E2 205 Error-Control Coding
Lecture 3

Scribe - Elizabath Peter

August 19, 2019

1 Mathematical Preliminaries

1.1 Groups

Definition: A group $(G, .)$ is a set G together with an operation, . under which

(i) $a,\, b \in G \implies a.b \in G$ CLOSURE

(ii) $a,\, b,\, c \in G \implies a.(b.c) = (a.b).c$ ASSOCIATIVE LAW

(iii) $\exists$ an element e such that
$a.e = e.a = a$ for all $a \in G$ IDENTITY ELEMENT

(iv) For every $a \in G$, $\exists$ an element a^{-1} such that
$a.(a^{-1}) = (a^{-1}).a = e$ INVERSE

Additionally, if the group is commutative, then

(v) $a.b = b.a$ for all $a,\, b \in G$

Commutative groups are also known as Abelian groups.
(Abel $\equiv$ Norwegian Mathematician)

Most of our groups will be Abelian.

Examples:

(i) $\{\mathbb{F}_2, +\}$

(ii) $\{\mathbb{F}_2^n, +\}$, + denotes componentwise addition.

For n=3

$$\mathbb{F}_2^n = \left\{ \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix} \right\}$$

$$\begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix} + \begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix} = \begin{bmatrix}a_1+b_1\\a_2+b_2\\a_3+b_3\end{bmatrix}$$

The above represents addition in $\mathbb{F}_2^3$ (XOR).

The identity element is

$$e = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

(iii) $\{\mathbb{Z}_n, .\}$

$\mathbb{Z}_n =$ "set of integers modulo n"

$= \{0, 1, ...(n-1)\}$

$a.b = Rem(\frac{a+b}{n})$

For n=4

$\mathbb{Z} = \{0, 1, 2, 3\}$

$e = 0$

Eg. $2.3 = 1$ $\{Rem(\frac{2+3}{4})\}$

(iv) $\{\mathbb{Z}_p^*, .\}$ p is prime

$\mathbb{Z}_p^* = \{$non-zero elements of $\mathbb{Z}_p\}$

$a.b = Rem(\frac{ab}{p})$

For $p = 5$

$\mathbb{Z}_p^* = \{1, 2, 3, 4\}$

$e = 1$

1.1.1 Extended Euclidean Division Algorithm(EDA)

Used for computing the GCD of two integers.

Examples:

(i) gcd(105,154)

Remainder	154	105	Quotient
154	1	0	
105	0	1	1
49	1	0	2
7	-2	3	7
0			

$gcd(105, 154) = 7.$
Therefore, $7 = (-2).154 + 3.(105)$

(ii) $(\mathbb{Z}_p^*, .)$
Let $a \in \mathbb{Z}_p^*$. To find a^{-1}, the extended EDA is used to compute the gcd of (a, p).

$$gcd(a, p) = u_1 a + u_2 p \qquad u_1, u_2 \in \mathbb{Z}$$

$$1 = u_1 a + u_2 p \qquad a \text{ and } p \text{ co-prime}$$

$$\therefore a^{-1} \text{ (mod p)} = u_1 \text{ (mod p)}$$

Eg. (i) $p = 5$ and $a = 2$
$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

Remainder	5	2	Quotient
5	1	0	
2	0	1	2
1	1	-2	2
0			

$$1 = 1.5 + (-2).2$$

$$\therefore 2^{-1} = -2 \text{ (mod 5)} = 3 \text{ (mod 5)} = 3$$

(ii) $p = 5$ and $a = 4$

Remainder	5	4	Quotient
5	1	0	
4	0	1	1
1	1	-1	4
0			

$$1 = 1.5 + (-1).4$$

$$\therefore 4^{-1} = -1 \pmod 5 = 4 \pmod 5 = 4$$

1.1.2 Derived Properties of a Group

(i) The identity element of group $(G, .)$ is unique.

Proof: Suppose e_1, e_2 are a pair of distinct identity elements. Then,

$$e_1.e_2 = e_1 \text{ and } e_1.e_2 = e_2$$

$$\therefore e_1 = e_2 \text{ (contradiction)}$$

(ii) The inverse a^{-1} of a is unique.

Proof: Suppose $ca = ac = e$ and $ba = ab = e$. Then,

$$cab = (ca)b = e.b = b$$

$$cab = c(ab) = e.c = c$$

$$\therefore b = c$$

(iii) $(ab)^{-1} = b^{-1}a^{-1}$

Proof:

$$\begin{aligned}(ab)^{-1} &= (ab)^{-1}.e\\ &= (ab)^{-1}.(aa^{-1})\\ &= (ab)^{-1}.(ae).a^{-1}\\ &= (ab)^{-1}.a(bb^{-1})a^{-1}\\ &= [(ab)^{-1}.(ab)]b^{-1}a^{-1}\\ &= e.(b^{-1}a^{-1})\\ \therefore (ab)^{-1} &= b^{-1}a^{-1}\end{aligned}$$

(iv) $(a^{-1})^{-1} = a$

(v) *Definition*: $a^m = \underbrace{a.a.a.....a}_{\text{m times}}$

Note: If $(a, +)$ is a group,

$$\underbrace{a + a + ...a}_{\text{m times}} = ma$$

1.2 Subgroups

Definition: A subgroup $(H, .)$ of a group $(G, .)$ is a subset H of G that forms a group on its own with respect to the same operator.
Eg: $(H, .) = (G, .)$, $(H, .) = (e, .)$. These two are trivial subgroups.

Given a subset H of G. How to test H for a subgroup?

(i) Brute Force Approach

- $a.b \in H, \forall\ a, b \in H$? CLOSURE
- $a(bc) = (ab)c, \forall\ a, b, c \in H$? ASSOCIATIVE LAW
- $e \in H$? IDENTITY ELEMENT
- $a^{-1} \in H, \forall\ a \in H$? INVERSES

Associative property is inherent. Hence, it suffices to check for the remaining properties.

(ii) Test for a subgroup
Claim: $H \subset G$, is a subgroup iff

$$ab^{-1} \in H \quad \text{for every } a, b \in H$$

Proof:

(i) Identity element

$$aa^{-1} \in H$$

$$\text{i.e, } e \in H$$

(ii) Inverse
Let $a = e$
Then, $ab^{-1} = eb^{-1} = b^{-1} \in H$

(iii) Closure
Let $x = a$ and $y = b^{-1}$
$xy^{-1} = a(b^{-1})^{-1} = ab \in H$

Claim: Let H be a finite subset of G. Then to show $H \subseteq G$ is a subgroup, it suffices to show that $a.b \in H$.
Proof: $H \subseteq (G, .)$. Let H be finite and $a \in H$. Then, $a^m = a^n$ for some $n > m$.

$$\underbrace{a^{-1}.a^{-1}....a^{-1}}_{\text{m times}})a^m = (\underbrace{a^{-1}.a^{-1}....a^{-1}}_{\text{m times}})a^n$$
$$\therefore e = a^{n-m}$$
$$\implies a^{n-m} = a.a^{n-m-1}$$
$$= a^{n-m-1}.a = e$$
$$\therefore a^{n-m-1} = a^{-1}$$

Examples

(i) $(G, .) = (\mathbb{Z}_6, +)$
$H = \{0, 2, 4\}$
$0 + 2 = 2$
$4 + 2 = 0 \pmod 6$

(ii) $(G, .) = (\mathbb{F}_2^7, +)$

$$H = \left\{ \begin{bmatrix} c_1 \\ c_2 \\ . \\ . \\ . \\ c_7 \end{bmatrix} : c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 = 0 \ (\text{mod}2) \right\}$$

=Single parity-check code
$|H| = 2^6 = 64$

$$H = \{\underline{c} \in \mathbb{F}_2^7 \;\mid\; \underline{1}^T c = 0\}$$

$$\underline{c_1}, \underline{c_2} \in H$$

To show: $\underline{c_1} + \underline{c_2} \in H$

$$\underline{c_1} \in H \implies \underline{1}^T \underline{c_1} = 0$$

$$\underline{c_2} \in H \implies \underline{1}^T \underline{c_2} = 0$$

$$\therefore 1^T(\underline{c_1} + \underline{c_2}) = 1^T \underline{c_1} + 1^T \underline{c_2} = 0 + 0 = 0$$

$$\therefore \underline{c_1} + \underline{c_2} \in H, \text{ for all } \underline{c_1}, \underline{c_2} \in H$$

$\therefore (H, +)$ is a subgroup

1.2.1 Cosets of a Code

The space under consideration is $\mathbb{F}_2^7$. The trivial coset of a code is the code itself.
(i) Single-Parity Check code
The odd-parity vectors form the coset of the code and it is non-linear.

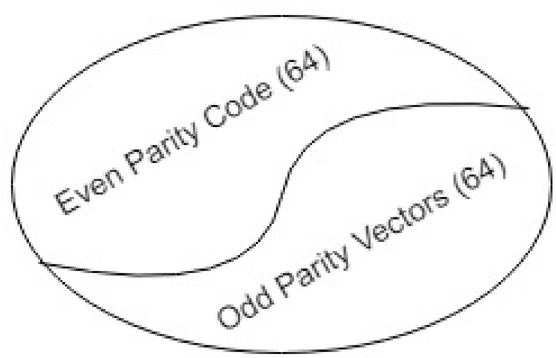

Figure 1: Partition of space by Single-Parity Check code

(ii) Hamming Code
There are 16 codewords. The space is partitioned into eight and each set has the same number of elements. Including the code, there are eight cosets.

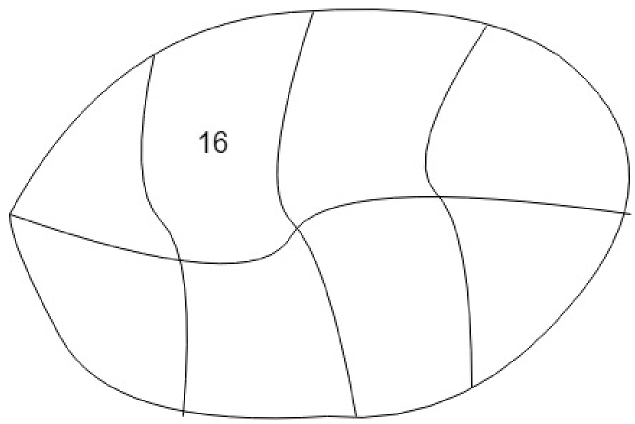

Figure 2: Partition of space by Hamming code

1.3 Equivalence Relation

Definition: Let A be a set. A relation R on a set A, is simply any subset R of

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

$A \times A$ represents the Cartesian product of A.
An equivalence relation on A is a relation R that satisfies:

(i) $(a, a) \in R$ REFLEXIVE

(ii) $(a, b) \in R \implies (b, a) \in R$ SYMMETRIC

(iii) $(a, b) \in R$, $(b, c) \in R \implies (b, c) \in R$ TRANSITIVE

The notion $a \sim b$ is commonly used instead of $(a, b) \in R$.
E_a : set of all elements that are equivalent to a, i.e, the EQUIVALENCE CLASS of a.

Claim: $a, b \in A \implies E_a \cap E_b = \phi$ or $E_a = E_b$.
Thus distinct equivalence classes are pairwise disjoint.

Proof: Suppose $E_a \cap E_b \neq \phi$. Let $x \in (E_a \cap E_b)$. Then,

$$a \sim x \quad \text{and} \quad b \sim x \implies x \sim b$$

$$\implies a \sim b$$

Let $y \in E_b \implies b \sim y \implies a \sim y$

$$\therefore y \in E_a$$

$$\therefore E_b \subseteq E_a$$

We can similarly show that $E_a \subseteq E_b$.

$$\therefore E_a = E_b$$