

MATHEMATICAL TRIPOS PART II (2018–19)

Coding and Cryptography - Example Sheet 3 of 4

R.D. Camina

- 1) Find generator and parity check matrices for the Hamming $(7, 4)$ -code, putting each in the form $(I|B)$ for I an identity matrix of suitable size. Repeat for the parity check extension of this code.
- 2) The Mariner mission to Mars used the $RM(5, 1)$ code. What was its information rate? What proportion of errors could it correct in a single codeword? How does it compare to the Hamming code of length 31?
- 3) Show that if C is a linear code, then so are its parity check extension C^+ and puncturing C^- . When is the shortening C' of C a linear code? Describe the effect of a parity check extension on the generator and parity check matrices.
- 4) Give a recursive definition of the Reed-Muller codes, using the bar product construction. Use this to compute the rank of $RM(d, r)$. Show that all but two codewords in $RM(d, 1)$ have the same weight.
- 5) Show that $RM(d, r)$ has dual code $RM(d, d - r - 1)$. (Hint: First show that every codeword in $RM(d, d - 1)$ has even weight.)
- 6) Factor the polynomials $X^3 - 1$ and $X^5 - 1$ into irreducibles in $\mathbb{F}_2[X]$. Hence find all cyclic codes of length 3 or 5 and relate them to codes you have already met.
- 7) (i) Show directly that the dual code C^\perp of a cyclic code C is cyclic. Explain how the generator polynomials of C and C^\perp are related.
(ii) Show that there are three cyclic codes of length 7 corresponding to irreducible polynomials of which two are versions of Hamming's original code. What are the other cyclic codes of length 7?
- 8) Consider the collection K of polynomials $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ with $a_j \in \mathbb{F}_2$, manipulated subject to the usual rules of polynomial arithmetic and the further condition $1 + \alpha + \alpha^4 = 0$. Show by direct calculation that $K^\times = K \setminus \{0\}$ is a cyclic group under multiplication and deduce that K is a finite field. (Of course, this follows directly from general theory but direct calculation is not uninteresting.)
- 9) Let C be the cyclic code of length $n = 2^d - 1$ defined by a primitive n th root of unity.
(i) Show that if $g(X) \in \mathbb{F}_2[X]$ then $g(X)^2 = g(X^2)$.
(ii) Show that C is a BCH code of design distance 3.
(iii) Deduce that C is (equivalent to) the Hamming $(n, n - d)$ -code.
- 10) Let $\alpha \in \mathbb{F}_{16}$ be a root of $X^4 + X + 1$. Let C be the BCH code of length 15 and design distance 5, with defining set the first few powers of α .
(i) Find the minimal polynomial for each element of the defining set, and then compute the generator polynomial of C as the least common multiple of these polynomials.
(ii) If possible, determine the error positions of the following received words
 - (a) $r(X) = 1 + X^6 + X^7 + X^8$
 - (b) $r(X) = 1 + X + X^4 + X^5 + X^6 + X^9$
 - (c) $r(X) = 1 + X + X^2$
 - (d) $r(X) = 1 + X + X^7$.(Your answer to Question 8 may help with the computations.)

- 11) Let C be a linear code of length n with A_j codewords of weight j . The weight enumerator polynomial is

$$W_C(x, y) = \sum_{j=0}^n A_j x^j y^{n-j}.$$

- (i) We transmit a codeword through a BSC with error probability p . Give a formula, in terms of the weight enumerator polynomial, for the probability that the word received is a codeword.
(ii) Show that $W_C(x, y) = W_C(y, x)$ if and only if $W_C(1, 0) = 1$.
- 12) Show that if $2^k \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n$ then $A(n, d) \geq 2^k$. Compare with the GSV bound in the case $n = 10$ and $d = 3$. (Hint: Construct a parity check matrix for a linear code by choosing one column at a time.)

Further Problems

- 13) Describe the effect on the dual code C^\perp when a linear code C is modified in the following ways.
(i) We puncture C in the last place. (You may assume $d(C) \geq 2$.)
(ii) We shorten C by 0 in the last place. (You may assume some codeword ends in a 1.)
- 14) Show that $RM(d, d-2)$ is the parity check extension of the Hamming $(n, n-d)$ code with $n = 2^d - 1$. (This is useful because we often want codes of length 2^d .)
- 15) We construct a perfect 3-error correcting $(23, 12)$ -code, starting from the factorisation

$$X^{23} - 1 = (X - 1)f_1(X)f_2(X)$$

in $\mathbb{F}_2[X]$ where $f_1(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$ and $f_2(X) = X^{11}f_1(1/X)$.

- (i) Show that if $g(X) \in \mathbb{F}_2[X]$ and β is a root of g (in some field extension of \mathbb{F}_2) then β^2 is also a root of g .
(ii) Make a list of the powers of 2 mod 23. Deduce that the cyclic code C with generator polynomial $f_1(X)$ has minimum distance at least 5.
(iii) Show that C^\perp is a subcode of C . Deduce that the parity check extension of C is a self-dual linear code.
(iv) Show that any self-dual linear code, generated by vectors of weight a multiple of 4, has minimum distance a multiple of 4.
(v) Deduce that C is a perfect 3-error correcting code.