Chapter 12

MATH32031 Coding Theory: end-of-semester revision problems 2022

Version 2022-12-12. To accessible online version of this chapter

We illustrate some of the revision topics by examples of questions form past assessment papers. A selection of these questions will be discussed in the Week 12 tutorial on Thursday 15 December 2022 at 10am in AT G.205.

12.1 General codes

- **find the Hamming distance between two words**
- **find the minimum distance of a code with a small number of codewords**
- **given parameters $(n, M, d)_q$ of a code C, find $[n, k, d]_q$ and the rate R**
- **given a code C as a list of codewords, decode a received word $\underline{y}$**
- **write down the parameters of a trivial code, of a repetition code**
- **given the minimum distance d of a code, write down the number of errors (per codeword) that the code can detect/correct**
- **write down the probability that i errors occur in a binary word of length n sent via BSC(p)**

From the 2013 Coding Theory exam paper - medium difficulty:

A4. Consider the following binary code of length 6: $C = \{000111, 110001, 011100\}$.

(a) Is C a linear code? Give a reason for your answer.

(b) Find $d(C)$.

(c) Show that there does not exist a vector $\underline{\mathrm{y}} \in \mathbb{F}_2^6$ such that $d(\underline{\mathrm{y}}, \underline{\mathrm{c}}) = 1$ for all $\underline{\mathrm{c}} \in C$.

Solution:

(a) C is not linear, e.g. because C does not contain 000000. (*There are other reasons.*)

(b) All pairwise distances between codewords are 4 so $d(C) = 4$.

(c) By the Triangle Inequality, $d(000111, 110001) \leq d(000111, \underline{y}) + d(\underline{y}, 110001)$. The left-hand side of this inequality is 4 so the right-hand side cannot be $1 + 1$.

12.2 Bounds

...write down:

- **the Hamming bound for q-ary codes of length n and minimum distance d**
- **the Singleton bound?**

...calculate:

- **the Hamming and Singleton bounds for a code with given parameters — and use these to check if the code is perfect/MDS?**

...give an example of:

- **perfect codes of minimum distance** 1, 3, 5, 7, 9, ...

From the 2013 Coding Theory exam paper, question A3:

(e) Prove:

1. The sphere $S_{10}(\underline{0})$ in $\mathbb{F}_3^{2013}$ consists of an odd number of elements.
2. Any perfect code in $\mathbb{F}_3^{2013}$ consists of an odd number of codewords.

Answer. 1. $|S_{10}(\underline{0})| = \binom{2013}{0} + \binom{2013}{1}2^1 + \ldots + \binom{2013}{10}2^{10}$. The first summand $\binom{2013}{0} = 1$ is odd, the rest of the summands contain powers of 2 so are even. Therefore, the sum is odd.
2. $M|S_t(\underline{0})| = 3^{2013}$ is odd, so M is a divisor of an odd integer, so M is odd.

More challenging: from the 2015 Coding Theory exam paper, question A3g, also used in coursework in later years:

(g) You are given that $C \subseteq D \subseteq \mathbb{F}_q^n$ where $|C| < |D|$ and C is a perfect code. Show that $d(C) > 2d(D)$. You may quote any result from the course without proof.

Answer. Take a codeword $\underline{x}$ of D such that $\underline{x} \notin C$. By a result from the course, $\underline{x}$ has unique nearest neighbour $\underline{c}$ in C where $d(\underline{x}, \underline{c}) \leq t$, where $t = [(d(C) - 1)/2]$. Note that both $\underline{x}$ and $\underline{c}$ are codewords of D, and $\underline{x} \neq \underline{c}$ (one word is in C, the other is not). So $d(D) \leq d(\underline{x}, \underline{c}) < d(C)/2$, as claimed.

12.3 Linear codes I

...write down:

- **the parameters of E_n (with explanation)?**
- **the parameters of ISBN-10 (with explanation)?**
- **the weight enumerators of the trivial code, the repetition code, the code E_n?**
- **the special values of the weight enumerator: $W_C(0,0)$, $W_C(1,0)$, $W_C(1,1)$?**

12.4 Linear codes II: encoding and decoding

- **given a generator matrix G of a code C, encode a message vector $\underline{u}$. What is the number of rows/columns of G? What must be the length of $\underline{u}$? What do you get as the output of the encoder?**

...calculate:

- **a generator matrix in standard form for a given code?**
- **all the codevectors, and the weight enumerator of the linear code, if a generator matrix is given?**
- **$P_{\mathbf{undetect}}(C)$? (what do you need to know to find it? for what codes and channels?)**
- **$P_{\mathbf{corr}}(C)$? (what do you need to know to find it? for what codes and channels?)**

12.5 Dual codes

...calculate:

- **the inner product of two vectors?**
- **a check matrix of a given code? (what data do you need?)**
- **the dual code of the trivial/repetition/even weight/ISBN-10 code?**
- **the length and dimension of $C^\perp$ if C has length n, dimension k?**

...check:

- **whether a given code is self-orthogonal? self-dual? (what data do you need?)**
- **calculate the syndrome of a vector? (what data do you need?)**
- **check if a given vector belongs to the code?**
- **construct a table of syndromes, and decode a received vector using your table?**
- **use the Average Weight Equation?**

12.6 Hamming codes and simplex codes

...write down:

- **the parameters of Ham(r, q)?**
- **the weight of any non-zero codevector and the parameters of $\Sigma(r, q)$?**
- **the weight enumerator of $\Sigma(r, q)$?**

...construct:

- **a check matrix for $\mathrm{Ham}(r, q)$ (q is a prime)? A generator matrix?**
- **given a check matrix for a Hamming code, decode a received vector?**

12.7 Cyclic codes

- **write the given vector in $\mathbb{F}_q^n$ as a polynomial, and a polynomial as a vector?**
- **given a (small) cyclic code C, find the generator polynomial of C?**
- **carry out long division of polynomials?**

...calculate:

- **the dimension of a cyclic code with a given generator polynomial?**
- **the check polynomial of a given cyclic code? (what do you need to know?)**
- **generator polynomials, check polynomials, generator matrices, check matrices of all possible cyclic codes in $\mathbb{F}_q^n$? (what do you need to know?)**

12.8 Classification of perfect codes

- **write down the parameters of the Golay codes, and prove that the codes are perfect?**
- **use the Classification Theorem for perfect codes where q is a prime power?**

12.9 Reed-Muller codes

...write down:

- **the parameters of $R(r, m)$?**