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

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

The aim of this chapter

- Is to construct codes C with good transmission-rates R and low error-probabilities Pr_E, as promised by Shannon's Fundamental Theorem.
  - This part of the subject goes under the name of Coding Theory (or Error-correcting Codes), as opposed to Information Theory.
- Will concentrate on a few simple examples to illustrate some of the methods used to construct more advanced codes

6.1 Introductory Concepts

- Assume channel Γ has input A and output B, and A = B = F, where F is a finite field.
- Note Z_p of integers mod (p) is a finite field, where p is a prime number.
- Theorem 6.1
  a) There is a finite field of order q if and only if $q = p^e$ for some prime p and integer $e \geq 1$.
  b) Any two finite fields of the same order are isomorphic.

Galois Field

- The essentially unique field of order $q = p^e$ is known as the Galois field F_q or $GF(q)$.
  - When e = 1, then q = p and $F_q = F_p = Z_p$.
  - When e > 1, $F_q = Z_p[x]/f(x)$, where f(x) is an irreducible polynomial of degree e on the field Z_p.
  - When e > 1, $F_q = Z_p[\alpha]$, where α is a root of $f(x)$ which an irreducible polynomial of degree e on the field Z_p.
- Example 6.2
  - The quadratic polynomial $f(x) = x^2 + x + 1$ has no roots in the field Z_2.

$$F_4 = \{a + bx \mid a, b \in Z_2\} = \{0, 1, x, 1 + x\}$$

$$F_4 = \{a + b\alpha \mid a, b \in \mathbf{Z}_2\} = \{0,\ 1,\ \alpha,\ 1 + \alpha\}$$

Linear Code

- Let F be a field, then the set $V = F^n$ of all n-tuples with coordinates in F is an n-dimensional vector space over F.
  - the operations are component wise addition and scalar multiplication
- Assume that any code-words in C are of length n
  - So C is a subset of the set $V = F^n$
- We say that C is a linear code (or a group code) if C is a non-empty linear subspace of V.
  - If $\boldsymbol{u}, \boldsymbol{v} \in C$ then $a\boldsymbol{u} + b\boldsymbol{v} \in C$ for all $a, b \in F$

The rate of a code C

- We will always denote $|C|$ by M
- When C is linear we have M = q^k, where k = dim(C) is the dimension of the subspace C.
  - We then call C a linear $[n, k]$-code.
- The rate of a code C is

$$R = \frac{\log_q M}{n} \qquad (6.1)$$

  - So in the case of a linear $[n, k]$-code we have

k information digits, carrying the information
n - k check digits, confirming or protecting that information

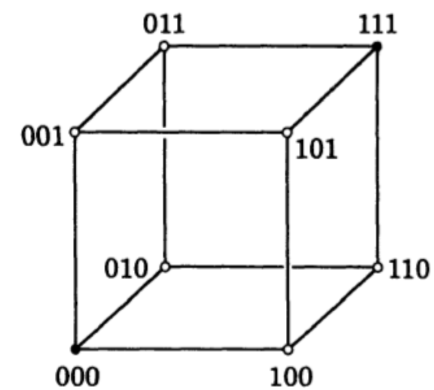
$$R = \frac{k}{n} \qquad (6.2)$$

Notes

- We will assume that all code-words in C are equiprobable, and that we use nearest neighbor decoding (with respect to the Hamming distance on V).

6.2 Examples of Codes

- Example 6.3: The repetition code R_n over F
  - the words $\boldsymbol{u} = uu \ldots u \in V = F^n$, where $u \in F$, so M = |F| = q.
  - F is a field. So, R_n is a linear code of dimension k = 1, spanned by the word (or vector) 11. . . 1
  - Example:
    - Binary code R_3 = {000, 111} as a subset of $V = Z_2^3$

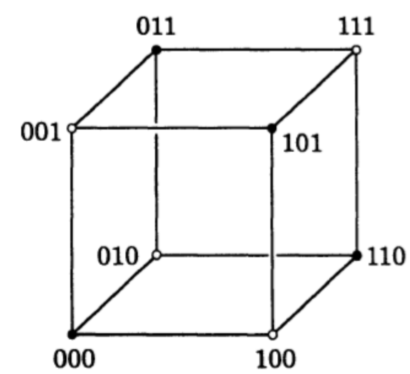


  - R_n corrects $\lfloor (n-1)/2 \rfloor$ errors
  - R_n has rate R = $1/n \rightarrow 0$ as $n \rightarrow \infty$,

Examples of Codes (Cont.)

- Example 6.4: The parity-check code P_n over a field $F = F_q$
  - All vectors $u = u_1 u_2 \dots u_n \in V$ such that $\sum_i u_i = 0$.
  - if n = 3 and k = 2

    then P_3={000, 011,101, 110}.

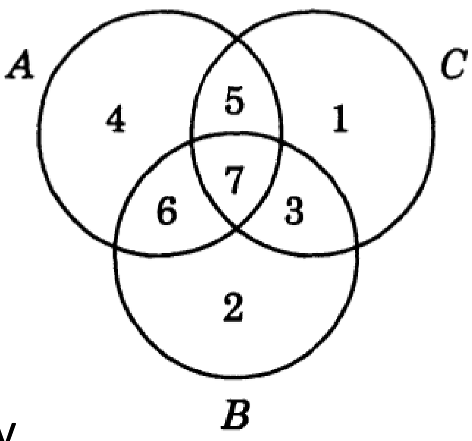


  - $M = q^{n-1}$
  - R = (n - 1)/n, so $R \rightarrow 1$ as $n \rightarrow \infty$
  - it will detect a single error, but cannot correct it.

- Example 6.4: The parity-check code P_n over a field $F = F_q$
  - All vectors $u = u_1 u_2 \ldots u_n \in V$ such that $\sum_i u_i = 0$.
  - Proof: Dim(P_n) = n-1

Hamming Code

- Example 6.5
  - The binary Hamming code H_7 is a linear code of length n = 7 over F_2
    - 4 bits for data **a** = $a_1a_2a_3a_4$
    - 3 bits for checking
  - How to construct the code for **a**
    - Let the code word **u** = $u_1u_2u_3u_4u_5u_6u_7$
    - Bits $u_3 = a_1$, $u_5 = a_2$, $u_6 = a_3$, and $u_7 = a_4$
    - Bits u_1, u_2, u_4 for checking, determined by

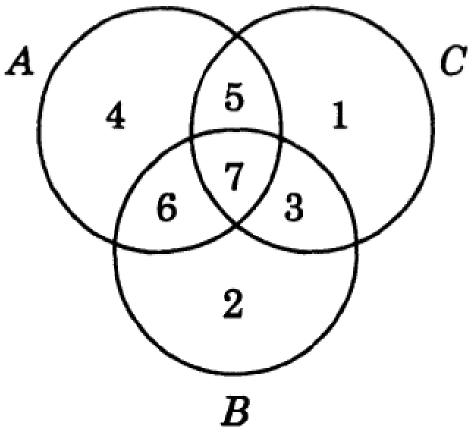


$$u_4 + u_5 + u_6 + u_7 = 0$$
$$u_2 + u_3 + u_6 + u_7 = 0$$
$$u_1 + u_3 + u_5 + u_7 = 0$$

ABC

A=4, B=2, C=1

Hamming Code (Cont.)



- Example 6.5
  - Example: **a** = 0110

	1	2	3	4	5	6	7
	001	010	011	100	101	110	111
4 (s_1)				100	100	100	100
2 (s_2)		010	010			010	010
1 (s_3)	001		001		001		001
u	1	1	0	0	1	1	0

$$s_1 = u_4 + u_5 + u_6 + u_7$$
$$s_2 = u_2 + u_3 + u_6 + u_7$$
$$s_3 = u_1 + u_3 + u_5 + u_7$$

- The receiver will compute s_1, s_2, s_3. If they are all zero then the code is no error.
- If not, the binary number $s_1s_2s_3$ tells which bit is wrong.
- Now, assume **v** = 1110110 is received with 1-bit error in bit 3. you will get s_1= 0, s_2= 1, and s_3 = 1. So, $s_1s_2s_3$ = 011 = 3.

Hamming Code (Cont.)

$$u_4 + u_5 + u_6 + u_7 = 0$$
$$u_2 + u_3 + u_6 + u_7 = 0$$
$$u_1 + u_3 + u_5 + u_7 = 0$$

- Example 6.5 (Cont.)
  - The binary Hamming code H_7 is a linear code with dimension k = 4.
    - $M = |H_7| = 16 = 2^4$
    - It can be generated by

      $\mathbf{u_1}$ = 1110000, $\mathbf{u_2}$ = 1001100, $\mathbf{u_3}$ = 0101010, $\mathbf{u_4}$ = 1101001
    - which are obtained from

      $\mathbf{e_1}$ = 1000, $\mathbf{e_2}$ = 0100, $\mathbf{e_3}$ = 0010, $\mathbf{e_4}$ = 0001
- Note:
  - Although the binary codes R_3 and H_7 both correct a single error, the rate R = 4/7 of H_7 is significantly better than the rate 1/3 of R_3.