UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS   Part III

Monday 3 June 2002   1.30 to 3.30

PAPER 30

ALGEBRAIC CODING

*Attempt **THREE** questions*

*There are **three** questions in total*

The questions carry equal weight

Candidates may bring into the examination any lecture notes made during the course, printed lecture notes, example sheets and model solutions, and books or their photocopies

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 Define Reed–Solomon codes and prove that they are maximum distance separable. Prove that the dual of a Reed–Solomon code is a Reed–Solomon code.

Find the minimum distance of a Reed–Solomon code of length 15 and rank 11 and the generator polynomial $g_1(X)$ over $\mathbb{F}_{16}$ for this code. Use the provided $\mathbb{F}_{16}$ field table to write $g_1(X)$ in the form $\omega^{i_0} + \omega^{i_1}X + \omega^{i_2}X^2 + \ldots$, identifying each coefficient as a single power of a primitive element ω of $\mathbb{F}_{16}$.

Find the generator polynomial $g_2(X)$ and the minimum distance of a Reed–Solomon code of length 10 and rank 6. Use the provided $\mathbb{F}_{11}$ field table to write $g_2(X)$ in the form $a_0 + a_1X + a_2X^2 + \ldots$, where each coefficient is a number from $\{0, 1, \ldots, 10\}$.

Determine a two-error correcting Reed–Solomon code over $\mathbb{F}_{16}$ and find its length, rank and generator polynomial.

The field table for $\mathbb{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, with addition and multiplication mod 11:

i	0	1	2	3	4	5	6	7	8	9
ω^i	1	2	4	8	5	10	9	7	3	6

The field table for $\mathbb{F}_{16} = \mathbb{F}_2^4$:

i	0	1	2	3	4	5	6	7	8
ω^i	0001	0010	0100	1000	0011	0110	1100	1011	0101

i	9	10	11	12	13	14
ω^i	1010	0111	1110	1111	1101	1001

2 Let $\mathcal{C}$ be a binary linear $[n, k]$ code and $\mathcal{C}^{\text{ev}}$ the set of words $x \in \mathcal{C}$ of even weight. Prove that either (i) $\mathcal{C} = \mathcal{C}^{\text{ev}}$ or (ii) $\mathcal{C}^{\text{ev}}$ is an $[n, k-1]$ linear subcode of $\mathcal{C}$.

[**Hint:** *For binary words x and x' of length n, $w(x+x') = w(x)+w(x')-2w(x\wedge x')$, where $(x \wedge x')_j = x_j x'_j$, $1 \leqslant j \leqslant n$.*]

Prove that if the generating matrix G of $\mathcal{C}$ has no zero column then the total weight $\sum\limits_{x\in\mathcal{C}} w(x)$ equals $n2^{k-1}$.

[**Hint:** *Consider the contribution from each column of G.*]

Denote by $\mathcal{C}_{\text{H},\ell}$ the binary Hamming code of length $n = 2^\ell - 1$ and by $\mathcal{C}^{\perp}_{\text{H},\ell}$ the dual simplex code, $\ell = 3, 4, \ldots$. Is it always true that the n-vector $(1, \ldots, 1)$ (with all digits one) is a codeword in $\mathcal{C}_{\text{H},\ell}$? Let A_s and $A^{\perp}_s$ denote the number of words of weight s in $\mathcal{C}_{\text{H},\ell}$ and $\mathcal{C}^{\perp}_{\text{H},\ell}$, respectively, with $A_0 = A^{\perp}_0 = 1$ and $A_1 = A_2 = 0$. Check that

$$A_3 = \frac{n(n-1)}{3!},\ A_4 = \frac{n(n-1)(n-3)}{4!},\ A_5 = \frac{n(n-1)(n-3)(n-7)}{5!}.$$

Prove that $A^{\perp}_{2^{\ell-1}} = 2^\ell - 1$ (i.e., all non-zero words $x \in \mathcal{C}^{\perp}_{\text{H},\ell}$ have weight $2^{\ell-1}$). By using the last fact and the Mac Williams identity for binary codes, give a formula for A_s in terms of $K_s(2^{\ell-1})$, the value of the Kravchuk polynomial:

$$K_s(2^{\ell-1}) = \sum_{j=0\vee s+2^{\ell-1}-2^\ell+1}^{s\wedge 2^{\ell-1}} \binom{2^{\ell-1}}{j} \binom{2^\ell - 1 - 2^{\ell-1}}{s-j} (-1)^j.$$

Here $0 \vee s + 2^{\ell-1} - 2^\ell + 1 = \max\,[0, s + 2^{\ell-1} - 2^\ell + 1]$ and $s \wedge 2^{\ell-1} = \min\,[s, 2^{\ell-1}]$. Check that your formula gives the right answer for $s = n = 2^\ell - 1$.

3 Let ω be a root of $m(X) = X^5 + X^2 + 1$ in $\mathbb{F}_{32}$; given that $m(X)$ is a primitive polynomial for $\mathbb{F}_{32}$, ω is a primitive $(31, \mathbb{F}_{32})$ root of unity. Use elements ω, ω^2, ω^3, ω^4 to construct a binary narrow sense primitive BCH code $\mathcal{X}$ of length 31 and designed distance 5. Identify the cyclotomic coset $\{i, 2i, \ldots, 2^{d-1}i\}$ for each of ω, ω^2, ω^3, ω^4. Check that ω and ω^3 suffice as defining zeros of $\mathcal{X}$ and that the actual minimum distance of $\mathcal{X}$ equals 5. Show that the generator polynomial $g(X)$ for $\mathcal{X}$ is the product

$$\begin{aligned}&(X^5 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1)\\&= X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + 1.\end{aligned}$$

Suppose you received a word $u(X) = X^{12} + X^{11} + X^9 + X^7 + X^6 + X^2 + 1$ from a sender who uses code $\mathcal{X}$. Check that $u(\omega) = \omega^3$ and $u(\omega^3) = \omega^9$, argue that $u(X)$ should be decoded as

$$c(X) = X^{12} + X^{11} + X^{10} + X^9 + X^7 + X^6 + X^2 + 1$$

and verify that $c(X)$ is indeed a codeword in $\mathcal{X}$.

[*You may quote, without proof, a theorem from the course (see below) but should check its conditions. The field table for $\mathbb{F}_{32} = \mathbb{F}_2^5$ and the list of irreducible polynomials of degree 5 over $\mathbb{F}_2$ are also provided to help with your calculations.*]

The field table for $\mathbb{F}_{32} = \mathbb{F}_2^5$:

i	0	1	2	3	4	5	6	7	8
ω^i	00001	00010	00100	01000	10000	00101	01010	10100	01101
i	9	10	11	12	13	14	15	16	17
ω^i	11010	10001	00111	01110	11100	11101	11111	11011	10011
i	18	19	20	21	22	23	24	25	26
ω^i	00011	00110	01100	11000	10101	01111	11110	11001	10111
i	27	28	29	30					
ω^i	01011	10110	01001	10010					

The list of irreducible polynomials of degree 5 over $\mathbb{F}_2$:

$$X^5 + X^2 + 1,\ \ X^5 + X^3 + 1,\ \ X^5 + X^3 + X^2 + X + 1,$$
$$X^5 + X^4 + X^3 + X + 1,\ \ X^5 + X^4 + X^3 + X^2 + 1;$$

they all have order 31. Polynomial $X^5 + X^2 + 1$ is primitive.

Theorem. *Let $n = 2^s - 1$. If $2^{sl} < \sum_{0 \leqslant i \leqslant l+1} \binom{n}{i}$ then the binary narrow-sense primitive BCH code of designed distance $2l + 1$ has minimum distance $2l + 1$.*