# Coding and Information Theory
# Chapter 7:
# Linear Codes - C

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

- Matrix Description of Linear Codes
  - Linear code $C \subseteq V$ = $F^n$ and let dim($C$) = $k$
  - Dual Code $D$ of $C$: dim($D$) = $n - k$
  - Orthogonal Code $C^\perp$ of $C$: $D = C^\perp$ and $C = D^\perp$
  - Examples:
    - $C = C^\perp$
    - ${R_n}^\perp = P_n$ and ${P_n}^\perp = R_n$
    - The code $H_7^\perp$ is a linear [7, 3]-code over $F_2$
  - The conditions for $H$ to be a parity-check matrix for $C$

# 7.2 Equivalence of Linear Codes

- The elementary row operations of matrix consist of
  - permuting rows,
  - multiplying a row by a non-zero constant, and
  - replacing a row $r_i$ with $r_i + ar_j$ where $j \neq i$ and $a \neq 0$.
- Two linear codes $C_1$ and $C_2$ are **equivalent** if they have generator matrices $G_1$ and $G_2$ which differ only by elementary row operations and permutations of columns.
  - Elementary row operations on generator $G$ may change the basis for $C$, but they do not change the subspace $C$.
  - Permutations of columns of $G$ may change $C$, but the new code will differ from $C$ only in the order of symbols within code-words.

# Equivalence of Linear Codes (Cont.)

- By systematically using elementary row operations and column permutations, one can convert any generator matrix into the form

$$G = (I_k \mid P) = \begin{pmatrix} 1 & & & & * & * & \dots & * \\ & 1 & & & * & * & \dots & * \\ & & \ddots & & \vdots & \vdots & & \vdots \\ & & & 1 & * & * & \dots & * \end{pmatrix} \quad (7.2)$$

- We then say that $G$ (or $C$) is in systematic form.
  - In this case, each $\boldsymbol{a} = a_1 \dots a_k \in F^k$ is encoded as

$$\mathbf{u} = \mathbf{a}G = a_1 \dots a_k a_{k+1} \dots a_n$$

  - where $a_1 \dots a_k$ are information digits and $a_{k+1} \dots a_n = \boldsymbol{a}P$ is a block of $n$ - $k$ check digits.

# Two Examples

- Example 7.18
  - The generator matrices $G$ for the codes $R_n$ and $P_n$ are in systematic form.

$$G = (1 \quad 1 \quad \ldots \quad 1)$$

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

- Example 7.19.
  - The generator matrix $G$ for $H_7$, is not in systematic form.
  - But, it can be transformed into systematic form.

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

# Equivalence of Linear Codes (Cont.)

- If we have a generator matrix $G = (I_k|P)$ in systematic form for a linear code $C$, then we can find a parity-check matrix for $C$.

$$H = (\,-P^{\mathrm{T}} \mid I_{n-k}\,) \qquad (7.3)$$

  - This is the systematic form for a parity-check matrix
- Prove this by using Lemma 7.17
  - H has n - k rows and n columns
  - Its rows are independent
  - $GH^{\mathrm{T}} = I_k(-P) + PI_{n-k} = -P + P = 0\,.$

# Parity-check matrix in systematic form

$G = (I_k|P)$ $H = (-P^T|I_{n-k})$

- Example 7.20: For the code $R_n$

$k = 1$

$G = (1,1, \dots, 1)_{1\times n}$

$P = (1, \dots, 1)_{1\times(n-1)}$

$$H = (-P^T|I_{n-1}) = \begin{pmatrix} -1 & 1 & & & \\ -1 & & 1 & & \\ \vdots & & & \ddots & \\ -1 & & & & 1 \end{pmatrix}_{(n-1)\times n}$$

- Example 7.21: For the code $P_n$

$k = n - 1$

$$G = \begin{pmatrix} 1 & & & & -1 \\ & 1 & & & -1 \\ & & \ddots & & \vdots \\ & & & 1 & -1 \end{pmatrix}_{(n-1)\times n}$$

$P^T = (-1, \dots, -1)_{1\times(n-1)}$

$H = (1,1, \dots, 1)_{1\times n}$

# Parity-check matrix in systematic form

$G = (I_k|P)$ $H = (-P^T|I_{n-k})$

- Example 7.22: for the code $H_7$

$k = 4$

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

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

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

# The Singleton Bound

- Exercise 6.18

  Prove the Singleton bound: if a code $C$ over $F_q$ has length $n$, minimum distance $d$, and $M$ code-words, then

  $$\log_q M \leq n - d + 1.$$

Deleting $d-1$ symbols from each code-words in $C$, then $C$ still has M distinct words of length $n-d+1$ over $F_{q.}$

There are at most $q^{n-d+1}$ words of length $n-d+1$ over $F_q$, so $M \leq q^{n-d+1}$

- Theorem 7.23

  If $C$ is a linear code of length $n$, dimension $k$, and minimum distance $d$, then

  $$d \leq 1 + n - k.$$

  - Two proofs

$M = q^k$

Generator of $C$ in systematic form $G = (I_k|P)$

Weight of each row vector of $G \leq 1 + n - k$

So, $d \leq 1 + n - k$

# The Singleton Bound

$$d \leq 1 + n - k.$$

- Example 7.24
  - The Singleton bound is attained by $R_n$
    - with $k$ = 1 and $d$ = n,
  - The Singleton bound is also attained by $P_n$
    - with $k$ = $n$ - 1 and $d$ = 2;
  - But, not by $H_7$,
    - with $d$ = 3 and 1 + $n$ - $k$ = 4,
- Corollary 7.25
  - A $t$-error-correcting linear [$n$, $k$]-code requires at least 2$t$ check digits.
- Example 7.26
  - The linear codes $R_3$ and $H_7$ both have $t$ = 1; the number of check digits is $n$ - $k$ = 2 or 3 respectively.

# 7.3 Minimum Distance of Linear Codes

- Theorem 7.27
  - Let $C$ be a linear code of minimum distance $d$, and let $H$ be a parity-check matrix for $C$. Then $d$ is the minimum number of linearly dependent columns of $H$.
- Proof
  - Let $v = v_1 v_2 \dots v_n \in V$ and $H = (c_1 c_2 \dots c_n)$
  - $v \in C \Leftrightarrow vH^T = 0 \Leftrightarrow v_1 c_1 + v_2 c_2 + \cdots + v_n c_n = 0$
  - weight of $v$ in $C$

    = number of non-zero $v_i$'s

    = number of $c_i$'s that are linearly dependent
  - $d$ = minimum weight of code-words in $C$

    = the minimum number of $c_i$'s that are linearly dependent

    = the minimum number of linearly dependent columns of $H$

# Minimum Distance of Linear Codes (Cont.)

- Meaning of linearly dependent of columns of $H$
  - One column $\boldsymbol{c_i}$ linearly dependent, then $\boldsymbol{c_i} = \boldsymbol{0}$
  - Two columns $\boldsymbol{c_i}$ and $\boldsymbol{c_j}$ linearly dependent, then $\boldsymbol{c_i}$ is multiple of $\boldsymbol{c_j}$ (or $\boldsymbol{c_j}$ is multiple of $\boldsymbol{c_i}$).
  - So, $d \geq 3$ if and only if the columns of H are non-zero and none is a multiple of any other.

- Example 7.28
  - The parity-check matrix $H$ = (1 1 … 1) for $P_n$ has its columns non-zero and equal , so $P_n$ has minimum distance $d$ = 2.

# Minimum Distance of Linear Codes (Cont.)

- Example 7.29

  In the parity-check matrix $H$ for $R_n$, any set of $n$ - 1 columns are linearly independent, while $c_1 + \cdots + c_n = 0$. So $d = n$.

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

- Example 7.30

  Now, look at the parity-check matrix $H$ for $H_7$

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