TOPICS IN DISCRETE MATHEMATICS 3/4: EXERCISES SHEET 2

Hand in Questions 2,6 and 11. Deadline - Fri. 22nd Feb.

(1) Let $\mathcal{C}$ be the $[5,3]_5$-linear code with generator matrix

$$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 4 & 1 \end{pmatrix}.$$

Find a parity check matrix for $\mathcal{C}$.

(2) List the elements of $\mathcal{C}^\perp$ for the $[4,2]_3$-linear code with generator matrix

$$G = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 2 & 0 & 2 \end{pmatrix}.$$

(3) Let $\mathcal{E}_n := \{\mathbf{v} \in \mathbb{F}_2^n \,|\, \mathrm{wt}(\mathbf{v}) \equiv 0 \mod 2\}$ - the set of even-weight vectors in $\mathbb{F}_2^n$. By Problem sheet 1 (question 6), this is a linear code. Prove that $\mathcal{E}_n^\perp = \mathcal{R}_n$.

(4) Let $\mathcal{C} \leq \mathbb{F}_q^n$ be a linear code, where $q = p$ a prime. Assume that $\mathcal{C} \subseteq \mathcal{C}^\perp$ - here we call $\mathcal{C}$ *weakly self-dual.*

(a) Show that $\sum_i^n c_i^2 = 0$ for all codewords $\mathbf{c} \in \mathcal{C}$.

(b) Deduce that if $q = 2, 3$ then $q \,|\, \mathrm{wt}(\mathbf{c})$ for all $\mathbf{c} \in \mathcal{C}$.

(c) For $q \geq 5$ show that the result in (b) fails in general - i.e. find a weakly self-dual linear code $\mathcal{C} \leq \mathbb{F}_q^n$ having a codeword whose weight is not divisible by q.

(5) For the following sets of parameters $\{n, k, d, q\}$, indicate whether or not there exists an $[n, k, d]_q$-linear code. Justify your answer.

(a) $n = 6$, $k = 4$, $d = 4$, $q = 3$.

(b) $n = 8$, $k = 2$, $d = 4$, $q = 2$.

(6) Suppose that $\mathcal{C}$ is an $[6,2]_5$-linear code. What is the largest possible error correcting index of $\mathcal{C}$?

(7) Show that the binary repetition code $\mathcal{R}_n$ is perfect if and only if n is odd.

(8) Consider the linear codes $\mathcal{C}_i \leq \mathbb{F}_3^4$ defined by the generator matrices G_i given below. Establish which codes are equivalent.

$$G_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}, G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}, G_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}, G_4 = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

(9) Fix $k \geq 3$. Show that any two binary Hamming codes $\mathcal{H}_k$ and $\mathcal{H}'_k$ are equivalent.

(10) Find the weight enumerators for the following linear codes over $\mathbb{F}_2$ and their dual codes:

Date: February 13, 2019.

(a) The linear code with generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

(b) The linear code with parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

(11) For each of the polynomials given below, determine (with justification) if it is the weight enumerator of a linear code over $\mathbb{F}_2$.

(a) $x^6y + 2x^4y^3 + y^7$

(b) $x^6 + 30x^4y^2 + x^3y^3 + y^6$

(c) $x^4 + 2x^2y^2 + y^4$

(d) $x^5 + 2x^4y + 2xy^4 + 3y^5$

(e) $\frac{1}{2}\left((x+y)^{16} + (x-y)^{16}\right)$.

(12) In lectures we demonstrated how to correct one error in a linear code. In the printed notes (at the end of chapter 4) there is a discussion of how to extend this to more than one error. Let's see a worked example (it will be useful to have the lectures to hand).

(a) Firstly, we need Lemma 4.6: Two vectors $\mathbf{u}, \mathbf{v}$ have the same syndrome if and only if $\mathbf{u} - \mathbf{v} \in \mathcal{C}$. Prove this.

(b) Now using Proposition 4.7, we can design an algorithm for correcting errors. This involves finding a set of coset leaders and storing the syndromes in a look-up table.

(c) Let $\mathcal{C}$ be the $[5, 1, 5]_2$-linear code over with parity check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Check that this in fact defines $\mathcal{C} = \mathcal{R}_5 = \{00000, 11111\}$. Now there are 16 cosets of $\mathcal{C}$ in $\mathbb{F}_2^5$ (why 16?) given by the coset leaders

$$\{\mathbf{0}\} \cup \{\mathbf{e_i} \,|\, 1 \le i \le 5\} \cup \{\mathbf{e_i} + \mathbf{e_j} \,|\, 1 \le i < j \le 5\}$$

These then have syndromes

Coset Leader	Syndrome
$\mathbf{0}$	0000
$\mathbf{e_1}$	1000
$\mathbf{e_2}$	0100
$\mathbf{e_3}$	0010
$\mathbf{e_4}$	0001
$\mathbf{e_1} + \mathbf{e_2}$	1100
$\mathbf{e_1} + \mathbf{e_3}$	1010
$\mathbf{e_1} + \mathbf{e_4}$	1001
$\mathbf{e_2} + \mathbf{e_3}$	0110
$\mathbf{e_2} + \mathbf{e_4}$	0101
$\mathbf{e_3} + \mathbf{e_4}$	0011
$\mathbf{e_4} + \mathbf{e_5}$	1110
$\mathbf{e_3} + \mathbf{e_5}$	1101
$\mathbf{e_2} + \mathbf{e_5}$	1011
$\mathbf{e_1} + \mathbf{e_5}$	0111
$\mathbf{e_5}$	1111

Notice how each syndrome of weight at most 2 is in a unique row, as expected. We can now decode some errors. Assuming that at most 2 errors have been made, follow the decoding algorithm described on page 14 of the printed notes, to correct the following vectors and find the intended codeword.

$$00110, 10001, 11101.$$

E-mail address: alex.malcolm@bristol.ac.uk