Lecture 35

DISCRETE STRUCTURES

Niloy Ganguly
Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology

Binary operations:

A binary operation on a set A is an everywhere defined function $f : AxA \rightarrow A$.

In view of the above definition following properties hold for all binary operations :

1. Since dom (f) = AxA , It is defined for every ordered pair (a, b) of AxA.
2. A is closed under the binary operation.
3. Only one element of A is assigned to an ordered pair.

A generic binary operation is denoted by *. Thus f (a, b) = c is same as saying that
a*b = c.

Examples:

1. Let A = Z. If we define a*b as a+b . Then * is a binary operation on Z.
2. Let A = P(S) for some set S. If U and V are subsets of S and we define U*V as U ^ V. (^ is union), then * is a binary operation on P(S).
3. let A = Z. If we define a*b = a number less than both a and b, then * is not a binary operation as corresponding rule f is not a function.

Properties of binary operations:

1. Commutative:
   If a*b = b*a , then * is said to be commutative binary operation.
   For ex. + in example 1 above is a commutative binary operation.

2. Associative :
   If a*(b*c) = (a*b)*c , then * is said to be associative.

3. Idempotent :
   If a*a = a , then * is said to be idempotent.

Example :

Let a*b = LCM (a , b). Then * is commutative, associative and idempotent.

Semigroups :

A semigroup is a non empty set S together with an associative binary operation (*) defined on S. It is denoted by (S, *). This semigroup is called a commutative semigroup if * is a commutative binary operation.

Example :

The power set of a set S , P(S) together with the operation of union is a commutative semigroup (P(S), U).

Let L be a lattice. Then if we define a*b = a^b, then L is a commutative semigroup.

Theorem 1.

If a1 , a2 , a3 .... An , n ≥3 are arbitrary elements of a semigroup, then all products of
a1 , a2 .... an that can be obtained by inserting meaningful parantheses are equal. Here by product we mean ab = a*b, call a*b as product of a and b. Thus a*b*c*d = (a*b*c)*d = (a*b)*(c*d) = a*(b*c)*d = a*(b*c*d) etc.

Identity element :

If the semigroup (S , *) is such that it has an element *e* for which
e * a = a *e* = a ,
Then *e* is called identity element of semigroup (S, *).

Example :

The semigroup (Z , +) has an identity element *e* = 0, as

0+a = a+0 = a, aϵ Z.

The semigroup (Z+ , +) does not have any identity element.

Let A be an alphabet with A* as the set of all regular expressions. If we define binary operation ▪ as catenation of one string s1 another string s2 i.e. , s1▪s2 .Then empty sequence

ˆ is the identity element of A*.

Monoid :

Definition : A monoid is a semigroup(S , *) with an identity element *e*. Examples of monoids are above given semigroups.

Subsemigroup and Submonoid :

Let (S , *) be a semigroup with T as its subset. If T is closed under the operation *.

(that is, if a, b ϵ T , then a*b ϵT) then T is called a subsemigroup. By similar logic a subset T of a monoid (M, *) such that identity element belongs to it and the set is closed under * is said to be submonoid (T, *).

Example:

1. If T be the set of all even integers then (T, +) is a subsemigroup of (Z,+).

   It is even a submonoid (identity element *e* = 0)

2. If (S, *) is semigroup and a ϵ S and T=ai i ϵ Z+} , then T is subsemigroup.

Furthermore if *e* identity element of (S, *) i.e., S is a monoid and we define a0 = *e* ,then T is a submonoid.