Combinatorics and Graph Theory I

Exercise sheet 9: coding theory

7 May 2018

1. Let C be a binary linear code. Show that the subset of C containing those codewords which have even weight is also a linear code. Deduce that either all codewords in C have even weight, or exactly half of them have even weight.

[N. Biggs, *Discrete Mathematics,* rev. ed., 1989, 17.2, exercise 4]

2. Let $([n^2+n+1], \mathcal{L})$ be a projective plane of order n, in which the set of points is identified with the set of integers $[n^2+n+1] := \{1, 2, \ldots, n^2+n+1\}$.

Define the $(n^2+n+1, \log_2(n^2+n+1), d)_2$ binary code C as the set of vectors $\{\mathbf{x}^{(L)} = (x_1^{(L)}, \ldots, x_{n^2+n+1}^{(L)}) : L \in \mathcal{L}\}$ in which

$$x_i^{(L)} = \begin{cases} 1 & i \in L \\ 0 & \text{otherwise.} \end{cases}$$

(The vector $\mathbf{x}^{(L)}$ is a row of the line–point incidence matrix of the projective plane.)

Show that the minimum distance of C is equal to $2n$.

[N. Biggs, *Discrete Mathematics,* rev. ed., 1989, 17.7, exercise 17]

3. Let

$$C = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \\ x_{k+1} \end{pmatrix} \in \mathbb{F}_q^{k+1} : \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} \in \mathbb{F}_q^k, \quad \sum_{i=1}^{k} x_i = x_{k+1} \right\},$$

where the summation involves addition in $\mathbb{F}_q$.

(i) Explain why the code C has $(k+1) \times k$ generator matrix

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

(ii) In lectures you saw that for $q = 2$ the code C has $(k+1) \times 1$ parity check matrix

$$H = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Write down a parity check matrix for C for general prime power q.

(iii) Show that C achieves the Singleton bound given in question 5(ii) below.

4.

(i) Suppose that C is a linear binary code of length n and dimension k. Show that if e is the maximum number of errors that C will correct by minimum distance decoding then

$$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}.$$

(ii) Deduce from (i) that no linear binary code of length 17 and dimension 10 can correct more than one error.

(iii) Suppose more generally that C is a linear code over $\mathbb{F}_q$ of length n and dimension k. Show that if e is the maximum number of errors that C will correct by minimum distance decoding then

$$q^{n-k} \geq \sum_{j=0}^{e} \binom{n}{k} (q-1)^j.$$

[N. Biggs, *Discrete Mathematics,* rev. ed., 1989, 17.2, extended]

5.

(i) Show that if C is a q-ary block code of length n and minimum distance d then

$$|C| \leq q^{n-d+1}.$$

[*By assumption any two codewords* $(x_1, x_2, \ldots, x_n)$ *and* $(y_1, y_2, \ldots, y_n)$ *differ in at least* d *places. Consider the map* $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-d+1})$ *with domain* C *defined by deleting the last* $d-1$ *letters of each codeword.*]

(ii) Deduce from (i) that if C is a linear code over $\mathbb{F}_q$ with block length n, dimension k and minimum distance d then

$$d \leq n - k + 1.$$

(iii) Derive the result of (ii) in a different way by using the fact that the rank of the parity check matrix for C is equal to $n - k$.