Week 12 Revision

* Thursday 15 December 10am G.205 - Final tutorial.

MATH32031

Two hours

This is a partially open book exam. You are allowed to bring a single sheet of A4 paper, with your own notes typed or handwritten on both sides. No other restricted materials are allowed into the exam.

* EXAM

THE UNIVERSITY OF MANCHESTER

CODING THEORY

25 January 2023

14:00 – 16:00

Answer **BOTH** questions in Section A and **TWO** of the **THREE** questions in Section B. If more than **TWO** questions are attempted in Section B, then credit will be given for the best **TWO** answers.

Electronic calculators may be used in accordance with the University regulations

---

P.T.O.

Chapter 12

MATH32031 Coding Theory: end-of-semester revision 2022

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

See suggested answers and hints at end
This list is not guaranteed to cover all possible topics that may arise in the exam. Your questions and suggestions are welcome; please post them to the Piazza discussion board or contact the lecturer during the revision period.

Suggested revision format: ask yourself ***Can I...*** followed by a question below. In case of difficulty/lack of confidence, revise the relevant part of the course material. Brief comments on a suggested approach are available below for most questions. Questions marked (*) are more challenging: they have not been covered in the course but follow from lecture material or exercises.

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** $M = q^k$, $R = k/n \leq 1$
- **given a code C as a list of codewords, decode a received word y** nearest neighbour
- **write down the parameters of a trivial code, of a repetition code** $[n, n, 1]_q$ $[n, 1, n]_q$
- **given the minimum distance d of a code, write down the number of errors (per codeword) that the code can detect/correct** $(d-1)$ detect, $t = \lfloor \frac{d-1}{2} \rfloor$ correct
- **write down the probability that i errors occur in a binary word of length n sent via BSC(p)** $\binom{n}{i}(1-p)^{n-i}p^i$

12.2 Bounds

...write down:

- **the Hamming bound for q-ary codes of length n and minimum distance d** log-Hamming: $k \leq n - \log_q \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$
- **the Singleton bound?** $k \leq n - d + 1$

...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 $1, 3, 5, 7, 9, \ldots$

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 u. What is the number of rows/columns of G? What must be the length of 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?
- $P_{\text{undetect}}(C)$? (what do you need to know to find it? for what codes and channels?)
- $P_{\text{corr}}(C)$? (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 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 $R(r, m)$?