DISCRETE MATHEMATICAL STRUCTURES

(Common to CSE & ISE)

Subject Code: 10CS34 I.A. Marks : 25
Hours/Week : 04 Exam Hours: 03
Total Hours : 52 Exam Marks: 100

PART – A

UNIT – 1 6 Hours

Set Theory: Sets and Subsets, Set Operations and the Laws of Set Theory, Counting and Venn Diagrams, A First Word on Probability, Countable and Uncountable Sets

UNIT – 2 7 Hours

Fundamentals of Logic: Basic Connectives and Truth Tables, Logic Equivalence – The Laws of Logic, Logical Implication – Rules of Inference

UNIT – 3 6 Hours

Fundamentals of Logic contd.: The Use of Quantifiers, Quantifiers, Definitions and the Proofs of Theorems

UNIT – 4 7 Hours

Properties of the Integers: Mathematical Induction, The Well Ordering Principle – Mathematical Induction, Recursive Definitions

PART – B

UNIT – 5 7 Hours

Relations and Functions: Cartesian Products and Relations, Functions – Plain and One-to-One, Onto Functions – Stirling Numbers of the Second Kind, Special Functions, The Pigeon-hole Principle, Function Composition and Inverse Functions

UNIT – 6 7 Hours

Relations contd.: Properties of Relations, Computer Recognition – Zero-One Matrices and Directed Graphs, Partial Orders – Hasse Diagrams, Equivalence Relations and Partitions

UNIT – 7 6 Hours

Groups: Definitions, Examples, and Elementary Properties, Homomorphisms, Isomorphisms, and Cyclic Groups, Cosets, and Lagrange’s Theorem.

Coding Theory and Rings: Elements of Coding Theory, The Hamming Metric, The Parity Check, and Generator Matrices

UNIT – 8 **6 Hours**

Group Codes: Decoding with Coset Leaders, Hamming Matrices Rings and Modular Arithmetic: The Ring Structure – Definition and Examples, Ring Properties and Substructures, The Integers Modulo n

Text Book:

1. Ralph P. Grimaldi: Discrete and Combinatorial Mathematics,5 Edition, Pearson Education, 2004. (Chapter 3.1, 3.2, 3.3, 3.4, Appendix 3, Chapter 2, Chapter 4.1, 4.2, Chapter 5.1 to 5.6, Chapter 7.1 to 7.4, Chapter 16.1, 16.2, 16.3, 16.5 to 16.9, and Chapter 14.1, 14.2, 14.3).

Reference Books:

1. Kenneth H. Rosen: Discrete Mathematics and its Applications, 7 Edition, McGraw Hill, 2010.
2. Jayant Ganguly: A Treatise on Discrete Mathematical Structures, Sanguine-Pearson, 2010.
3. D.S. Malik and M.K. Sen: Discrete Mathematical Structures: Theory and Applications, Cengage Learning, 2004.
4. Thomas Koshy: Discrete Mathematics with Applications, Elsevier, 2005, Reprint 2008.

INDEX SHEET

PART – A

UNIT – 1 Set Theory: 6 Hours

- Sets and Subsets,
- Set Operations and the Laws of Set Theory,
- Counting and Venn Diagrams,
- A First Word on Probability,
- Countable and
- Uncountable Sets

DISRETE MATHEMATICAL STRUCTURES

UNIT I 6 Hours

Set Theory

Sets: A set is a collection of objects, called elements of the set. A set can be presented by listing its elements between braces: $A = \{1, 2, 3, 4, 5\}$. The symbol e is used to express that an element is (or belongs to) a set. For instance 3 e A. Its negation is represented by /e, e.g. 7 /e A. If the set Is finite, its number of elements is represented |A|, e.g. if $A = \{1, 2, 3, 4, 5\}$ then $|A| = 5$

Some important sets are the following:

1. $N = \{0, 1, 2, 3, \cdots\}$ = the set of natural numbers.
2. $Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ = the set of integers.
3. Q = the set of rational numbers.
4. R = the set of real numbers.
5. C = the set of complex numbers.

If S is one of those sets then we also use the following notations :

1. S^+ = set of positive elements in S, for instance

   $Z^+ = \{1, 2, 3, \cdots\}$ = the set of positive integers.
2. S^- = set of negative elements in S, for instance

   $Z^- = \{-1, -2, -3, \cdots\}$ = the set of negative integers.
3. S^* = set of elements in S excluding zero, for instance R^* = the set of non zero real numbers.

Set-builder notation: An alternative way to define a set, called set- builder notation, is by stating a property (predicate) P (x) verified by exactly its elements, for instance A = {x e Z | $1 \le x \le 5$} = "set of integers x such that $1 \le x \le 5$"—i.e.: $A = \{1, 2, 3, 4, 5\}$. In general: A = {x e U | p(x)}, where U is the universe of discourse in which the predicate P (x) must be interpreted, or $A = \{x \mid P(x)\}$ if the universe of discourse for P (x) is implicitly understood. In set theory the term universal set is often used in place of "universe of discourse" for a given predicate.

Principle of Extension: Two sets are equal if and only if they have the same elements, i.e.: $A = B \equiv \forall x\,(x\ e\ A \leftrightarrow x\ e\ B)$.

Subset: We say that A is a subset of set B, or A is contained in B, and we represent it "$A \subseteq B$", if all elements of A are in B, e.g., if $A = \{a, b, c\}$ and $B = \{a, b, c, d, e\}$ then $A \subseteq B$.

Proper subset: A is a proper subset of B, represented "$A \subset B$", if $A \subseteq B$ but $A = B$, i.e., there is some element in B which is not in A.

Empty Set: A set with no elements is called empty set (or null set, or void set), and is represented by $\varnothing$ or $\{\}$.

Note that nothing prevents a set from possibly being an element of another set (which is not the same as being a subset!). For instance if $A = \{1, a, \{3, t\}, \{1, 2, 3\}\}$ and $B = \{3, t\}$, then obviously B is an element of A, i.e., B e A.

Power Set: The collection of all subsets of a set A is called the power set of A, and is represented P(A). For instance, if $A = \{1, 2, 3\}$, then

$$P(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\} .$$

Multisets: Two ordinary sets are identical if they have the same elements, so for instance, $\{a, a, b\}$ and $\{a, b\}$ are the same set because they have exactly the same elements, namely a and b. However, in some applications it might be useful to allow repeated elements in a set. In that case we use multisets, which are mathematical entities similar to sets, but with possibly repeated elements. So, as multisets, $\{a, a, b\}$ and $\{a, b\}$ would be considered different, since in the first one the element a occurs twice and in the second one it occurs only once.

Set Operations:

1. Intersection: The common elements of two sets:

$$A \cap B = \{x \mid (x\ e\ A) \wedge (x\ e\ B)\} .$$

If $A \cap B = \varnothing$, the sets are said to be disjoint.

2. Union: The set of elements that belong to either of two sets:

$$A \cup B = \{x \mid (x\ e\ A) \vee (x\ e\ B)\} .$$

3. <u>Complement</u> : The set of elements (in the universal set) that do not belong to a given set:

$$A = \{x \text{ e } U \mid x \text{ /e } A\} .$$

4. <u>Difference or Relative Complement</u> : The set of elements that belong to a set but not to another:

$$A - B = \{x \mid (x \text{ e } A) \overline{\wedge} (x \text{ /e } B)\} = A \cap B .$$

5. <u>Symmetric Difference</u> : Given two sets, their symmetric differ- ence is the set of elements that belong to either one or the other set but not both.

$$A \oplus B = \{x \mid (x \text{ e } A) \oplus (x \text{ e } B)\} .$$

It can be expressed also in the following way:

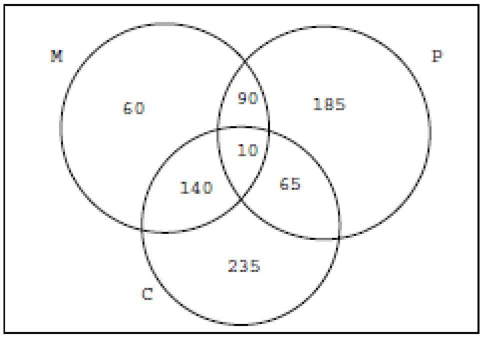
$$A \oplus B = A \cup B - A \cap B = (A - B) \cup (B - A) .$$

Counting with Venn Diagrams:

A Venn diagram with n sets intersecting in the most general way divides the plane into 2^n regions. If we have information about the number of elements of some portions of the diagram, then we can find the number of elements in each of the regions and use that information for obtaining the number of elements in other portions of the plane.

Example : Let M , P and C be the sets of students taking Mathe- matics courses, Physics courses and Computer Science courses respec- tively in a university. Assume
$|M| = 300$, $|P| = 350$, $|C| = 450$,
$|M \cap P| = 100$, $|M \cap C| = 150$, $|P \cap C| = 75$, $|M \cap P \cap C| = 10$. How
many students are taking exactly one of those courses? (fig. 2.7)

We see that $|(M \cap P) - (M \cap P \cap C)| = 100-10 = 90$, $|(M \cap C) - (M \cap P \cap C)| = 150 - 10 = 140$ and $|(P \cap C) - (M \cap P \cap C)| = 75 - 10 = 65$.
Then the region corresponding to students taking Mathematics courses only has cardinality $300-(90+10+140) = 60$. Analogously we compute the number of students taking Physics courses only (185) and taking Computer Science courses only (235). The sum $60 + 185 + 235 = 480$ is the number of students taking exactly one of those courses.



Venn Diagrams:

Venn diagrams are graphic representa- tions of sets as enclosed areas in the plane. For instance, in figure 2.1, the rectangle represents the universal set (the set of all elements con- sidered in a given problem) and the shaded region represents a set A. The other figures represent various set operations.

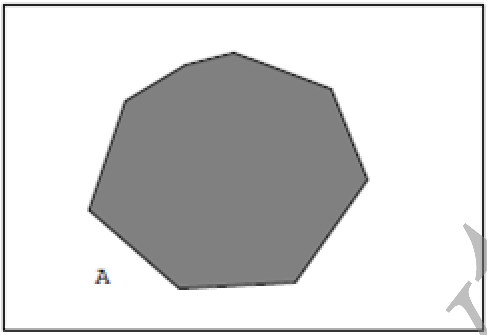


FIGURE 2.1. Venn Diagram.

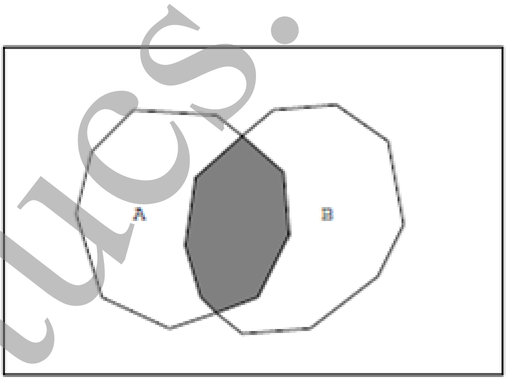


FIGURE 2.2. Intersection $A \cap B$.

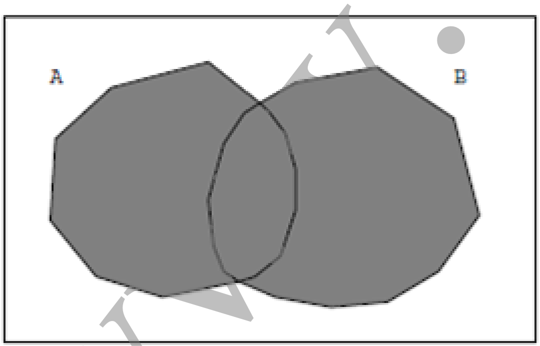


FIGURE 2.3. Union $A \cup B$.

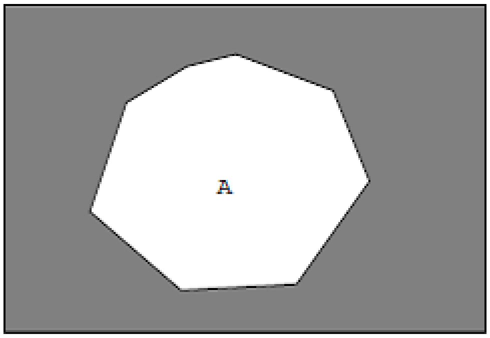
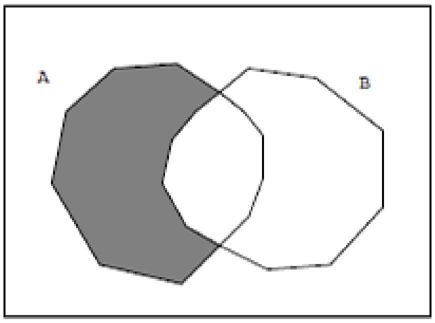


FIGURE 2.4. Complement $\overline{A}$.



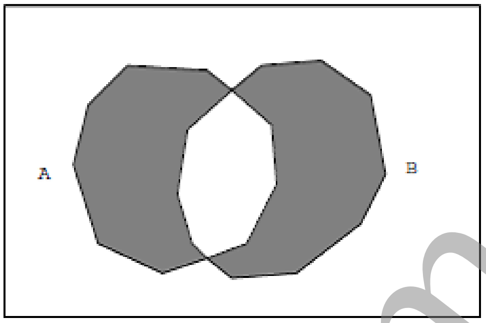


FIGURE 2.5. Difference $A - B$. FIGURE 2.6. Symmetric Difference $A \oplus B$.

Laws of set theory: The set operations verify the following properties:

1. *Associative Laws:*

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

2. *Commutative Laws:*

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

3. *Distributive Laws:*

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

4. *Identity Laws:*

$$A \cup \emptyset = A$$
$$A \cap \mathfrak{U} = A$$

5. *Complement Laws:*

$$A \cup \overline{A} = \mathfrak{U}$$
$$A \cap \overline{A} = \emptyset$$

6. *Idempotent Laws:*

$$A \cup A = A$$
$$A \cap A = A$$

7. *Bound Laws:*

$$A \cup \mathfrak{U} = \mathfrak{U}$$
$$A \cap \emptyset = \emptyset$$

8. *Absorption Laws:*

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

9. *Involution Law:*

$$\overline{\overline{A}} = A$$

10. 0/1 *Laws:*

$$\overline{\emptyset} = \mathfrak{U}$$
$$\overline{\mathfrak{U}} = \emptyset$$

11. *DeMorgan's Laws:*

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

Generalized Union and Intersection: Given a collec- tion of sets A_1 , A_2, . . . , A_N , their union is defined as the set of elements that belong to at least one of the sets (here n represents an integer in the range from 1 to N):

$$\bigcup_{n=1}^{N} A_n = A_1 \cup A_2 \cup \cdots \cup A_N = \{x \mid \exists n\,(x \in A_n)\}\,.$$

Analogously, their intersection is the set of elements that belong to all the sets simultaneously:

$$\bigcap_{n=1}^{N} A_n = A_1 \cap A_2 \cap \cdots \cap A_N = \{x \mid \forall n \, (x \in A_n)\} .$$

These definitions can be applied to infinite collections of sets as well. For instance assume that S_m = {kn | k = 2, 3, 4, . . . } = set of multiples of n greater than n. Then

$$\bigcup_{n=2}^{\infty} S_n = S_2 \cup S_3 \cup S_4 \cup \cdots = \{4, 6, 8, 9, 10, 12, 14, 15, \ldots\}$$

$$= \text{set of composite positive integers} .$$

Partitions: A partition of a set X is a collection S of non overlapping non empty subsets of X whose union is the whole X. For instance a partition of X = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} could be

S = {{1, 2, 4, 8}, {3, 6}, {5, 7, 9, 10}} .

Given a partition S of a set X, every element of X belongs to exactly one member of S.

Example: The division of the integers Z into even and odd numbers is a partition: S = {E, O}, where E = {2n | n e Z}, O = {2n + 1 | n e Z}.

Example : The divisions of Z in negative integers, positive integers and zero is a partition: S = $\{Z^+, Z^-, \{0\}\}$.

Ordered Pairs, Cartesian Product:

An ordinary pair {a, b} is a set with two elements. In a set the order of the elements is irrelevant, so {a, b} = {b, a}. If the order of the elements is relevant, then we use a different object called ordered pair, represented (a, b). Now (a, b) = (b, a) (unless a = b). In general (a, b) = $(a^!, b^!)$ iff a = $a^!$ and b = $b^!$.

Given two sets A, B, their Cartesian product A × B is the set of all ordered pairs (a, b) such that a e A and b e B:

A × B = {(a, b) | (a e A) ∧ (b e B)} .

Analogously we can define triples or 3-tuples (a, b, c), 4-tuples (a, b, c, d), . . . , n-tuples $(a_1, a_2, \ldots, a_m)$, and the corresponding 3-fold, 4-fold,. . . , n-fold Cartesian products:

$A_1 \times A_2 \times \cdots \times A_m$ =

$\{(a_1, a_2, \ldots, a_m) \mid (a_1 \text{ e } A_1) \wedge (a_2 \text{ e } A_2) \wedge \cdots \wedge (a_m \text{ e } A_m)\}$.

If all the sets in a Cartesian product are the same, then we can use an exponent: $A^2 = A \times A$, $A^3 = A \times A \times A$, etc. In general:

(m times)

$^m = A \times A \times \cdots \times A$.

A First Word on Probability:

Introduction: Assume that we perform an experiment such as tossing a coin or rolling a die. The set of possible outcomes is called the sample space of the experiment. An event is a subset of the sample space. For instance, if we toss a coin three times, the sample space is

$$S — \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\} .$$

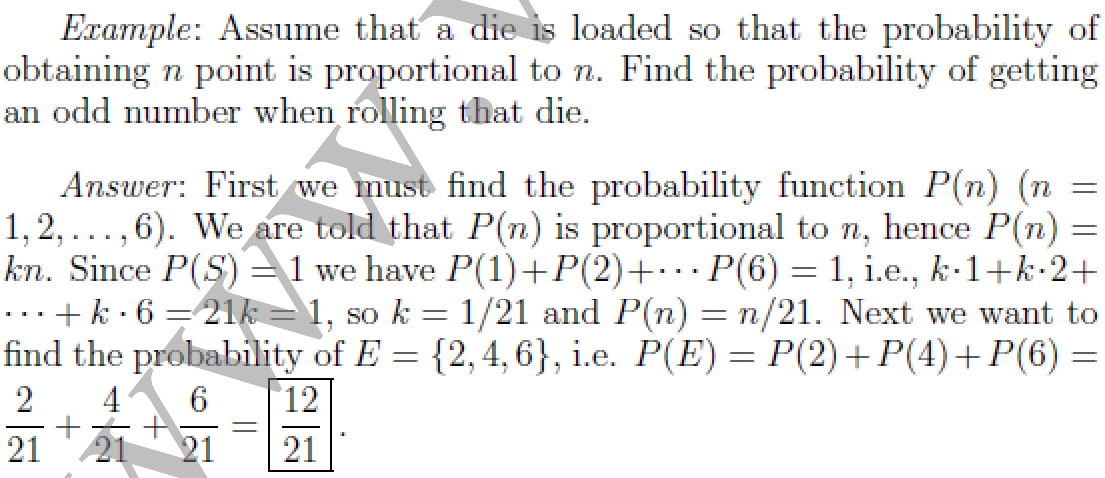
The event "at least two heads in a row" would be the subset

$$E — \{HHH, HHT, THH\} .$$

If all possible outcomes of an experiment have the same likelihood of occurrence, then the probability of an event A ⊂ S is given by Laplace's rule:

$$P(E) = \frac{|E|}{|S|}$$

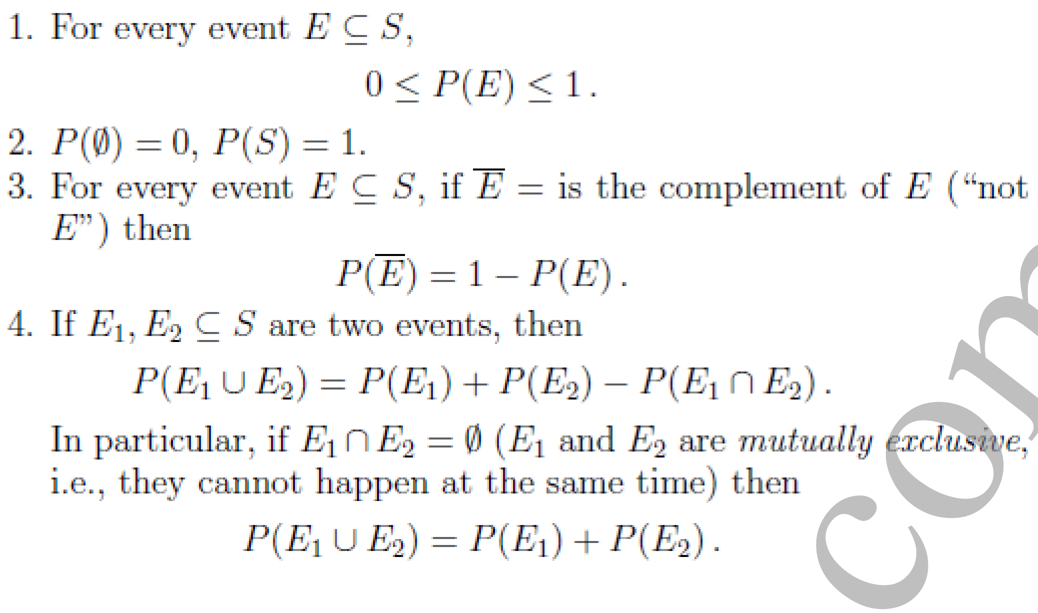
For instance, the probability of getting at least two heads in a row in the above experiment is 3/8.



Example: Assume that a die is loaded so that the probability of obtaining n point is proportional to n. Find the probability of getting an odd number when rolling that die.

Answer: First we must find the probability function $P(n)$ $(n = 1, 2, \ldots, 6)$. We are told that $P(n)$ is proportional to n, hence $P(n) = kn$. Since $P(S) = 1$ we have $P(1) + P(2) + \cdots P(6) = 1$, i.e., $k \cdot 1 + k \cdot 2 + \cdots + k \cdot 6 = 21k = 1$, so $k = 1/21$ and $P(n) = n/21$. Next we want to find the probability of $E = \{2, 4, 6\}$, i.e. $P(E) = P(2) + P(4) + P(6) = \frac{2}{21} + \frac{4}{21} + \frac{6}{21} = \boxed{\frac{12}{21}}$.

Properties of probability: Let P be a probability func- tion on a sample space S. Then:



1. For every event $E \subseteq S$,

$$0 \leq P(E) \leq 1 .$$

2. $P(\emptyset) = 0$, $P(S) = 1$.
3. For every event $E \subseteq S$, if $\overline{E}$ = is the complement of E ("not E") then

$$P(\overline{E}) = 1 - P(E) .$$

4. If $E_1, E_2 \subseteq S$ are two events, then

$$P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2) .$$

In particular, if $E_1 \cap E_2 = \emptyset$ (E_1 and E_2 are *mutually exclusive*, i.e., they cannot happen at the same time) then

$$P(E_1 \cup E_2) = P(E_1) + P(E_2) .$$

THE CONCEPT OF PROBALITY:

Pr(A)=|A| / |S| where |A| is an event and |S| is sample space

Pr(A)=|A| / |S|=(|S|-|A|)/|S|= 1- (|A|/|S|)= 1-Pr(A).

Pr(A)=0 if and only if Pr(A)=1 and Pr(A)=1 if and only if

Pr(A)=0

ADDITION THEROM:

Suppose A and B are 2 events is a sample space S then A UB is an event in S consisting of outcomes that are in A or B or both and A ∩ B is an event is S consisting of outcomes thatarecommon to A and B. accordingly by the principle of addition we have |AUB|=|A|+|B|-|A ∩B| and formula 1 gives

Pr(AUB)=|AUB|/|S|=(|A|+|B|-|A ∩B|)/|S|

= |A|/|S| + |B|/|S| - |A ∩ B| / |S|

Pr(AUB) =Pr(A)+Pr(B)-Pr(A ∩ B)

MUTUALY EXCLUSIVE EVENTS:

Two events A and B in a sample space are said to be mutual exclusive if A ∩ B =Ø then Pr(A ∩B)=0 and the addition theorem reduces to Pr(AUB)= Pr(A)+Pr(B)

If A1,A2…….An are mutualy exclusive events, then Pr(A1UA2U…….UAn)= Pr(A1)+Pr(A2)+….+Pr(An)

CONDITIONAL PROBABILITY:

If E is an event in a finite sample S with Pr(E)>0 then the probability that an event A in S occurs when E has already occurred is called the probability of A relative to E or the conditional probability of A , given E

This probability, denoted by Pr(A|E) is defined by

Pr(A|E)=|A∩ E|/ |E| from this |A∩ E|=|E| . Pr(A|E)

Pr(A∩ E)= |A∩ E|/ S=|=|E|/|S| . Pr(A|E)=Pr(E) . Pr(A|E)

Example: Find the probability of obtaining a sum of 10 after rolling two fair dice. Find the probability of that event if we know that at least one of the dice shows 5 points.

Answer: We call E — “obtaining sum 10” and F — “at least one of the dice shows 5 points”. The number of possible outcomes is 6 × 6 —
36. The event “obtaining a sum 10” is E — {(4, 6), (5, 5), (6, 4)}, so
|E| — 3. Hence the probability is P (E) — |E|/|S| — 3/36 — 1/12.
Now, if we know that at least one of the dice shows 5 points then the
sample space shrinks to
F — {(1, 5), (2, 5), (3, 5), (4, 5), (5, 5), (6, 5), (5, 1), (5, 2), (5, 3), (5, 4), (5, 6)} ,
so |F| — 11, and the ways to obtain a sum 10 are E n F — {(5, 5)},
|E n F| — 1, so the probability is P (E | F) — P (E n F)/P (F) — 1/11.

MUTUALLY INDEPENDENT EVENTS:

The event A and E in a sample space S are said to be mutually independent if the probability of the occurrence of A is independent of the probability of the occurrence of E, So that Pr(A)=Pr(A|E). For such events Pr(A ∩ E)=Pr(A).Pr(E)

This is known as the product rule or the multiplication theorem for mutually independent events .

A generalization of expression is if A1,A2,A3………..An are mutually independent events in a sample space S then

Pr(A1∩ A2∩ ……………∩ An)=Pr(A1).Pr(A2)………..Pr(An)

Example: Assume that the probability that a shooter hits a target is p — 0.7, and that hitting the target in different shots are independent events. Find:

1. The probability that the shooter does not hit the target in one shot.
2. The probability that the shooter does not hit the target three times in a row.
3. The probability that the shooter hits the target at least once after shooting three times.

Answer:

1. P (not hitting the target in one shot) — 1 — 0.7 — 0.3.
2. P (not hitting the target three times in a row) — 0.3^3 — 0.027.
3. P (hitting the target at least once in three shots) — 1—0.027 —

0.973.

COUNTABLE AND UNCOUNTABLE SETS

A set A is said to be the countable if A is a finite set .
A set which is not countable is called an uncountable set.

THE ADDITION PRINCIPLE:

- $|AUB|=|A|+|B|-|A\cap B|$ is the addition principle rule or the principle of inclusion – exclusion.
- $|A-B|=|A|-|A\cap B|$
- $|A \cap B|=|U|-|A|-|B| +|A\cap B|$
- $|AUBUC|=|A|+|B|+|C|-|A \cap B|-|B \cap C|-|A \cap C|+|A \cap B \cap C|$ is extended addition principle
- NOTE: $|A \cap B \cap C|=|AUBUC|$
  $=|U|-|AUBUC|$
  $= |U|-|A|-|B| -|C|+|B \cap C|+|A \cap B|+|A \cap C|- |A \cap B \cap C|$
  $|A-B-C|=|A|-|A \cap B|-|A \cap C|+|A \cap B \cap C|$

UNIT – 2 Fundamentals of Logic: 7 Hours

- Basic Connectives and Truth Tables,
- Logic Equivalence
- The Laws of Logic,
- Logical Implication
- Rules of Inference

UNIT 2 7 Hours

Fundamentals of Logic

SYLLABUS

Fundamentals of Logic: Basic Connectives and Truth Tables, Logic Equivalence – The Laws of Logic, Logical Implication – Rules of Inference

Introduction:

Propositions:

A proposition is a declarative sentence that is either true or false (but not both). For instance, the following are propositions: "Paris is in France" (true), "London is in Denmark" (false), "$2 < 4$" (true), "$4 = 7$ (false)". However the following are not propositions: "what is your name?" (this is a question), "do your homework" (this is a command), "this sentence is false" (neither true nor false), "x is an even number" (it depends on what x represents), "Socrates" (it is not even a sentence). The truth or falsehood of a proposition is called its truth value.

Basic Connectives and Truth Tables:

Connectives are used for making compound propositions. The main ones are the following (p and q represent given propositions):

Name	Represented	Meaning
Negation	$\neg p$	"not p"
Conjunction	$p \wedge q$	"p and q"
Disjunction	$p \vee q$	"p or q (or both)"
Exclusive Or	$p \oplus q$	"either p or q, but not both"
Implication	$p \longrightarrow q$	"if p then q"
Biconditional	$p \leftrightarrow q$	"p if and only if q"

The truth value of a compound proposition depends only on the value of its components. Writing F for "false" and T for "true", we can summarize the meaning of the connectives in the following way:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \longrightarrow$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

Note that ∨ represents a non-exclusive or, i.e., p ∨ q is true when any of p, q is true and also when both are true. On the other hand ⊕ represents an exclusive or, i.e., p ⊕ q is true only when exactly one of p and q is true.

Tautology, Contradiction, Contingency:

1. A proposition is said to be a tautology if its truth value is T for any assignment of truth values to its components. Example: The proposition p ∨ ¬p is a tautology.

2. A proposition is said to be a contradiction if its truth value is F for any assignment of truth values to its components. Example: The proposition p ∧ ¬p is a contradiction.

3. A proposition that is neither a tautology nor a contradiction is called a contingency.

p	¬p	p ∨ ¬p	p ∧ ¬p
T	F	T	F
T	F	T	F
F	T	T	F
F	T	T	F

* *

tautology contradiction

Conditional Propositions: A proposition of the form "if p then q" or "p implies q", represented "p ⟶ q" is called a conditional proposition. For instance: "if John is from Chicago then John is from Illinois". The proposition p is called hypothesis or antecedent, and the proposition q is the conclusion or consequent.

Note that p ⟶ q is true always except when p is true and q is false. So, the following sentences are true: "if 2 < 4 then Paris is in France" (true ⟶ true), "if London is in Denmark then 2 < 4" (false ⟶ true),

"if 4 = 7 then London is in Denmark" (false ⟶ false). However the following one is false: "if 2 < 4 then London is in Denmark" (true ⟶ false).

In might seem strange that "p ⟶ q" is considered true when p is false, regardless

of the truth value of q. This will become clearer when we study predicates such as “if x is a multiple of 4 then x is a multiple of 2”. That implication is obviously true, although for the particular
case x = 3 it becomes “if 3 is a multiple of 4 then 3 is a multiple of 2”.

The proposition $p \leftrightarrow q$, read “p if and only if q”, is called bicon- ditional. It is true precisely when p and q have the same truth value, i.e., they are both true or both false.

Logical Equivalence: Note that the compound proposi- tions $p \longrightarrow q$ and $\neg p \vee q$ have the same truth values:

p	q	¬p	¬p ∨ q	p ⟶
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

When two compound propositions have the same truth values no matter what truth value their constituent propositions have, they are called logically equivalent. For instance $p \longrightarrow q$ and $\neg p \vee q$ are logically equivalent, and we write it:

$$p \longrightarrow q \equiv \neg p \vee q$$

Note that that two propositions A and B are logically equivalent precisely when $A \leftrightarrow B$ is a tautology.

Example : De Morgan’s Laws for Logic. The following propositions are logically equivalent:

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

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

p	q	¬p	¬q	p ∨ q	¬(p ∨ q)	¬p ∧ ¬q	p ∧ q	¬(p ∧ q)	¬p ∨ ¬q
T	T	F	F	T	F	F	T	F	F
T	F	F	T	T	F	F	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	T	T	F	T	T	F	T	T

Example: The following propositions are logically equivalent:

p ↔ q ≡ (p ⟶ q) ∧ (q ⟶ p)

Again, this can be checked with the truth tables:

p	q	p ⟶	q ⟶	(p ⟶ q) ∧ (q	p ↔ q
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Exercise: Check the following logical equivalences:

¬(p ⟶ q) ≡ p ∧ ¬q
p ⟶ q ≡ ¬q ⟶ ¬p
¬(p ↔ q) ≡ p ⊕ q

Converse, Contrapositive: The converse of a conditional proposition p ⟶ q is the proposition q ⟶ p. As we have seen, the bi- conditional proposition is equivalent to the conjunction of a conditional proposition an its converse.

p ↔ q ≡ (p ⟶ q) ∧ (q ⟶ p)

So, for instance, saying that "John is married if and only if he has a spouse" is the same as saying "if John is married then he has a spouse" and "if he has a spouse then he is married".

Note that the converse is not equivalent to the given conditional proposition, for instance "if John is from Chicago then John is from Illinois" is true, but the converse "if John is from Illinois then John is from Chicago" may be false.
The contrapositive of a conditional proposition p ⟶ q is the propo- sition ¬q ⟶ ¬p. They are logically equivalent. For instance the con- trapositive of "if John is from Chicago then John is from Illinois" is "if
John is not from Illinois then John is not from Chicago".

LOGICAL CONNECTIVES: New propositions are obtained with the aid of word or phrases like "not","and","if….then",and "if and only if". Such words or phrases are called logical connectives. The new propositions obtained by the use of connectives are called compound propositions. The original propositions from which a compound proposition is obtained are called the components or the primitives of the compound proposition. Propositions which do not contain any logical connective are called simple propositions

NEGATION: A Proposition obtained by inserting the word "not" at an appropriate place in a given proposition is called the negation of the given proposition. The negation of a proposition p is denoted by ~p(read "not p")

Ex: p: 3 is a prime number

~p: 3 is not a prime number

Truth Table:

p	~p
0	1
1	0

CONJUNCTION:

A compound proposition obtained by combining two given propositions by inserting the word "and" in between them is called the conjunction of the given proposition.The conjunction of two proposition p and q is denoted by p^q(read "p and q").

- The conjunction p^q is true only when p is true and q is true; in all other cases it is false.
- Ex: p:√2 is an irational number q: 9 is a prime number
  p^q: √2 is an irational number and 9 is a prime number
- Truth table:

p	q	p^q
0	0	0
0	1	0
1	0	0
1	1	1

DISJUNCTION:

A compound proposition obtained by combining two given propositions by inserting the word "or" in between them is called the disjunction of the given proposition.The disjunction of two proposition p and q is denoted by p∨q(read "p or q").

- The disjunction p∨q is false only when p is false and q is false ; in all other cases it is true.
- Ex: p:√2 is an irational number q: 9 is a prime number
  p∨q : √2 is an irational number or 9 is a prime number Truth table:

-

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

EXCLUSIVE DISJUNCTION:

- The compound proposition “p or q” to be true only when either p is true or q is true but not both. The exclusive or is denoted by symbol $\underline{\vee}$.

- Ex: p:√2 is an irrational number q: 2+3=5

$P \underline{\vee} q$: Either √2 is an irrational number or 2+3=5 but not both.

- Truth Table:

p	q	$p \underline{\vee} q$
0	0	0
0	1	1
1	0	1
1	1	0

CONDITIONAL(or IMPLICATION):

- A compound proposition obtained by combining two given propositions by using the words “if” and “then” at appropriate places is called a conditional or an implication..

- Given two propositions p and q, we can form the conditionals “if p, then q” and “if q, then p:. The conditional “if p, then q”is denoted by $p \rightarrow q$ and the conditional “if q, then p” is denoted by $q \rightarrow p$.

- The conditional $p \rightarrow q$ is false only when p is true and q is false ;in all other cases it is true.

- Ex: p: 2 is a prime number q: 3 is a prime number

$p \rightarrow q$: If 2 is a prime number then 3 is a prime number; it is true

- Truth Table:

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

BICONDITIONAL:

- Let p and q be two propositions,then the conjunction of the conditionals $p \to q$ and $q \to p$ is called bi-conditional of p and q. It is denoted by $p \leftrightarrow q$.

- $p \leftrightarrow q$ is same as $(p \to q) \wedge (q \to p)$. As such $p \leftrightarrow q$ is read as " if p then q and if q then p".

- Ex: p: 2 is a prime number q: 3 is a prime number $p \leftrightarrow q$ are true.

Truth Table:

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

COMBINED TRUTH TABLE

P	q	~p	p^q	$p \vee q$	$p \underline{\vee} q$	$p \to q$	$p \leftrightarrow q$
0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0
1	0	0	0	1	1	0	0
1	1	0	1	1	0	1	1

TAUTOLOGIES; CONTRADICTIONS:

A compound proposition which is always true regardless of the truth values of its components is called a tautology.

A compound proposition which is always false regardless of the truth values of its components is called a contradiction or an absurdity.

A compound proposition that can be true or false (depending upon the truth values of its components) is called a contingency I.e contingency is a compound proposition which is neither a tautology nor a contradiction.

LOGICAL EQUIVALENCE

- Two propositions 'u' and 'v' are said to be logically equivalent whenever u and v have the same truth value, or equivalently .

- Then we write $u \Leftrightarrow v$. Here the symbol $\Leftrightarrow$stands for "logically equivalent to".

- When the propositions u and v are not logically equivalent we write $u \Leftrightarrow v$.

LAWS OF LOGIC:

To denote a tautology and To denotes a contradiction.

- Law of Double negation: For any proposition p,$(\sim\sim p) \Leftrightarrow p$
- Idempotent laws: For any propositions p, 1) $(p \vee p) \Leftrightarrow p$ 2) $(p \wedge p) \Leftrightarrow p$
- Identity laws: For any proposition p, 1)$(p \vee Fo) \Leftrightarrow p$ 2)$(p \wedge To) \Leftrightarrow p$
- Inverse laws: For any proposition p, 1) $(p \vee \sim p) \Leftrightarrow To$ 2)$(p \wedge \sim p) \Leftrightarrow Fo$
- Commutative Laws: For any proposition p and q, 1)$(p \vee q) \Leftrightarrow (q \vee p)$ 2)$(p \wedge q) \Leftrightarrow (q \wedge p)$
- Domination Laws: For any proposition p, 1) $(p \vee To) \Leftrightarrow To$ 2) $(p \wedge Fo) \Leftrightarrow Fo$
- Absorption Laws: For any proposition p and q,1) $[p \vee (p \wedge q)] \Leftrightarrow p$ 2)$[p \wedge (p \vee q)] \Leftrightarrow p$
- De-Morgan Laws: For any proposition p and q, 1)$\sim (p \vee q) \Leftrightarrow \sim p \wedge \sim q$ 2) $\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$
- Associative Laws : For any proposition p ,q and r, 1) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ 2) $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
- Distributive Laws: For any proposition p ,q and r, 1) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ 2) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
- Law for the negation of a conditional : Given a conditional $p \rightarrow q$, its negation is obtained by using the following law: $\sim(p \rightarrow q) \Leftrightarrow [p \wedge (\sim q)]$

NOTE:

- $\sim (p \vee q) \equiv \sim p \wedge \sim q$
- $\sim(p \wedge q) \equiv \sim p \vee \sim q$
- $\sim(p \rightarrow q) \equiv [p \wedge (\sim q)]$
- $(p \rightarrow q) \equiv \sim \sim (p \rightarrow q) \equiv \sim[p \wedge (\sim q)] \equiv \sim p \vee q$

TRANSITIVE AND SUBSTITUTION RULES If u,v,w are propositions such that $u \Leftrightarrow v$ and $v \Leftrightarrow w$, then $u \Leftrightarrow w$. (this is transitive rule)

- Suppose that a compound proposition u is a tautology and p is a component of u, we replace each occurrence of p in u by a proposition q, then the resulting compound proposition v is also a tautology(This is called a substitution rule).

- Suppose that u is a compound proposition which contains a proposition p. Let q be a proposition such that q $\Leftrightarrow$p , suppose we replace one or more occurrences of p by q and obtain a compound proposition v. Then u $\Leftrightarrow$v (This is also substitution rule)

APPLICATION TO SWITCHING NETWORKS

- If a switch p is open, we assign the symbol o to it and if p is closed we assign the symbol 1 to it.

- Ex: current flows from the terminal A to the terminal B if the switch is closed i.e if p is assigned the symbol 1. This network is represented by the symbol p

A P B

- Ex: parallel network consists of 2 switches p and q in which the current flows from the terminal A to the terminal B , if p or q or both are closed i.e if p or q (or both) are assigned the symbol 1. This network is represent by p$\vee$q

Ex: Series network consists of 2 switches p and q in which the current flows from the terminal A to the terminal B if both of p and q are closed; that is if both p and q are assigned the symbol 1. This network is represented by p$\wedge$q

DUALITY:

Suppose u is a compound proposition that contains the connectives $\wedge$ and $\vee$. Suppose we replace each occurrence of $\wedge$ and $\vee$ in u by $\vee$ and $\wedge$ respectively.

Also if u contains To and Fo as components, suppose we replace each occurrence of To and Fo by Fo and To respectively, then the resulting compound proposition is called the dual of u and is denoted by u^d.

Ex: u: p $\wedge$(q $\vee$ ~r) $\vee$ (s $\wedge$ To) u^d: p $\vee$ (q $\wedge$~ r) $\wedge$ (s $\vee$ Fo)

NOTE:

- $(u^d)^d \Leftrightarrow$u. The dual of the dual of u is logically equivalent to u.

- For any two propositions u and v if u $\Leftrightarrow$v, then $u^d \Leftrightarrow v^d$. This is known as the principle of duality.

The connectives NAND and NOR

$(p \uparrow q) = \sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$

$(p \downarrow q) = \sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$

CONVERSE,INVERSE AND CONTRAPOSITIVE

Consider a conditional $(p\rightarrow q)$, Then :

1) $q\rightarrow p$ is called the converse of $p\rightarrow q$

2) $\sim p\rightarrow\sim q$ is called the inverse of $p\rightarrow q$

3) $\sim q\rightarrow\sim p$ is called the contrapositive of $p\rightarrow q$

RULES OF INFERENCE:

There exist rules of logic which can be employed for establishing the validity of arguments . These rules are called the Rules of Inference.

1) Rule of conjunctive simplification: This rule states that for any two propositions p and q if $p\wedge q$ is true, then p is true i.e $(p\wedge q) \Rightarrow p$.

2) Rule of Disjunctive amplification: This rule states that for any two proposition p and q if p is true then $p\vee q$ is true i.e $p\Rightarrow(p \vee q)$

3) 3) Rule of Syllogism: This rule states that for any three propositions p,q r if $p\rightarrow q$ is true and $q\rightarrow r$ is true then $p\rightarrow r$ is true. i.e $\{(p\rightarrow q)\wedge(q\rightarrow)\} \Rightarrow(p \rightarrow r)$ In tabular form:

$p\rightarrow q$ $q\rightarrow r$ $\therefore (p \rightarrow r)$

4) 4) Modus pones(Rule of Detachment): This rule states that if p is true and $p\rightarrow q$ is true, then q is true, ie $\{p \wedge(p\rightarrow q)\} \Rightarrow q$. Tabular form

p $p\rightarrow q$ $\therefore$ q

5) Modus Tollens: This rule states that if $p\rightarrow q$ is true and q is false, then p is false. $\{(p\rightarrow q)\wedge\sim q\}\Rightarrow q$ Tabular form: $p\rightarrow q$

$\sim q$ $\therefore\sim p$

6) Rule of Disjunctive Syllogism: This rule states that if $p\vee q$ is true and p is false, then q is true i.e. $\{(p\vee q)\wedge\sim p\}\Rightarrow q$ Tabular Form $p\vee q$

$\sim p$ $\therefore$ q

QUANTIFIERS:

1. The words “ALL”,”EVERY”,”SOME”,”THERE EXISTS” are called quantifiers in the proposition

2. The symbol $\forall$ is used to denote the phrases “FOR ALL”,”FOR EVERY”,”FOR EACH” and “FOR ANY”.this is called as universal quantifier.

3. $\exists$ is used to denote the phrases “FOR SOME”and “THERE EXISTS”and “FOR ATLEAST ONE”.this symbol is called existential quantifier.

A proposition involving the universal or the existential quantifier is called a quantified statement

LOGICAL EQUIVALENCE:

1. $\forall$ x,$[p(x)\wedge q(x)]\Leftrightarrow(\forall x\ p(x))\wedge(\forall x,q(x))$

2. $\exists$ x, $[p(x)\vee q(x)]\Leftrightarrow(\exists x\ p(x))\vee(\exists x,q(x))$

3. $\exists$ x, $[p(x)\rightarrow q(x)]\Leftrightarrow\exists x,[\sim p(x)\vee q(x)]$

RULE FOR NEGATION OF A QUANTIFIED STATEMENT:

$\sim\{\forall x,p(x)\}\equiv\exists x\{\sim p(x)\}$ $\sim\{\exists x,p(x)\}\equiv\forall x\{\sim p(x)\}$

RULES OF INTERFERENCE:

1. RULE OF UNIVERSAL SPECIFICATION

2. RULE OF UNIVERSAL GENERALIZATION

If an open statement p(x) is proved to be true for any (arbitrary)x chosen from a set S, then the quantified statement $\forall x€S$, p(x) is true.

METHODS OF PROOF AND DISPROOF:

1.DIRECT PROOF:

The direct method of proving a conditional $p\rightarrow q$ has the following lines of argument:

a) hypothesis : First assume that p is true

b) Analysis: starting with the hypothesis and employing the rules /laws of logic and other known facts , infer that q is true

c) Conclusion:p→q is true.

2. INDIRECT PROOF:

Condition p→q and its contrapositive ~q→~p are logically equivalent. On basis of this proof, we infer that the conditional p→q is true. This method of proving a conditional is called an indirect method of proof.

3.PROOF BY CONTRADICTION

The indirect method of proof is equivalent to what is known as the proof by contradiction. The lines of argument in this method of proof of the statement p→q are as follows:

1) Hypothesis: Assume that p→q is false i.e assume that p is true and q is false.

2)Analysis: starting with the hypothesis that q is false and employing the rules of logic and other known facts , infer that p is false. This contradicts the assumption that p is true

3)Conculsion: because of the contradiction arrived in the analysis , we infer that p→q is true

4.PROOF BY EXHAUSTION:

"∀x *€S*,p(x)" is true if p(x)is true for every (each) x in S.If S consists of only a limited number of elements , we can prove that the statement "∀x *€S*,p(x)" is true by considering p(a) for each a in S and verifying that p(a) is true .such a method of prove is called method of exhaustion.

5.PROOF OF EXISTENCE:

"∃x *€S*,p(x)" is true if any one element a € S such that p(a) is true is exhibited. Hence , the best way of proving a proposition of the form "∃x *€S*,p(x)" is to exhibit the existence of one a€S such that p(a) is true. This method of proof is called proof of existence.

6.DISPROOF BY CONTRADICTION :

Suppose we wish to disprove a conditional p→q. for this propose we start with the hypothesis that p is true and q is true, and end up with a contradiction. In view of the contradiction , we conclude that the conditional p→q is false.this method of disproving p→q is called DISPROOF BY CONTRADICTION

7.DISPROOF BY COUNTER EXAMPLE:

“∀x €S,p(x)” is false if any one element a€S such that p(a) is false is exhibited hence the best way of disproving a proposition involving the universal quantifiers is to exhibit just one case where the proposition is false. This method of disproof is called DISPROOF BY COUNTER EXAMPLE

UNIT – 3 Fundamentals of Logic contd.: 6 Hours

- The Use of Quantifiers
- Quantifiers
- Definitions and
- Proofs of Theorems

Unit 3 6 Hours

Fundamentals of Logic *contd.*:

SYLLABUS

Fundamentals of Logic *contd.*: The Use of Quantifiers, Quantifiers, Definitions and the Proofs of Theorems

Predicates, Quantifiers

Predicates:

A predicate or propositional function is a state- ment containing variables. For instance "x + 2 = 7", "X is American", "x < y", "p is a prime number" are predicates. The truth value of the predicate depends on the value assigned to its variables. For instance if we replace x with 1 in the predicate "x + 2 = 7" we obtain "1 + 2 = 7", which is false, but if we replace it with 5 we get "5 + 2 = 7", which is true. We represent a predicate by a letter followed by the variables enclosed between parenthesis: P (x), Q(x, y), etc. An example for P (x) is a value of x for which P (x) is true. A counterexample is a value of x for which P (x) is false. So, 5 is an example for "x + 2 = 7", while 1 is a counterexample.

Each variable in a predicate is assumed to belong to a universe (or domain) of discourse, for instance in the predicate "n is an odd integer"
'n' represents an integer, so the universe of discourse of n is the set of all integers. In "X is American" we may assume that X is a human being, so in this case the universe of discourse is the set of all human beings.[1]

Quantifiers:

Given a predicate P (x), the statement "for some x, P (x)" (or "there is some x such that p(x)"), represented "∃x P (x)", has a definite truth value, so it is a proposition in the usual sense. For instance if P (x) is "x + 2 = 7" with the integers as

universe of discourse, then ∃x P (x) is true, since there is indeed an integer, namely 5, such that P (5) is a true statement. However, if

Q(x) is "2x = 7" and the universe of discourse is still the integers, then ∃x Q(x) is

false. On the other hand, ∃x Q(x) would be true if we extend the universe of discourse to the rational numbers. The symbol

$\exists$ is called the existential quantifier.

Analogously, the sentence “for all x, P (x)”—also “for any x, P (x)”, “for every x, P (x)”, “for each x, P (x)”—, represented “$\forall x\, P(x)$”, has a definite truth value. For instance, if P (x) is “$x + 2 = 7$” and the universe of discourse is the integers, then $\forall x\, P(x)$ is false. However if Q(x) represents “$(x + 1)^2 = x^2 + 2x + 1$” then $\forall x\, Q(x)$ is true. The symbol $\forall$ is called the universal quantifier.

In predicates with more than one variable it is possible to use several quantifiers at the same time, for instance $\forall x \forall y \exists z\, P(x, y, z)$, meaning “for all x and all y there is some z such that P (x, y, z)”.

Note that in general the existential and universal quantifiers cannot be swapped, i.e., in general $\forall x \exists y\, P(x, y)$ means something different from $\exists y \forall x\, P(x, y)$. For instance if x and y represent human beings and P (x, y) represents “x is a friend of y”, then $\forall x \exists y\, P(x, y)$ means that everybody is a friend of someone, but $\exists y \forall x\, P(x, y)$ means that there is someone such that everybody is his or her friend.

A predicate can be partially quantified, e.g. $\forall x \exists y\, P(x, y, z, t)$. The variables quantified (x and y in the example) are called bound variables, and the rest (z and t in the example) are called free variables. A partially quantified predicate is still a predicate, but depending on fewer variables.

Generalized De Morgan Laws for Logic:

If $\exists x\, P(x)$ is false then there is no value of x for which P (x) is true, or in other words, P (x) is always false. Hence

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

On the other hand, if $\forall x\, P(x)$ is false then it is not true that for every x, P (x) holds, hence for some x, P (x) must be false. Thus:

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

This two rules can be applied in successive steps to find the negation of a more complex quantified statement, for instance:

$\neg\exists x \forall y\, p(x, y) \equiv \forall x \neg\forall y\, P(x, y) \equiv \forall x \exists y\, \neg P(x, y)$.

Exercise : Write formally the statement "for every real number there is a greater real number". Write the negation of that statement.

Answer : The statement is: $\forall x\ \exists y\ (x < y)$ (the universe of discourse is the real numbers). Its negation is: $\exists x\ \forall y\ \neg(x < y)$, i.e., $\exists x\ \forall y\ (x < y)$. (Note that among real numbers $x < y$ is equivalent to $x \geq y$, but formally they are different predicates.)

Proofs

Mathematical Systems, Proofs:

A Mathematical Sys- tem consists of:

1. Axioms: propositions that are assumed true.
2. Definitions : used to create new concepts from old ones.
3. Undefined terms : corresponding to the primitive concepts of the system (for instance in set theory the term "set" is undefined).

A theorem is a proposition that can be proved to be true. An argument that establishes the truth of a proposition is called a proof.

Example: Prove that if $x > 2$ and $y > 3$ then $x + y > 5$.

Answer : Assuming $x > 2$ and $y > 3$ and adding the inequalities term by term we get: $x + y > 2 + 3 = 5$.

That is an example of direct proof. In a direct proof we assume the hypothesis together with axioms and other theorems previously proved and we derive the conclusion from them.

An indirect proof or proof by contrapositive consists of proving the contrapositive of the desired implication, i.e., instead of proving $p \longrightarrow q$ we prove $\neg q \longrightarrow \neg p$.

Example: Prove that if $x + y > 5$ then $x > 2$ or $y > 3$.

Answer: We must prove that $x + y > 5 \longrightarrow (x > 2) \vee (y > 3)$. An indirect proof consists of proving $\neg((x > 2) \vee (y > 3)) \longrightarrow \neg(x + y > 5)$. In fact: $\neg((x > 2) \vee (y > 3))$ is the same as $(x \leq 2) \wedge (y \leq 3)$, so adding both inequalities we get $x + y \leq 5$, which is the same as $\neg(x + y > 5)$.

Proof by Contradiction. In a proof by contradiction or (Reductio ad Absurdum) we assume the hypotheses and the negation of the conclu- sion, and try to derive a contradiction, i.e., a proposition of the form $r \wedge \neg r$.

Example: Prove by contradiction that if $x + y > 5$ then either $x > 2$ or $y > 3$.

Answer: We assume the hypothesis $x + y > 5$. From here we must conclude that $x > 2$ or $y > 3$. Assume to the contrary that "$x > 2$ or $y > 3$" is false, so $x \leq 2$ and $y \leq 3$. Adding those inequalities we get
$x \leq 2 + 3 = 5$, which contradicts the hypothesis $x + y > 5$. From here we conclude that the assumption "$x \leq 2$ and $y \leq 3$" cannot be right, so "$x > 2$ or $y > 3$" must be true.

Remark : Sometimes it is difficult to distinguish between an indirect proof and a proof by contradiction. In an indirect proof we prove an implication of the form $p \longrightarrow q$ by proving the contrapositive $\neg q \longrightarrow \neg p$. In an proof by contradiction we prove an statement s (which may or may not be an implication) by assuming $\neg s$ and deriving a contradiction. In fact proofs by contradiction are more general than indirect proofs.

Exercise: Prove by contradiction that $\sqrt{2}$ is not a rational number, i.e., there are no integers a, b such that $\sqrt{2} = a/b$.

Answer: Assume that $\sqrt{2}$ is rational, i.e., $\sqrt{2} = a/b$, where a and b are integers and the fraction is written in least terms. Squaring both sides we have $2 = a^2/b^2$, hence $2b^2 = a^2$. Since the left hand side is even, then a^2 is even, but this implies that a itself is even, so $a = 2a^!$. Hence: $2b^2 = 4a^{!2}$, and simplifying: $b^2 = 2a^{!2}$. This implies that b^2 is even, so b is even: $b = 2b^!$. Consequently $a/b = 2a^!/2b^! = a^!/b^!$, contradicting the hypothesis that a/b was in least terms.

Arguments, Rules of Inference:

An argument is a se- quence of propositions $p_1, p_2, \ldots, p_n$ called hypotheses (or premises) followed by a proposition q called conclusion. An argument is usually written:

$$\begin{array}{l} p_1 \\ p_2 \\ . \\ p_n \\ \hline \therefore\ q \end{array}$$

or

$p_1, p_2, \ldots, p_n / \therefore\ q$

The argument is called valid if q is true whenever $p_1, p_2, \ldots, p_n$ are true; otherwise it is called invalid.

Rules of inference are certain simple arguments known to be valid and used to make a proof step by step. For instance the following argument is called modus ponens or rule of detachment :

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

In order to check whether it is valid we must examine the following truth table:

p	q	$p \longrightarrow$	p	q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

If we look now at the rows in which both $p \longrightarrow q$ and p are true (just the first row) we see that also q is true, so the argument is valid.

Other rules of inference are the following:

1. *Modus Ponens* or *Rule of Detachment*:

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

2. *Modus Tollens*:

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

3. *Addition*:

$$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$$

4. *Simplification*:

$$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$$

5. *Conjunction*:

$$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$$

6. *Hypothetical Syllogism*:

$$\begin{array}{rl} & p \rightarrow q \\ & q \rightarrow r \\ \hline \therefore & p \rightarrow r \end{array}$$

7. *Disjunctive Syllogism*:

$$\begin{array}{rl} & p \vee q \\ & \neg p \\ \hline \therefore & q \end{array}$$

8. *Resolution*:

$$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$$

Arguments are usually written using three columns. Each row con- tains a label, a statement and the reason that justifies the introduction of that statement in the argument. That justification can be one of the following:

1. The statement is a premise.
2. The statement can be derived from statements occurring earlier in the argument by using a rule of inference.

Example: Consider the following statements: “I take the bus or I walk. If I walk I

get tired. I do not get tired. Therefore I take the bus." We can formalize this by calling B = "I take the bus", W = "I walk" and T = "I get tired". The premises are B $\vee W$, $W \longrightarrow T$ and
$\neg T$, and the conclusion is B. The argument can be described in the following steps:

step	statement	reason
1)	$W \longrightarrow T$	Premise
2)	$\neg T$	Premise
3)	$\neg W$	1,2, Modus Tollens
4)	$B \vee W$	Premise
5)	$\therefore B$	4,3, Disjunctive Syllogism

Rules of Inference for Quantified Statements:

We state the rules for predicates with one variable, but they can be gener- alized to predicates with two or more variables.

1. Universal Instantiation. If $\forall x\, p(x)$ is true, then p(a) is true for each specific element a in the universe of discourse; i.e.:

$\forall x\, p(x)$

$\therefore\ p(a)$

For instance, from $\forall x\,(x + 1 = 1 + x)$ we can derive $7 + 1 = 1 + 7$.

2. Existential Instantiation. If $\exists x\, p(x)$ is true, then p(a) is true for some specific element a in the universe of discourse; i.e.:

$\exists x\, p(x)$

$\therefore\ p(a)$

The difference respect to the previous rule is the restriction in the meaning of a, which now represents some (not any) element of the universe of discourse. So, for instance, from $\exists x\,(x^2 = 2)$ (the universe of discourse is the real numbers) we derive the existence of some element, which we may represent $\pm\sqrt{2}$, such that $(\pm\sqrt{2})^2 = 2$.

3. Universal Generalization. If p(x) is proved to be true for a generic element in the universe of discourse, then $\forall x\, p(x)$ is true; i.e.:

$p(x)$

$\therefore\ \forall x\, p(x)$

By "generic" we mean an element for which we do not make any assumption other than its belonging to the universe of discourse. So, for instance, we can prove $\forall x\,[(x + 1)^2 = x^2 + 2x + 1]$ (say, for real numbers) by assuming that x is a generic real number and using algebra to prove $(x + 1)^2 = x^2 + 2x + 1$.

4. Existential Generalization. If p(a) is true for some specific ele- ment a in the universe of discourse, then ∃x p(x) is true; i.e.:

$$\frac{p(a)}{\therefore\ \exists x\, p(x)}$$

For instance: from 7 + 1 = 8 we can derive ∃x (x + 1 = 8).

Example: Show that a counterexample can be used to disprove a universal statement, i.e., if a is an element in the universe of discourse,
then from ¬p(a) we can derive ¬∀x p(x). Answer: The argument is as follows:

step statement reason

1) ¬p(a)	Premise
2) ∃x ¬p(x)	Existential Generalization
3) ¬∀x p(x)	Negation of Universal Statement

UNIT – 4 Properties of the Integers: 7 Hours

- Mathematical Induction
- The Well Ordering Principle
- Mathematical Induction
- Recursive Definitions

UNIT 4 6 Hours

Properties of the Integers

SYLLABUS

Properties of the Integers: Mathematical Induction, The Well Ordering Principle – Mathematical Induction, Recursive Definitions

MATHEMATICAL INDUCTION:

The method of mathematical induction is based on a principle called the induction principle .

INDUCTION PRINCIPLE:

The induction principle states as follows : let S(n) denote an open statement that involves a positive integer n .suppose that the following conditions hold ;

1. S(1) is true
2. If whenever S(k) is true for some particular , but arbitrarily chosen k €Z^+ , then S(k+1) is true. Then S(n) is true for all n € Z+ . Z+ denotes the set of all positive integers .

METHOD OFMATHEMATICAL INDUCTION

Suppose we wish to prove that a certain statement S(n) is true for all integers n ≥1 , the method of proving such a statement on the basis of the induction principle is calledd the method of mathematical induction. This method consist of the following two steps, respectively called the basis step and the induction step

1) Basis step: verify that the statement S(1) is true ; i.e. verify that S(n) is true for n=1.
2) Induction step: assuming that S(k) is true , where k is an integer≥1, show that S(k+1) is true.

Many properties of positive integers can be proved by mathematical induction.

Principle of Mathematical Induction:

Let P be a prop- erty of positive integers such that:

1. Basis Step: P (1) is true, and

2. Inductive Step: if P (n) is true, then P (n + 1) is true.

Then P (n) is true for all positive integers.

Remark : The premise P (n) in the inductive step is called Induction Hypothesis.

The validity of the Principle of Mathematical Induction is obvious. The basis step states that P (1) is true. Then the inductive step implies that P (2) is also true. By the inductive step again we see that P (3) is true, and so on. Consequently the property is true for all positive integers.

Remark : In the basis step we may replace 1 with some other integer m. Then the conclusion is that the property is true for every integer n greater than or equal to m.

Example: Prove that the sum of the n first odd positive integers is n^2, i.e., 1 + 3 + 5 + ··· + (2n — 1) ‘ n^2.

Answer: Let S(n) ‘ 1 + 3 + 5 + ··· + (2n — 1). We want to prove by induction that for every positive integer n, S(n) ‘ n^2.

1. Basis Step: If n ‘ 1 we have S(1) ‘ 1 ‘ 1^2, so the property is true for 1.
2. Inductive Step: Assume (Induction Hypothesis) that the prop- erty is true for some positive integer n, i.e.: S(n) ‘ n^2. We must prove that it is also true for n + 1, i.e., S(n + 1) ‘ $(n + 1)^2$. In fact:

S(n + 1) ‘ 1 + 3 + 5 + ··· + (2n + 1) ‘ S(n) + 2n + 1 .

But by induction hypothesis, S(n) ‘ n^2, hence:

S(n + 1) ‘ n^2 + 2n + 1 ‘ $(n + 1)^2$.

This completes the induction, and shows that the property is true for all positive integers.

Example: Prove that 2n + 1 ≤ 2^m for n ≥ 3.

Answer : This is an example in which the property is not true for all positive integers but only for integers greater than or equal to 3.

1. Basis Step: If n ‘ 3 we have 2n + 1 ‘ 2 · 3 + 1 ‘ 7 and 2^m ‘ 2^3 ‘ 8, so the property is true in this case.

2. Inductive Step: Assume (Induction Hypothesis) that the prop- erty is true for some positive integer n, i.e.: $2n + 1 \le 2^m$. We must prove that it is also true for n + 1, i.e., $2(n + 1) + 1 \le 2^{m+1}$. By the induction hypothesis we know that $2n \le 2^m$, and we also have that $3 \le 2^m$ if $n \ge 3$, hence

   $$2(n + 1) + 1 \text{ ‘ } 2n + 3 \le 2^m + 2^m \text{ ‘ } 2^{m+1} .$$

This completes the induction, and shows that the property is true for all n ≥ 3.

Exercise: Prove the following identities by induction:

- $1 + 2 + 3 + \cdots + n$ ‘ $\dfrac{n(n+1)}{2}$.
- $1^2 + 2^2 + 3^2 + \cdots + n^2$ ‘ $\dfrac{n(n+1)(2n+1)}{6}$.
- $1^3 + 2^3 + 3^3 + \cdots + n^3$ ‘ $(1 + 2 + 3 + \cdots + n)^2$.

Strong Form of Mathematical Induction:

Let P be a property of positive integers such that:

1. Basis Step: P (1) is true, and

2. Inductive Step: if P (k) is true for all $1 \le k \le n$ then P (n + 1) is true.

Then P (n) is true for all positive integers.

Example: Prove that every integer $n \ge 2$ is prime or a product of primes. Answer :

1. Basis Step: 2 is a prime number, so the property holds for

n ‘ 2.

2. Inductive Step: Assume that if $2 \leq k \leq n$, then k is a prime number or a product of primes. Now, either $n + 1$ is a prime number or it is not. If it is a prime number then it verifies the property. If it is not a prime number, then it can be written as the product of two positive integers, $n + 1$ ‘ $k_1 k_2$, such that $1 < k_1, k_2 < n + 1$. By induction hypothesis each of k_1 and k_2 must be a prime or a product of primes, hence $n + 1$ is a product of primes.

This completes the proof.

The Well-Ordering Principle

Every nonempty set of positive integers has a smallest element.

Example: Prove that $\sqrt{2}$ is irrational (i.e., $\sqrt{2}$ cannot be written as a quotient of two positive integers) using the well-ordering principle.

Answer: Assume that $\sqrt{2}$ is rational, i.e., $\sqrt{2}$ ‘ a/b, where a and b are integers. Note that since $\sqrt{2} > 1$ then $a > b$. Now we have 2 ‘ a^2/b^2, hence $2b^2$ ‘ a^2. Since the left hand side is even, then a^2 is even, but this implies that a itself is even, so a ‘ $2a^!$. Hence: $2b^2$ ‘ $4a^{!2}$, and simplifying: b^2 ‘ $2a^{!2}$. From here we see that $\sqrt{2}$ ‘ $b/a^!$.

Hence starting with a fractional representation of $\sqrt{2}$ ‘ a/b we end up with another fractional representation $\sqrt{2}$ ‘ $b/a^!$ with a smaller numerator $b < a$. Repeating the same argument with the fraction $b/a^!$ we get another fraction with an even smaller numerator, and so on. So the set of possible numerators of a fraction representing $\sqrt{2}$ cannot have a smallest element, contradicting the well-ordering principle. Consequently, our assumption that $\sqrt{2}$ is rational has to be false.

Reccurence relations

Here we look at recursive definitions under a different point of view. Rather than definitions they will be considered as equations that we must solve. The point is that a recursive definition is actually a def- inition when there is one and only one object satisfying it, i.e., when the equations involved in that definition have a unique solution. Also, the solution to those equations may provide a closed-form (explicit) formula for the object defined.

The recursive step in a recursive definition is also called a recurrence relation. We will focus on kth-order linear recurrence relations, which are of the form

$C_0\, x_m + C_1\, x_{m-1} + C_2\, x_{m-2} + \cdots + C_k\, x_{m-k}$ ‘ b_m ,

where C_0 ‘ O. If b_m ‘ O the recurrence relation is called homogeneous. Otherwise it is called non-homogeneous.

The basis of the recursive definition is also called initial conditions of the recurrence. So, for instance, in the recursive definition of the Fibonacci sequence, the recurrence is

F_m ‘ $F_{m-1} + F_{m-2}$

or

$F_m - F_{m-1} - F_{m-2}$ ‘ O ,

and the initial conditions are

F_0 ‘ O, F_1 ‘ 1 .

One way to solve some recurrence relations is by iteration, i.e., by using the recurrence repeatedly until obtaining a explicit close-form formula. For instance consider the following recurrence relation:

x_m ‘ $r\, x_{m-1}$ (n > O) ; x_0 ‘ A .

By using the recurrence repeatedly we get:

x_m ‘ $r\, x_{m-1}$ ‘ $r^2\, x_{m-2}$ $r^3\, x_{m-3}$ ‘ $\cdots$ ‘ $r^m\, x_0$ ‘ $A\, r^m$,

hence the solution is x_m ‘ $A\, r^m$.

In the following we assume that the coefficients $C_0, C_1, \ldots, C_k$ are constant.

First Order Recurrence Relations. The homogeneous case can be written in the following way:

x_n ‘ $r\, x_{n-1}$ (n > O) ; x_0 ‘ A .

Its general solution is

x_n ‘ $A\,r^n$,

which is a geometric sequence with ratio r.

The non-homogeneous case can be written in the following way:

x_n ‘ $r\,x_{n-1} + c_n$ (n > O) ; x_0 ‘ A .

Using the summation notation, its solution can be expressed like this:

$$x_n \text{ ‘ } A\,r^n + \underset{k=1}{\overset{n}{X}} c_k\, r^{n-k} .$$

We examine two particular cases. The first one is

x_n ‘ $r\,x_{n-1} + c$ (n > O); x_0 ‘ A .

where c is a constant. The solution is

$$x_n \text{ ‘ } A\,r^n + c \underset{k=1}{\overset{n}{X}} r^{n-k} \text{ ‘ } A\,r^n + c\,\frac{r^n - 1}{r - 1} \qquad \text{if } r \text{ ‘ } 1 ,$$

and

$$x_n \text{ ‘ } A + c\,n \qquad \text{if } r \text{ ‘ } 1 .$$

Example : Assume that a country with currently 1OO million people has a population growth rate (birth rate minus death rate) of 1% per year, and it also receives 1OO thousand immigrants per year (which are quickly assimilated and reproduce at the same rate as the native population). Find its population in 1O years from now. (Assume that all the immigrants arrive in a single batch at the end of the year.)

Answer: If we call x_n ‘ population in year n from now, we have:

x_n ‘ 1.O1 x_{n-1} + 1OO, OOO (n > O); x_0 ‘ 1OO, OOO, OOO .

This is the equation above with r ‘ 1.O1, c ‘ 1OO, OOO and A ‘ 1OO, OOO, OO, hence:

$$x_n \text{ ‘ } 1OO,\ OOO,\ OOO \cdot 1.O1^n + 1OO, OOO\ \frac{1.O1^n - 1}{1.O1 - 1}$$

‘ 1OO, OOO, OOO $\cdot$ $1.O1^n$ + 1OOO $(1.O1^n - 1)$.

So:

462, 317

.

The second particular case is for $\mathbf{r} = 1$ and $c_m = c + d\,n$, where c and d are constant (so c_m is an arithmetic sequence):

$$x_m = x_{m-1} + c + d\,n \qquad (n > 0)\,; \qquad x_0 = A\,.$$

The solution is now

$$x_m = A + \sum_{k=1}^{m} (c + d\,k) = A + c\,n + \frac{d\,n\,(n+1)}{2}\,.$$

Second Order Recurrence Relations. Now we look at the recurrence relation

$$C_0\,x_m + C_1\,x_{m-1} + C_2\,x_{m-2} = 0\,.$$

First we will look for solutions of the form $x_m = c\,\mathbf{r}^m$. By plugging in the equation we get:

$$C_0\,c\,\mathbf{r}^m + C_1\,c\,\mathbf{r}^{m-1} + C_2\,c\,\mathbf{r}^{m-2} = 0\,,$$

hence $\mathbf{r}$ must be a solution of the following equation, called the characteristic equation of the recurrence:

$$C_0\,\mathbf{r}^2 + C_1\,\mathbf{r} + C_2 = 0\,.$$

Let $\mathbf{r}_1$, r_2 be the two (in general complex) roots of the above equation. They are called characteristic roots. We distinguish three cases:

1. Distinct Real Roots. In this case the general solution of the recurrence relation is

$$x_m = c_1\,\mathbf{r}_1^m + c_2\,\mathbf{r}_2^m\,,$$

where c_1, c_2 are arbitrary constants.

2. Double Real Root. If $r_1 = r_2 = r$, the general solution of the recurrence relation is

$$x_m \text{ ‘ } c_1 \mathbf{r}^m + c_2 n \mathbf{r}^m ,$$

where c_1, c_2 are arbitrary constants.

3. Complex Roots. In this case the solution could be expressed in the same way as in the case of distinct real roots, but in order to avoid the use of complex numbers we write $r_i — \mathbf{r}\, e^{\alpha i}$, $r_2 — \mathbf{r}\, e^{—\alpha i}$, $k_i — c_i + c_2$, $k_2 — (c_i — c_2)\, i$, which yields:[i]

$$x_m — k_i \mathbf{r}^m \cos n\alpha + k_2 \mathbf{r}^m \sin n\alpha .$$

Example: Find a closed-form formula for the Fibonacci sequence defined by:

$$F_{m+i} — F_m + F_{m—i} \quad (n > 0) ; \qquad F_0 — 0,\ F_i — 1 .$$

Answer: The recurrence relation can be written

$$F_m — F_{m—i} — F_{m—2} — 0 .$$

The characteristic equation is

$$\mathbf{r}^2 — \mathbf{r} — 1 — 0 .$$

Its roots are:[2]

$$r_i — \varphi — \frac{1+\sqrt{5}}{2} ; \qquad r_2 — —\varphi^{—i} — \frac{1 - \sqrt{5}}{2} .$$

They are distinct real roots, so the general solution for the recurrence is:

$$F_m — c_i \varphi^m + c_2 (—\varphi^{—i})^m .$$

Using the initial conditions we get the value of the constants:

$$\big(\; (n — 0) \quad c_i + c_2 \quad — \; 0 \qquad c_i \; — \; 1/\sqrt{5}$$

$$\sqrt{\_}$$

RECURSIVE DEFINITIONS:

RECURRENCE RELATIONS:- The important methods to express the recurrance formula in explict form are

1) BACKTRACKING METHOD
2) CHARACTERISTIC EQUATION METHOD

BACKTRACKING METHOD:

This is suitable method for linear non-homogenous recurrence relation of the type

$x_n= r\ x_{n-1} +s$

The general method to find explicit formula

$xn = r^{n-1}\ x_1 + s(r^{n-1}-1)/\ (r-1)$ where $r\neq 1$ is the general explicit

CHARACTERISTIC EQUATION METHOD:

This is suitable method to find an explicit formula for a linear homogenous recurrance relation

LINEAR HOMOGENOUS RELATION :

A recurrence relation of the type $a_n = r_1\ a_{n-1} +r_2\ a_{n-2}+\ldots\ldots.+ r_k\ a_{n-k}$ where r_i 's' are constants is a linear homogenous recurrence relation (LHRR) of degree k

1) A relation $c_n = -2\ c_{n-1}$ is a LHRR of degree 1 .
2) A relation $x_n = 4\ x_{n-1} + 5$ is a linear non HRR because 2nd term in RHS is a constant . It doesn't contain x_{n-2} factor .
3) A relation $x_n = x_{n-1} +2x_{n-2}$ is a LHRR of degree 2
4) A relation $x_n = x^2_{n-1} + x_{n-2}$ is a non linear , non HRR because the 1st term in RHS is a second degree term.

CHARACTERISTIC EQUATION:

$a_n = r_1\ a_{n-1} + r_2\ a_{n-2}+\ldots..+ r_k\ a_{n-k}$..(1) is a LHRR of degree K .

$x^k = r_1\ x^{k-1} + r_2\ x^{k-2}+\ldots.+r_k$ is called characteristic equation.

- Let $a_n = r_1\ a_{n-1} + r_2\ a_{n-2}$ be LHRR of degree 2. its characteristic equation is $x^2 = r_1\ x + r_2$ or $x^2 - r_1\ x- r_2=0$. if the characteristic equation has 2 distinct roots e_1 , e_2 then the explicit formula of the recurrence relation in $a_n= u\ e^n{}_1 + v\ e^n{}_2$ where u and v depends on the initial values.
- Let $a_n = r_1\ a_{n-1} + r_2\ a_{n-2}$ be a LHRR of degree 2 . Its characteristic equation is $x^2 - r_1\ x - r_2 =0$ if the characteristic equation has repeated roots e, then the explicit formula is $a_n =u\ e^n + v\ n\ e^n$ where u and v depends on the initial values.

PART – B

UNIT – 5 Relations and Functions: 7 Hours

- Cartesian Products and Relations
- Functions
- Plain and One-to-One
- Onto Functions
- Stirling Numbers of the Second Kind
- Special Functions
- The Pigeon-hole Principle
- Function Composition and
- Inverse Functions

UNIT 5 7 Hours

Relations

SYLLABUS

Relations and Functions: Cartesian Products and Relations, Functions – Plain and One-to-One, Onto Functions – Stirling Numbers of the Second Kind, Special Functions, The Pigeon-hole Principle, Function Composition and Inverse Functions

Introduction

Product set: If A and B are any 2 non-empty sets then the product set of A and B are the Cartesian product or product of A and B.

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

$$A \times B \neq B \times A$$

Example: (a) Let, A = {1, 2, 3} B = {a, b}

Then, A X B = {(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)}

B X A = {(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)}

$A \times B \neq B \times A$

(b) Let, A = {1, 2} B = {a, b} C={x, y}

B X C = {(a, x), (a, y), (b, x), (b, y)}

A X (B X C) = {(1, (a, x)), (1, (a, y)), (1, (b, x)), (1, (b, y)),
(2, (a, x)) (2, (a, y)), (2, (b, x)), (2, (b, y))}

A X B = {(1, a), (1, b), (2, a), (2, b)}

(A X B) X C = {((1, a), x), ((1, a), y), ((1, b), x), ((1, b), y),
((2, a), x), ((2, a), y), ((2, b),x),((2,b),y),}

*Remarks:

a. A X (B X C) = (A X B) X C

b. A X A = A^2

c. If R is the set of all real numbers then R x R = R^2, set of all points in plane.

d. (a, b) = (c, d) if a = c and b = d

Partition set: Let 'A' be a non-empty set. A partition of 'A' or quotient set of 'A' is a collection P of subsets of

'A' such that.

(a) Every element of A belongs to some set in P

(b) If A_1 and A_2 are any two distinct members of P, then A_1 n A_2 = ϕ.

(c) The members of P are called 'blocks' or 'cells'.

Example:

Let,

A = {1, 2, 3, 4, 5} then,

P_1 = {{1, 2, 3}, {4}, {5}}

P_2 = {{1, 5}, {4, 3}, {2}}

P_3 = {{1}, {2}, {3}, {4}, {5}}

Relations: Let A and B be any two non-empty sets. A relation R from a set A to the set B is a subset of A x B.

If (a, b) Є R then we write a R b, otherwise we write a ~~R~~ b (ie. a not related to b).

Example:

Let,

A = {1, 2, 3, 4, 5}, Let R be a relation on A defined as a R b if a<b. R = {(1, 2), (1, 3), (1, 4), (1, 5) (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)}

=> R ⊆ A X A.

Domain of R: Dom (R) = {1, 2, 3, 4} ⊆ A

Range of R: Ran (R) = {2, 3, 4, 5} ⊆ B

Dom (R) = {x ЄA / x R y for some x Є A}

Ran (R) = {y Є B / x R y for some y Є B}

R - Relative set: If R is a relation from A to B and if x ЄA then the R relative set of x is defined as

$$R(x) = \{y \in B / x \ R \ y\}$$

If $A_1 \subseteq A$ then the R relative set of A_1 is defined as,

$$R(A_1) = \{y \in B / x \ R \ y \text{ for some } x \in A_1\}$$

$$= \cup R(x) \text{ for } x \in A_1$$

Example:

Let,

$A = \{a, b, c, d\}$

$R = \{(a, a), (a, b), (b, c), (c, a)\ (c, b)\ (d, a)\}$

$R(a) = \{a, b\}$

$R(b) = \{c\}$

$R(c) = \{a, b\}$

$R(d) = \{a\}$

Let,

$A_1 = \{a, c\}$ be a subset of A,

Then, $R(A_1) = R(a) \cup R(c)$

$= \{a, b\} \cup \{a, b\}$

$= \{a, b\}$

Matrix of a relation / Relation Matrix: Let $A = \{a_1, a_2, a_3 \ldots\ldots\ldots a_m\}$ and $B = \{b_1, b_2, b_3 \ldots b_n\}$ be any two finite sets.

Let R be relation from A to B then the matrix of the relation R is defined as the m x n matrix,

$$M_R = [M_{ij}]$$

Where $M_{ij} = 1$, if $(a_i, b_j) \in R$

$= 0$, if $(a_i, b_j) \notin R$

Example:

(a)Let,

A = {1, 2, 3} and B = {x, 4}

R = {(1, x) (1, 4), (2, 4) (3, x)}

Thus, $M_r = \begin{bmatrix}10\\01\\10\end{bmatrix}$

(b) Given $M_R = \begin{bmatrix}1001\\0110\\1010\end{bmatrix}$. Find Relation R.

Define set,

A = {a_1, a_2, a_3} and

B = {b_1, b_2, b_3, b_4}

R = {(a_1, b_2) (a_1, b_4) (a_2, b_2) (a_2, b_3) (a_3, b_1) (a_3, b_3)}

Digraph of a relation: Let A be a finite set and R be a relation on A. Then R can be represented pictorially as follows,

(a)Draw a small circle for each element of A and label the circles with the corresponding element of A. These circles are called "Vertices".

(b)Draw an arrow from a_i to a_j if a_i R a_j. These arrows are called "edges".

(c)The resulting picture representing the relation R is called the "directed graph of R" or "digraph of R".

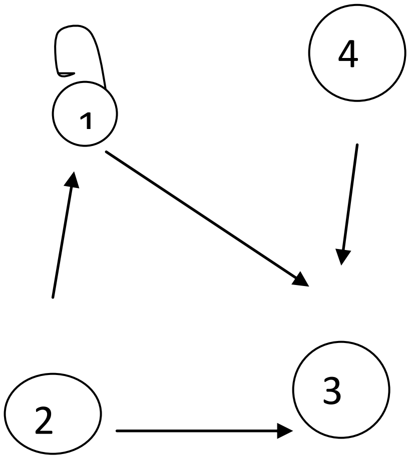
Example:

(a)Let, A be equal to the set

A = {1, 2, 3, 4}

R = {(1, 1), (1, 3), (2, 1), (2, 3), (3, 2), (4, 3)}

Diagram:



The "indegree" of a ЄA is the number of elements b Є A such that b R a.

The "outdegree" of a Є A is the number of elements b Є A such that a R b

Elements	Indegree	Outdegree
1	2	2
2	1	2
3	3	1
4	0	1

(b) If A = {1, 2, 3, 4} and B = {1, 4, 6, 8, 9} and R: A $\rightarrow$B defined by

a R b if b = a^2.Find the domain, Range, and M_R

A = {1, 2, 3, 4} B = {1, 4, 6, 8, 9}

R = {(x, y)/x A, y B and y = X^2}

R = {(1, 1), (2, 4), (3, 9)}

Domain: Dom (R) = {1, 2, 3}

Range: Ran (R) = {1, 4, 9}

$$M_r = \begin{bmatrix} 10000 \\ 01000 \\ 00001 \\ 00000 \end{bmatrix}$$

<u>Properties of a relation:</u>

1. **Reflexive:** Let R be a relation on a set A.

The "R is reflexive" if (a, a) Є R ∀ a ЄA or a R a, ∀ a Є A.

<u>Example:</u> A = {I, 2, 3}

R = {(1, 1), (2, 2) (1, 2), (3, 2) (3, 3)}

Therefore, R is reflexive.

A relation R on a set A is "non-reflexive" if ‘a’ is not relation to ‘a’ for some a ЄA or (a, a) ∉R for some a Є A

A = {1, 2, 3}

R = {(1, 1), (2, 1), (3, 2), (3, 3)} => (2, 2) ∉R

Therefore, R is *not-reflexive.*

2. **Irreflexive**: A relation R on a set A is irreflexive if a R a, ∀ a Є A.

<u>Example:</u> R = {(1, 2) (2, 1) (3, 2) (3, 1)}

(1, 1), (2, 2) (3, 3) ∉R hence R is irreflexive.

A relation R on a set A is “not irreflexive” if ‘a’ is not Relation to ‘a’ for some a Є A.

<u>Example:</u> R= {(1, 1) (1, 2) (2, 1) (3, 2) (3, 1)}

(1, 1) Є R hence R is “not irreflexive”.

3. **Symmetric Relation:** Let R be a relation on a set A, then R is “symmetric” if whenever a R b, then b R a; ∀ a Є A, b Є A.

<u>Example:</u> Let A = {1, 2, 3} and R = {(1, 1) (1, 2) (2, 1) (3, 2) (2, 3)}

Therefore, R is symmetric.

A relation R on a set A is said to be "not symmetric" if a R b and b ~~R~~ a for some a, b Є A.

Example: A = {1, 2, 3} and R = {(1, 2) (3, 2) (1, 3) (2, 1) (2, 3)}

Therefore, R is not symmetric.

4. **Asymmetric:** Let R be a relation on a set A then R is "Asymmetric", if whenever a R b then b R a, Ɐ a, b Є A.

R = {(1, 2), (1, 3) (3, 2)}

Therefore, R is asymmetric.

A relation R on a set A is said to be "not Asymmetric" if a R b and b R a for some a, b ЄA   R = {(1, 1) (1, 2) (1, 3) (3, 2)}

R is not symmetric.

5. **Anti – symmetric:** Let R be a relation on a set A, then R is anti symmetric if whenever a R b and b R a then a = b (for some a, b Є A)

Example: Let, A = {1, 2, 3} and R = {(1, 1), (1, 2), (3, 2)}

R is anti-symmetric Є 1R1 and 1 = 1.

Example: R = {(1, 2) (2, 1)}

1R2, 2R1 but 2 = 1 hence R is not anti symmetric.

6. **Transitive Property:** Let R be a relation on a set A, then R is transitive if whenever a R b and b R c, then a R c Ɐ a, b, c Є , A.

Example: Let, A = {1, 2, 3} and R = {(1, 1), (1, 3), (2, 3), (3, 1) (2, 1), (3, 3)} (all should satisfy)

Equivalence relation: A Relation R is said to be an equivalence relation if it is,

(a) Reflexive

(b) Symmetric and

(c) Transitive.

Therefore, R is an equivalence Relation.

Symmetric: Let a R b

=> Є 1R2

2 is not Related to 1 and also b is not Related to a

Hence, R is not symmetric

Transitive: Let a R b and b R c

=> 1 R 2 and 2 R 3 but, 1 is not Related to 3 and also a is not Related to c

Hence, R is not transitive.

Therefore, R is not an equivalence Relation.

b. R = {(1, 2), (2, 1) (1, 3) (3, 1) (2, 3) (3, 2)}

Reflexive: a R a Ɐ a Є A

=> 1 R1, 2 R 2, 3 R 3 not true,

Hence, R is not reflexive

Symmetric: Let a R b

=> 1 R 3

=> 3 R 1

=> b R a

Hence, R is symmetric.

Transitive: Let a R b and b R c

=> 1 R 2 and 2 R 3

=> 1 R 3

=> a R c

Hence, R is transitive

Therefore, R is not an equivalence Relation.

c. A = {1, 2, 3}

R = A x A = {(1, 1)(1, 2)(1, 3)(2, 1)(2, 2)(2, 3)(3, 1)(3, 2)(3, 3)}

It is reflexive, symmetric and transitive and hence R is an equivalence Relation.

Theorem: "Let R be an equivalence relation on a set A, and P be the collection of all distinct R - relative set of A. Then P is a partition of A, and R is the equivalence relation determined by P"

OR

"Show that an equivalence relation R in a set S which is non-empty, determine a partition of S"

Proof: Given, P = {R (a) / Ɐ a Є A}

We know that Ɐ a Є A, we have, a R a

=> (a, a) Є R

=> a Є R (a)

Therefore, for every element of A belongs to one of the sets of P.

If R (a) and R (b) are 2 distinct relative sets R(a) n R(b) = Φ

If possible, let x Є R (a) n R (b)

=>x Є R (a) and x Є R (b)

=>a R x and b R x

=>a R x and x R b (since R is symmetric)

=>a R b (since R is transitive)

=>R (a) = R (b) (by theorem)

Therefore, If R (a) = R (b), then R (a) n R (b) = Φ.

Therefore, from the above, P is a partition of the set A.

This partition determines the relation R in the sense that a R b if a and b belong to the same block of the partition.

Hence proved…..

<u>*NOTE:</u> The partition of a set A determined by an equivalence relation R is called the partition induced by R and is denoted by A/R.

<u>Manipulation of relations:</u>

1. **Complement:** Let R be a relation from A to B. The complement of R is a relation defined as a R b if a $R^{\sim}$ b, where $R^{\sim}$ is the complement of R.

=> (a, b) $R^{\sim}$ if (a, b) $R^{\sim}$

2. **Union:** Let R and S be 2 relations from A to B. The union R U S is a relation from A to B defined as,

a (R U S) b if either a R b or a S b

That is (a, b) Є R U S if either (a, b) Є R or (a, b) Є S.

3. **Intersection:** Let Rand S be relations from A to B. The intersection R n S is a relation from A to B defined as,

a (R n S) b if a R b and a S b

That is (a, b) Є R n S if (a, b) Є R and (a, b) Є S.

4. **Inverse:** Let R be a relation from A to B. The inverse R^{-1} is a relation from B to A defined as, a R b if b R^{-1} a

i.e., (a, b) Є R if (b, a) Є R^{-1}

<u>Composition of relations:</u> Let Rand S be relations from A to Band B to C respectively. The composition of Rand S is the

relation S o R from A to C defined as,

a(S o R) c if there-exist b E B/a R b and b S c.

R^2 =R o R = {(a, a), (a, c) (a, b) (b, a) (b, c) (b, b) (c, a) (c, b) (c, c)}

S^2 = S o S = {(a, a) (b, b) (b, c) (b, a) (c, a) (c, c)}

<u>Reflexive closure:</u> Let R be a relation on a set' A'. Suppose R lacks a particular property, the smallest relation that contain R and which, processes the desired property is called the closure of R with respective a property in question.

Given a relation R on a set' A' the relation R1 =∆(A U R) is the "reflexive closure of R".

<u>Example:</u>

A = {1, 2, 3}

R = {(1, 1)(1,2)(2, 1)(1,3)(3, 2)} find the reflexive closure of R.

Solution: We know that, R is not reflexive because (2, 2) Є Rand (3, 3) Є R.

Now, A= {(1, 1) (2, 2) (3, 3)}

Therefore, R_1 = R U A= {(1, 1) (1, 2) (2, 1) (2, 2) (1, 3) (3, 2) (3, 3)}

R_1 is the reflexive closure of R.

Symmetric closure : If R is not symmetric then there exists (x, y) A such that (x, y) Є R, but (y, x) Є R. To make R symmetric we need to add the ordered pairs of R^{-1}.

R_1 = R U R^{-1} is the "symmetric closure of R".

A = {1, 2, 3}

R = {(1, 1) (1, 2) (2, 1) (1, 3) (3, 2)} find the symmetric closure of R.

Solution: We know that, R is not symmetric because (1, 3) Є R but (3, 1) Є R and (3, 2) Є R but (2, 3) Є R.

Example: R^{-1} = {(1, 1) (2, 1) (1, 2) (3, 1) (2, 3)}

Therefore, R_1 = R U R^{-l} = {(1, 1) (1, 2) (2, 1) (1, 3) (3, 1) (3, 2) (2, 3)}

R_1 is called the symmetric closure of R.

Transitive closure: Let R be a relation on a set A the smallest transition relation containing R is called the "Transitive closure of R".

UNIT – 6 Relations contd.: 7 Hours

- Properties of Relations
- Computer Recognition
- Zero-One Matrices
- Directed Graphs
- Partial Orders
- Hasse Diagrams
- Equivalence Relations and
- Partitions

UNIT 6 7 Hours

Functions

SYLLABUS

Relations *contd.*: Properties of Relations, Computer Recognition – Zero-One Matrices and Directed Graphs, Partial Orders – Hasse Diagrams, Equivalence Relations and Partitions

Introduction

A person counting students present in a class assigns a number to each student under consideration. In this case a correspondence between two sets is established: between students understand whole numbers. Such correspondence is called functions. Functions are central to the study of physics and enumeration, but they occur in many other situations as well. For instance, the correspondence between the data stored in computer memory and the standard symbols a, b, c... z, 0, 1,...9,?,!, +... into strings of O's and I's for digital processing and the subsequent decoding of the strings obtained: these are functions. Thus, to understand the general use of functions, we must study their properties in the general terms of set theory, which is will be we do in this chapter.

Definition: Let A and B be two sets. A function f from A to B is a rule that assigned to each element x in A exactly one element y in B. It is denoted by

f: $A \rightarrow B$

Note:

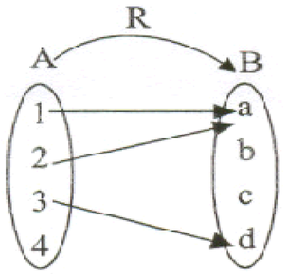
1. The set A is called domain of f.
2. The set B is called domain of f.

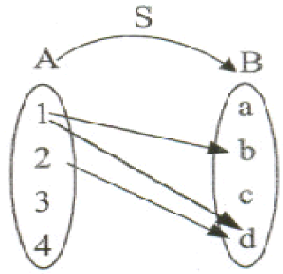
Value of f: If x is an element of A and y is an element of B assigned to x, written y = f(x) and call function value of f at x. The element y is called the image of x under f.

Example: A = {1, 2, 3, 4} and B= {a, b, c, d}

R = {(1, a), (2, b), (3, c), {4, d)}

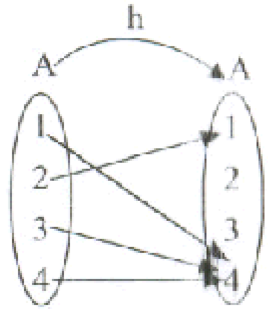
S = {(I, b), (I, d), (2, d)}





Therefore, R is a function and S is not a function. Since the element 1has two images band d, S is not a function.

Example: Let A = {1, 2, 3, 4} determine whether or not the following relations on A are functions.



1. f= {(2, 3), (1, 4), (2, 1), (312), (4, 4)}

(Since element 2 has 2 images 3 and 1, f is not a function.)

2. g={(3,1),(4,2),(1,1)}

g is a function

3. h={(2,1),(3,4),(1,4),(2,1),(4,4)}

h is a function

4. Let A= {0, ±1, ±2, 3}. Consider the function F: A→ R, where R is the set of all real numbers, defined by $f(x) = x^3 - 2x^2 + 3x + 1$ for $x \in A$. Find the range of f.

f (0) =1

f (1) =1-2+3+1=3

f (-1) =-1-2-3+1=-5

f (2) =8-8-6+1=7

f (-2) =-8-8-6+1= -21

f (3) =27-18+9+1=19

∴ Range = {1, 3,-5, 7,-21, 19}

5. If A= {0, ±1, ±2} and f: A→ R is defined by f(x) =x^2-x+1, x∈A find the range.

f (0) =1

f (1) =1-1+1=1

f (-1) =1+1+1=3

f (2) =4-2+1=3

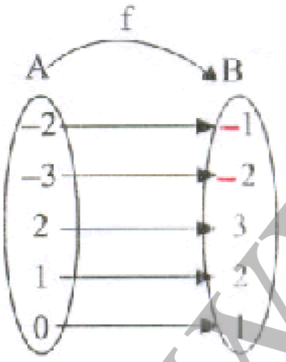
f (-2) =4+2+1=7

∴ Range = {1, 3, 7}

Types of functions:

1. ***Everywhere defined* -2**

   A function f: A ~ B is everywhere defined if domain of f equal to A (dom f = A)



   Example: Y =f(x) =x+1

   Here, dom f=A

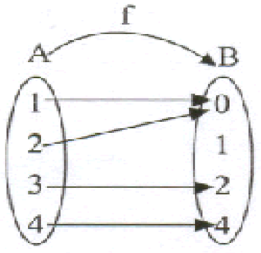
2. ***Onto or surjection function***

A function f: A → B is onto or surjection if Range of f = B. In other words, a function f is surjection or onto if for any value *l in* B, there is at least one element x in A for which f(x) = y.

3. *Many to one function*

A function F is said to be a many-to-one function if a *:f*= b, f(a) = f(b), where (a, b) E A.

Example:



Here, *1: f*=2 but f (1) = f (2), where 1,2 E A

4. One-to-one function or injection

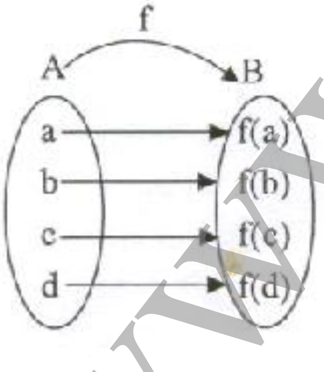
A function f: A → B is one-to-one or injection if (a) =f (b) then a = b, where a, b E A.

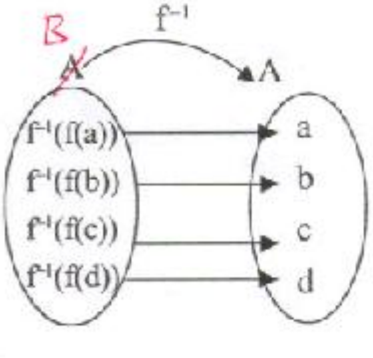
In other words if a*: f*=b then f (a): f= f (b).

5. *Bijection function*

A function f: A → B is Bijection if it is both onto and one-to-one.

6. Invertible function

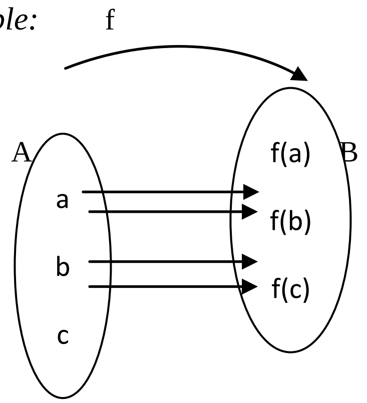


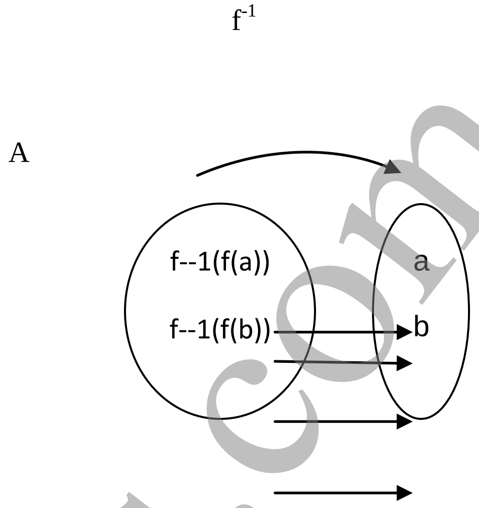


A function f: A ---+ B is said to be an invertible function if its inverse relation, f-I is a function from B → A.

If f: A → B is Bijection, then [-I: B ---+A exists, f is said to be invertible.

Example:





Here f: A → B f^{-1} B → A

A = $\{a_1, a_2, a_3\}$ B = $\{b_1, b_2, b_3\}$ C = $\{ c_1, c_2\}$ D = $\{d_1, d_2, d_3, d_4\}$

Let f_1: A → B, f_2: A → D, f_3: B → C, f4: D → B be functions defined as follows,

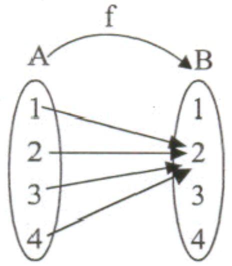
1. f1 = {(a1, b2) (a2, b3) (a3 ,b1)}
2. $f_2 = \{(a_1, d_2) (a_2, d_1) (a_3 , d_4)\}$
3. $f_3 = \{(b_1, c_2)(b_2, c_2) (b_3, c_1)\}$
4. $f_4 = \{ (d_1, b_1) (d_2, b_2) (d_3,b_1)\}$

Identity function

A function f: A~ A such that f (a) = a, 'if a Є A is called the identity function or identity mapping on A. Dom (t) = Ran (t) = A

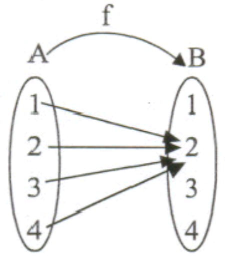
Constant function

A function f: A → B such that f (a) =c, ∀a∈ dom (f) where c is a fixed element of B, is called a constant function.



Into function

A function f: A → B is said to be an into function if there exist some b in B which is not the image of any a in A under f.



3 is not the image of any element.

One-to-one correspondence

If f: A → B is everywhere defined and is Bijective, then corresponding to every a∈A there is an unique b∈B such that b=f(a) and corresponding to every b∈B there is an unique a∈A such that f(a)=b. for this reason a everywhere defined bijection function from A → B is called as one-one correspondence from A → B

Composition of function

Let f: A (B and g: B (C is any 2 functions, and then the composition of f and g is a function g o f: A (C defined as, g of (a) =g [f (a)] (C, (a (dom f).

Inverse function

Consider a function f: A (B. Then f is a relation from A to B with Dom (f) (A and Ran (f) (B. Its inverse, f -1, is a relation from B to A which is such that if whenever (a, b) (f then (b, a) (f -1)

Also, Dom (f -1) = Ran (f)

Ran (f -1) =Dom (f) and

(f -1) -1 = f

Definition

A function f: A (B is invertible if it is inverse relation f -1 is a function from B to A. Then, f -1 is called the inverse function of f.

Ex: let A = {a, b, c, d} and B = {e, f, g, h} and f: A (B be a function defined by

f (a) = =e, f (b) = e, f (c) = h, f (d) = g

Then, as a relation from A to B, f reads

f = {(a, e), (b, e), (c, h), (d, g)}

And f^{-1} is a relation from B to A, given by

f^{-1} = {(e, a), (e, b), (h, c), (g, d)}

Now, Dom (f^{-1}) = [e, h, g} = Ran(f) and

Ran (f^{-1}) = {a, b, c, d} = A = Dom (f)

Also, $(f^{-1})^{-1}$ = f

Although f^{-1} is a relation from B to A, it is not function from B to A, because e is related to two elements ‘a’ and ‘b’ under f -1.

Let A = {1,2,3,4} and B = {5,6,7,8} and the function f: A (B defined by

f (1) = 6, f(2) = =8, f(3) = 5, f(4) = 7

Then, f = {(1, 6), (2, 8), (3, 5), (4, 7)}

∴ f -1 = {(6 , 1), (8 , 2), (3 , 5), (7 , 4)}
In this case, f -1 is not only a relation from B to A but a function as well.

Characteristic function

Introduction

Characteristic function is a special type of function. It is very useful in the field of computer science. Through this function one can tell whether an element present in the set or not. If the function has the value 1 then the particular element belongs to the set and if it has value 0 then the element is not present in the set.

Definition

Associated with the subset a of $\cup$ we can define a characteristic function of A over $\cup$ as f: $\cup \rightarrow \{0, 1\}$ where

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Properties of the characteristics function

1. $f_{\mathbf{A\ n\ B}}(x) = f_{\mathbf{A}}(x).\ f_{\mathbf{B}}(x)$

Proof:

i. if $x \in AnB$ then $x \in A$ and $x \in B$

$\Rightarrow f_A(x) = 1$ and $f_{B\,(}x) =1$

$\therefore \quad f_{AnB}(x) = 1 = f_{\mathbf{A}}(x).\ f_{\mathbf{B}}(x)$

ii. if $x \notin AnB$ then $f_{AnB}(x) = 0$. but if $x \notin AnB$ then $x \notin A$ and $x \notin B$

$\Rightarrow f_A(x) = 0$ and $f_{B\,(}x) =0$

$\therefore \quad f_{AnB}(x) = 0 = f_{\mathbf{A}}(x).\ f_{\mathbf{B}}(x)$

$\therefore$ From case 1 and 2

$f_{AnB}(x) = f_{\mathbf{A}}(x).\ f_{\mathbf{B}}(x)$

2. $f_{\mathbf{AUB}}(x) = f_{\mathbf{A}}(x) + f_{\mathbf{B}}(x) - f_{\mathbf{A}}(x).\ f_{\mathbf{B}}(x)$

Proof:

i. Let $x \in AUB$ then $f_{AUB}(x) = 1$. But if $x \in AUB$ then there are three cases

case1: let $x \in A$ but not in B then $f_A(x) = 1$ and $f_B(x)=0$ $\Rightarrow f_{AUB}(x) = 1 = f_A(x) + f_A(x) - f_A(x) . f_B(x)$

[Because 1+0+0]

case2: let $x \in B$ but not in A

Then $f_B(x) = 1$ and $f_A(x) = 0$

$\Rightarrow$ $f_{AUB}(x) = 1 = f_A(x) + f_B(x) - f_A(x) . f_B(x)$
[Because 0+1-0]

case3: let $x \in A$ and $x \in B$

Then $f_A(x) = 1$ and $f_B(x) = 1$

$\Rightarrow$ $f_{AUB}(x) = 1 = f_A(x) + f_B(x) - f_A(x) . f_B(x)$
[Because 1+1-1]

$\therefore$ $f_{AUB}(x) = f_A(x) + f_B(x) - f_A(x) . f_B(x)$

ii. Let $x \notin A \cup B$ then $f_{AUB}(x) = 0$

If $x \notin A \cup B$ then $x \notin A$ and $x \notin B$ then

$\therefore$ $f_A(x) = 0$ and $f_B(x) = 0$

$\Rightarrow$ $f_{AUB}(x) = 0 = f_A(x) + f_B(x) - f_A(x) . f_B(x)$
[because 0+0-1]

$\therefore$ From case i and ii.
$\therefore$ $f_{AUB}(x) = f_A(x) + f_B(x) - f_A(x) . f_B(x)$

A symmetric difference is associative on sets

To prove $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ we have to prove

$f_{(A \oplus B) \oplus C}(x) = f_{A \oplus (B \oplus C)}(x) \quad \forall x$

LHS = $f_{(A \oplus B) \oplus C}$

= $f_{(D \oplus C)}$ where $D = A \oplus B$

$= f_D + f_{c\,-} 2 f_D f_c$

$= f_c + f_D (1\text{-}2 f_c)$

$= f_D + f_{A \oplus B} (1\text{-}2 f_c)$

$= f_c + (f_A + f_B - 2 f_A f_B) (1 - 2 f_c)$

$= f_c + f_A + f_B - 2 f_A f_B - 2 f_A f_C - 2 f_B f_C + 4 f_A f_B f_C$

$= f_A + (f_B + f_c - 2 f_B f_C) - 2 f_A (f_B + f_C - 2 f_B f_C)$

$= f_A + f_B + f_C - 2 f_B f_C (1\text{-} 2 f_A)$

$= f_A + f_{B\oplus C} (1 - 2 f_A)$

$= f_A + f_{B\oplus C} - 2 f_A f_{B\oplus C}$

$= f_{A \oplus(B\oplus C)}$

= RHS

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$

Permutation function

A permutation on ‘A’ is a bijection of ‘A’ onto itself. Let ‘A’ = {a1, a2, a3, ----------- a_n}.Where A is a finite set, if P is a permutation on A then P can be represented as ,

$$P = \begin{pmatrix} a1 & a2 & a3\text{-----------}an \\ P(a1) & P(a2) & P(a3)\text{-------}P(an) \end{pmatrix}$$

This is called as two line notation of a permutation of A.

NOTE: (a) if |A| =n, then there n! Permutation on A

(b) The composition of two permutations is again a permutation called Product of permutation.

Cycle

Consider a permutation P of a set A = {a1, a2, a3, --------an}

In this permutation suppose r elements of A say {b1, b2, b3, -------- br} are such that P (b1) =b2, P (b2) =b3, ...P(b_{r-1}) =b_r , P(b_r) =b_1 , and the remaining elements of A are images of themselves, Then P is called a cycle of length ‘r’ , and is denoted by (b1, b2, b3 ……. br).

Example 1:

A = {1, 2, 3, 4} and P(A) = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

P(1) = 3 ; P(3) = 4; P(4) = 1

∴ (1, 3, 4) forms a cycle of length 3.

∴ In P the elements (1, 3, 4) forms a cycle and ‘2’ remains unchanged.

∴ P is a cycle of length 3.

Example 2:

A = {1, 2, 3, 4, 5, 6} and P = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 5 & 1 \end{pmatrix}$

P(1) = 3; P(3) = 4; P(4) = 6; P(6) = 1

∴ (1, 3, 4, 6) forms a cycle (2 and 5 remain unchanged)

∴ P is a cycle of length 4.

Transposition

A cycle of length 2 is called a “transposition” if A = {a1, a2, a3, ---- an} then P = (ai, aj), i ≠ j is a transposition of A.

Example:

A = {1, 2, 3, 4, 5, 6} compute

1. (4, 1, 3, 5) o (5, 6, 3) and

2. (5, 6, 3) o (4, 1, 3, 5)

P_1 = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \end{pmatrix}$

3 2 5 1 4 6

$P_2 = (5, 6, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$

$P_1 0 P_2 =$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$$

2. $P_2 0 P_1 = (5, 6, 3) \text{ o } (4, 1, 3, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$

Even and odd permutations

Example:

A = {1, 2, 3, 4, 5, 6, 7, 8} find whether the following permutation are even or odd

1. $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \\ \end{pmatrix}$

P = (1, 3) o (1, 8) o (1, 6) o (1, 4)

∴ P is an even permutation.

a. P = (4, 8) o (3, 5, 2, 1) o (2, 4, 7, 1)
P = (4, 8) o (3, 1) o (3, 5) o (2, 1) o (2, 7) o (2, 4)

∴ P is an odd permutation because gn per is expressed as a composition of odd number of transportation.

Note: Product of even-even permutation is even

Product of even-odd permutation is odd

Product of odd-odd permutation is odd

Even permutation cannot be expressed in terms of odd

Odd permutation cannot be expressed in terms of even.

Hashing function

Introduction

Suppose we want to store the mail address of all voters of a large city in n number of files, numbered from 0 to n-1 , in such a way that the file containing the address any chosen voter can be located almost instantly. The following is one way of doing this task First, to each voter let us assign a unique positive integer as an identification number. Next, to each identification number, let us assign a unique positive integer called a key. The keys can be such that two identification numbers can have the same key but two different keys are not assigned to the same identification number.

Therefore the number of identification number will be equal to the number of voters , but the number, of keys can be less than the no. of identification number.

Definition

Let A denote the set of all keys and B = {0, 1, 2, ------- (n-1)} , the set of all files.

Consider an everywhere defined function ' h_n ; $h_n : A \rightarrow B$ specified by h_n (a) = r, where r is the remainder, r= a/n and $a \in A$. This function determines a unique r. for any specified $a \in A$, this r will be one and only one of the numbers from 0 to n-1 , (both inclusive).

The function h_n is called hashing function. For this function a set of all keys is domain.

NOTE: The key need not be different from the identification number. If the keys are identical with the identification number, then the domain of the hashing function is the set of all identification number.

UNIT – 7 Groups: 6 Hours

- Definitions,
- Examples,
- Elementary Properties,
- Homomorphisms,
- Isomorphisms, and
- Cyclic Groups,
- Cosets, and
- Lagrange’s Theorem.

Coding Theory and Rings:

- Elements of Coding Theory,
- The Hamming Metric,
- The Parity Check, and
- Generator Matrices

UNIT 7 6 hrs

GROUPS

SYLLABUS

Groups: Definitions, Examples, and Elementary Properties, Homomorphisms, Isomorphisms, and Cyclic Groups, Cosets, and Lagrange's Theorem

Coding Theory and Rings: Elements of Coding Theory, The Hamming Metric, The Parity Check, and Generator Matrices

Introduction:

Definitions, Examples, and Elementary Properties:

In mathematics, a **discrete group** is a group *G* equipped with the discrete topology. With this topology *G* becomes a topological group. A **discrete subgroup** of a topological group *G* is a subgroup *H* whose relative topology is the discrete one. For example, the integers, **Z**, form a discrete subgroup of the reals, **R**, but the rational numbers, **Q**, do not.

Any group can be given the discrete topology. Since every map from a discrete space is continuous, the topological homomorphisms between discrete groups are exactly the group homomorphisms between the underlying groups. Hence, there is an isomorphism between the category of groups and the category of discrete groups. Discrete groups can therefore be identified with their underlying (non-topological) groups. With this in mind, the term **discrete group theory** is used to refer to the study of groups without topological structure, in contradistinction to topological or Lie group theory. It is divided, logically but also technically, into finite group theory, and infinite group theory.

There are some occasions when a topological group or Lie group is usefully endowed with the discrete topology, 'against nature'. This happens for example in the theory of the Bohr compactification, and in group cohomology theory of Lie groups.

Properties:

Since topological groups are homogeneous, one need only look at a single point to determine if the group is discrete. In particular, a topological group is discrete if and only if the singleton containing the identity is an open set.

A discrete group is the same thing as a zero-dimensional Lie group (uncountable discrete groups are not second-countable so authors who require Lie groups to satisfy this axiom do not regard these groups as Lie groups). The identity component of a discrete group is just the trivial subgroup while the group of components is isomorphic to the group itself.

Since the only Hausdorff topology on a finite set is the discrete one, a finite Hausdorff topological group must necessarily be discrete. It follows that every finite subgroup of a Hausdorff group is discrete.

A discrete subgroup *H* of *G* is co compact if there is a compact subset *K* of *G* such that *HK* = *G*.

Discrete normal subgroups play an important role in the theory of covering groups and locally isomorphic groups. A discrete normal subgroup of a connected group *G* necessarily lies in the center of *G* and is therefore abelian.

Other properties:

- every discrete group is totally disconnected
- every subgroup of a discrete group is discrete.
- every quotient of a discrete group is discrete.
- the product of a finite number of discrete groups is discrete.
- a discrete group is compact if and only if it is finite.
- every discrete group is locally compact.
- every discrete subgroup of a Hausdorff group is closed.
- every discrete subgroup of a compact Hausdorff group is finite.

Examples:

- Frieze groups and wallpaper groups are discrete subgroups of the isometry group of the Euclidean plane. Wallpaper groups are cocompact, but Frieze groups are not.
- A space group is a discrete subgroup of the isometry group of Euclidean space of some dimension.
- A crystallographic group usually means a cocompact, discrete subgroup of the isometries of some Euclidean space. Sometimes, however, a crystallographic group can be a cocompact discrete subgroup of a nilpotent or solvable Lie group.
- Every triangle group *T* is a discrete subgroup of the isometry group of the sphere (when *T* is finite), the Euclidean plane (when *T* has a **Z** + **Z** subgroup of finite index), or the hyperbolic plane.

- Fuchsian groups are, by definition, discrete subgroups of the isometry group of the hyperbolic plane.
    - A Fuchsian group that preserves orientation and acts on the upper half-plane model of the hyperbolic plane is a discrete subgroup of the Lie group PSL(2,**R**), the group of orientation preserving isometries of the upper half-plane model of the hyperbolic plane.
    - A Fuchsian group is sometimes considered as a special case of a Kleinian group, by embedding the hyperbolic plane isometrically into three dimensional hyperbolic space and extending the group action on the plane to the whole space.
    - The modular group is PSL(2,**Z**), thought of as a discrete subgroup of PSL(2,**R**). The modular group is a lattice in PSL(2,**R**), but it is not cocompact.
- Kleinian groups are, by definition, discrete subgroups of the isometry group of hyperbolic 3-space. These include quasi-Fuchsian groups.
    - A Kleinian group that preserves orientation and acts on the upper half space model of hyperbolic 3-space is a discrete subgroup of the Lie group PSL(2,**C**), the group of orientation preserving isometries of the upper half-space model of hyperbolic 3-space.
- A lattice in a Lie group is a discrete subgroup such that the Haar measure of the quotient space is finite.

Group homomorphism:

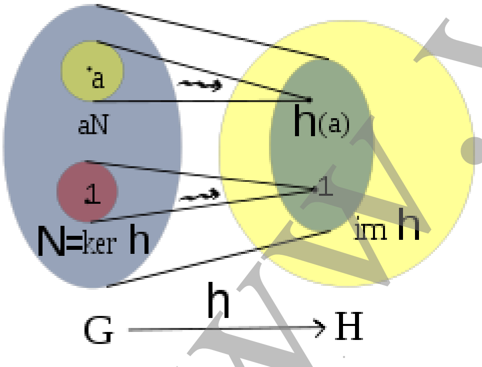


Image of a Group homomorphism(**h**) from **G**(left) to **H**(right). The smaller oval inside **H** is the image of **h**. **N** is the kernel of **h** and **aN** is a coset of **h**.

In mathematics, given two groups (*G*, *) and (*H*, ·), a **group homomorphism** from (*G*, *) to (*H*, ·) is a function $h : G \to H$ such that for all *u* and *v* in *G* it holds that

$$h(u * v) = h(u) \cdot h(v)$$

where the group operation on the left hand side of the equation is that of *G* and on the right hand side that of *H*.

From this property, one can deduce that *h* maps the identity element e_G of *G* to the identity element e_H of *H*, and it also maps inverses to inverses in the sense that

$$h(u^{-1}) = h(u)^{-1}.$$

Hence one can say that *h* "is compatible with the group structure".

Older notations for the homomorphism *h*(*x*) may be x_h, though this may be confused as an index or a general subscript. A more recent trend is to write group homomorphisms on the right of their arguments, omitting brackets, so that *h*(*x*) becomes simply *x h*. This approach is especially prevalent in areas of group theory where automata play a role, since it accords better with the convention that automata read words from left to right.

In areas of mathematics where one considers groups endowed with additional structure, a *homomorphism* sometimes means a map which respects not only the group structure (as above) but also the extra structure. For example, a homomorphism of topological groups is often required to be continuous.

The category of groups

If $h : G \rightarrow H$ and $k : H \rightarrow K$ are group homomorphisms, then so is $k \text{ o } h : G \rightarrow K$. This shows that the class of all groups, together with group homomorphisms as morphisms, forms a category.

Types of homomorphic maps

If the homomorphism *h* is a bijection, then one can show that its inverse is also a group homomorphism, and *h* is called a *group isomorphism*; in this case, the groups *G* and *H* are called *isomorphic*: they differ only in the notation of their elements and are identical for all practical purposes.

If h: $G \rightarrow G$ is a group homomorphism, we call it an *endomorphism* of *G*. If furthermore it is bijective and hence an isomorphism, it is called an *automorphism*. The set of all automorphisms of a group *G*, with functional composition as operation, forms itself a group, the *automorphism group* of *G*. It is denoted by Aut(*G*). As an example, the automorphism group of (**Z**, +) contains only two elements, the identity transformation and multiplication with -1; it is isomorphic to **Z**/2**Z**.

An **epimorphism** is a surjective homomorphism, that is, a homomorphism which is *onto* as a function. A **monomorphism** is an injective homomorphism, that is, a homomorphism which is *one-to-one* as a function.

Homomorphisms of abelian groups

If *G* and *H* are abelian (i.e. commutative) groups, then the set Hom(*G*, *H*) of all group homomorphisms from *G* to *H* is itself an abelian group: the sum *h* + *k* of two homomorphisms is defined by

$$(h + k)(u) = h(u) + k(u) \quad \text{for all } u \text{ in } G.$$

The commutativity of *H* is needed to prove that *h* + *k* is again a group homomorphism. The addition of homomorphisms is compatible with the composition of homomorphisms in the following sense: if *f* is in Hom(*K*, *G*), *h*, *k* are elements of Hom(*G*, *H*), and *g* is in Hom(*H*,*L*), then

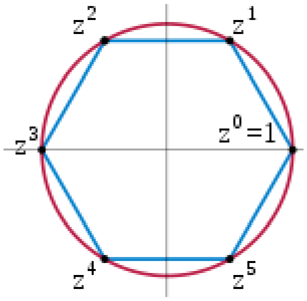
$$(h + k) \text{ o } f = (h \text{ o } f) + (k \text{ o } f) \quad \text{and} \quad g \text{ o } (h + k) = (g \text{ o } h) + (g \text{ o } k).$$

This shows that the set End(*G*) of all endomorphisms of an abelian group forms a ring, the *endomorphism ring* of *G*. For example, the endomorphism ring of the abelian group consisting of the direct sum of *m* copies of **Z**/**nZ** is isomorphic to the ring of m-by-m matrices with entries in **Z**/n**Z**. The above compatibility also shows that the category of all abelian groups with group homomorphisms forms a preadditive category; the existence of direct sums and well-behaved kernels makes this category the prototypical example of an abelian category.

Cyclic group

In group theory, a **cyclic group** is a group that can be generated by a single element, in the sense that the group has an element *g* (called a "generator" of the group) such that, when written multiplicatively, every element of the group is a power of *g* (a multiple of *g* when the notation is additive).

Definition



The six 6th complex roots of unity form a cyclic group under multiplication. *z* is a primitive element, but z^2 is not, because the odd powers of *z* are not a power of z^2.

A group *G* is called cyclic if there exists an element *g* in *G* such that $G = \langle g \rangle = \{ g^n \mid n$ is an integer $\}$. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains *g* is *G* itself suffices to show that G is cyclic.

For example, if $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$ is a group, then $g^6 = g^0$, and *G* is cyclic. In fact, *G* is essentially the same as (that is, isomorphic to) the set { 0, 1, 2, 3, 4, 5 } with addition modulo 6. For example, 1 + 2 = 3 (mod 6) corresponds to $g^1 \cdot g^2 = g^3$, and 2 + 5 = 1 (mod 6) corresponds to $g^2 \cdot g^5 = g^7 = g^1$, and so on. One can use the isomorphism φ defined by $\varphi(g^i) = \text{i}$.

For every positive integer *n* there is exactly one cyclic group (up to isomorphism) whose order is *n*, and there is exactly one infinite cyclic group (the integers under addition). Hence, the cyclic groups are the simplest groups and they are completely classified.

The name "cyclic" may be misleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every g^n is distinct. (It can be said that it has one infinitely long cycle.) A group generated in this way is called an **infinite cyclic group**, and is isomorphic to the additive group of integers **Z**.

Furthermore, the circle group (whose elements are uncountable) is *not* a cyclic group—a cyclic group always has countable elements.

Since the cyclic groups are abelian, they are often written additively and denoted $\mathbf{Z}_n$. However, this notation can be problematic for number theorists because it conflicts with the usual notation for *p*-adic number rings or localization at a prime ideal. The quotient notations **Z**/*n***Z**, **Z**/*n*, and **Z**/(*n*) are standard alternatives. We adopt the first of these here to avoid the collision of notation. See also the section Subgroups and notation below.

One may write the group multiplicatively, and denote it by C_n, where *n* is the order (which can be ∞). For example, $g^3g^4 = g^2$ in C_5, whereas 3 + 4 = 2 in **Z**/5**Z**.

Properties

The fundamental theorem of cyclic groups states that if *G* is a cyclic group of order *n* then every subgroup of *G* is cyclic. Moreover, the order of any subgroup of *G* is a divisor of *n* and for each positive divisor *k* of *n* the group *G* has exactly one subgroup of order *k*. This property characterizes finite cyclic groups: a group of order *n* is cyclic if and only if for every divisor *d* of *n* the group has at most one subgroup of order *d*. Sometimes the equivalent statement is used: a group of order *n* is cyclic if and only if for every divisor *d* of *n* the group has exactly one subgroup of order *d*.

Every finite cyclic group is isomorphic to the group { [0], [1], [2], ..., [*n* − 1] } of integers modulo *n* under addition, and any infinite cyclic group is isomorphic to **Z** (the set of all integers) under addition. Thus, one only needs to look at such groups to understand the properties of cyclic groups in general. Hence, cyclic groups are one of the simplest groups to study and a number of nice properties are known.

Given a cyclic group *G* of order *n* (*n* may be infinity) and for every *g* in *G*,

- G is abelian; that is, their group operation is commutative: *gh* = *hg* (for all *h* in *G*). This is so since *g* + *h* mod *n* = *h* + *g* mod *n*.
- If *n* is finite, then $g^n = g^0$ is the identity element of the group, since *kn* mod *n* = 0 for any integer *k*.
- If *n* = ∞, then there are exactly two elements that generate the group on their own: namely 1 and −1 for **Z**
- If *n* is finite, then there are exactly φ(n) elements that generate the group on their own, where φ is the Euler totient function
- Every subgroup of *G* is cyclic. Indeed, each finite subgroup of G is a group of { 0, 1, 2, 3, ... *m* − 1} with addition modulo m. And each infinite subgroup of G is *m***Z** for some m, which is bijective to (so isomorphic to) **Z**.
- G_n is isomorphic to **Z**/*n***Z** (factor group of **Z** over *n***Z**) since **Z**/*n***Z** = {0 + *n***Z**, 1 + *n***Z**, 2 + *n***Z**, 3 + *n***Z**, 4 + *n***Z**, ..., *n* − 1 + *n***Z**} $\cong$ { 0, 1, 2, 3, 4, ..., *n* − 1} under addition modulo *n*.

More generally, if *d* is a divisor of *n*, then the number of elements in **Z**/*n* which have order *d* is φ(*d*). The order of the residue class of *m* is *n* / gcd(*n*,*m*).

If p is a prime number, then the only group (up to isomorphism) with p elements is the cyclic group C_p or $\mathbf{Z}/p\mathbf{Z}$.

The direct product of two cyclic groups $\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$ is cyclic if and only if n and m are coprime. Thus e.g. $\mathbf{Z}/12\mathbf{Z}$ is the direct product of $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$, but not the direct product of $\mathbf{Z}/6\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$.

The definition immediately implies that cyclic groups have very simple group presentation $C_\infty = < x \mid >$ and $C_n = < x \mid x^n >$ for finite n.

A primary cyclic group is a group of the form $\mathbf{Z}/p^k$ where p is a prime number. The fundamental theorem of abelian groups states that every finitely generated abelian group is the direct product of finitely many finite primary cyclic and infinite cyclic groups.

$\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}$ are also commutative rings. If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a finite field, also denoted by $\mathbf{F}_p$ or $\mathbf{GF}(p)$. Every field with p elements is isomorphic to this one.

The units of the ring $\mathbf{Z}/n\mathbf{Z}$ are the numbers coprime to n. They form a group under multiplication modulo n with $\varphi(n)$ elements (see above). It is written as $(\mathbf{Z}/n\mathbf{Z})^\times$. For example, when $n = 6$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,5\}$. When $n = 8$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,3,5,7\}$.

In fact, it is known that $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is 1 or 2 or 4 or p^k or 2 p^k for an odd prime number p and $k \geq 1$, in which case every generator of $(\mathbf{Z}/n\mathbf{Z})^\times$ is called a primitive root modulo n. Thus, $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic for $n = 6$, but not for $n = 8$, where it is instead isomorphic to the Klein four-group.

The group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic with $p - 1$ elements for every prime p, and is also written $(\mathbf{Z}/p\mathbf{Z})^*$ because it consists of the non-zero elements. More generally, every *finite* subgroup of the multiplicative group of any field is cyclic.

Examples

In 2D and 3D the symmetry group for n-fold rotational symmetry is C_n, of abstract group type Z_n. In 3D there are also other symmetry groups which are algebraically the same, see *Symmetry groups in 3D that are cyclic as abstract group*.

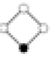
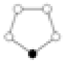
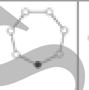
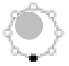
Note that the group S^1 of all rotations of a circle (the circle group) is *not* cyclic, since it is not even countable.

The n^{th} roots of unity form a cyclic group of order n under multiplication. e.g., $0 = z^3 - 1 = (z - s^0)(z - s^1)(z - s^2)$ where $s^i = e^{2\pi i / 3}$ and a group of $\{s^0,s^1,s^2\}$ under multiplication is cyclic.

The Galois group of every finite field extension of a finite field is finite and cyclic; conversely, given a finite field F and a finite cyclic group G, there is a finite field extension of F whose Galois group is G.

Representation

The cycle graphs of finite cyclic groups are all n-sided polygons with the elements at the vertices. The dark vertex in the cycle graphs below stand for the identity element, and the other vertices are the other elements of the group. A cycle consists of successive powers of either of the elements connected to the identity element.

							
C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8

The representation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group decomposes into a direct sum of linear characters, making the connection between character theory and representation theory transparent. In the positive characteristic case, the indecomposable representations of the cyclic group form a model and inductive basis for the representation theory of groups with cyclic Sylow subgroups and more generally the representation theory of blocks of cyclic defect.

Subgroups and notation

All subgroups and quotient groups of cyclic groups are cyclic. Specifically, all subgroups of **Z** are of the form m**Z**, with m an integer ≥0. All of these subgroups are different, and apart from the trivial group (for m=0) all are isomorphic to **Z**. The lattice of subgroups of **Z** is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. All factor groups of **Z** are finite, except for the trivial exception **Z**/{0} = **Z**/0**Z**. For every positive divisor d of n, the quotient group **Z**/n**Z** has precisely one subgroup of order d, the one generated by the residue class of n/d. There are no other subgroups. The lattice of subgroups is thus isomorphic to the set of divisors of n, ordered by divisibility. In particular, a cyclic group is simple if and only if its order (the number of its elements) is prime.

Using the quotient group formalism, **Z**/*n***Z** is a standard notation for the additive cyclic group with *n* elements. In ring terminology, the subgroup *n***Z** is also the ideal (*n*), so the quotient can also be written **Z**/(*n*) or **Z**/*n* without abuse of notation. These alternatives do not conflict with the notation for the *p*-adic integers. The last form is very common in informal calculations; it has the additional advantage that it reads the same way that the group or ring is often described verbally, "Zee mod en".

As a practical problem, one may be given a finite subgroup *C* of order *n*, generated by an element *g*, and asked to find the size *m* of the subgroup generated by g^k for some integer *k*. Here *m* will be the smallest integer > 0 such that *mk* is divisible by *n*. It is therefore *n*/*m* where *m* = (*k*, *n*) is the greatest common divisor of *k* and *n*. Put another way, the index of the subgroup generated by g^k is *m*. This reasoning is known as the **index calculus algorithm**, in number theory.

Endomorphisms

The endomorphism ring of the abelian group **Z**/*n***Z** is isomorphic to **Z**/*n***Z** itself as a ring. Under this isomorphism, the number *r* corresponds to the endomorphism of **Z**/*n***Z** that maps each element to the sum of *r* copies of it. This is a bijection if and only if *r* is coprime with *n*, so the automorphism group of **Z**/*n***Z** is isomorphic to the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$ (see above).

Similarly, the endomorphism ring of the additive group **Z** is isomorphic to the ring **Z**. Its automorphism group is isomorphic to the group of units of the ring **Z**, i.e. to $\{-1, +1\} \cong C_2$.

Virtually cyclic groups

A group is called **virtually cyclic** if it contains a cyclic subgroup of finite index (the number of cosets that the subgroup has). In other words, any element in a virtually cyclic group can be arrived at by applying a member of the cyclic subgroup to a member in a certain finite set. Every cyclic group is virtually cyclic, as is every finite group. It is known that a finitely generated discrete group with exactly two *ends* is virtually cyclic (for instance the product of **Z**/*n* and **Z**). Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

Group isomorphism

In abstract algebra, a **group isomorphism** is a function between two groups that sets up a one-to-one correspondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are called **isomorphic**. From the standpoint of group theory, isomorphic groups have the same properties and need not be distinguished.

Definition and notation

Given two groups (*G*, *) and (*H*, $\odot$), a *group isomorphism* from (*G*, *) to (*H*, $\odot$) is a bijective group homomorphism from *G* to *H*. Spelled out, this means that a group isomorphism is a bijective function $f : G \rightarrow H$ such that for all *u* and *v* in *G* it holds that

$$f(u * v) = f(u) \odot f(v).$$

The two groups (*G*, *) and (*H*, $\odot$) are isomorphic if an isomorphism exists. This is written:

$$(G, *) \cong (H, \odot)$$

Often shorter and more simple notations can be used. Often there is no ambiguity about the group operation, and it can be omitted:

$$G \cong H$$

Sometimes one can even simply write *G* = *H*. Whether such a notation is possible without confusion or ambiguity depends on context. For example, the equals sign is not very suitable when the groups are both subgroups of the same group. See also the examples.

Conversely, given a group (*G*, *), a set *H*, and a bijection $f : G \rightarrow H$, we can make *H* a group (*H*, $\odot$) by defining

$$f(u) \odot f(v) = f(u * v).$$

If *H* = *G* and $\odot$= * then the bijection is an automorphism (*q.v.*)

Intuitively, group theorists view two isomorphic groups as follows: For every element *g* of a group *G*, there exists an element *h* of *H* such that *h* 'behaves in the same way' as *g* (operates with other elements of the group in the same way as *g*). For instance, if *g* generates *G*, then so does *h*. This implies in particular that *G* and *H* are in bijective correspondence. So the definition of an isomorphism is quite natural.

An isomorphism of groups may equivalently be defined as an invertible morphism in the category of groups.

Examples

- The group of all real numbers with addition, ($\mathbb{R}$,+), is isomorphic to the group of all positive real numbers with multiplication ($\mathbb{R}^+$,×):

  $$(\mathbb{R},+) \cong (\mathbb{R}^+,\times)$$

via the isomorphism

$f(x) = e^x$

(see exponential function).

- The group $\mathbb{Z}$of integers (with addition) is a subgroup of $\mathbb{R}$, and the factor group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group S^1 of complex numbers of absolute value 1 (with multiplication):

  $$\mathbb{R}/\mathbb{Z} \cong S^1$$

An isomorphism is given by

$$f(x+\mathbb{Z}) = e^{2\pi xi}$$

for every x in $\mathbb{R}$.

- The Klein four-group is isomorphic to the direct product of two copies of $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$(see modular arithmetic), and can therefore be written $\mathbb{Z}_2 \times \mathbb{Z}_2$. Another notation is Dih_2, because it is a dihedral group.

- Generalizing this, for all odd n, Dih_{2n} is isomorphic with the direct product of Dih_n and Z_2.

- If (G, *) is an infinite cyclic group, then (G, *) is isomorphic to the integers (with the addition operation). From an algebraic point of view, this means that the set of all integers (with the addition operation) is the 'only' infinite cyclic group.

Some groups can be proven to be isomorphic, relying on the axiom of choice, while it is even theoretically impossible to construct concrete isomorphisms. Examples:

- The group ($\mathbb{R}$, +) is isomorphic to the group ($\mathbb{C}$, +) of all complex numbers with addition.
- The group ($\mathbb{C}^*$, ·) of non-zero complex numbers with multiplication as operation is isomorphic to the group S^1 mentioned above.

Properties

- The kernel of an isomorphism from (G, *) to (H, $\odot$), is always {e_G} where e_G is the identity of the group (G, *)

- If (G, *) is isomorphic to (H,$\odot$), and if G is abelian then so is H.

- If (G, *) is a group that is isomorphic to (H, $\odot$) [where f is the isomorphism], then if a belongs to G and has order n, then so does $f(a)$.

- If (G, *) is a locally finite group that is isomorphic to (H, $\odot$), then (H, $\odot$) is also locally finite.

- The previous examples illustrate that 'group properties' are always preserved by isomorphisms.

Cyclic groups

All cyclic groups of a given order are isomorphic to $\mathbb{Z}_n, +_n$.

Let G be a cyclic group and n be the order of G. G is then the group generated by $< x > = \{e,x,...,x^{n-1}\}$. We will show that

$$G \cong \mathbb{Z}_n, +_n$$

Define

$\varphi : G \to \mathbb{Z}_n = \{0, 1, ..., n-1\}$, so that $\varphi(x^a) = a$. Clearly, $\varphi$is bijective.

Then

$\varphi(x^a \cdot x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) +_n \varphi(x^b)$which proves that $G \cong \mathbb{Z}_n, +_n$.

Consequences

From the definition, it follows that any isomorphism $f : G \rightarrow H$ will map the identity element of *G* to the identity element of *H*,

$f(e_G) = e_H$

that it will map inverses to inverses,

$$f(u^{-1}) = [f(u)]^{-1}$$

and more generally, *n*th powers to *n*th powers,

$$f(u^n) = [f(u)]^n$$

for all *u* in *G*, and that the inverse map $f^{-1} : H \rightarrow G$ is also a group isomorphism.

The relation "being isomorphic" satisfies all the axioms of an equivalence relation. If *f* is an isomorphism between two groups *G* and *H*, then everything that is true about *G* that is only related to the group structure can be translated via *f* into a true ditto statement about *H*, and vice versa.

Automorphisms

An isomorphism from a group (*G*,*) to itself is called an automorphism of this group. Thus it is a bijection $f : G \rightarrow G$ such that

$f(u) * f(v) = f(u * v)$.

An automorphism always maps the identity to itself. The image under an automorphism of a conjugacy class is always a conjugacy class (the same or another). The image of an element has the same order as that element.

The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group *G*, denoted by Aut(*G*), forms itself a group, the *automorphism group* of *G*.

For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse this is the trivial automorphism, e.g. in the Klein four-group. For that group all permutations of the three non-identity elements are automorphisms, so the automorphism group is isomorphic to S_3 and Dih_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with corresponding changes in the other elements. The automorphism group is isomorphic to Z_{p-1}. For example, for $n = 7$, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 = 1$ (modulo 7), while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely.

The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these.

The automorphism group of $Z_2 \times Z_2 \times Z_2 = \mathrm{Dih}_2 \times Z_2$ has order 168, as can be found as follows. All 7 non-identity elements play the same role, so we can choose which plays the role of (1,0,0). Any of the remaining 6 can be chosen to play the role of (0,1,0). This determines which corresponds to (1,1,0). For (0,0,1) we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphisms. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements. The lines connecting three points correspond to the group operation: a, b, and c on one line means a+b=c, a+c=b, and b+c=a. See also general linear group over finite fields.

For Abelian groups all automorphisms except the trivial one are called outer automorphisms.

Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer automorphisms.

Coding Theory and Rings

Elements of Coding Theory

Coding theory is studied by various scientific disciplines — such as information theory, electrical engineering, mathematics, and computer science — for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction (or detection) of errors in the transmitted data. It also includes the study of the properties of codes and their fitness for a specific application.

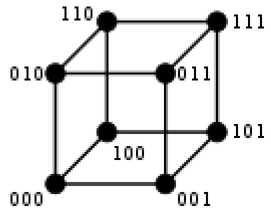
Thus, there are essentially two aspects to Coding theory:

1. Data compression (or, *source coding*)
2. Error correction (or, *channel coding*'*)*

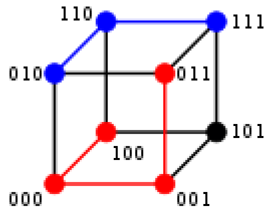
These two aspects may be studied in combination.

The first, source encoding, attempts to compress the data from a source in order to transmit it more efficiently. This practice is found every day on the Internet where the common "Zip" data compression is used to reduce the network load and make files smaller. The second, channel encoding, adds extra data bits to make the transmission of data more robust to disturbances present on the transmission channel. The ordinary user may not be aware of many applications using channel coding. A typical music CD uses the Reed-Solomon code to correct for scratches and dust. In this application the transmission channel is the CD itself. Cell phones also use coding techniques to correct for the fading and noise of high frequency radio transmission. Data modems, telephone transmissions, and NASA all employ channel coding techniques to get the bits through, for example the turbo code and LDPC codes.

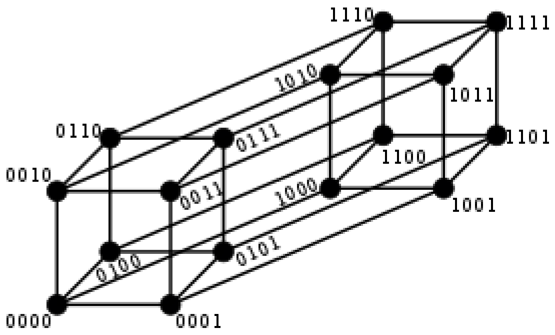
The hamming metric:



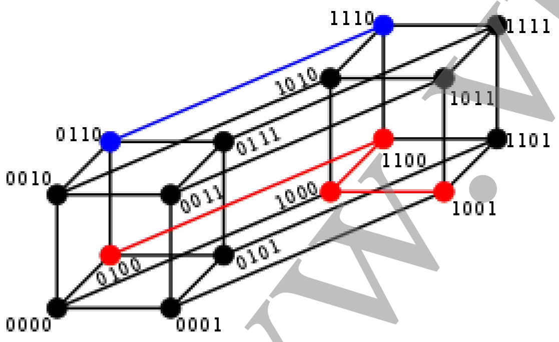
3-bit binary cube for finding Hamming distance



Two example distances: 100->011 has distance 3 (red path); 010->111 has distance 2 (blue path)



4-bit binary hypercube for finding Hamming distance



Two example distances: 0100->1001 has distance 3 (red path); 0110->1110 has distance 1 (blue path)

In information theory, the **Hamming distance** between two strings of equal length is the number of positions at which the corresponding symbols are different. Put another way, it measures the minimum number of *substitutions* required to change one string into the other, or the number of *errors* that transformed one string into the other.

Examples

The Hamming distance between:

- "**toned**" and "**roses**" is 3.
- **1011101** and **1001001** is 2.
- **2173896** and **2233796** is 3.

Special properties

For a fixed length n, the Hamming distance is a metric on the vector space of the words of that length, as it obviously fulfills the conditions of non-negativity, identity of indiscernibles and symmetry, and it can be shown easily by complete induction that it satisfies the triangle inequality as well. The Hamming distance between two words a and b can also be seen as the Hamming weight of $a-b$ for an appropriate choice of the − operator.

For **binary strings** a and b the Hamming distance is equal to the number of ones in a XOR b. The metric space of length-n binary strings, with the Hamming distance, is known as the *Hamming cube*; it is equivalent as a metric space to the set of distances between vertices in a hypercube graph. One can also view a binary string of length n as a vector in R^n by treating each symbol in the string as a real coordinate; with this embedding, the strings form the vertices of an n-dimensional hypercube, and the Hamming distance of the strings is equivalent to the Manhattan distance between the vertices.

History and applications

The Hamming distance is named after Richard Hamming, who introduced it in his fundamental paper on Hamming codes *Error detecting and error correcting codes* in 1950.[1] It is used in telecommunication to count the number of flipped bits in a fixed-length binary word as an estimate of error, and therefore is sometimes called the **signal distance**. Hamming weight analysis of bits is used in several disciplines including information theory, coding theory, and cryptography. However, for comparing strings of different lengths, or strings where not just substitutions but also insertions or deletions have to be expected, a more sophisticated metric like the Levenshtein distance is more appropriate. For q-ary strings over an alphabet of size $q \geq 2$ the Hamming distance is applied in case of orthogonal modulation, while the Lee distance is used for phase modulation. If $q = 2$ or $q = 3$ both distances coincide.

The Hamming distance is also used in systematics as a measure of genetic distance.

On a grid (such as a chessboard), the points at a Lee distance of 1 constitute the von Neumann neighborhood of that point.

Algorithm example

The Python function hamming_distance() computes the Hamming distance between two strings (or other iterable objects) of equal length, by creating a sequence of zero and one values indicating mismatches and matches between corresponding positions in the two inputs, and then summing the sequence.

```
def hamming_distance(s1, s2):
    assert len(s1) == len(s2)
    return sum(ch1 != ch2 for ch1, ch2 in zip(s1, s2))
```

The following C function will compute the Hamming distance of two integers (considered as binary values, that is, as sequences of bits). The running time of this procedure is proportional to the Hamming distance rather than to the number of bits in the inputs. It computes the bitwise exclusive or of the two inputs, and then finds the Hamming weight of the result (the number of nonzero bits) using an algorithm of Wegner (1960) that repeatedly finds and clears the lowest-order nonzero bit.

The Hamming metric

We've seen so far come simple examples of codes. What is needed is some notion of how to compare codewords. Geormetrically, two codewords are ``far'' from each other if there are ``a lot'' of coordinates where they differ. This notion is made more precide in the following definition.

Definition 3.4.1 If $\mathbf{v} = (v_1, v_2, ..., v_n)$, $\mathbf{w} = (w_1, w_2, ..., w_n)$ are vectors in $V = F^n$ then we define

$$d(\mathbf{v}, \mathbf{w}) = |\{i \mid 1 \le i \le n,\ v_i \neq w_i\}|$$

to be the **Hamming distance** between $\mathbf{v}$ and $\mathbf{w}$. The function $d : V \times V \to \mathbb{N}$ is called the **Hamming metric**. The **weight** of a vector (in the Hamming metric) is $d(\mathbf{v}, \mathbf{0})$.

Note that

$$d(\mathbf{v},\mathbf{w}) = |\{i \mid 1 \le i \le n,\ v_i - w_i \ne 0\}| = d(\mathbf{v}-\mathbf{w},\mathbf{0}) \qquad (3.1)$$

for any vectors $\mathbf{v},\mathbf{w} \in F^n$ (or, more generally, any vectors in a linear code). Using this, it is easy to show that $d$satisfies the properties of a metric:

- $d(\mathbf{v},\mathbf{w}) \ge 0$ for all $\mathbf{v},\mathbf{w} \in F^n$ and $d(\mathbf{v},\mathbf{w}) = 0$ if and only if $\mathbf{v} = \mathbf{w}$.
- $d(\mathbf{v},\mathbf{w}) = d(\mathbf{w},\mathbf{v})$, for all $\mathbf{v},\mathbf{w} \in F^n$.
- $d(\mathbf{u},\mathbf{w}) \le d(\mathbf{u},\mathbf{v}) + d(\mathbf{v},\mathbf{w})$, for all $\mathbf{u},\mathbf{v},\mathbf{w} \in F^n$.

Let $v \in F^n$ and let

$$B(v,r,F^n) = \{w \in Fn \mid d(v,w) \le r\}.$$

This is called the **ball of radius r about v**. Since $F^n$is finite, this ball has only a finite number of elements. It is not hard to count them using a little bit of basic combinitorics. Since this count shall be needed later, we record it in the following result.

Lemma 3.4.2 If $0 \le r \le n$ and $q = |F|$ then

$$|B(v,r,F^n)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

proof: Let

$$B_i(v,r,F^n) = \{w \in Fn \mid d(v,w) = i\}.$$

This is called the **shell of radius** i **about** v. It is consists of all vectors with exactly i coordinates different from v. There are $\left(\begin{array}{c} n \\ i \end{array} \right)$ ways to choose i out of n coordinates. There are $(q-1)^i$ ways to choose these i coordinates to be different from those in v. Thus,

$$|B(v,r,F^n)| = \sum_{i=0}^{r} |B_i(v,r,F^n)| = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i.$$

□**Example 3.4.3** If $F = \mathbb{F}_{11}$ and $V = F^{10}$ then

$$C = \{(x_1, x_2, ..., x_{10}) \ \mid x_i \in F, \ x_1 + 2x_2 + 3x_3 + ... + 9x_9 + 10x_{10} \equiv 0 \pmod{11}\}$$

is called the **ISBN code**. This is an 11-ary linear code of length 10. This is the same code used in book numbering except that the number $10$is denoted by X on the inside cover of a book. For example, $(1,0,0,0,0,0,0,0,0,1)$ and $(1,1,1,1,1,1,1,1,1,1)$ are code words. Their Hamming distance is 8.

Generator matrix

In coding theory, a **generator matrix** is a basis for a linear code, generating all its possible codewords. If the matrix is *G* and the linear code is *C*,

w=**c**G

where *w* is a unique codeword of the linear code *C*, **c** is a unique row vector, and a bijection exists between *w* and **c**. A generator matrix for a (n, $M = q^k$, d)$_q$-code is of dimension *k*×*n*. Here *n* is the length of a codeword, *k* is the number of information bits, *d* is the minimum distance of the code, and *q* is the number of symbols in the alphabet (thus, $q = 2$ indicates a binary code, etc.). Note that the number of redundant bits is denoted $r = n - k$.

The systematic form for a generator matrix is

$$G = \left[I_k | P \right]$$

where I_k is a $k \times k$ identity matrix and P is of dimension $k \times r$.

A generator matrix can be used to construct the parity check matrix for a code (and vice-versa).

Equivalent Codes

Codes C_1 and C_2 are equivalent (denoted $C_1 \sim C_2$) if one code can be created from the other via the following two transformations:

1. permute components, and
2. scale components.

Equivalent codes have the same distance.

The generator matrices of equivalent codes can be obtained from one another via the following transformations:

1. permute rows
2. scale rows
3. add rows
4. permute columns, and
5. scale columns.

Parity-check matrix

In coding theory, a **parity-check matrix** of a linear block code **C** is a generator matrix of the dual code. As such, a codeword c is in **C** if and only if the matrix-vector product $\mathbf{H}^{\mathbf{T}}c=\mathbf{0}$.

The rows of a parity check matrix are parity checks on the codewords of a code. That is, they show how linear combinations of certain digits of each codeword equal zero. For example, the parity check matrix

$$H = \begin{bmatrix} 0011 \\ 1100 \end{bmatrix}$$

specifies that for each codeword, digits 1 and 2 should sum to zero and digits 3 and 4 should sum to zero.

Creating a parity check matrix

The parity check matrix for a given code can be derived from its generator matrix (and vice-versa). If the generator matrix for an [*n*,*k*]-code is in standard form

$$G = \begin{bmatrix} I_k | P \end{bmatrix},$$

then the parity check matrix is given by

$$H = \begin{bmatrix} -P^T | I_{n-k} \end{bmatrix},$$

because

$$GH^T = P - P = 0.$$

Negation is performed in the finite field mod *q*. Note that if the characteristic of the underlying field is 2 (i.e., 1 + 1 = 0 in that field), as in binary codes, then $-P = P$, so the negation is unnecessary.

For example, if a binary code has the generator matrix

$$G = \begin{bmatrix} 10|101 \\ 01|110 \end{bmatrix}$$

The parity check matrix becomes

$$H = \begin{bmatrix} 11|100 \\ 01|010 \\ 10|001 \end{bmatrix}$$

For any valid codeword *x*, $Hx = 0$. For any invalid codeword $\tilde{x}$, the syndrome *S* satisfies $H\tilde{x} = S.$

Parity check

If no error occurs during transmission, then the received codeword *r* is identical to the transmitted codeword *x*:

$$\mathbf{r} = \mathbf{x}$$

The receiver multiplies *H* and *r* to obtain the **syndrome** vector $\mathbf{z}$, which indicates whether an error has occurred, and if so, for which codeword bit. Performing this multiplication (again, entries modulo 2):

$$\mathbf{z} = \mathbf{Hr} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Since the syndrome *z* is the null vector, the receiver can conclude that no error has occurred. This conclusion is based on the observation that when the data vector is multiplied by $\mathbf{G}$, a change of basis occurs into a vector subspace that is the kernel of $\mathbf{H}$. As long as nothing happens during transmission, $\mathbf{r}$will remain in the kernel of $\mathbf{H}$and the multiplication will yield the null vector.

Coset

In mathematics, if *G* is a group, *H* is a subgroup of *G*, and *g* is an element of *G*, then

> *gH* = {*gh* : *h* an element of *H* } is a **left coset of *H*** in *G*, and
>
> *Hg* = {*hg* : *h* an element of *H* } is a **right coset of *H*** in *G*.

Only when *H* is normal will the right and left cosets of *H* coincide, which is one definition of normality of a subgroup.

A **coset** is a left or right coset of *some* subgroup in *G*. Since $Hg = g\,(g^{-1}Hg)$, the right cosets *Hg* (of *H*) and the left cosets $g\ (g^{-1}Hg)$ (of the conjugate subgroup $g^{-1}Hg$) are the same. Hence it is not meaningful to speak of a coset as being left or right unless one first specifies the underlying subgroup.

For abelian groups or groups written additively, the notation used changes to *g*+*H* and *H*+*g* respectively.

Examples

The additive cyclic group $\mathbf{Z}_4$ = {0, 1, 2, 3} = *G* has a subgroup *H* = {0, 2} (isomorphic to $\mathbf{Z}_2$). The left cosets of *H* in *G* are

$0 + H = \{0, 2\} = H$

$1 + H = \{1, 3\}$

$2 + H = \{2, 0\} = H$

$3 + H = \{3, 1\}$.

There are therefore two distinct cosets, H itself, and $1 + H = 3 + H$. Note that every element of G is either in H or in $1 + H$, that is, $H \cup (1 + H) = G$, so the distinct cosets of H in G partition G. Since $\mathbf{Z}_4$ is an abelian group, the right cosets will be the same as the left.

Another example of a coset comes from the theory of vector spaces. The elements (vectors) of a vector space form an Abelian group under vector addition. It is not hard to show that subspaces of a vector space are subgroups of this group. For a vector space V, a subspace W, and a fixed vector $\boldsymbol{a}$ in V, the sets

$$\{x \in V : x = a + n, n \in W\}$$

are called affine subspaces, and are cosets (both left and right, since the group is Abelian). In terms of geometric vectors, these affine subspaces are all the "lines" or "planes" parallel to the subspace, which is a line or plane going through the origin.

General properties

We have $gH = H$ if and only if g is an element of H, since as H is a subgroup, it must be closed and must contain the identity.

Any two left cosets of H in G are either identical or disjoint — i.e., the left cosets form a partition of G such that every element of G belongs to one and only one left coset.[1] In particular the identity is in precisely one coset, and that coset is H itself; this is also the only coset that is a subgroup. We can see this clearly in the above examples.

The left cosets of H in G are the equivalence classes under the equivalence relation on G given by $x \sim y$ if and only if $x^{-1}y \in H$. Similar statements are also true for right cosets.

A **coset representative** is a representative in the equivalence class sense. A set of representatives of all the cosets is called a transversal. There are other types of equivalence relations in a group, such as conjugacy, that form different classes which do not have the properties discussed here. Some books on very applied group theory erroneously identify the conjugacy class as 'the' equivalence class as opposed to a particular type of equivalence class.

Index of a subgroup

All left cosets and all right cosets have the same order (number of elements, or cardinality in the case of an infinite *H*), equal to the order of *H* (because *H* is itself a coset). Furthermore, the number of left cosets is equal to the number of right cosets and is known as the **index** of *H* in *G*, written as $[G : H]$. Lagrange's theorem allows us to compute the index in the case where *G* and *H* are finite, as per the formula:

$$|G| = [G : H] \cdot |H|.$$

This equation also holds in the case where the groups are infinite, although the meaning may be less clear.

Cosets and normality

If *H* is not normal in *G*, then its left cosets are different from its right cosets. That is, there is an *a* in *G* such that no element *b* satisfies $aH = Hb$. This means that the partition of *G* into the left cosets of *H* is a different partition than the partition of *G* into right cosets of *H*. (It is important to note that *some* cosets may coincide. For example, if *a* is in the center of *G*, then $aH = Ha$.)

On the other hand, the subgroup *N* is normal if and only if $gN = Ng$ for all *g* in *G*. In this case, the set of all cosets form a group called the quotient group G/N with the operation $*$ defined by $(aN)*(bN) = abN$. Since every right coset is a left coset, there is no need to differentiate "left cosets" from "right cosets".

Lagrange's theorem (group theory)

Lagrange's theorem, in the mathematics of group theory, states that for any finite group *G*, the order (number of elements) of every subgroup *H* of *G* divides the order of *G*. The theorem is named after Joseph Lagrange.

Proof of Lagrange's Theorem

This can be shown using the concept of left cosets of *H* in *G*. The left cosets are the equivalence classes of a certain equivalence relation on *G* and therefore form a partition of *G*. Specifically, *x* and *y* in *G* are related if and only if there exists *h* in *H* such that $x = yh$. If we can show that all cosets of *H* have the same number of elements, then each coset of H has precisely $|H|$ elements. We are then done since the order of H times the number of cosets is equal to the number of elements in G, thereby proving that the order H divides the order of G. Now, if aH and bH are two left cosets of H, we can define a map $f : aH \rightarrow bH$ by setting $f(x) = ba^{-1}x$. This map is bijective because its inverse is given by $f^{-1}(y) = ab^{-1}y$.

This proof also shows that the quotient of the orders $|G| / |H|$ is equal to the index $[G : H]$ (the number of left cosets of H in G). If we write this statement as

$$|G| = [G : H] \cdot |H|,$$

then, seen as a statement about cardinal numbers, it is equivalent to the Axiom of choice.

Using the theorem

A consequence of the theorem is that the order of any element a of a finite group (i.e. the smallest positive integer number k with $a^k = e$, where e is the identity element of the group) divides the order of that group, since the order of a is equal to the order of the cyclic subgroup generated by a. If the group has n elements, it follows

$$a^n = e.$$

This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved.

The theorem also shows that any group of prime order is cyclic and simple.

Existence of subgroups of given order

Lagrange's theorem raises the converse question as to whether every divisor of the order of a group is the order of some subgroup. This does not hold in general: given a finite group G and a divisor d of $|G|$, there does not necessarily exist a subgroup of G with order d. The smallest example is the alternating group $G = A_4$ which has 12 elements but no subgroup of order 6. A *CLT group* is a finite group with the property that for every divisor of the order of the group, there is a subgroup of that order. It is known that a CLT group must be solvable and that every supersolvable group is a CLT group: however there exists solvable groups which are not CLT and CLT groups which are not supersolvable.

There are partial converses to Lagrange's theorem. For general groups, Cauchy's theorem guarantees the existence of an element, and hence of a cyclic subgroup, of order any prime dividing the group order; Sylow's theorem extends this to the existence of a subgroup of order equal to the maximal power of any prime dividing the group order. For solvable groups, Hall's theorems assert the existence of a subgroup of order equal to any unitary divisor of the group order (that is, a divisor coprime to its cofactor).

History

Lagrange did not prove Lagrange's theorem in its general form. He stated, in his article *Réflexions sur la résolution algébrique des équations,*[1] that if a polynomial in n variables has its variables permuted in all n ! ways, the number of different polynomials that are obtained is always a factor of n !. (For example if the variables x, y, and z are permuted in all 6 possible ways in the polynomial $x + y - z$ then we get a total of 3 different polynomials: $x + y - z$, $x + z - y$, and $y + z - x$. Note that 3 is a factor of 6.) The number of such polynomials is the index in the symmetric group S_n of the subgroup H of permutations which preserve the polynomial. (For the example of $x + y - z$, the subgroup H in S_3 contains the identity and the transposition (xy).) So the size of H divides n !. With the later development of abstract groups, this result of Lagrange on polynomials was recognized to extend to the general theorem about finite groups which now bears his name.

Lagrange did not prove his theorem; all he did, essentially, was to discuss some special cases. The first complete proof of the theorem was provided by Abbati and published in 1803.

UNIT – 8 Group Codes: 6 Hours

- Decoding with Coset Leaders,
- Hamming Matrices Rings and
- Modular Arithmetic
- The Ring Structure
- Definition and Examples
- Ring Properties and Substructures,
- The Integers Modulo n

UNIT 8 7 Hours

Group codes

SYLLABUS

Group Codes: Decoding with Coset Leaders, Hamming Matrices

Rings and Modular Arithmetic: The Ring Structure – Definition and Examples, Ring Properties and Substructures, The Integers Modulo n

In computer science, **group codes** are a type of code. Group codes consist of *n* linear block codes which are subgroups of G^n, where G is a finite Abelian group.

A systematic group code C is a code over G^n of order $|G|^k$ defined by $n - k$ homomorphisms which determine the parity check bits. The remaining k bits are the information bits themselves.

Construction

Group codes can be constructed by special generator matrices which resemble generator matrices of linear block codes except that the elements of those matrices are endomorphisms of the group instead of symbols from the code's alphabet. For example, consider the generator matrix

$$G = \begin{pmatrix} \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 01 \\ 01 \end{pmatrix} & \begin{pmatrix} 11 \\ 01 \end{pmatrix} \\ \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 11 \\ 11 \end{pmatrix} & \begin{pmatrix} 00 \\ 00 \end{pmatrix} \end{pmatrix}$$

The elements of this matrix are 2*x*2 matrices which are endomorphisms. In this scenario, each codeword can be represented as $g_1^{m_1} g_2^{m_2} \cdots g_r^{m_r}$ where $g_1, \ldots g_r$ are the generators of *G*.

Decoding with Coset leader

In the field of coding theory, a **coset leader** is defined as a word of minimum weight in any particular coset - that is, a word with the lowest amount of non-zero entries. Sometimes there are several words of equal minimum weight in a coset, and in that case, any one of those words may be chosen to be the coset leader.

Coset leaders are used in the construction of a standard array for a linear code, which can then be used to decode received vectors. For a received vector *y*, the decoded message is *y* - *e*, where *e* is the coset leader of *y*. Coset leaders can also be used to construct a fast decoding strategy. For each coset leader *u* we calculate the syndrome *uH′*. When we receive *v* we evaluate *vH′* and find the matching syndrome. The corresponding coset leader is the most likely error pattern and we assume that *v*+*u* was the codeword sent.

Example

A standard array for an [*n*,*k*]-code is a q^{n-k} by q^k array where:

1. The first row lists all codewords (with the 0 codeword on the extreme left)
2. Each row is a coset with the coset leader in the first column
3. The entry in the i-th row and j-th column is the sum of the i-th coset leader and the j-th codeword.

For example, the [*n*,*k*]-code C_3 = {0, 01101, 10110, 11011} has a standard array as follows:

0 01101 10110 11011

10000 11101 00110 01011

01000 00101 11110 10011

00100 01001 10010 11111

00010 01111 10100 11001

00001 01100 10111 11010

11000 10101 01110 00011

10001 11100 00111 01010

Note that the above is only one possibility for the standard array; had 00011 been chosen as the first coset leader of weight two, another standard array representing the code would have been constructed.

Note that the first row contains the 0 vector and the codewords of C_3 (0 itself being a codeword). Also, the leftmost column contains the vectors of minimum weight enumerating vectors of weight 1 first and then using vectors of weight 2. Note also that each possible vector in the vector space appears exactly once.

Because each possible vector can appear only once in a standard array some care must be taken during construction. A standard array can be created as follows:

1. List the codewords of *C*, starting with 0, as the first row
2. Choose any vector of minimum weight not already in the array. Write this as the first entry of the next row. This vector is denoted the '**coset leader**'.
3. Fill out the row by adding the coset leader to the codeword at the top of each column. The sum of the i-th coset leader and the j-th codeword becomes the entry in row i, column j.
4. Repeat steps 2 and 3 until all rows/cosets are listed and each vector appears exactly once.

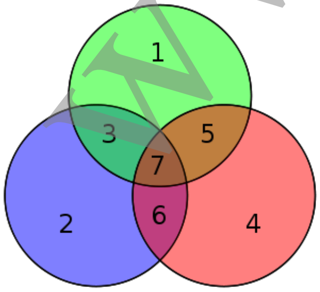
Hamming matrices

Hamming codes can be computed in linear algebra terms through matrices because Hamming codes are linear codes. For the purposes of Hamming codes, two **Hamming matrices** can be defined: the **code generator matrix** $\mathbf{G}$and the **parity-check matrix** $\mathbf{H}$:

$$\mathbf{G} := \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\mathbf{H} := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$



Bit position of the data and parity bits

As mentioned above, rows 1, 2, & 4 of $\mathbf{G}$should look familiar as they map the data bits to their parity bits:

- p_1 covers d_1, d_2, d_4
- p_2 covers d_1, d_3, d_4
- p_3 covers d_2, d_3, d_4

The remaining rows (3, 5, 6, 7) map the data to their position in encoded form and there is only 1 in that row so it is an identical copy. In fact, these four rows are linearly independent and form the identity matrix (by design, not coincidence).

Also as mentioned above, the three rows of $\mathbf{H}$should be familiar. These rows are used to compute the **syndrome vector** at the receiving end and if the syndrome vector is the null vector (all zeros) then the received word is error-free; if non-zero then the value indicates which bit has been flipped.

The 4 data bits — assembled as a vector $\mathbf{p}$— is pre-multiplied by $\mathbf{G}$(i.e., $\mathbf{Gp}$) and taken modulo 2 to yield the encoded value that is transmitted. The original 4 data bits are converted to 7 bits (hence the name "Hamming(7,4)") with 3 parity bits added to ensure even parity using the above data bit coverages. The first table above shows the mapping between each data and parity bit into its final bit position (1 through 7) but this can also be presented in a Venn diagram. The first diagram in this article shows three circles (one for each parity bit) and encloses data bits that each parity bit covers. The second diagram (shown to the right) is identical but, instead, the bit positions are marked.

For the remainder of this section, the following 4 bits (shown as a column vector) will be used as a running example:

$$\mathbf{p} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Rings and Modular Arithmetic

Ring theory

In mathematics, **ring theory** is the study of rings—algebraic structures in which addition and multiplication are defined and have similar properties to those familiar from the integers. Ring theory studies the structure of rings, their representations, or, in different language, modules, special classes of rings (group rings, division rings, universal enveloping algebras), as well as an array of properties that proved to be of interest both within the theory itself and for its applications, such as homological properties and polynomial identities.

Commutative rings are much better understood than noncommutative ones. Due to its intimate connections with algebraic geometry and algebraic number theory, which provide many natural examples of commutative rings, their theory, which is considered to be part of commutative algebra and field theory rather than of general ring theory, is quite different in flavour from the theory of their noncommutative counterparts. A fairly recent trend, started in the 1980s with the development of noncommutative geometry and with the discovery of quantum groups, attempts to turn the situation around and build the theory of certain classes of noncommutative rings in a geometric fashion as if they were rings of functions on (non-existent) 'noncommutative spaces'.

Elementary introduction

Definition

Formally, a ring is an Abelian group (R, +), together with a second binary operation * such that for all a, b and c in R,

$$a * (b * c) = (a * b) * c$$

$$a * (b + c) = (a * b) + (a * c)$$

$$(a + b) * c = (a * c) + (b * c)$$

also, if there exists a *multiplicative identity* in the ring, that is, an element e such that for all a in R,

$$a * e = e * a = a$$

then it is said to be a *ring with unity*. The number 1 is a common example of a unity.

The ring in which e is equal to the additive identity must have only one element. This ring is called the trivial ring.

Rings that sit inside other rings are called subrings. Maps between rings which respect the ring operations are called ring homomorphisms. Rings, together with ring homomorphisms, form a category (the category of rings). Closely related is the notion of ideals, certain subsets of rings which arise as kernels of homomorphisms and can serve to define factor rings. Basic facts about ideals, homomorphisms and factor rings are recorded in the isomorphism theorems and in the Chinese remainder theorem.

A ring is called *commutative* if its multiplication is commutative. Commutative rings resemble familiar number systems, and various definitions for commutative rings are designed to recover properties known from the integers. Commutative rings are also important in algebraic geometry. In commutative ring theory, numbers are often replaced by ideals, and the definition of prime ideal tries to capture the essence of prime numbers. Integral domains, non-trivial commutative rings where no two non-zero elements multiply to give zero, generalize another property of the integers and serve as the proper realm to study divisibility. Principal ideal domains are integral domains in which every ideal can be generated by a single element, another property shared by the integers. Euclidean domains are integral domains in which the Euclidean algorithm can be carried out. Important examples of commutative rings can be constructed as rings of polynomials and their factor rings. Summary: Euclidean domain => principal ideal domain => unique factorization domain => integral domain => Commutative ring.

Non-commutative rings resemble rings of matrices in many respects. Following the model of algebraic geometry, attempts have been made recently at defining non-commutative geometry based on non-commutative rings. Non-commutative rings and associative algebras (rings that are also vector spaces) are often studied via their categories of modules. A module over a ring is an Abelian group that the ring acts on as a ring of endomorphisms, very much akin to the way fields (integral domains in which every non-zero element is invertible) act on vector spaces. Examples of non-commutative rings are given by rings of square matrices or more generally by rings of endomorphisms of Abelian groups or modules, and by monoid rings.

The congruence relation

Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations of the ring of integers: addition, subtraction, and multiplication. For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n*, written:

$$a \equiv b \pmod{n},$$

if their difference *a* − *b* is an integer multiple of *n*. The number *n* is called the **modulus** of the congruence. An equivalent definition is that both numbers have the same remainder when divided by *n*.

For example,

$$38 \equiv 14 \pmod{12}$$

because 38 − 14 = 24, which is a multiple of 12. For positive *n* and non-negative *a* and *b*, congruence of *a* and *b* can also be thought of as asserting that these two numbers have the same remainder after dividing by the modulus *n*. So,

$$38 \equiv 2 \pmod{12}$$

because both numbers, when divided by 12, have the same remainder (2). Equivalently, the fractional parts of doing a full division of each of the numbers by 12 are the same: 0.1666... (38/12 = 3.1666..., 2/12 = 0.1666...). From the prior definition we also see that their difference, *a* − *b* = 36, is a whole number (integer) multiple of 12 (*n* = 12, 36/12 = 3).

The same rule holds for negative values of *a*:

$$-3 \equiv 2 \pmod{5}.$$

A remark on the notation: Because it is common to consider several congruence relations for different moduli at the same time, the modulus is incorporated in the notation. In spite of the ternary notation, the congruence relation for a given modulus is binary. This would have been clearer if the notation $a \equiv_n b$ had been used, instead of the common traditional notation.

The properties that make this relation a congruence relation (respecting addition, subtraction, and multiplication) are the following.

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n},$$

then:

- $(a_1 + a_2) \equiv (b_1 + b_2) \pmod{n}$
- $(a_1 - a_2) \equiv (b_1 - b_2) \pmod{n}$
- $(a_1 a_2) \equiv (b_1 b_2) \pmod{n}.$

Multiplicative group of integers modulo n

In modular arithmetic the set of congruence classes relatively prime to the modulus *n* form a group under multiplication called the **multiplicative group of integers modulo *n***. It is also called the group of **primitive residue classes modulo *n*.** In the theory of rings, a branch of abstract algebra, it is described as the group of units of the ring of integers modulo *n*. (Units refers to elements with a multiplicative inverse.)

This group is fundamental in number theory. It has found applications in cryptography, integer factorization, and primality testing. For example, by finding the order (ie. the size) of the group, one can determine if *n* is prime: *n* is prime if and only if the order is *n* − 1.

Group axioms

It is a straightforward exercise to show that under multiplication the congruence classes (mod *n*) which are relatively prime to *n* satisfy the axioms for an abelian group.

Because *a* ≡ *b* (mod *n*) implies that gcd(*a*, *n*) = gcd(*b*, *n*), the notion of congruence classes (mod *n*) which are relatively prime to *n* is well-defined.

Since gcd(*a*, *n*) = 1 and gcd(*b*, *n*) = 1 implies gcd(*ab*, *n*) = 1 the set of classes relatively prime to *n* is closed under multiplication.

The natural mapping from the integers to the congruence classes (mod *n*) that takes an integer to its congruence class (mod *n*) is a ring homomorphism. This implies that the class containing 1 is the unique multiplicative identity, and also the associative and commutative laws.

Given *a*, gcd(*a*, *n*) = 1, finding *x* satisfying *ax* ≡ 1 (mod *n*) is the same as solving *ax* + *ny* = 1, which can be done by Bézout's lemma.

Notation

The ring of integers (mod *n*) is denoted $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ (i.e., the ring of integers modulo the ideal *n***Z** = (*n*) consisting of the multiples of *n*) or by $\mathbb{Z}_n$. Depending on the author its group of units may be written $(\mathbb{Z}/n\mathbb{Z})^*,\ (\mathbb{Z}/n\mathbb{Z})^\times,\ U(\mathbb{Z}/n\mathbb{Z}),$ $E(\mathbb{Z}/n\mathbb{Z})$ (for German *Einheit* = unit) or similar notations. This article uses $(\mathbb{Z}/n\mathbb{Z})^\times.$

Structure

Powers of 2

Modulo 2 there is only one relatively prime congruence class, 1, so $(\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\}$is trivial.

Modulo 4 there are two relatively prime congruence classes, 1 and 3, so $(\mathbb{Z}/4\mathbb{Z})^\times \cong C_2,$the cyclic group with two elements.

Modulo 8 there are four relatively prime classes, 1, 3, 5 and 7. The square of each of these is 1, so $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2,$the Klein four-group.

Modulo 16 there are eight relatively prime classes 1, 3, 5, 7, 9, 11, 13 and 15. $\{\pm 1, \pm 7\} \cong C_2 \times C_2,$is the 2-torsion subgroup (ie. the square of each element is 1), so $(\mathbb{Z}/16\mathbb{Z})^\times$is not cyclic. The powers of 3, {1,3,9,11} are a subgroup of order 4, as are the powers of 5, {1,5,9,13}. Thus $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4.$

The pattern shown by 8 and 16 holds[1] for higher powers 2^k, $k > 2$: $\{\pm 1, 2^{k-1} \pm 1\} \cong C_2 \times C_2,$is the 2-torsion subgroup (so $(\mathbb{Z}/2^k\mathbb{Z})^\times$is not cyclic) and the powers of 3 are a subgroup of order 2^{k-2}, so $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong C_2 \times C_{2^{k-2}}.$

Powers of odd primes

For powers of odd primes p^k the group is cyclic:[2] $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)} \cong C_{\varphi(p^k)}.$

General composite numbers

The Chinese remainder theorem[3] says that if $n = p_1^{k_1}p_2^{k_2}p_3^{k_3}\dots$,then the ring $\mathbb{Z}/n\mathbb{Z}$is the direct product of the rings corresponding to each of its prime power factors:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/{p_1^{k_1}}\mathbb{Z}\; \times \;\mathbb{Z}/{p_2^{k_2}}\mathbb{Z} \;\times\; \mathbb{Z}/{p_3^{k_3}}\mathbb{Z}\dots$$

Similarly, the group of units $(\mathbb{Z}/n\mathbb{Z})^\times$is the direct product of the groups corresponding to each of the prime power factors:

$$(\mathbb{Z}/n\mathbb{Z})^\times\cong (\mathbb{Z}/{p_1^{k_1}}\mathbb{Z})^\times \times (\mathbb{Z}/{p_2^{k_2}}\mathbb{Z})^\times \times (\mathbb{Z}/{p_3^{k_3}}\mathbb{Z})^\times \dots\;.$$

Order

The order of the group is given by Euler's totient function: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.This is the product of the orders of the cyclic groups in the direct product.

Exponent

The exponent is given by the Carmichael function λ(*n*), the least common multiple of the orders of the cyclic groups. This means that if *a* and *n* are relatively prime, $a^{\lambda(n)} \equiv 1 \pmod n$.

Generators

$(\mathbb{Z}/n\mathbb{Z})^\times$is cyclic if and only if $\varphi(n) = \lambda(n)$.This is the case precisely when *n* is 2, 4, a power of an odd prime, or twice a power of an odd prime. In this case a generator is called a **primitive root modulo n.**

Since all the $(\mathbb{Z}/n\mathbb{Z})^\times$,*n* = 1, 2, ..., 7 are cyclic, another way to state this is: If *n* < 8 then $(\mathbb{Z}/n\mathbb{Z})^\times$has a primitive root. If *n* ≥ 8 $(\mathbb{Z}/n\mathbb{Z})^\times$has a primitive root unless *n* is divisible by 4 or by two distinct odd primes.

In the general case there is one generator for each cyclic direct factor.

Table

This table shows the structure and generators of $(\mathbb{Z}/n\mathbb{Z})^\times$ for small values of *n*. The generators are not unique (mod *n*); e.g. (mod 16) both {−1, 3} and {−1, 5} will work. The generators are listed in the same order as the direct factors.

For example take *n* = 20. $\varphi(20) = 8$ means that the order of $(\mathbb{Z}/20\mathbb{Z})^\times$ is 8 (i.e. there are 8 numbers less than 20 and coprime to it); λ(20) = 4 that the fourth power of any number relatively prime to 20 is ≡ 1 (mod 20); and as for the generators, 19 has order 2, 3 has order 4, and every member of $(\mathbb{Z}/20\mathbb{Z})^\times$ is of the form $19^a \times 3^b$, where *a* is 0 or 1 and *b* is 0, 1, 2, or 3.

The powers of 19 are {±1} and the powers of 3 are {3, 9, 7, 1}. The latter and their negatives (mod 20), {17, 11, 13, 19} are all the numbers less than 20 and prime to it. The fact that the order of 19 is 2 and the order of 3 is 4 implies that the fourth power of every member of $\mathbb{Z}_{20}^\times$ is ≡ 1 (mod 20).