Coding and Information Theory Chapter 6: Error-correcting Codes - B

Xuejun Liang

Chapter 6: Error-correcting Codes

1. Introductory Concepts
2. Examples of Codes
3. Minimum Distance
4. Hamming's Sphere-packing Bound
5. The Gilbert-Varshamov Bound
6. Hadamard Matrices and Codes

Quick Review of Last Lecture

- Introductory Concepts
  - Galois Field: F
  - Linear Code: $C \subseteq F^n$
  - The rate of a code: $R = \frac{\log_q M}{n}$ $\qquad$ $R = \frac{k}{n}$
  - Notes
    - Chanel Γ: A→B, where A=B=F
    - Equiprobable, Nearest neighbor decoding
- Examples of Codes
  - Repetition code R_n over a field F
  - Parity-check code P_n over a field F
  - Hamming Code H_n

Examples of Codes (Cont.)

- Example 6.6
  - Suppose that C is a code of length n over a field F. Then we can form a code of length n + 1 over F, called **the extended code** $\bar{C}$. by
    - Adjoining an extra digit u_{n+1} to every code-word $\boldsymbol{u}$ = $u_1 u_2 \dots u_n \in C$ such that $u_1 + u_2 + \cdots + u_{n+1} = 0$.
    - Clearly $|\bar{C}| = |C|$, and if C is linear then so is $\bar{C}$, with the same dimension
    - Example: if $C = V = F^n$ then $\bar{C} = P_{n+1} \subset F^{n+1}$
- Example 6.7
  - If C is a code of length n, we can form a **punctured code** C° of length n - 1 by
    - Choosing a coordinate position i, and deleting the symbol u_i from each codeword $u_1 u_2 \dots u_n \in C$.

6.3 Minimum Distance

- Define the minimum distance of a code C to be

$$d = d(\mathcal{C}) = \min\{d(\mathbf{u}, \mathbf{u}') \mid \mathbf{u}, \mathbf{u}' \in \mathcal{C},\ \mathbf{u} \neq \mathbf{u}'\}, \tag{6.3}$$

- (n, M, d)-code
  - A code of length n, with M code-words, and with minimum distance d.
- [n, k, d]-code
  - A linear (n, M, d)-code, of dimension k.
- Our aim is to choose codes C for which d is large, so that $\Pr_E$ will be small.

Minimum Distance (Cont.)

- Define the weight of any vector $v = v_1 v_2 \ldots v_n \in V$ to be

$$\mathrm{wt}(\mathbf{v}) = d(\mathbf{v}, \mathbf{0}), \tag{6.4}$$

- It is easy to see that for all $u, u' \in V$, we have

$$d(\mathbf{u}, \mathbf{u}') = \mathrm{wt}(\mathbf{u} - \mathbf{u}')$$

- Lemma 6.8
  - If C is a linear code, then its minimum distance d is given by

$$d = \min\{\mathrm{wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}, \mathbf{v} \neq \mathbf{0}\}.$$

- Proof: Lemma 6.8
  - Let $d_1 = \min\{\mathrm{wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}, \mathbf{v} \neq \mathbf{0}\}.$
  - Let $d_2 = \min\{d(\mathbf{u}, \mathbf{u}') \mid \mathbf{u}, \mathbf{u}' \in \mathcal{C},\ \mathbf{u} \neq \mathbf{u}'\}$
  - Want to prove $d_1 = d_2$

Minimum Distance (Cont.)

- We say that a code C corrects t errors, or is ***t*-error-correcting**, if, whenever a code-word $u \in C$ is transmitted and is then received with errors in at most t of its symbols, the resulting received word v is decoded correctly as u.
- Equivalently, whenever $u \in C$ and v $\in V$ satisfy d(u, v) $\leq t$, the decision rule Δ gives Δ(v) = u.
- Example 6.9
  - A repetition code R_3 corrects one error, but not two.

Minimum Distance (Cont.)

- If u is sent and v is received, we call the vector e = v - u the **error pattern**.
  - $d(u, v) = wt(e) = \text{the number of incorrect symbols}$
  - A code corrects t errors if and only if it can correct all error-patterns $e \in V$ of weight wt(e) $\leq t$.
- Theorem 6.10
  - A code C of minimum distance d corrects t errors if and only if $d \geq 2t$ + 1. (Equivalently, C corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.)
- Example 6.11
  - A repetition code R_n of length *n* has minimum distance d = *n*, since d(u, u') = n for all u $\neq$ u' in R_n. This code therefore corrects t = $\lfloor (n-1)/2 \rfloor$ errors.

- Proof of Theorem 6.10
  - A code C of minimum distance d corrects t errors if and only if $d \geq 2t + 1$.

Minimum Distance (Cont.)

- Example 6.12
  - Exercise 6.3 shows that the Hamming code H_7 has minimum distance d = 3, so it has t = 1 (as shown in §6.2). Similarly, $\overline{H_7}$ has d = 4 (by Exercise 6.4), so this code also has t = 1.
- Example 6.13
  - A parity-check code P_n of length n has minimum distance d = 2; for instance, the code-words u =110 ... 0 and u' = 0 = 00 . . . 0 are distance 2 apart, but no pair are distance 1 apart. It follows that the number of errors corrected by P_n is 0.

Minimum Distance (Cont.)

- C detects d - 1 errors
  - $d(u,v)$ = the number of incorrect symbols
- Example 6.14
  - The codes R_n and P_n have $d = n$ and 2 respectively, so R_n detects n-1 errors, while P_n detects one; H_7 has d = 3, so it detects two errors.