E2 205 Error-Control Coding
Lecture 5

Scribe: Krishnan Namboodiri K K

August 26, 2019

Note: Subspaces and Subgroups

a) Let $(V, +)$ be a group and $W \subseteq V$. Then W is a subgroup of V if and only if $x - y \in W$, $\forall x, y \in W$.

b) Suppose $(V, +, \mathbb{F}, \cdot)$ is a vector space. Then $W \subseteq V$ is a subspace of V if and only if $\underline{x} + c\underline{y} \in W$, $\forall \underline{x}, \underline{y} \in W$ and $c \in \mathbb{F}$.

Consider the case where $V = \mathbb{F}_2^n$ and $\mathbb{F} = \mathbb{F}_2$. Then $W \subseteq \mathbb{F}_2^n$ is a subgroup of V if and only if $\underline{x} + \underline{y} \in W$, $\forall \underline{x}, \underline{y} \in W$.
On the other hand, $W \subseteq \mathbb{F}_2^n$ is a subspace of $(\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$ if and only if $\underline{x} + \underline{y} \in W$. Thus for the case $V = \mathbb{F}_2^n$, $\mathbb{F} = \mathbb{F}_2$, a subgroup of $(\mathbb{F}_2^n, +)$ is also a subspace of $(\mathbb{F}_2^n, +, \mathbb{F}_2, \cdot)$ and vice versa.

1 Column space, Row space and Nullspace

Let $A \in \mathbb{F}^{m \times n}$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} a_1^t \\ a_2^t \\ \vdots \\ a_m^t \end{bmatrix} \qquad \text{where } a_i = \begin{bmatrix} a_{i1} \\ a_{i2} \\ \vdots \\ a_{in} \end{bmatrix}$$

Definition 1 *Row space of A is defined as, $Row(A) = \{\sum_{j=1}^{m} c_j \underline{a_j^t} \mid c_j \in \mathbb{F}\}$.*

That is, every element in the row space of a matrix can be written as some linear combination of the rows of that matrix.
Similarly, A can be written as

$$A = \begin{bmatrix} b_1 & b_2 & \dots & b_n \end{bmatrix} \qquad \text{where } b_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{bmatrix}$$

Then,

Definition 2 *Column space of A is defined as, $Col(A) = \{\sum_{j=1}^{n} c_j \underline{b_j} \mid c_j \in \mathbb{F}\}$.*

$Col(A)$ lies in the span of the columns of A.

Exercise: Verify that $Row(A)$ is a subspace of $\mathbb{F}^n$. Also, verify $Col(A)$ is a subspace of $\mathbb{F}^m$.
Let $A \in \mathbb{F}^{m \times n}$ and $\underline{p}$, $\underline{q} \in Col(A)$.
That means, there exist two elements $\underline{x}, \underline{y} \in \mathbb{F}^n$ such that $A\underline{x} = \underline{p}$ and $A\underline{y} = \underline{q}$.
And, $\underline{p} + c\underline{q} = A\underline{x} + cA\underline{y} = A(\underline{x} + c\underline{y})$ for any $c \in \mathbb{F}$.
$\Rightarrow \underline{p} + c\underline{q} \in Col(A) \Rightarrow Col(A)$ is a subspace of $\mathbb{F}^m$.
$Row(A)$ is the $Col(A^t)$. So, similarly we can show that $Row(A)$ is a subspace of $\mathbb{F}^n$.

Definition 3 *Nullspace of A is defined as, $\mathcal{N}(A) = \{\underline{x} \in \mathbb{F}^n \mid A\underline{x} = 0\}$.*

If $\underline{x}, \underline{y} \in \mathcal{N}(A)$, then $A\underline{x} = 0, A\underline{y} = 0$. Then, $A(\underline{x} + c\underline{y}) = A\underline{x} + cA\underline{y} = 0 + 0 = 0 \Rightarrow \underline{x} + c\underline{y} \in \mathcal{N}(A)$. Which means, $\mathcal{N}(A)$ is a subspace of $\mathbb{F}^n$.

2 Linear Codes

A binary linear code $\mathscr{C}$ of block length n is any subspace of $\mathbb{F}_2^n$ (Thus a binary linear code $\mathscr{C}$ may also be viewed as a subgroup of $\mathbb{F}_2^n$ and for this reason, binary linear codes are sometimes referred as group codes).
Examples

i) Let $\mathscr{C}$ be the simple parity check code of block length $n = 7$. Then $\mathscr{C}$ is a linear code because $\underline{c} \in \mathscr{C}$ if and only if $\underline{1}^t\underline{c} = 0 \Leftrightarrow \sum_{t=1}^{7} c_t = 0$
ie, if $\underline{c_1}, \underline{c_2} \in \mathscr{C}$, then $\underline{1}^t\underline{c_1} = 0, \underline{1}^t\underline{c_2} = 0$
$\underline{1}^t(\underline{c_1} + \underline{c_2}) = \underline{1}^t\underline{c_1} + \underline{1}^t\underline{c_2} = 0 + 0 = 0$

ii) The repetition code of block length $n = 7$ is also a linear code. $\mathscr{C} = \{\underline{0}, \underline{1}\}$

iii) The Hamming code, $n = 7$
For a code word $\underline{c} = [c_0, c_1, c_2, c_3, c_4, c_5, c_6]^t$ in Hamming code,$\mathscr{C}$, in

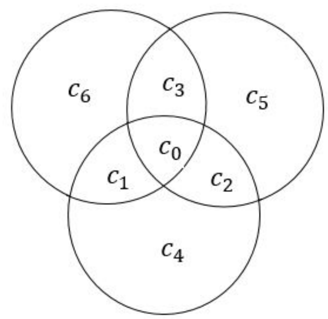

Figure 1: Hamming code: Even parity in all the three circles

each circle, even parity has to be maintained. So we can create a matrix H such that every code word will lie in the nullspace of H.

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

For every codeword $\underline{c} \in \mathscr{C}$, $H\underline{c} = 0$, H is called the parity check matrix for Hamming code.
Let $\underline{c_1}$ and $\underline{c_2}$ are codewords in $\mathscr{C}$. Then
$H(\underline{c_1} + \underline{c_2}) = H\underline{c_1} + H\underline{c_2} = 0 + 0 = 0 \Rightarrow \mathscr{C}$ is linear.

2.1 Linear independence, Basis and Dimension

Definition 4 *Let $(V, +, \mathbb{F}, \cdot)$ be a vector space. Then $\underline{\alpha_1}, \underline{\alpha_2}, \ldots, \underline{\alpha_n} \in V$ are said to be linearly independent if and only if $\sum_{j=1}^{n} c_j \underline{\alpha_j} = \underline{0}$ is possible only with $c_j = 0, \forall j$.*

Examples

i) Characterize all linearly independent subsets of $\mathbb{R}^3$.
Any three non-coplanar vectors are linearly independent in $\mathbb{R}^3$. We cannot find more than 3 independent vectors in $\mathbb{R}^3$.

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\} \text{ are independent}$$

.

ii) Let $A \in \mathbb{R}^{4\times5}$. Which rows of A are linearly independent? Which columns of A are linearly independent?

$$A = \begin{bmatrix} 1 & 0 & 2 & 1 & 3 \\ 0 & 0 & 6 & 1 & 7 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Ans: The given matrix A is in row echelon form. The first non-zero entry in each row(in echelon form) is called a pivot. Rows containing pivots are linearly independent. Columns containing pivots are also linearly independent. So in matrix A, 3 linearly independent rows are there(first, second and third rows are linearly independent). Similarly, there are 3 linearly independent columns as well(First, third/fourth and fifth columns are linearly independent).

iii) Consider the vector space, $V = \mathbb{F}[X]$, the collection of all the polynomials over the field $\mathbb{F}$. Verify, $\alpha_1(x) = x + a$, $\alpha_2(x) = x^2 + bx + c$, $\alpha_3(x) = x^5$ are linearly independent.
Ans: Take any three elements $c_1, c_2, c_3 \in \mathbb{F}$.
$c_1\alpha_1(x) + c_2\alpha_2(x) + c_3\alpha_3(x) = 0$
$c_1(x + a) + c_2(x^2 + bx + c) + c_3(x^5) = 0 \Rightarrow c_3 = 0, c_2 = 0, c_1 = 0$
Therefore, $\alpha_1(x), \alpha_2(x)$ and $\alpha_3(x)$ are linearly independent.

2.1.1 Span of a set

Definition 5 *A set* $\{\underline{\alpha_1}, \underline{\alpha_2}, \ldots, \underline{\alpha_n}\} \subseteq V$ *is said to span* V *if*
$V = \{\sum_{j=1}^{n} c_j\underline{\alpha_j} \mid c_j \in \mathbb{F}\}$
And it is written as $V \triangleq < \underline{\alpha_1}, \underline{\alpha_2}, \ldots, \underline{\alpha_n} >$ *(Notation)*

Examples

i) $\alpha_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ $\alpha_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$. Then $< \alpha_1, \alpha_2 > = \mathbb{R}^2$

ii) What is the space over $\mathbb{F}_2$, spanned by

$$A = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

.

Ans: All the elements in the set are of even parity. ie, for each $\alpha_i \in A$, $\underline{1}^t \alpha_i = 0$. And the span of these elements are single parity check code with $n = 7$.

2.1.2 Basis

Definition 6 *A basis B for a vector space $(V, +, \mathbb{F}, \cdot)$ is a collection of vectors that*

1) are linearly independent

2) span V

Examples

i)

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\} \text{ is a basis for } \mathbb{R}^3.$$

Infact, any three non-coplanar vectors in $\mathbb{R}^3$ can be a basis for $\mathbb{R}^3$. So, it is important to note that, basis for any space is not a unique set.

ii) Conisder the space of all polynomials, $(\mathbb{F}[X], +, \mathbb{F}, \cdot)$.
The set $A = \{1, X, X^2, \ldots\}$ is a basis for $\mathbb{F}[X]$. But, the cardinality of the basis is not finite.

A vector space is said to be finite dimensional if it has a basis consisting of a finite number of elements.
Let V be a finite dimensional vector space having basis, $B = \{\underline{\alpha_1}, \underline{\alpha_2}, \ldots, \underline{\alpha_n}\}$. Then,

a) Any collection of $m > n$ vectors drawn from V is linearly dependent.

b) Any collection of $m < n$ vectors from B cannot span V.

It follows that if V is finite dimensional, any two bases for V have the same size.
The common size of a basis for a finite dimensional vector space V is called the **dimension** of V.