EC5.102: Information and Communication

(Lec-6)

Channel coding-2

(17-March-2025)

Arti D. Yardi

Email address: arti.yardi@iiit.ac.in
Office: A2-204, SPCRC, Vindhya A2, 1st floor

Vector spaces

Preliminaries: Basics of vector spaces

- Vector space spanned by the given set of vectors
- A subspace of a vector space
- Linearly independent vectors
- Basis and dimension of a vector space
- Orthogonal subspaces

Understanding vector space

- What is a vector space?

  A space in which:
  - Any two vectors can be "added"
  - Or "scaled"

  ... **without leaving the space!**

  (Note: To define a vector space, we need a few more properties.)

- Examples: Which of the following are vector spaces?
  - X-Y plane
  - Positive quadrant of X-Y plane
  - $\mathcal{S} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$

Linear combination and vector space

- Linear combination of two vectors:

  For two vectors $v_1, v_2 \in \mathbb{R}^n$ consider the following two operations

  1. Multiply v_1 or v_2 by scalars $a_1, a_2 \in \mathbb{R}$: $a_1 v_1$ and $a_2 v_2$
  2. Add $a_1 v_1$ and $a_2 v_2$: $\underbrace{a_1 v_1 + a_2 v_2}_{\downarrow}$

  Linear combination of v_1 and v_2

- Vector space V **spanned** by vectors v_1 and v_2 is defined as

$$V := \left\{ v \in \mathbb{R}^n \text{ such that } v = a_1 v_1 + a_2 v_2 \text{ for some } a_1, a_2 \in \mathbb{R} \right\}$$
$$= \text{span}\{v_1, v_2\}$$

- Vector space spanned by k vectors $v_1, v_2, \ldots, v_k$:

$$V := \left\{ v \in \mathbb{R}^n \text{ s. t. } v = a_1 v_1 + a_2 v_2 + \ldots + a_k v_k \text{ for some } a_1, \ldots, a_k \in \mathbb{R} \right\}$$
$$= \text{span}\{v_1, v_2, \ldots, v_k\}$$

Subspace of a vector space

- A subspace of a vector space is a nonempty subset that satisfies the requirements of a vector space: Linear combinations stay in the subspace.

- Example:
  - Suppose $V = \text{span}\left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}\right\}$ and $W = \text{span}\left\{\begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\4\\0\end{bmatrix}\right\}$
  - Is W a subspace of V?
  - Consider a set $S = \left\{\begin{bmatrix}0\\0\\0\end{bmatrix}\right\}$. Is S a subspace of V?

- Questions:
  - What is the difference between a subspace and a subset?
  - $V = \text{span}\left\{\begin{bmatrix}1\\4.7\\-2\\3\end{bmatrix}, \begin{bmatrix}4\\33\\19\\-1.8\end{bmatrix}\right\}$, $W = \text{span}\left\{\begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\4\\0\end{bmatrix}\right\}$. Is W a subspace of V?

Linear independence

- Linear independence:

$$\begin{bmatrix} \{v_1, v_2, \ldots, v_n\} \text{ are said to} \\ \text{be linearly independent} \end{bmatrix} \text{ if } \begin{bmatrix} a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0 \text{ can happen} \\ \text{only when } a_1 = a_2 = \ldots = a_n = 0 \end{bmatrix}$$

- Interpretation in terms of null space:

$$\begin{bmatrix} \{v_1, v_2, \ldots, v_n\} \text{ are said to} \\ \text{be linearly independent} \end{bmatrix} \text{ if } \begin{bmatrix} \text{Nullspace of the matrix with } v_1, \ldots, v_n \\ \text{as columns contains only zero vector.} \end{bmatrix}$$

Towards defining a basis of a vector space

- Vector space V **spanned** by vectors $v_1, v_2, \ldots, v_n$ is defined as

$$V := \left\{ v \in \mathbb{R}^n \text{ s. t. } v = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \text{ for some } a_1, \ldots, a_n \in \mathbb{R} \right\}$$
$$= \text{span}\{v_1, v_2, \ldots, v_n\}$$

- Consider the following three vector spaces V, W, and U.

$$V = \text{span}\left\{ \underbrace{\begin{bmatrix}1\\0\\0\end{bmatrix}}_{v_1}, \underbrace{\begin{bmatrix}0\\1\\0\end{bmatrix}}_{v_2} \right\} \quad W = \text{span}\left\{ \underbrace{\begin{bmatrix}1\\0\\0\end{bmatrix}}_{w_1}, \underbrace{\begin{bmatrix}0\\1\\0\end{bmatrix}}_{w_2}, \underbrace{\begin{bmatrix}1\\1\\0\end{bmatrix}}_{w_3} \right\} \quad U = \text{span}\left\{ \underbrace{\begin{bmatrix}2\\0\\0\end{bmatrix}}_{u_1}, \underbrace{\begin{bmatrix}0\\3\\0\end{bmatrix}}_{u_2} \right\}$$

Vector spaces V, W, and U are the same!

- Observations:
  - w_3 can be written as linear combination of w_1 and w_2.
  - v_1 and v_2 are linearly independent, similarly u_1 and u_2.
- Is there any unique way of representing a given vector space? **No!**
- What could be unique? **Minimum number of vectors spanning vector space**

Definition: Basis for a vector space V

- (Definition) A basis of V is a set of vectors having the following properties:
  - Vectors are linearly independent
  - They span the space V
- **Examples:**
  - $\underbrace{\left\{ \underset{e_1}{\begin{bmatrix}1\\0\\0\end{bmatrix}}, \underset{e_2}{\begin{bmatrix}0\\1\\0\end{bmatrix}}, \underset{e_3}{\begin{bmatrix}0\\0\\1\end{bmatrix}} \right\}}_{\text{coordinate vectors: columns of identity matrix}}$ is a basis for the vector space $\mathbb{R}^3$.
  - Is $\left\{ \underset{e_1}{\begin{bmatrix}1\\0\\0\end{bmatrix}}, \underset{e_2}{\begin{bmatrix}0\\1\\0\end{bmatrix}}, \underset{v_3}{\begin{bmatrix}1\\1\\0\end{bmatrix}} \right\}$ a basis for $\mathbb{R}^3$? No! Why? e_1, e_2, and v_3 are not independent.
  - Is $\left\{ \underset{e_1}{\begin{bmatrix}1\\0\\0\end{bmatrix}}, \underset{e_2}{\begin{bmatrix}0\\1\\0\end{bmatrix}} \right\}$ a basis for $\mathbb{R}^3$? No! Why? e_1 and e_2 do not span $\mathbb{R}^3$.

Orthogonal subspaces

- (Definition) Orthogonal subspaces:

  Suppose V and W are subspaces of a vector space U. Then V and W are said to be orthogonal if

  $$v^T w = 0 \text{ for all } v \in V \text{ and } w \in W.$$

- Example: $V = \text{span}\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\}$ and $W = \text{span}\left\{ \begin{bmatrix} 0 \\ 0 \\ 4 \\ 5 \end{bmatrix} \right\}$.

  Are V and W are orthogonal subspaces?

- Do we need to check condition $v^T w = 0$ for all $v \in V$ and $w \in W$? Justify.

Preliminaries: Basics of vector spaces

- Vector space spanned by the given set of vectors
- A subspace of a vector space
- Linearly independent vectors
- Basis and dimension of a vector space
- Orthogonal subspaces

Our focus

Our focus

- Our focus: Vector space spanned by vectors over $\mathbb{F}_2 = \{0, 1\}$.
- Scalars can be either 0 or 1.
- Vector space V spanned by k vectors $v_1, v_2, \ldots, v_k$ where each $v_i \in \mathbb{F}_2^n$:

$$V := \left\{ v \in \mathbb{F}_2^n \text{ s. t. } v = a_1 v_1 + a_2 v_2 + \ldots + a_k v_k \text{ for some } a_1, \ldots, a_k \in \mathbb{F}_2 \right\}$$

- Questions:
  - Consider the following vector space.

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

  - Can you write V as a span of some vectors?

Self quiz

Self-quiz

- When do we say the set of k vectors $v_1, v_2, \ldots, v_k$, where each $v_i \in \mathbb{R}^n$ for $i = 1, 2, \ldots, k$, are linearly independent?

- Are the following set of vectors linearly independent?

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ -3 \\ 2 \end{bmatrix} \; v_2 = \begin{bmatrix} 0 \\ 1 \\ -5 \\ 4 \end{bmatrix} \; v_3 = \begin{bmatrix} 3 \\ -2 \\ 1 \\ -2 \end{bmatrix} \; v_4 = \begin{bmatrix} -4 \\ -6 \\ 1 \\ 5.2 \end{bmatrix} \; v_5 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

- Set of m vectors in $\mathbb{R}^n$ must be linearly dependent if $m > n$. True/False?

Self-quiz

- Write down the set of all possible vectors in the vector space V spanned the following set of vectors over $\mathbb{F}_2$.

$$V = \text{span}\left\{ \begin{bmatrix}1\\0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \right\}$$

  Are these vectors linearly independent? Justify your answer.

- What is the dimension of the following vector space? Write down a basis.

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

- Is $\mathbb{F}_2^3$ a vector space? Yes/No?

- Is there any connection between W and $\mathbb{F}_2^3$? Yes/No? If yes, what is the connection?

Introduction to binary linear block codes

What are channel codes?

Channel

Alice

Bob

Can Alice do “something” so that Bob is able to interpret her message possibly after doing “some processing”?

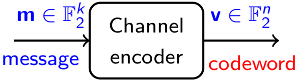
Recap

- Two channel models:
  - Binary erasure channel (BEC(ϵ))
  - Binary symmetric channel (BSC(p))
- Two channel codes:
  - Repetition codes (REP-n)
  - Single parity check codes (SPC-n)

Binary linear block codes

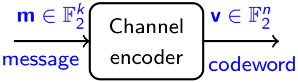
- Write down the set of codewords of REP-3 and SPC-3 codes.
- Is there any connection between $\mathbb{F}_2^3$ and codewords of REP-3/SPC-3 codes?
- Definition of a binary linear block code
- Basics of a binary linear block code $\mathcal{C}(n, k)$:
  - Definition
  - Length of a code: n
  - Size of a code: M
  - Dimension of a code: k
  - Rate of a code: R
- Block diagram of a channel encoder

Example of a channel code: Repetition code



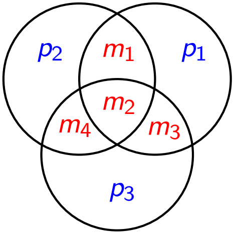
- k : Dimension of the code
- n : Length of the code
- For repetition code we have $k = 1$
- When $\mathbf{m} = 0$, codeword is $\mathbf{v} = [0, 0, \ldots, 0]$. Thus 0 is repeated n times for n-repetition code.
- When $\mathbf{m} = 1$, codeword is $\mathbf{v} = [1, 1, \ldots, 1]$.
- Rate $R = k/n$.

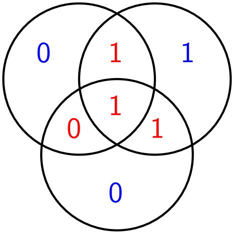
Example of a channel code: Single parity check code (SPC)

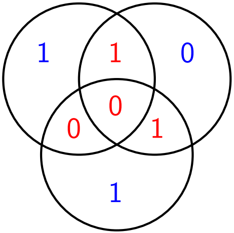


- For SPC code we have $n = k + 1$.
- SPC for $k = 2$ is given by
  - When $\mathbf{m} = [0\ 0]$, codeword is $\mathbf{v} = [0\ 0\ 0]$.
  - When $\mathbf{m} = [0\ 1]$, codeword is $\mathbf{v} = [0\ 1\ 1]$.
  - When $\mathbf{m} = [1\ 0]$, codeword is $\mathbf{v} = [1\ 0\ 1]$.
  - When $\mathbf{m} = [1\ 1]$, codeword is $\mathbf{v} = [1\ 1\ 0]$.
- Observe: n-th bit of $\mathbf{m}$ is modulo-2 sum of previous $(n-1)$-bits.
- Codeword $[v_0\ v_1\ \ldots\ v_{n-1}]$ is said to satisfy **one** parity check equation given by $v_0 + v_1 + \ldots + v_{n-1} = 0$. Hence the name single parity check code.
- Rate $R = (n-1)/n$. Codewords of an arbitrary linear block code satisfy many parity check equations. We shall study this in detail later.

Example of a channel code: Hamming code







- Suppose $m_1\ m_2\ m_3\ m_4$ are message bits.
- Parity p_1 is obtained using $m_1\ m_2\ m_3$ such that $m_1 + m_2 + m_3 + p_1 = 0$.
  Parity p_2 is obtained using $m_1\ m_2\ m_4$ such that $m_1 + m_2 + m_4 + p_2 = 0$.
  Parity p_3 is obtained using $m_2\ m_3\ m_4$ such that $m_2 + m_3 + m_4 + p_3 = 0$.
- Codeword is given by $[m_1\ m_2\ m_3\ m_4\ p_1\ p_2\ p_3]$
- Codeword-1: [1 1 1 0 1 0 0]
  Codeword-2: [1 0 1 0 0 1 1]

Designing binary linear block codes

- Do I always have to add parity bits at the end of message bits to get a codeword?
- Any subspace of $\mathbb{F}_2^n$ gives us a binary linear block code. What about any arbitrary code?
- For the given n and k, how many distinct linear block codes are possible?
- Why the name "binary" "linear" "block" codes?
- Is there any systematic method to represent a code?
- How to do encoding?