Computer Networks

Linear Block Code

Fall 24-25, CS 3204, Section A

Dr. Nazib Abdun Nasir

Assistant Professor, CS, AIUB

nazib.nasir@aiub.edu

January 12, 2025

Outline

- Linear Block Code
- Parameters of LBC
- Mathematical Representation of LBC
- Generating the Generator Matrix
- Generating the Parity Check Matrix
- Example: (7, 4) Hamming Code

Linear Block Code

- Linear block codes are a fundamental concept in coding theory, primarily used for error detection and correction in digital communications.

- These codes allow the efficient transmission of data over noisy channels by adding redundancy to the original message.

- A linear block code is defined as an error-correcting code where any linear combination of *codewords* is also a *codeword*.
  - → This property allows for effective encoding and decoding processes.

Parameters of LBC

- **Length (n):** The total number of bits in each codeword.
- **Dimension (k):** The number of information bits in the original message.
- **Redundancy (r):** The number of parity bits added, calculated as $r = n - k$.
- **Code Rate (R):** The rate of a code is given by $R = k / n$, representing the ratio of information bits to total bits.

Mathematical Representation of LBC

- **Generator Matrix (G):** This matrix is used to generate codewords (*c*) from datawords (*d*) – a row vector.

  → $\boldsymbol{c = dG}$

- **Parity Check Matrix (H):** This matrix helps in error detection and correction. It is derived from the generator matrix and satisfies the following equation.

  → $\boldsymbol{Hc^T = 0}$ $\boldsymbol{c^T}$ is the transpose of the codeword vector.

Generating the Generator Matrix

- $G=[I_k|P]$; Alternate append is also valid. $G=[P|I_k]$;

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

  - → I_k is the identity matrix of size k×k (in this case, k=4).
  - → P is the parity matrix that contains information about how the parity bits are derived from the data bits.
  - → **Generator Matrix:** Combining I_k and P, we get:

$$G = [I_4|P] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Generating the Parity Check Matrix

- $H=[P^T|I_r]$
  - → P^T is the transpose matrix of P.
  - → r = 3;

$$P^T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

- **Parity Check Matrix (H):**

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

  - → These examples all use different parity matrices, and they are not related.

Example: (7, 4) Hamming Code

- Let's consider a specific example of a linear block code known as the Hamming code, which is designed to detect and correct single-bit errors.
- **Define Parameters:** For a (7, 4) Hamming code:
  - → $n=7$: Total bits in the codeword.
  - → $k=4$: Number of information bits.
  - → $r=n-k=3$: Number of parity bits.

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

- **Generator Matrix:** The generator matrix ***G*** for this code can be represented using the identity and parity matrices like this: $G=[I_k|P]$.

Example: (7, 4) Hamming Code

- **Encoding Process:** To encode a dataword, say d=[1,0,1,1], we multiply it by the generator matrix.

$$c = dG = [1,0,1,1]\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\0 & 1 & 0 & 0 & 1 & 0 & 1\\0 & 0 & 1 & 0 & 0 & 1 & 1\\0 & 0 & 0 & 1 & 1 & 1 & 1\end{bmatrix}$$

$$c = [1,0,1,1,0,1,1].$$

- **Parity Check Matrix:** The parity check matrix ***H*** can be derived from $[P^T|I_r]$.

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

- **Error Detection and Correction**
  - → When a transmitted codeword is received with potential errors due to noise in the channel, the received vector can be checked using the parity check matrix.
  - → $s = Hc^T$, where s is the syndrome vector, c^T is the transpose of the codeword c;
  - → if s ≠ [000], it indicates an error. How do we correct the error?

References

- Online Website Research
- 4. Linear Block Code - Provided Materials