EC5.102: Information and Communication

(Lec-7)

Channel coding-3

(20-March-2025)

Arti D. Yardi

Email address: arti.yardi@iiit.ac.in

Office: A2-204, SPCRC, Vindhya A2, 1st floor

Summary of the last class

Recap

- Simple examples of channel codes:
  - Repetition codes (REP-n)
  - Single parity check codes (SPC-n)
  - Hamming code with $(n = 7, k = 4)$
- Arbitrary channel code
- Definition of binary linear block codes (LBC), denoted by $\mathcal{C}(n, k)$

Designing binary linear block codes

- Do I always have to add parity bits at the end of message bits to get a codeword?
- Think: Any subspace of $\mathbb{F}_2^n$ gives us a binary linear block 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?

Generator matrix of a linear block code

Generator matrix of a linear block code

- Is there any systematic method to represent a code?
- REP-3 code: $0 \to [0\ 0\ 0]$ and $1 \to [1\ 1\ 1]$

$$[0] \times \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$
$$[1] \times \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

- SPC-3 code: $[0\ 0] \to [0\ 0\ 0]$, $[0\ 1] \to [0\ 1\ 1]$, $[1\ 0] \to [1\ 0\ 1]$ and $[1\ 1] \to [1\ 1\ 0]$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$$

- In general, for any linear block code there exists a matrix G such that $\mathbf{u}G = \mathbf{v}$, i.e.,

$$\underbrace{\begin{bmatrix} u_0 & u_1 & \dots & u_{k-1} \end{bmatrix}}_{\mathbf{u}} \times \underbrace{\begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & & & \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}}_{G} = \underbrace{\begin{bmatrix} v_0 & v_1 & \dots & v_{n-1} \end{bmatrix}}_{\mathbf{v}}$$

- This matrix G is called as generator matrix of linear block code.

Generator matrix of a linear block code

- In general, for any linear block code we have $\mathbf{v} = \mathbf{u}G$, i.e.,

$$\begin{bmatrix} v_0 & v_1 & \dots & v_{n-1} \end{bmatrix} = \begin{bmatrix} u_0 & u_1 & \dots & u_{k-1} \end{bmatrix} \times \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & & & \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

$$\mathbf{v} = \begin{bmatrix} u_0 & u_1 & \dots & u_{k-1} \end{bmatrix} \times \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

$$\mathbf{v} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \ldots + u_{k-1}\mathbf{g}_{k-1}$$

- Does this look familier? $\mathbf{v}$ is a linear combination of $\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}$.
- A linear block code $\mathcal{C}$ is a subspace of vector space $\mathbb{F}_2^n$.
- Given the codebook $\mathcal{C}$, how to find generator matrix G? A set of k linearly independent vectors is chosen to be the rows of G: Basis

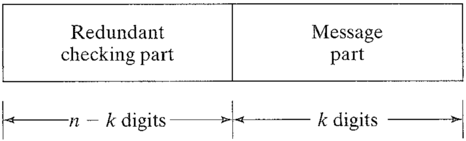
Generator matrix: Example

- Find the set of codewords of the linear block code with generator matrix G given by

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

Systematic generator matrix

- When all codewords can be written as a concatenation of message bits and parity check bits, then the linear block code is called as **systematic**.



- The generator matrix of a systematic linear block code can be written as

$$G = \left[\begin{array}{cccc|ccccc} p_{0,0} & p_{0,1} & \dots & p_{0,n-k-1} & 1 & 0 & 0 & \dots & 0 \\ p_{1,0} & p_{1,1} & \dots & p_{1,n-k-1} & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & & & & \\ p_{k-1,0} & p_{k-1,1} & \dots & p_{k-1,n-k-1} & 0 & 0 & 0 & \dots & 1 \end{array}\right]$$

$$G = \left[P \mid I_k\right]$$

- Is it necessary that a linear block code should be systematic always?

Generator matrix of Hamming code of length 7

- The set of codewords of the Hamming code of length 7 is given below. Find a generator matrix. Can you find a generator matrix with cyclic structure and a systematic generator matrix?

Codewords
(0 0 0 0 0 0 0)
(1 1 0 1 0 0 0)
(0 1 1 0 1 0 0)
(1 0 1 1 1 0 0)
(1 1 1 0 0 1 0)
(0 0 1 1 0 1 0)
(1 0 0 0 1 1 0)
(0 1 0 1 1 1 0)
(1 0 1 0 0 0 1)
(0 1 1 1 0 0 1)
(1 1 0 0 1 0 1)
(0 0 0 1 1 0 1)
(0 1 0 0 0 1 1)
(1 0 0 1 0 1 1)
(0 0 1 0 1 1 1)
(1 1 1 1 1 1 1)

Efficient representation of a linear block code

- A linear block code can be represented efficiently using a generator matrix.
- Can we represent a given code efficiently using any other method? Yes
  - A linear block code can be represented efficiently using a parity check matrix (to be studied next).
  - For cyclic codes one can represent codewords using polynomials and represent a cyclic code using a generator polynomial.
  - BCH codes, which is a subclass of cyclic codes. BCH codes can be represented using the roots of the generator polynomial.
  - Convolutional codes are represented efficiently using shift registers.
  - Turbo codes are represented efficiently using shift registers.
  - Low-density parity-check (LDPC) codes are represented efficiently using bipartite graphs.