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

Xuejun Liang

Fall 2022

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 (1/2)

- Hamming's Sphere-packing Bound
  - Theorem 6.15: n, q, d, t = $\lfloor (d-1)/2 \rfloor$

$$M\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right) \leq q^n$$

  - Example 6.16: q = 2 and t = 1, $M \leq \lfloor 2^n/(1+n) \rfloor$
  - Corollary 6.17: For linear code

$$\sum_{i=0}^{t}\binom{n}{i}(q-1)^i \leq q^{n-k}$$

  - A code C is **perfect**
  - Example 6.18**:** R_n is perfect, if n is odd and q = 2.
  - Example 6.19: The binary Hamming code H_7 is perfect.
  - Hamming's upper bound

$$H_2\left(\frac{t}{n}\right) \leq 1-R$$

Quick Review of Last Lecture (2/2)

- Hamming's Sphere-packing Bound
  - For a code C with maximum number of cardinality M=$A_q(n,d)$

$$A_q(n,d)\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\leq q^n$$

- The Gilbert-Varshamov Bound
  - Theorem 6.21

$$A_q(n,d)\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{d-1}(q-1)^{d-1}\right)\geq q^n$$

  - Example 6.20

$$A_2(n,3)\leq\lfloor 2^n/(n+1)\rfloor$$

  - Example 6.22

$$A_2(n,3)\left(1+n+\frac{n(n-1)}{2}\right)\geq 2^n$$

The Gilbert-Varshamov Bound (Cont.)

- In the binary case, Theorem 6.21 takes the form

$$A_2(n,d)\left(1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{d-1}\right)\geq 2^n.$$

- For $Q < 1/2$, Exercise 5.7 gives

$$\sum_{i\leq nQ}\binom{n}{i}\leq 2^{nH(Q)} \Rightarrow \sum_{i\leq (d-1)}\binom{n}{i}\leq 2^{H_2(\frac{d-1}{n})}$$

$$nQ = d-1$$

$$Q = \frac{d-1}{n}$$

- So for $d \leq \lfloor n/2 \rfloor$, we have

$$A_2(n,d)\geq 2^n/2^{nH_2(\frac{d-1}{n})} = 2^{n(1-H_2(\frac{d-1}{n}))}$$

- Taking logarithms in both sides, we have

$$\log_2 A_2(n,d)\geq n\left(1-H_2\left(\frac{d-1}{n}\right)\right)$$

The Gilbert-Varshamov Bound (Cont.)

- For $d \le \lfloor n/2 \rfloor$, we have

$$\log_2 A_2(n, d) \ge n\left(1 - H_2\left(\frac{d-1}{n}\right)\right)$$

- Thus for $d \le \lfloor n/2 \rfloor$, we have a lower bound

$$R \ge 1 - H_2\left(\frac{d-1}{n}\right)$$

$$R = \frac{1}{n} \log_2 M$$

- From Section 6.4, we have Hamming's upper bound

$$R \le 1 - H_2\left(\frac{t}{n}\right)$$

See (6.7)

where $t = \lfloor (d-1)/2 \rfloor$

6.6 Hadamard Matrices and Codes

- A real n x n matrix $H = (h_{ij})$ (of order n) is called a Hadamard matrix, if it satisfies
  a) each h_{ij} = ±1, and
  b) distinct rows r_i, of H are orthogonal, that is, $r_i \cdot r_j = 0$ for all $i \neq j$.
- Note: $|\det(H)| = n^{n/2}$
  - Proof: Let

$$H = \begin{pmatrix} r_1 \\ r_2 \\ \\ \cdots \\ r_n \end{pmatrix} \Rightarrow HH^T = \begin{pmatrix} r_1r_1 & r_1r_2 & & r_1r_n \\ r_2r_1 & r_2r_2 & & r_2r_2 \\ & & & \\ r_nr_1 & r_nr_2 & & r_nr_n \end{pmatrix} = \begin{pmatrix} n & 0 & & 0 \\ 0 & n & & 0 \\ & & & \\ 0 & 0 & & n \end{pmatrix}$$

$$\boxed{H^T = (r_1 \quad r_2 \quad \cdots \quad r_n)} \quad \boxed{\det(H^T) = \det(H)} \quad \boxed{\det(H)^2 = \det(HH^T) = n^n}$$

Hadamard Matrices (Cont.)

- Example 6.23
  - The matrices H = (1) and $\begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$ are Hadamard matrices of order 1 and 2, with $|\det H|$= 1 and 2 respectively.

- Lemma 6.24
  - Let H be a Hadamard matrix of order n, and let

$$H' = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

Then H' is a Hadamard matrix of order 2n.

Hadamard Matrices (Cont.)

- Corollary 6.25
  - There is a Hadamard matrix of order 2^m for each integer $m \geq 0$.
  - Proof: Start with H = (1), and apply Lemma 6.24 m times
- Example 6.26
  - The Hadamard matrices of order 2^m obtained by this method are called Sylvester matrices. For instance, taking m = 1 or 2, ……

- Lemma 6.27

  If there is a Hadamard matrix H of order $n > 1$, then n is even.

The orthogonality of distinct rows $\mathbf{r}_i$ and $\mathbf{r}_j$ gives

$$h_{i1}h_{j1} + \cdots + h_{in}h_{jn} = 0.$$

$$h_{ik}h_{jk} = \pm 1$$

⇒ n must be even.

- Lemma 6.28

  If there is a Hadamard matrix H of order $n > 2$, then n is divisible by 4.

$$r_1 = (1 \quad 1 \quad \ldots \quad 1 \quad 1 \quad 1 \quad \ldots \quad 1)$$

$$\mathbf{r}_2 = (1 \quad 1 \quad \ldots \quad 1 \quad -1 \quad -1 \quad \ldots \quad -1).$$

$$r_3 = (\quad u\ 1's \quad\quad v\ 1's \quad)$$

$$0 = \mathbf{r}_1.\mathbf{r}_3 = u - \left(\frac{n}{2} - u\right) + v - \left(\frac{n}{2} - v\right) = 2u + 2v - n$$

$$0 = \mathbf{r}_2.\mathbf{r}_3 = u - \left(\frac{n}{2} - u\right) - v + \left(\frac{n}{2} - v\right) = 2u - 2v$$

so $u = v$, and hence $n = 2u + 2v = 4u$ is divisible by 4.

Hadamard Matrices and Codes

- Theorem 6.29
  - Each Hadamard matrix H of order n gives rise to a binary code of length n, with $M = 2n$ code-words and minimum distance $d = n/2$.
- Any code C constructed as in Theorem 6.29 is called a Hadamard code of length n.

Form 2n vectors from the rows r_i of H

$\pm\mathbf{r}_1, \ldots, \pm\mathbf{r}_n \in \mathbf{R}^n$

Changing each entry -1 into 0 to get

$\mathbf{u}_1, \overline{\mathbf{u}}_1, \ldots, \mathbf{u}_n, \overline{\mathbf{u}}_n \in \mathcal{V} = F_2^n$

where $\overline{\mathbf{u}} = \mathbf{1} - \mathbf{u}$.

$d(\mathbf{u}_i, \overline{\mathbf{u}}_i) = n$

$d(u_i, u_j) = n/2$

⇒ $d = n/2$

Hadamard Codes

- The transmission rate of any Hadamard code of length n is

$$R = \frac{\log_2(2n)}{n} = \frac{1 + \log_2 n}{n} \to 0 \quad \text{as} \quad n \to \infty$$

- The number of errors corrected (if $n > 2$) is

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-2}{4} \right\rfloor = \frac{n}{4} - 1$$

- so the proportion of errors corrected is

$$\frac{t}{n} = \frac{1}{4} - \frac{1}{n} \to \frac{1}{4} \quad \text{as} \quad n \to \infty$$