

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 minimum distance at least d .

Exercise 4.3. Recall that, for integer parameters n, q , we defined Krawtchouk polynomials as

$$K_\ell(x) := \sum_{r=0}^{\ell} \binom{x}{r} \binom{n-x}{\ell-r} (-1)^r (q-1)^{\ell-r}.$$

First, show that

$$(1 + (q - 1)z)^{n-x}(1 - z)^x = \sum_{r=0}^x \binom{x}{r} (1 + (q - 1)z)^{n-r} (-qz)^r.$$

Then, compute and compare the coefficients of z^ℓ on both sides. Using this, derive an alternative form of Krawtchouk polynomials.

Exercise 4.4. Denote by $A(n, d, w)$ the maximal number of codewords in a binary code of length n and minimum distance at least d for which all codewords have the same weight w .

1. Let \mathcal{C} be an (n, k, d) -code containing the zero codeword. Show that the number of nonzero words in \mathcal{C} with weight up to d is at most $A(n, d, d)$.
2. Show that $A(n, 2k - 1, w) = A(n, 2k, w)$.
3. Show that $A(n, 2k, w) \leq nA(n - 1, 2k, w - 1)/w$.
(*Hint:* Suppose that \mathcal{C} is a binary code of length n , minimum distance at least $2k$ for which all codewords have weight w . As in the proof of Plotkin bound, arrange the words of \mathcal{C} as rows of a matrix and upper bound the number of ones in each column of this matrix.)
4. Conclude that

$$A(n, 2k, w) \leq \left\lfloor \frac{n}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \dots \left\lfloor \frac{n-w+k}{k} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor.$$