_1} x_2 \overline{x_3} + \overline{x_1}\,\overline{x_2}\,\overline{x_3} + x_1\overline{x_2}\,\overline{x_3} + x_1 x_2 x_3 + x_1 \overline{x_2} x_3$$

look at minterms which are the same except at one value

$$\overline{x_1} x_2 \overline{x_3} + \overline{x_1}\,\overline{x_2}\,\overline{x_3} = \overline{x_1}\,\overline{x_3}(x_2+\overline{x_2}) = \overline{x_1}\,\overline{x_3}(1) = \overline{x_1}\cdot\overline{x_3}$$

$$x_1x_2x_3 + x_1\overline{x_2}x_3 = x_1x_3(x_2+\overline{x_2}) = x_1x_3(1) = x_1x_3$$

→ can add $x_1\overline{x_2}x_3$ to sum because $a + a = 1$

$$x_1\overline{x_2}\,\overline{x_3} + x_1\overline{x_2}x_3 = x_1\overline{x_2}(\overline{x_3}+x_3) = x_1\overline{x_2}(1) = x_1\overline{x_2}$$

7/30/97

Karnaugh map - visual aid to minimize circuits (switching functions)

	y	$\bar{y}$
x		
$\bar{x}$		

Two variables

Every cell represents a minterm. If the minterm appears in the disjunctive normal form, then put a 1 in the appropriate box.

Adjacent cells have minterms that differ in only one variable, ∴ adjacent cells can be collapsed.

Combine 2 adjacent cells → eliminate 1 variable
Combine 4 adjacent cells → eliminate 2 variables
Combine 8 adjacent cells → eliminate 3 variables

ex)

	y	$\bar{y}$
x	1	
$\bar{x}$	1	

$xy + \bar{x}y$ ← disjunctive form

∴ $f(x,y) = y$

equal

	y	$\bar{y}$
x		1
$\bar{x}$	1	1

$\bar{x}y + \bar{x}\bar{y} + x\bar{y}$

$f(x,y) = \bar{x} + x\bar{y}$

$= \bar{x} + \bar{y}$

Three variables

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	A			A
$\bar{x}$	B			B

(A) and (B) are adjacent

ex)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1			
$\bar{x}$	1			

$f(x,y,z) = yz$

a)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1		
$\bar{x}$	1	1		

$f(x,y,z) = yz + y\bar{z} = y(z+\bar{z}) = y(1) = y$

OR

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1		
$\bar{x}$	1	1		

$f(x,y,z) = y$

a)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1	1	1
$\bar{x}$				

$f(x,y,z) = x$

a)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1		1
$\bar{x}$	1	1		1

$f(x,y,z) = y + \bar{y}z$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1		
$\bar{x}$	1	1		

$f(x,y,z) = y + z$

a)

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x	1	1		
$\bar{x}$			1	1

$f(x,y,z) = xy + \bar{x}\bar{y}$

FOUR VARIABLES

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx	A	B		
$w\bar{x}$				
$\bar{w}\bar{x}$				
$\bar{w}x$	A	B		

A and B are adjacent cells