Tutorial: Channel Coding

EC5.102: Information & Communication

Arti Yardi

March 26, 2025

---

1. Find the systematic generator matrix G and the parity check matrix H for the following linear block codes:
   (a) the $(n, k = 1)$ repetition code
   (b) the $(n, k = n - 1)$ single parity code
   (c) the $(n = 7, k = 4)$ Hamming code

2. Find the expressions for the parity bits and write the parity check matrix H for the $(n = 2^m - 1, k = 2^m - m - 1)$ Hamming code, for $m = 4$.

3. Find the relation between generator matrix G and parity check matrix H for a linear block code.

4. Consider the linear code defined by the generator matrix $G = \left(I_k \mid \mathbf{1}\right)$, where $\mathbf{1}$ denotes an all-one column vector of length k.
   (a) What is the dimension and rate of this code?
   (b) Describe the set of all codewords of this code. Obtain the codewords corresponding to the message vector $(1, 0, 1, 0, \dots, 0)$ of length k. (Note: The ellipsis '$\dots$' here denotes 0 sequence, as it is sandwiched between two 0s).
   (c) What are the set of parity check equations for this code? Obtain a parity check matrix of this code.

5. Consider a linear code defined by the parity check matrix $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$.
   (a) What is the rate of this code?
   (b) Find a generator matrix for this code.
   (c) List the codewords for this code.

Solutions

1. Find below $G = [I_k \mid A]$ for each part; write $H = [A^T \mid I_{n-k}]$.

   (a) For the $(n, 1)$ repetition code, $G = \underbrace{(1 \mid 1 \quad \ldots \quad 1)}_{n \text{ times}}$.

   (b) For the $(n, n-1)$ single parity code, $G = (I_n \mid \mathbf{1}_n)$, where $\mathbf{1}$ is an all-one column vector. For example, for $n = 3$, $G = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right)$.

   (c) For the $(7, 4)$ Hamming code, $G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$.

2. Refer to the figure below.

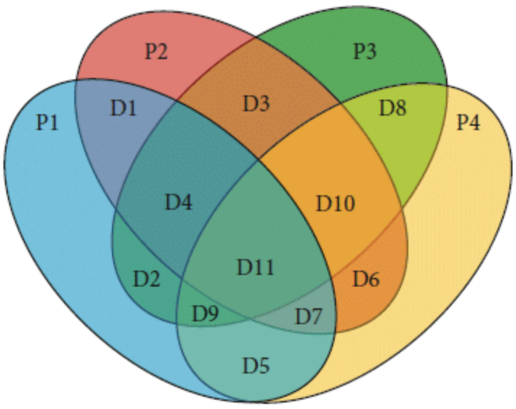

Figure 1: Hamming code for $m = 4$

   The parity equations are then given as:

$$
\begin{aligned}
P_1 &= D_1 \oplus D_2 \oplus D_4 \oplus D_5 \oplus D_7 \oplus D_9 \oplus D_{11} \\
P_2 &= D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7 \oplus D_{10} \oplus D_{11} \\
P_3 &= D_2 \oplus D_3 \oplus D_4 \oplus D_8 \oplus D_9 \oplus D_{10} \oplus D_{11} \\
P_4 &= D_5 \oplus D_6 \oplus D_7 \oplus D_8 \oplus D_9 \oplus D_{10} \oplus D_{11}
\end{aligned}
$$

   Then, we have $H = \left(\begin{array}{ccccccccccc|cccc} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$.

3.
   - For $G = [I_k \mid A]$, we have $H = [A^T \mid I_{n-k}]$.
   - $\boldsymbol{c}_n = \boldsymbol{u}_k G_{k \times n}$ is the codeword for message sequence $\boldsymbol{u}$.
   - For a codeword $\boldsymbol{c}$, we have $H_{(n-k)\times n} {\boldsymbol{c}_n}^T = 0$.
   - We thus get $H(\boldsymbol{u}G)^T = HG^T \boldsymbol{u}^T = 0 \implies HG^T = 0$. This means that the rows of H are orthogonal to the rows of G.

4. (a) The dimension of the code is k and the rate is $R = \frac{k}{n} = \frac{k}{k+1}$.

(b) The codewords follow from $\boldsymbol{c} = \boldsymbol{u}G$. Thus, the set of codewords is the set of all vectors $(u_1, u_2, \ldots, n_k, \oplus_{i=1}^{k} u_i)$, where $u_i \in \{0,1\}$ and $\oplus_{i=1}^{k} u_i$ is modulo 2. For the message vector $(1,0,1,0,\ldots,0)$, the codeword is $(1,0,1,0,\ldots,0,1)$.

(c) The parity check equation is $u_{k+1} = \oplus_{i=1}^{k} u_i$, and $H = \underbrace{\begin{pmatrix}1 & 1 & \ldots & 1\end{pmatrix}}_{n+1 \text{ times}}$.

5. (a) The rate of the code is $R = \frac{k}{n} = \frac{4}{7}$.

(b) Rearranging the columns of H, we get it in the form $H = [A^T \mid I_{n-k}]$ as

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right). \text{ Then, } G = [I_k \mid A] = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right).$$

(c) Using $\boldsymbol{c} = \boldsymbol{u}G$, where, $\boldsymbol{u}$ is of the form (u_1, u_2, u_3, u_4) the codewords are of the form $(u_1, u_2, u_3, u_4, u_1 \oplus u_2 \oplus u_4, u_2 \oplus u_3 \oplus u_4, u_1 \oplus u_2 \oplus u_3)$.