E2 205 Error-Control Coding
Lecture 6

Sanjhi Gupta

August 28, 2019

1 Linear Independence

Let (V,+,$\mathbb{F}$,.) be a vector space. Let A = $\{\underline{\alpha}_1, \underline{\alpha}_2, \ldots\ldots\}$ be a (possibly infinite) set of vectors drawn from V.
By "a Linear Combination of Vectors from A" we mean terms of the form:

$$\sum_{j=0}^{n} c_{i_j} \underline{\alpha}_{i_j}, \qquad c_{i_j} \in \mathbb{F}, \ \ j = 1, 2, \ldots, n, \ \ n \geq 1 \text{ is an integer.}$$

We say that A is a linearly independent set if for any finite collection

$$\{\underline{\alpha}_{i_j} \in A \mid j = 1, 2, \ldots, n\},$$

we have that

$$\sum_{i=0}^{n} c_{i_j} \underline{\alpha}_{i_j} = 0 \ \text{ iff } c_{i_j} = 0 \text{ for all } j = 1, 2, \ldots, n.$$

We say that A spans V, if given a vector $\underline{v} \in V$, there exist $\{\underline{\alpha}_{i_j} \in A \mid j = 1, 2...n\}$ for some integer $n \geq 1$ such that

$$\underline{v} = \sum_{j=1}^{n} c_{i_j} \underline{\alpha}_{i_j}.$$

The space spanned by A is the set

$$\left\{ \sum_{j=0}^{n} c_{i_j} \underline{\alpha}_{i_j} \mid c_{i_j} \in \mathbb{F} \ , \ j = 1, 2, \ldots, n, \ \underline{\alpha}_{ij} \in A \right\}$$

Example 1 *Consider the vector space* $(\mathbb{F}[X], +, \mathbb{F}, .)$ *and set* $A = \{1, x, x^2.....\}$ *then*

- *the elements of set* A *are linearly independent,*
- *the elements of set* A *span* $\mathbb{F}[X]$.

2 Basis

Definition 2 *A basis B for a vector space (V,+,*$\mathbb{F}$*,.) is a collection of vectors* $\{\underline{\alpha}_1, \underline{\alpha}_2, \dots\}$ *such that:*

1. *the set is a linearly independent set,*
2. *the set spans the vector space V.*

2.1 Does every vector space have a basis?

1. If V is finitely generated, i.e, V is of the form
$$V = < \underline{r}_1,\ \underline{r}_2\ .....\ \underline{r}_m >,$$
then this is clearly a yes.

2. In the general case, the answer is still yes but the proof relies upon *Zorn's Lemma* which is equivalent to the Axiom of Choice.

Lemma 3 *In our setting, Zorn's Lemma tells us that if* T *is a set,* $\mathcal{A}$ *is a collection of subsets of* T *and if for every chain of subset*

$$S_1 \subseteq S_2 \subseteq S_3 ...... \subseteq S_m ....,$$

the union $\cup_{j=1}^{\infty} S_j \in \mathcal{A}$ *, then* T *contains a maximal subset that is not contained in any other subset.*

Claim 4 *Every vector space has a basis.*

Proof: Let T be the vector space V, $\mathcal{A}$ be the collection of all linearly independent subsets S_j of V. Then for every chain

$$S_1 \subseteq S_2 \subseteq S_3 ...... \subseteq S_m ....,$$

the union $\cup_{j=1}^{\infty} S_j \in \mathcal{A}$. Thus T has a maximal linearly independent subset B.

Claim 5 *B is a basis of V.*

Proof: Clearly B is a linearly independent set. Now it remains to show that B spans V. Suppose it does not span V.
Let $\underline{x} \in V$ and $\underline{x} \notin <B>$.
This implies that $B \cup \{\underline{x}\}$ set contradicts that B is the maximal linearly independent subset. Hence B is the basis for V.

However, it is hard to construct a basis in general.

Example 6 *Vector space ($\mathbb{R}^\infty$,+,$\mathbb{R}$,.).*
$\underline{x} \in \mathbb{R}^\infty \Rightarrow \underline{x} = (x_1, x_2, \ldots, x_n, \ldots)$. *This is an ∞-dimensional space.*

3 Finite dimensional vector space

Definition 7 *A vector space is said to be finite dimensional if it contains a basis consisting of a finite number of elements.*

Theorem 8 *Let (V,+,$\mathbb{F}$,.) be a finite dimensional vector space. Then any two basis for V must contain the same number of elements.*

The proof will make use of following two lemmas.

Lemma 9 *If a vector space V has a basis consisting of m elements, then any collection of n>m elements is a linearly dependent set.*

Lemma 10 *If a vector space V has a basis consisting of n elements, then any collection of m<n elements cannot span the space.*

From these two lemmas, it follows that a basis is simultaneously:

1. a maximal linearly independent set
2. a minimal spanning set

Proof(Theorem 8): Let $\{\underline{\alpha}_1, \underline{\alpha}_2, \ldots, \underline{\alpha}_m\} = \{\underline{\beta}_1, \underline{\beta}_2, \ldots, \underline{\beta}_n\}$be two basis for the vector space V.
Since $\{\underline{\alpha}_1, \underline{\alpha}_2, \ldots, \underline{\alpha}_m\}$ form a basis and the set $\{\underline{\beta}_1, \underline{\beta}_2, , \ldots, \underline{\beta}_n\}$ is a linearly independent set, it follows that $n \leq m$.
Also, since $\{\underline{\alpha}_1, \underline{\alpha}_2, \ldots, \underline{\alpha}_m\}$ form a basis and the set $\{\underline{\beta}_1, \underline{\beta}_2, \ldots, \underline{\beta}_n\}$ span the vector space V, it follows that $n \geq m$.
$\therefore n = m$ if both are basis.

3.1 Dimension

Definition 11 *The dimension k of a finite dimensional vector space (V,+,$\mathbb{F}$,.) is the number of elements in any basis for the vector space.*

3.2 Dimension of a Linear Code

Definition 12 *The dimension of a binary linear code $\mathcal{C}$ of block length n is its dimension when viewed as a subspace of ($\mathbb{F}_2^n$,+,$\mathbb{F}$,.).*

4 Notation of Linear Code

A linear code is characterised by three parameters $[n, k, d_{min}]$ where :

* n is the block length,
* k is the dimension,
* d_{min} is the minimum Hamming distance between any two code words.

Therefore,
Size of a linear code = 2^k,
Rate of a linear code = $\frac{\log_2^{2^k}}{n} = \frac{k}{n}$.

Example 13 *Single Parity Check Code, n=7*

$$[n, k, d_{min}] = [7, 6, 2]$$

Example 14 *Repetition Code, n=7*

$$[n, k, d_{min}] = [7, 1, 7]$$

Example 15 *Hamming Code, n=7*

$$[n, k, d_{min}] = [7, 4, 3]$$

5 Generator Matrix

Definition 16 *Let $\mathcal{C}$ be an [n,k] binary code. Then a generator matrix G to $\mathcal{C}$ is any $(k \times n)$ matrix whose rows form a basis for $\mathcal{C}$.*

$$G = \begin{bmatrix} \underline{g}_1^t \\ \underline{g}_2^t \\ . \\ . \\ \underline{g}_k^t \end{bmatrix}$$

where $\{\underline{g}_1, \ \underline{g}_2, \ . \ .\underline{g}_k\}$ are a basis.

Note

1. A code can in general, have more than one generator matrix.
2. $\mathcal{C}$ is the rowspace of G.

Example 17 *For single parity check code, generator matrix can be given by:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Example 18 *For repetition code, generator matrix can be given by:*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Example 19 *For Hamming code, generator matrix can be given by:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

6 Dual Code

Definition 20 *The dual $\mathcal{C}^{\perp}$ of an [n,k] binary code $\mathcal{C}$ is the set :*

$$\mathcal{C}^{\perp} = \{\underline{y} \mid \underline{x}^t \underline{y} = 0, \quad all\ \underline{x} \in \mathcal{C}\}$$

Theorem 21 *If $G =$*

$$\begin{bmatrix} \underline{g}_1^t \\ \underline{g}_2^t \\ \cdot \\ \cdot \\ \underline{g}_k^t \end{bmatrix}$$

is any $(k \times n)$ generator matrix for $\mathcal{C}$, then the nullspace of generator matrix is precisely the dual code,i.e, $\mathcal{C}^{\perp} = \eta(G)$.

Proof: Clearly, from the definition of the dual code, it follows that if y $\in \mathcal{C}^{\perp}$

$$\Rightarrow \underline{g}_j^t \underline{y} = \underline{0} \qquad , all\ 1 \leq j \leq k$$

$$\therefore \underline{y} \in \eta(G)$$

$$\Rightarrow \mathcal{C}^{\perp} \subseteq \eta(G) \tag{1}$$

Next suppose $\underline{\mathrm{y}} \in \eta(G)$

$$\Rightarrow \underline{g}_j^t \underline{y} = \underline{0} \qquad , all\ 1 \leq j \leq k$$

If $\underline{x}$ is a codeword of $\mathcal{C}$, then $\underline{x} = \sum_{j=1}^{k} m_j \underline{g}_j$, $m_j \in \mathbb{F}_2$.

$$\Rightarrow (\sum_{j=1}^{k} m_j \underline{g}_j^t) \underline{y} = \underline{0}$$

$$\Rightarrow \underline{x}^t \underline{y} = \underline{0} \qquad , for\ all\ \underline{x} \in \mathcal{C}$$

$$\Rightarrow \underline{y} \in \mathcal{C}^{\perp}$$

$$\Rightarrow \eta(G) \subseteq \mathcal{C}^{\perp} \tag{2}$$

Therefore from equation (1) and (2) $\eta(G) = \mathcal{C}^{\perp}$

7 Parity Check Matrix

Definition 22 *A parity check matrix for an* $[n, k]$ *linear code* $\mathcal{C}$ *is any generator matrix for* $\mathcal{C}^{\perp}$

Theorem 23 *Let* H *be a parity check matrix for* $\mathcal{C}$*, then* $\mathcal{C} = \eta(H)$*.*

Proof:
Let H =

$$\begin{bmatrix} \underline{h}_1^t \\ \underline{h}_2^t \\ . \\ . \\ \underline{h}_{n-k}^t \end{bmatrix}$$

Let $\underline{\text{y}} \in \mathcal{C}$, then clearly from the definition of parity check matrix

$$\Rightarrow \underline{h}_j^t \underline{y} = \underline{0}$$

$$\therefore \underline{y} \in \eta(H)$$

$$\Rightarrow \mathcal{C} \subseteq \eta(H)$$

Also

$$dim(\mathcal{C}) = k$$

$$dim(\eta(H)) = n - (n - k) = k$$

$$\therefore \mathcal{C} = \eta(H)$$

Aside: Let A be any matrix, U is the row reduced echelon form of A. For example,

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

It follows that dimension of row space of A is equal to the dimension of column space of A which is further equal to the number of pivots in the row reduced echelon form U of A.

dim(Row Space of A)=dim(Column Space of A)=Number of pivots in U
The common dimension is called the rank of A.

Theorem 24 ***Fundamental Theorem of Linear Algebra*** *If A is an $(m \times n)$ matrix, then*
$rank(A) + dim(nullspace(A)) = n$ *, where n is the number of columns of A.*

Corollary 25 *The dual of the dual is the code itself,i.e,* $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

1. (Repetition code)$^{\perp}$ = (Single Parity Check Code)
2. (Single Parity Check Code)$^{\perp}$ = (Repetition code)

Theorem 26 *Let H be a* $(n - k \times n)$ *matrix such that*

1. *rank(H) = n-k,*
2. $\eta(H) = \mathcal{C}$,

then H is a parity check matrix for $\mathcal{C}$.

Proof: Consider the equation

$$\begin{bmatrix} \underline{h}_1^t \\ \underline{h}_2^t \\ . \\ . \\ \underline{h}_{n-k}^t \end{bmatrix} [\underline{x}] = \underline{0}$$

We know that

$$\underline{h}_j^t \underline{x} = \underline{0} \Rightarrow \underline{y}_j^t \underline{x} = \underline{0} \quad , \quad all\ x \in \mathcal{C} \ , \ \ \underline{y} \in RowSpace(H)$$

Clearly by the definition of the dual code

$$\Rightarrow RowSpace(H) \subseteq \mathcal{C}^{\perp}$$

But on the other hand, since the matrix H has rank = n-k, it follows that these vectors actually span the dual code and therefore the row space of H matrix is dual code.

$$dim(RowSpace(H)) \;=\; n-k$$

$$dim(\mathcal{C}^{\perp}) \;=\; dim(\eta(G)) \;=\; n-k$$

$$\therefore RowSpace(H) \;=\; \mathcal{C}^{\perp}$$

So, it follows that H is a generator matrix for $\mathcal{C}^{\perp}$ $\therefore$ H is a parity check matrix for $\mathcal{C}$.