ELG 5372 Error Control Coding

Claude D'Amours

Lecture 3: Algebra (1): Groups, Subgroups and Cosets

Groups

- Let G be a set of elements and * is a binary operation defined on G such that for all elements a, $b \in$ G then $c = a * b$.
  - If c $\in$ G, for all a and b, then G is closed under the operation *.
  - For example, if G is the set of all real numbers, then G is closed under the real addition (+) operation.
  - Also, the operation is said to be associative if for a, b, c $\in$ G, then (a*b)*c = a*(b*c)

Definition of a Group

- The set G on which the binary operation * is defined is referred to as a group if the following conditions are met:
  - * is associative
  - G contains an identity element. In other words, for a, $e \in$ G, e is an identity element if $a * e = a$ for all a.
  - For any element $a \in$ G, there exists an inverse element $a' \in$ G such that $a * a' = e$.
- The groups is commutative if for any a, $b \in$ G, $a * b = b * a$

Examples

- G is the set of all real numbers under multiplication.
  - Multiplication is associative
  - $a \times 1 = a$ for all $a \in G$ and $1 \in G$.
  - $a \times (1/a) = 1$ and $1/a \in G$.

Example 2

- H is the set of all positive integers plus 0 under addition
  - Addition is associative
  - $a + 0 = a$, $0 \in H$.
  - $a + (-a)$, but $-a \notin H$.
  - Therefore H is not a group under addition.

Theorem 1

- The identity element of any group is unique

Theorem 2

- The inverse of a group element is unique.
  - For any element a, there exists only one inverse, a', such that $a*a' = e$.

Subgroups

- Let G be a group under the binary operation *. Let H be a nonempty subset of G. H is a subgroup of G if the following conditions are met:
  - H is closed under *. (property 1)
  - For any element $a \in$ H,

    the inverse of a, $a' \in$ H. (property 2)

Subgroups

- If H is a subgroup of G, then H is also a group on its own.
  - Since *a* and *a*' are elements of H, then *e* must be an element of H (property 1).
  - Since H is made up of elements in G, for which he associative property holds, it must also hold of H.

Example

- G is the set of all integers under addition.
  - G is a commutative group under addition.
- H is the set of all even integers under addition.
- All elements of H are in G.
- If a is in H, $-a$ is also in H.

Example 2

- Let H2 be the set of all odd integers under addition.
- Is H2 a subgroup of G?

Cosets

- Let H be a subgroup of a group G under the binary operation *. Let a be any element in G.
  - Then the set of elements $a*\mathrm{H}$ which is defined as $\{a*h : h \in \mathrm{H}\}$ is called a left coset of H and
  - the set of elements $\mathrm{H}*a$ which is defined as $\{h*a : h \in H\}$ is called a right coset of H.

Example

- G = {0, 1, 2, 3, 4, 5} under modulo-6 addition is a group.
- Let H = {0, 2, 4}
- Let *a* = 1
- (*a*+H)mod6 = {1, 3, 5} is a left coset of H. (H + *a*)mod6 = {1, 3, 5} is a right coset of H.
- If, for the same *a*, the left and right cosets are equal, then G must be a commutative group. In this case, we don’t refer to cosets as being left or right cosets. They are simply referred to as cosets of H.
- (setting *a* = 2 or 4 produces H}
- (setting *a* = 3 or 5 produces (1+H)mod6)

Subgroup and its cosets

- A subgroup and its cosets are distinct and the union of a subgroup and its cosets form G.

Theorem 3

- Let H be a subgroup of G under *. No two elements in a coset of H are identical.

Theorem 4

- No two elements in different cosets of the subgroup H of a group G are identical.