Coding and Information Theory
Chapter 7:
Linear Codes - B

Xuejun Liang

2022 Fall

Chapter 7: Linear Codes

1. Matrix Description of Linear Codes
2. Equivalence of Linear Codes
3. Minimum Distance of Linear Codes
4. The Hamming Codes
5. The Golay Codes
6. The Standard Array
7. Syndrome Decoding

Quick Review of Last Lecture (1)

- Matrix Description of Linear Codes
  - Generator matrix $\boldsymbol{G}$ for C
  - Encoding of Source (Given data, to compute codeword)
  - Whether a Vector is a Code Word?
    - A vector is a codeword if and only if it satisfies a set of simultaneous linear equations
  - Parity-Check Matrix H for C
    - Matrix of coefficients of the set of simultaneous linear equations
    - A vector v is a codeword if and only if $vH^T = 0$
  - Three examples
    - R_n, P_n, H_7

Quick Review of Last Lecture (2)

- Matrix Description of Linear Codes
  - Linear code $C \subseteq V = F^n$ and let dim(C) = k
  - Generator matrix $\boldsymbol{G}$ for C is $k \times n$
  - Parity-Check Matrix $\boldsymbol{H}$ for C is $(n-k) \times n$
  - Example H_7
    - $n = 7,\ k = 4$
    - $n - k = 3$

$$v_4 + v_5 + v_6 + v_7 = 0,$$
$$v_2 + v_3 + v_6 + v_7 = 0,$$
$$v_1 + v_3 + v_5 + v_7 = 0.$$

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

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

Dual Code of C

- Parity-Check Matrix H for C can be viewed as the matrix of a linear transformation $h: V \to W = F^{n-k}$
  - $\boldsymbol{v} \mapsto h(\boldsymbol{v}) = \boldsymbol{v}H^T$
- We have
  - $C = \ker(h) = \{\boldsymbol{v}: h(\boldsymbol{v}) = 0\}$
  - $im(h) = \{h(\boldsymbol{v}): v \in V\}$
  - $\dim(V) = \dim(\ker(h)) + \dim(im(h))$
  - H has rank $n - k$.
- So, n-k rows of H forms a basis of a linear space $D \subseteq V$ of dimension n-k. This linear code, with generator matrix H, called the dual code of C.

Orthogonal Code of C

- A scalar product on $V = F^n$ is defined as
  - $u \cdot v = (u_1 \ldots u_n) \cdot (v_1 \ldots v_n) = u_1 v_1 + \cdots + u_n v_n \in F$
- ***u*** and **v** are orthogonal if ***u·v*** = 0
- We define the orthogonal code of C as below

$$\mathcal{C}^{\perp} = \{ \mathbf{w} \in \mathcal{V} \mid \mathbf{v}.\mathbf{w} = 0 \ \text{ for all } \ \mathbf{v} \in \mathcal{C} \}$$

- Then, we have $\mathcal{D} = \mathcal{C}^{\perp}$, where D is dual code of C.

$uv^T = u \cdot v$ $\Rightarrow$ $v(aH)^T = vH^T a^T = 0a^T = 0$

$C = \{v \mid vH^T = 0\}$

$D = \{aH \mid a \in F^{n-k}\}$ $\Rightarrow$ $D = C^{\perp}$, $C = D^{\perp}$

- Example 7.14
  - Let q = 2, let n = 2m, and let C be the linear code with basis vectors $u_i = e_{2i-1} + e_{2i}$ for i = 1, ..., m. we have $C = C^{\perp}$.
- Proof

  For any i and j, we have

  $u_i \cdot u_j = (e_{2i-1} + e_{2i}) \cdot (e_{2j-1} + e_{2j})$

  $= e_{2i-1} \cdot e_{2j-1} + e_{2i-1} \cdot e_{2j} + e_{2i} \cdot e_{2j-1} + e_{2i} \cdot e_{2j} = 0$

  So, when j changes, we have $u_i \in C^{\perp}$

  So, when i changes, we have $C \subseteq C^{\perp}$

  Now, because dim(C) = m and 2m = n = dim(C) + dim($C^{\perp}$),

  we have dim(C) = dim($C^{\perp}$)

  So, $C = C^{\perp}$

- Example 7.15
  - The repetition code R_n is spanned by **1** = 1 ... 1, so

$$\mathcal{R}_n^{\perp} = \{\mathbf{w} \in \mathcal{V} \mid \mathbf{1}.\mathbf{w} = 0\} = \{\mathbf{w} \in \mathcal{V} \mid w_1 + \cdots + w_n = 0\} = \mathcal{P}_n$$

  - Similarly, we have

$$\begin{aligned}\mathcal{P}_n^{\perp} &= \{\mathbf{w} \in \mathcal{V} \mid (\mathbf{e}_i - \mathbf{e}_n).\mathbf{w} = 0 \text{ for } i = 1, \ldots, n-1\} \\ &= \{\mathbf{w} \in \mathcal{V} \mid w_i = w_n \text{ for } i = 1, \ldots, n-1\} \\ &= \mathcal{R}_n .\end{aligned}$$

$$\begin{pmatrix} 1 & & & & -1 \\ & 1 & & & -1 \\ & & \ddots & & \vdots \\ & & & 1 & -1 \end{pmatrix} \Rightarrow$$

A generator matrix for P_n and a parity-check matrix for R_n

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix} \Rightarrow$$

A generator matrix for R_n and a parity-check matrix for P_n

- Example 7.16
  - The code $H_7^{\perp}$ is a linear [7, 3]-code over F_2
  - A generator matrix for $H_7^{\perp}$ is the parity-check matrix H_7

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

  - Taking linear combinations of the rows, we have $H_7^{\perp}$ includes eight codewords:

    0 0 0 1 1 1 1   0 1 1 0 0 1 1   1 0 1 0 1 0 1   0 1 1 1 1 0 0

    1 0 1 1 0 1 0   1 1 0 0 1 1 0   1 1 0 1 0 1 0   0 0 0 0 0 0 0

  - The minimal distance d = 4

- Lemma 7.17
  - Let C be a linear $[n, k]$-code over F with generator matrix G, and let H be a matrix over F with n columns and n - k rows. Then H is a parity-check matrix for C if and only if H has rank n - k and satisfies GH^{T} = 0.
- Proof:
  - The rows of H form n - k vectors in V
  - (1) GH^{T} = 0 if and only if
    - These rows are orthogonal to those of G, i.e. $\in C^{\perp}$
  - (2) H has rank n - k if and only if
    - These rows are linearly independent, or equivalently,
    - These rows form a basis of $C^{\perp}$
  - (1) + (2) if and only if
    - H is a generator matrix for $C^{\perp}$, i.e., a parity-check matrix for C.