MATHEMATICAL TRIPOS PART II (2004–05)

Coding and Cryptography - Example Sheet 3 of 4 **T.A. Fisher**

41) An (n, k)-linear code is used to transmit through a binary erasure channel. Find a necessary and sufficient condition on the parity check matrix so that t errors can be corrected. Relate t to k in a useful manner.

42) (i) Show that if C is linear, then so are its parity extension C^+, puncturing C^- and shortening C', provided the symbol chosen to shorten by is 0. Give an example to show that C' may not be linear if we shorten by 1.
(ii) Give an example where shortening reduces the information rate and an example where shortening increases the information rate.
(iii) Show that shortening cannot decrease the minimum distance but give examples to show that the minimum distance can stay the same or increase.

43) 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 extension of this code.

44) If C_1 and C_2 are of appropriate type with generator matrices G_1 and G_2 write down a generator matrix for $C_1|C_2$.

45) 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 code word?

46) 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.

47) Show that the $RM(d, d-2)$ code is the parity extension code of the Hamming $(n, n-d)$ code with $n = 2^d - 1$. (This is useful because we often want codes of length 2^d.)

48) 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 uninstructive.]

49) 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 met before.

50) 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.

51) 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?

52) Let $K \supset \mathbb{F}_2$ be a finite field.
(i) Show that if $\alpha \in K$ and $g(X) \in \mathbb{F}_2[X]$ then $g(\alpha) = 0$ implies $g(\alpha^2) = 0$.
(ii) Show that if $\beta \in K$ is a primitive 23rd root of unity then the cyclic code of length 23 defined by β has weight at least 5.

(iii) It turns out that the code in (ii) is a perfect code. Assuming this, what is its weight?

53) 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 generator polynomial of C.
(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) $r(X) = 1 + X + X^7$.
[Your answer to Question 48 may help with the computations.]

54) A binary linear feedback shift register was used to generate the following stream

$$110001110001\ldots$$

Recover the feedback polynomial by the Berlekamp-Massey method. [The LFSR has length 4 but you should work through the trials for length r for $1 \leq r \leq 4$.]

Further Problems

Note: the examples above are minimal to cover the course; you are encouraged to do those below also.

55) 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.]

56) Show that $RM(d,r)$ has dual code $RM(d, d-r-1)$.

57) We identify $\mathbb{F}_2^n$ with indicator functions on $X = \mathbb{F}_2^d$ where $n = 2^d$. Let $A \subset X$ be a vector subspace of dimension at least $d-r$. Determine whether the indicator function of A is a codeword in $RM(d,r)$.

58) Let $\rho > 0$. Let $C_1, C_2, \ldots$ be a sequence of Reed-Muller codes, each with information rate at least ρ. Show that if they are used to transmit through a BSC with error probability $p < 1/2$, and we use minimum distance decoding, then $\hat{e}(C_n) \not\to 0$ as $n \to \infty$. (Recall that $\hat{e}(C)$ denotes the maximum error probability of a code C.)

59) Show that the Hamming $(n, n-d)$-code is the cyclic code of length $n = 2^d - 1$ defined by a primitive nth root of unity.

60) Consider the linear recurrence

$$x_n = a_0 x_{n-d} + a_1 x_{n-d+1} \ldots + a_{d-1} x_{n-1} \qquad (*)$$

with $a_j \in \mathbb{F}_2$ and $a_0 \neq 0$.
Show that if the auxiliary polynomial $P(X)$ factors over $K \supset \mathbb{F}_2$, say as $P(X) = \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$ for $\alpha_1, \ldots, \alpha_r$ distinct, then $(*)$ has general solution

$$x_n = \sum_{i=1}^{r} \sum_{j=0}^{m_i - 1} b_{i,j} \binom{n}{j} \alpha_i^n$$

for some $b_{i,j} \in K$. If $x_0, x_1, \ldots, x_{d-1} \in \mathbb{F}_2$, show that $x_n \in \mathbb{F}_2$ for all n.
[Hint : First show that the functions $f_j : \mathbb{Z} \to \mathbb{F}_2$ given by $f_j(n) = \binom{n}{j}$ are linearly independent in the sense that $\sum_{j=0}^{m} a_j f_j(n) = 0$ for all n implies $a_j = 0$ for $1 \leq j \leq m$.]