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

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

- Examples of Codes
  - Hamming Code H_n
  - Extended code $\bar{C}$.
  - Punctured code C°
- Minimum Distance
  - $\min\{d(\mathbf{u},\mathbf{u}') \mid \mathbf{u},\mathbf{u}' \in \mathcal{C},\ \mathbf{u} \neq \mathbf{u}'\}$ = $\min\{\mathrm{wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}, \mathbf{v} \neq \mathbf{0}\}$.
  - $\boldsymbol{t}$-error-correcting
  - C corrects up to $\boldsymbol{t}$ = $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors
  - C detects up to $d-1$ errors
  - Examples: R_n, P_n, H_n

6.4 Hamming's Sphere-packing Bound

- Define Hamming's sphere to be

$$S_t(\mathbf{u}) = \{\, \mathbf{v} \in \mathcal{V} \mid d(\mathbf{u}, \mathbf{v}) \le t \,\} \qquad (\mathbf{u} \in \mathcal{C}) \tag{6.5}$$

- We have

$$|S_t(\mathbf{u})| = 1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t \tag{6.6}$$

- Theorem 6.15
  - Let C be a q-ary t-error-correcting code of length n, with M code-words. Then

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

Hamming's Sphere-packing Bound (Cont.)

- Given $S_t(\mathbf{u}) = \{\, \mathbf{v} \in \mathcal{V} \mid d(\mathbf{u}, \mathbf{v}) \leq t \,\} \qquad (\mathbf{u} \in \mathcal{C}) \qquad (6.5)$
- Prove

$$|S_t(\mathbf{u})| = 1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t \qquad (6.6)$$

Hamming's Sphere-packing Bound (Cont.)

- Example 6.16

  If we take q = 2 and t = 1 then Theorem 6.15 gives

  $M \leq 2^n/(1+n)$, so

  $M \leq \lfloor 2^n/(1+n) \rfloor$ since M must be an integer.

  Thus

  $M \leq$ 1, 1, 2, 3, 5, 9, 16, ... for

  n = 1, 2, 3, 4, 5, 6, 7, ...

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

Hamming's Sphere-packing Bound (Cont.)

- Corollary 6.17
  - Every t-error-correcting linear [n, k]-code C over F_q satisfies

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

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

Hamming's Sphere-packing Bound (Cont.)

- Corollary 6.17 therefore gives us a lower bound on the number of check digits (n-k) required to correct t errors

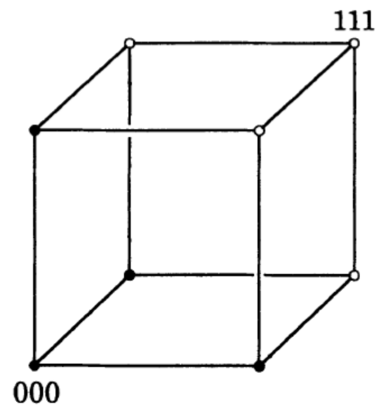
$$n - k \geq \log_q \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right)$$

- A code C is **perfect** if it attains equality in Theorem 6.15 (equivalently in Corollary 6.17, in the case of a linear code).

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

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

- Example 6.18
  - The binary repetition code R_n of odd length n is perfect!
  - However, when n is even or $q > 2$, R_n is not perfect.



$q = 2, k = 1$

Want to prove

$$\sum_{i=0}^{t} \binom{n}{i} = 2^{n-1}$$

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

$$2^n = (1+1)^n = \sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{t} \binom{n}{i} + \sum_{i=t+1}^{n} \binom{n}{i}$$

$t = (n-1)/2$

$t = n - (t+1)$

Let j $= n - i$

$$\sum_{i=t+1}^{n} \binom{n}{i} = \sum_{j=n-(t+1)}^{0} \binom{n}{n-j} = \sum_{j=t}^{0} \binom{n}{j} = \sum_{i=0}^{t} \binom{n}{i}$$

$$\Rightarrow \quad 2^n = 2\sum_{i=0}^{t} \binom{n}{i} \quad \Rightarrow \quad 2^{n-1} = \sum_{i=0}^{t} \binom{n}{i}$$

Hamming's Sphere-packing Bound (Cont.)

- Example 6.19

  The binary Hamming code H_7 is perfect.

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

Hamming's Sphere-packing Bound (Cont.)

- If C is any binary code then Theorem 6.15 gives

$$2^n \geq M\binom{n}{t} = 2^{nR}\binom{n}{t}$$

- Thus

$$2^{n(1-R)} \geq \binom{n}{t}$$

- So taking logarithms and dividing n gives

$$1 - R \geq \frac{1}{n}\log_2\binom{n}{t}$$

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

$$R = \frac{\log_q M}{n}$$

Hamming's Sphere-packing Bound (Cont.)

$$1 - R \geq \frac{1}{n} \log_2 \binom{n}{t}$$

- Apply Stirling's approximation

$$n! \sim (n/e)^n \sqrt{2\pi n}$$

to the three factorials in $\binom{n}{t} = n!/t!\,(n-t)!$

- We get the Hamming's upper bound on the proportion t/n of errors corrected by binary codes of rate R, as $n \to \infty$.

$$H_2\left(\frac{t}{n}\right) \leq 1 - R \qquad (6.7)$$

where H_2 is the binary entropy function.

6.5 The Gilbert-Varshamov Bound

- Let $A_q(n, d)$ denote the greatest number of code-words in any q-ary code of length n and minimum distance d, where $d \leq n$. Let $t = \lfloor (d-1)/2 \rfloor$, we have (by Theorem 6.15)

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

- Example 6.20
  - If q = 2 and d = 3 then t = 1, so as in Example 6.16 we find that $A_2(n, 3) \leq \lfloor 2^n/(n+1) \rfloor$. Thus for n = 3, 4, 5, 6, 7, ... we have $A_2(n, 3) \leq$ 2, 3, 5, 9, 16, ...

$$M \leq \lfloor 2^n/(1+n) \rfloor$$

The Gilbert-Varshamov Bound (Cont.)

- Theorem 6.21
  If $q \geq 2$ and $n \geq d \geq 1$ then
  $$A_q(n,d)\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{d-1}(q-1)^{d-1}\right) \geq q^n$$
- Proof
  - Let C have the maximum number of code-words
  - So $M = |\mathcal{C}| = A_q(n,d)$
  - Let $u \in C$, The following spheres must cover $V = {F_q}^n$
    $$S_{d-1}(\mathbf{u}) = \{\mathbf{v} \in \mathcal{V} \mid d(\mathbf{u},\mathbf{v}) \leq d-1\}$$

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

- Example 6.22
  - If we take q = 2 and d = 3 again (so that t = 1), then for all n $\geq$ 3, we have

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

  - This gives $A_2(n,3) \geq$ 2, 2, 2, 3, 5, ... for n = 3, 4, 5, 6, 7,
  - Compared with the upper bounds given in Example 6.20

    $A_2(n,3) \leq$ 2, 3, 5, 9, 16, … for n = 3, 4, 5, 6, 7, ...

    - $2 \leq A_2(3,3) \leq 2$ → $A_2(3,3) = 2$ (Note: R_3 attains this bound)
    - $2 \leq A_2(4,3) \leq 3$ → $A_2(4,3) = 2$ or $A_2(4,3) = 3$