EC5.102: Information and Communication

(Lec-8)

Channel coding-4

(24-March-2025)

Arti D. Yardi

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

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

Announcements

- No class on 27-March-2025 (Next class), make-up class was conducted on 5-March-2025
- Quiz-2: 3rd April, Thursday, During class time
- Syllabus for Quiz-2: Post mid-sem topics till today
- We will post an assignment by tonight
- Assignment submission deadline: 2-April-2025, 11pm (A day before Quiz-2)

Summary of the last class

Recap

- Definition of binary linear block codes (LBC), denoted by $\mathcal{C}(n, k)$
- Generator matrix $G \in \mathbb{F}_2^{k \times n}$ of $\mathcal{C}(n, k)$
  - Rows of generator matrix G are a basis of $\mathcal{C}(n, k)$
  - Any generator matrix G for the given codebook $\mathcal{C}(n, k)$
  - Find generator matrix G when the codebook $\mathcal{C}(n, k)$ and the corresponding messages are given
  - Encoding: $\mathbf{v} = \mathbf{u}G$
  - Systematic generator matrix
- Today: How to represent the same codebook $\mathcal{C}(n, k)$ using "parity check matrix", denoted by H

Parity check matrix a linear block code

Towards defining a parity check matrix

- Consider the LBC generated by the following generator matrix G.

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

- Claim: Any codeword $\mathbf{v} = \begin{bmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 \end{bmatrix}$ satisfies the following three parity check equations.
  - $v_0 + v_4 + v_5 = 0$
  - $v_1 + v_3 + v_5 = 0$
  - $v_2 + v_3 + v_4 = 0$

- Can I define a code using the set of parity check equations it satisfies?

Towards defining a parity check matrix

- Generator matrix: $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

- Any codeword $\mathbf{v} = \begin{bmatrix} v_0 & v_1 & \dots & v_{n-1} \end{bmatrix}$ satisfies: $v_0 + v_4 + v_5 = 0$, $v_1 + v_3 + v_5 = 0, v_2 + v_3 + v_4 = 0$.

- Can you find any other parity check equation?

- Can you find any other linearly independent parity check equation?

- Write $\mathbf{h}_0, \mathbf{h}_1, \mathbf{h}_2$ and parity check matrix H.

- Can you identify a relationship between G and H?

- Can you relate this to orthogonal subspaces?

Parity check matrix a linear block code

- Codewords of a code $\mathcal{C}(n, k)$ can also be represented using a parity check matrix H of size $(n-k) \times n$. Suppose H is given by

$$H = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{bmatrix}$$

  where each $\mathbf{h}_i$ is a row vector of length n.

- Any codeword $\mathbf{v} \in \mathcal{C}$ satisfies $\mathbf{v}\mathbf{h}_i^T = 0$. $\mathbf{v}\mathbf{h}_i^T = 0$ means $\mathbf{v}$ satisfies the parity check equation $\mathbf{h}_i$. Hence the name parity check matrix.

- **Alternative definition of a LBC $\mathcal{C}(n, k)$:**

  A LBC $\mathcal{C}(n, k)$ consists of all possible vectors in $\mathbb{F}_2^n$ that satisfies all parity check equations given by H, i.e.,

$$\mathcal{C}(n, k) = \left\{ \mathbf{v} \in \mathbb{F}_2^n \;\middle|\; \mathbf{v}\mathbf{h}_i^T = 0 \text{ for } i = 0, 1, \ldots, n-k-1 \right\}$$

Parity check matrix of a systematic linear block code

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

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

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

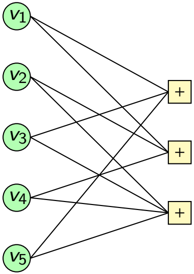
- The parity check matrix of a systematic linear block code can be written as

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

$$H = \left[I_{n-k} \mid P^T\right]$$

- Why???

Tanner graph representation of a parity check matrix



$c_1 \rightarrow \; v_1 + v_3 + v_5 = 0$

$c_2 \rightarrow \; v_1 + v_2 + v_4 = 0$

$c_3 \rightarrow \; v_2 + v_3 + v_4 + v_5 = 0$

- Parity check matrix is given by

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

Self-quiz

- Consider a systematic code of length 8 and dimension 4 whose parity check equations are:

$$p_0 = u_1 + u_2 + u_3$$
$$p_1 = u_0 + u_1 + u_2$$
$$p_2 = u_0 + u_1 + u_3$$
$$p_3 = u_1 + u_2 + u_3$$

where u_0, u_1, u_2, u_3 are message bits and p_0, p_1, p_2, p_3 are parity bits. Find the generator and parity check matrices for this code.

Dual of a LBC $\mathcal{C}(n, k)$

Dual of a LBC $\mathcal{C}(n, k)$

- Let us denote LBC $\mathcal{C}(n, k)$ by $\mathcal{C}$.
- Dual of $\mathcal{C}$: The dual code of $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$ consists of all vectors $\mathbf{w} \in \mathbb{F}_2^n$ such that $\mathbf{w}\mathbf{v}^T = 0$ for all $\mathbf{v} \in \mathcal{C}$.
- Codewords of $\mathcal{C}^{\perp}$ are "orthogonal" to codewords in $\mathcal{C}$.
- Example: Find $\mathcal{C}^{\perp}$ of REP-3 code. Do you observe anything special?
- Let G be a generator matrix of $\mathcal{C}$. Can you see the following?

$$\mathcal{C}^{\perp} = \left\{ \mathbf{w} \in \mathbb{F}_2^n \middle| \mathbf{w} G^T = 0 \right\}$$

Dual of a LBC

- Consider a LBC $\mathcal{C}$ with generator matrix G and parity check matrix H.

$$G = \begin{bmatrix} \leftarrow \mathbf{g}_0 \rightarrow \\ \leftarrow \mathbf{g}_1 \rightarrow \\ \vdots \\ \leftarrow \mathbf{g}_{k-1} \rightarrow \end{bmatrix}_{k \times n} \qquad H = \begin{bmatrix} \leftarrow \mathbf{w}_0 \rightarrow \\ \leftarrow \mathbf{w}_1 \rightarrow \\ \vdots \\ \leftarrow \mathbf{w}_{n-k-1} \rightarrow \end{bmatrix}_{n-k \times n}$$

- $\mathcal{C} = \text{span}\{\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}\}$
- $\mathcal{C}^{\perp} = \text{span}\{\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{n-k-1}\}$
- We refer $(\mathcal{C}, \mathcal{C}^{\perp})$ as a dual pair.

Hamming codes

Hamming codes: Introduction

- Consider the following generator matrix of Hamming code of length 7 and dimension 4

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

- Write down parity check matrix of this code.

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

- Do you notice anything special about this parity check matrix H?

Hamming code of length n

- Hamming codes will always have length $n = 2^m - 1$, where m is a positive integer such that $m \geq 3$.
- Consider the set of vectors of length m that correspond to binary representation of decimal numbers $1, 2, \ldots, 2^m - 1$.
- Parity check matrix of the Hamming code of length $n = 2^m - 1$ is obtained by considering these vectors as its columns.
- Parity check matrix of Hamming code with $m = 3$ is given by

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

- What will be the dimension of Hamming code with parameter m?

Hamming code of length n

- The parameters of a Hamming code are:
  - Consider an integer $m \geq 3$
  - Number of parity check equations $n - k = m$
  - Length of the code $n = 2^m - 1$
  - Dimension of the code $k = 2^m - m - 1$
  - Error correcting capability $t = 1$ (We will see this soon)

Homework

- Write down parity check matrix of Hamming code of length 15.
- Can you write systematic parity check matrix?
- Can you write down parity check matrix such that each row is a cyclically shifted version of the previous row?

Summary: Basics of binary linear block codes

Summary

- Binary linear block codes: Definition, Generator matrix, Parity check matrix
- Examples:
  - REP$(n, k = 1)$
  - SPC$(n, k = n - 1)$
  - Hamming$(n = 2^m - 1, k = 2^m - m - 1)$ where $m \geq 3$.
- How to design "nice" generator matrices?
- "nice": Rich structural properties, Cyclic property, Easy to encode, Easy to decode, Suitable for some application and so on...
- Examples: Cyclic codes, Reed-Solomon codes, BCH codes, LDPC codes, Convolutional codes, and many more...