Exercise Sheet 4

Exercise 4.1. Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$. Consider the $[8,5]_4$-code with check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 \\ 0 & 0 & 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 \end{pmatrix}$$

(This code is obtained from an algebraic geometric construction using a maximal elliptic curve over the field. Such codes will be the topic of a later lecture.)

1. Show that the minimum distance of this code is 3.
2. We would like to prove the optimality of this $[8,5,3]_4$-code using the linear programming bound. What is the objective function we wish to maximize? Write down the Krawtchouk polynomials $K_k(x)$ for $k = 0, 1, 2$ and the corresponding linear constraints.

See the solution sheet for a full description of the linear program and its solution.

Exercise 4.2. Let n, k, d be positive integers ($k \leq n - d + 1$), and consider the ensemble of all $(n-k) \times n$ matrices over $\mathbb{F}_q$ of the form

$$H = (A \mid I)\,,$$

where I is the $(n-k) \times (n-k)$ identity matrix and A is arbitrary, and define a probability distribution on this ensemble induced by a uniform distribution over the $(n-k) \times k$ matrices A over $\mathbb{F}_q$.

1. Show that for every nonzero vector $y \in \mathbb{F}_q^n$,

$$\Pr[Hy^\top = 0] = \begin{cases} 0 & \text{if the first } k \text{ entries in } y \text{ are zero} \\ q^{k-n} & \text{otherwise.} \end{cases}$$

2. Show that

$$\Pr[H \text{ contains } d-1 \text{ dependent columns}] \leq \rho,$$

where

$$\rho := q^{k-n} \cdot \sum_{i=1}^{d-1} \left(\binom{n}{i} - \binom{n-k}{i} \right) (q-1)^{i-1}.$$

3. Deduce that all but a fraction at most ρ of the systematic linear $[n,k]$ codes over $\mathbb{F}_q$ (i.e., codes with parity check matrices of the form above) have minumum distance at least d.

Exercise 4.3. An (n, M, d)-code is called an $(n, M, d; w)$ *constant-weight code* if each nonzero codeword has Hamming weight w. Let $\mathcal{C}$ be an $(n, M, d = 2t+1; w = 2t+1)$ constant-weight code over $\mathbb{F}_q$.

1. For every codeword $c \in \mathcal{C}$, how many words y of Hamming weight $t+1$ are there in $\mathbb{F}_q^n$ that are at Hamming distance t from c?
2. Show that
$$M \leq \frac{\binom{n}{t+1}(q-1)^{t+1}}{\binom{2t+1}{t}}.$$

Exercise 4.4. A *burst of length* ℓ is the event of having errors in a codeword such that the locations i and j of the first (leftmost) and last (rightmost) errors, respectively, satisfy $j - i = \ell - 1$. Let $\mathcal{C}$ be a linear $[n,k]_q$-code that is able to correct every burst of length t or less.

1. Show that in every nonzero codeword $c \in \mathcal{C}$, the locations i and j of the first and last nonzero entries in c must satisfy $j - i \geq 2t$.
2. Show that $n - k \geq 2t$.
3. Show that
$$q^{n-k} \geq 1 + n(q-1) + (q-1)^2 \sum_{i=0}^{t-2} (n-i-1)q^i.$$
(Hint: proceed similarly to the sphere-packing bound, but now the shape of the "balls" are different: for a given codeword w, we only care to count the vectors that differ from w by a burst of size at most t.)

Exercise 4.5. Let $A(n,d)$ denote the largest number M of codewords in any code of length n and minimum distance d.

1. Show that $A(n, 2r-1) = A(n+1, 2r)$. Hence it is enough to find $A(n,d)$ for even values of d.
2. Show that $A(n,d) \leq 2A(n-1,d)$.