Topics in Discrete Mathematics: Error-Correcting Codes: Exercise sheet 1.

Dan Fretwell

Spring semester 2017/18

These exercises cover up to chapter 4 of the notes. A handful of them will be set as homework but you should attempt **all** problems.

1. For each of the following codes over $\mathbb{F}_3$ find the values of n, M and d. If the code is linear state also the value of k.

   (a) $C = \{000, 122\}$,

   (b) $C = \{0000, 1221, 2112, 2200, 2002, 1001, 0220, 0110, 1201\}$,

   (c) $C = \{000, 111, 222, 100, 200, 211, 022, 011, 122\}$,

   (d) $C = \mathrm{Span}_{\mathbb{F}_3}(\{2002010, 0000100, 0100001\})$,

   (e) $C = \mathrm{Span}_{\mathbb{F}_3}(\{21212, 11022, 12121, 00200, 10000\})$.

   Do you now see why linear codes are the best thing since sliced bread? Write a short poem to express your gratitude for the existence of Proposition 4.14. A prize will be awarded for the most bad-ass rhymes.

2. Find the values of n, k, d and M for the follwing linear codes over $\mathbb{F}_7$:

   (a) The code with generator matrix:

   $$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 4 & 2 \end{pmatrix}$$

   (b) The code with parity check matrix:

   $$\begin{pmatrix} 1 & 2 & 1 & 6 & 2 & 0 & 3 \\ 0 & 1 & 2 & 1 & 4 & 5 & 0 \\ 0 & 0 & 1 & 5 & 2 & 4 & 2 \end{pmatrix}$$

3. In this question we investigate the ISBN code.

   (a) Find the values of n, k and d for the ISBN code. How many codewords are there?

   (b) Find the missing digits in these ISBN numbers:

$$0330a19026$$
$$000723b184$$
$$055c818104$$
$$034051308d$$

   (c) For each $i \in \{1, .., 9\}$ find an ISBN number of the form $\mathbf{c}_i = \mathbf{e}_i + a_i \mathbf{e}_{10}$ for some $a_i \in \mathbb{F}_{11}$. Hence write down a generator matrix for the ISBN code.

   (d) Consider errors made by swapping two (distinct) entries of a word. Can ISBN detect one such error? Can it correct one?

4. Let C be a $[n, k, d]$-linear code over $\mathbb{F}_p$. For each $m \geq 2$ consider the code C_m whose words are of the form $x|x|...|x \in \mathbb{F}_p^{mn}$ for $x \in C$. Find the parameters for C_m and show that its error correcting index t_m satisfies $t_m \geq mt$, with strict inequality when $m \geq 3$. Deduce that for $m \geq 3$ the code C_m corrects at least one error.

5. Let $C = \{00000, 01011, 10101, 11110\} \subseteq \mathbb{F}_2^5$.

   (a) Show that C is a $[5, 2, 3]$-linear code.

   (b) Let

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

   Use the Rank-Nullity theorem to show that $\text{nullity}(A) = 2$.

   (c) Show that $C \subseteq \text{NullSpace}(A)$ and hence deduce that A is a parity check matrix for C.

   (d) Alternatively show that A is a parity check matrix for C by explicitly finding $\text{Null}(A)$.

   (e) Which method was quicker? Which method would be quicker if the proposed parity check matrix A has 1000000 columns and 999998 linearly independent rows? Describe a life or death situation in which using the "clever" method would allow you to live and the "mundane" method would give you an untimely death. A prize will be awarded for the most elaborate submission.

6. Show that there does not exist a $[13, 8, 5]$-linear code over $\mathbb{F}_3$.

7. Let C be a perfect $[n, k]$-linear code over $\mathbb{F}_p$. Show that if $t = 1$ then $n = \frac{p^{n-k}-1}{p-1}$. Deduce that a perfect binary code with $t = 1$ satisfies $(n, k) = (2^r - 1, 2^r - r - 1)$ where $r = n - k$ (later we will see an example of such a code for each choice of r, the Hamming codes).

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