

CODES AND CRYPTOGRAPHY – Example Sheet 3

TKC Michaelmas 2007

- For a natural number d there are $N = 2^d - 1$ non-zero vectors in \mathbb{F}_2^d . Take these as the columns of an $d \times N$ matrix S . The kernel of S is then the code book for a Hamming code

$$c : \mathbb{F}_2^{N-d} \rightarrow \mathbb{F}_2^N .$$

Check that the case $d = 3$ gives the Hamming code we constructed earlier.

Show that each of these Hamming codes is a perfect 1-error correcting code.

- Let $C(X) = c_0 + c_1X + \dots + c_{K-1}X^{K-1} + X^K$ be the feedback polynomial for a linear feedback shift register over \mathbb{F}_q with $c_0 \neq 0$. Show that the output stream (x_j) is periodic. Show that there is a $K \times K$ matrix M with

$$\begin{pmatrix} x_j \\ x_{j+1} \\ \vdots \\ x_{j+K-1} \end{pmatrix} = M^j \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{K-1} \end{pmatrix} \quad \text{for } j = 0, 1, 2, \dots .$$

Prove that $M^N = I$ for some integer N . Find the characteristic and minimal polynomials for M .

What happens when the coefficient c_0 is allowed to be 0? Do we still get periodicity when the feedback function is not assumed to be a polynomial?

- Find generator and syndrome matrices for the Hamming code (of length 7), putting each in the form $\begin{pmatrix} I \\ A \end{pmatrix}$ or $(-A \quad I)$ for I an identity matrix of suitable size.

A new code is formed by adding a single parity check bit to the end of the Hamming code, show that this is linear and repeat the exercise above for this code.

- 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 $31 = 2^5 - 1$?
- Let C_1, C_2 be the code books for two linear codes of length N with C_2 a subset of C_1 . The *bar product* $C_1|C_2$ is the code of length $2N$ with code book:

$$\{(\mathbf{x}|\mathbf{x} + \mathbf{y}) : \mathbf{x} \in C_1 \text{ and } \mathbf{y} \in C_2\} .$$

Show that this is a linear code.

Let d_j be the minimum distance of C_j . Prove that the minimum distance for $C_1|C_2$ is at least $\min(2d_1, d_2)$.

Show that the Reed – Muller codes satisfy

$$RM(d, r) = RM(d - 1, r)|RM(d - 1, r - 1)$$

and deduce that $RM(d, r)$ has minimum distance 2^{d-r} .

- Let C be the $N \times K$ matrix defining a linear code and S a $(N - K) \times N$ syndrome matrix. Show that the transposed matrix S^T also defines a linear code with syndrome matrix C^T . This is called the *dual code*. Show that the set of code words for the dual code is

$$\{\mathbf{v} \in \mathbb{F}_2^N : \mathbf{v} \cdot \mathbf{c} = 0 \text{ for all code words } \mathbf{c} \text{ for } C\} .$$

If a code is cyclic with generating polynomial $G(X)$ and syndrome polynomial $H(X)$, show that the dual code is also cyclic and find its generating polynomial.

Find the dual of the Hamming code; show that it is cyclic; and find its generating polynomial.

- Factor the polynomials $X^3 - 1$, $X^5 - 1$ and $X^7 - 1$ into irreducibles in $\mathbb{F}_2[X]$. Hence find all binary cyclic codes of length 3, 5 or 7 and relate them to codes you have already met.

8. Show that we can identify $\mathbb{F}_2[X]/(X^4+X+1)$ with the set K of polynomials: $p_0+p_1\alpha+p_2\alpha^2+p_3\alpha^3$ in a variable α that we assume satisfies $\alpha^4+\alpha+1=0$. Show by direct calculation that $K^\times = K \setminus \{0\}$ is a cyclic group and deduce that K is finite field with 2^4 elements. (We already know this from general results about finite fields but it is instructive to do the calculations.)
9. 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 $\alpha, \alpha^2, \alpha^3, \alpha^4$.
- (a) Show that if β is a zero of $P(X) \in \mathbb{F}_2[X]$, then so is β^2 . Hence 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.
- (b) If possible, determine the error positions of the following received words
- (i) $R(X) = 1 + X^6 + X^7 + X^8$
- (ii) $R(X) = 1 + X + X^4 + X^5 + X^6 + X^9$
- (iii) $R(X) = 1 + X + X^7$.

[Your answer to Question 8 may help with the computations.]

10. Let C be the binary cyclic code of length $N = 2^d - 1$ defined by a primitive N th root of unity. (So its generating polynomial is the minimal polynomial for the root.)
- (a) Show that if $g(X) \in \mathbb{F}_2[X]$ then $g(X)^2 = g(X^2)$.
- (b) Show that C is a BCH code of design distance 3, rank d and length N .
- (c) Deduce that C is equivalent to the Hamming code of length N defined in question 1.
11. Let C be a binary, linear code of length n with A_j codewords of weight j . The weight enumerator polynomial is

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

- (a) We transmit a codeword through a binary symmetric channel with error probability p . Give a formula, in terms of the weight enumerator polynomial, for the probability that the word received is a codeword.
- (b) Show that $W_C(x, y) = W_C(y, x)$ if and only if $W_C(1, 0) = 1$.
12. Show that $RM(m, r)$ has dual code $RM(m, m - r - 1)$.

[Hint: First show that, for subsets I, J of $\{1, 2, 3, \dots, m\}$, we have

$$x_I \cdot x_J = \begin{cases} 0 & \text{when } I \cup J \neq \{1, 2, 3, \dots, m\}; \\ 1 & \text{when } I \cup J = \{1, 2, 3, \dots, m\}. \end{cases}$$

13. Show that if $2^K \sum_{j=0}^{\delta-2} \binom{N-1}{j} < 2^N$ then $A(N, \delta) \geq 2^K$. Compare this with the GSV bound in the case $n = 10$ and $\delta = 3$.
- [Hint: See question 9 of Example Sheet 2 for the definition of $A(N, \delta)$. Construct a syndrome matrix for a linear code by choosing one column at a time.]
14. What is a linear feedback shift register? Show that, subject to a suitable non-degeneracy condition, any output stream x_0, x_1, x_2, \dots produced by a linear feedback shift register is periodic.
- Give an upper bound for the period of the output sequence from a linear feedback shift register with R registers over \mathbb{F}_q . Show that if this upper bound is achieved then it is achieved by any non-zero initial vector.
15. A non-linear feedback register over \mathbb{F}_2 of length 4 has defining relation $x_{n+1} = x_n x_{n-1} + x_{n-3}$. Show that the state space contains 4 cycles of lengths 1, 2, 4 and 9.

Please send any comments or corrections to me at: t.k.carne@dpmms.cam.ac.uk.