Topics in Discrete Mathematics: Error-Correcting Codes: Exercise sheet 2.

Dan Fretwell

Spring semester 2017/18

These exercises cover chapter 5 of the notes and beyond. A handful of them will be set as homework but you should attempt **all** problems.

1. (a) I challenge you to a dual! List the elements of $C^\perp$ for the linear code over $\mathbb{F}_3$ with generator matrix:
$$G = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 2 & 0 & 2 \end{pmatrix}.$$
   (b) Find a parity check matrix for the linear code over $\mathbb{F}_5$ with generator matrix:
$$G = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 3 & 0 & 1 \\ 0 & 0 & 1 & 4 & 1 \end{pmatrix}.$$
2. Let C be a linear code of length n over $\mathbb{F}_p$. Assume C is weakly self dual, i.e. $C \subseteq C^\perp$.
   (a) Show that $\sum_{i=1}^n c_i^2 = 0$ for each codeword $\mathbf{c} \in C$.
   (b) Deduce that if $p = 2, 3$ then $p \mid \mathrm{wt}(\mathbf{c})$ for each $\mathbf{c} \in C$.
   (c) For $p \geq 5$ show that the result in (b) fails in general, i.e. find a weakly self dual linear code over $\mathbb{F}_p$ having a codeword whose weight is not divisible by p.
3. We say that a linear code C is self dual if $C = C^\perp$.
   (a) Show that the length n of such a code is even and that the dimension is $k = \frac{n}{2}$.
   (b) Show that for dual codes the set of parity check matrices is the same as the set of generator matrices.
   (c) Let n be even. Show that any matrix $G \in M_{\frac{n}{2},n}(\mathbb{F}_p)$ of full rank satisfying $GG^T = 0$ defines a self dual code.
4. In this Question you may need to use Question 3.

(a) Show that no Hamming code is self dual.

(b) Consider the extended Hamming code $\mathbf{Ham}_3^{\text{ext}} \subseteq \mathbb{F}_2^8$ consisting of words $\mathbf{c} = c_1...c_8$ such that $c_1...c_7 \in \mathbf{Ham}_3$ and $\sum_{i=1}^{8} c_i = 0$. Write down a parity check matrix for $\mathbf{Ham}_3^{\text{ext}}$ and show that this code is self dual.

(c) Show that $4|\text{wt}(\mathbf{c})$ for each $\mathbf{c} \in \mathbf{Ham}_3^{\text{ext}}$ (i.e. the extended code is doubly even). Hence find the weight enumerator of $\mathbf{Ham}_3^{\text{ext}}$.

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

(a) The linear code with generator matrix:

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

(b) The linear code with parity check matrix:

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

6. Show that if C is a binary self dual code (i.e. $C = C^{\perp}$) then its weight enumerator is invariant under the linear transformations defined by $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (You may need to use questions 2 and 3).

Challenge: Show that every such polynomial can be written as a polynomial in $x^2 + y^2$ and $x^2y^2(x^2 - y^2)^2$.

7. Fix $n \geq 1$. Define the Krawtchouk polynomials for $j \geq 0$:

$$P_j(x) = \sum_{m=0}^{j} (-1)^m \binom{x}{m} \binom{n-x}{j-m},$$

where the binomial coefficients are defined for $f(x) \in \mathbb{Z}[x]$ by:

$$\binom{f(x)}{m} = \begin{cases} \frac{f(x)(f(x)-1)...(f(x)-(m-1))}{m!} & \text{if } m \geq 1 \\ 1 & \text{if } m = 0 \\ 0 & \text{if } m < 0 \end{cases}$$

(a) If C is a binary $[n, k]$-linear code with weight distribution $\mathbf{A} = (A_0, ..., A_n)$, show that $C^{\perp}$ has weight distribution $\mathbf{A}' = (A'_0, ..., A'_n)$ satisfying:

$$A'_i = \frac{1}{2^k} \sum_{j=0}^{n} A_j P_i(j),$$

i.e. $2^k \mathbf{A}' = P\mathbf{A}$ with matrix $P = (P_i(j))$.

(b) Deduce that if C is self dual then the weight distribution is a $2^{\frac{n}{2}}$-eigenvector of P whose entries are natural numbers summing to $2^{\frac{n}{2}}$.

8. (a) Suppose the code $\mathbf{Ham}_4$ is used and you receive the message $\mathbf{v} = 111100000001111$. Show that at least one error has been made and correct it (under the assumption that exactly one error has been made).

   (b) Suppose the BCH code from Example 7.15 is used and you receive the message $\mathbf{v} = 1000001$. Deduce that two or more errors have been made and correct them (under the assumption that exactly two errors have been made).

   (c) Show that the BCH code from Example 7.15 is boring since it is really just the repetition code $\mathcal{R}_7$. Hence deduce that this code actually corrects 3 errors, even though we only designed it to correct 2.