Telecom ParisTech
Teacher: Aslan Tchamkerten

ACCQ204, Coding Theory
November 2018

ASSIGNMENT 2

Exercise 1. Determine the parameters (n, k, d) of the binary code

$$C = \{00001100, 00001111, 01010101, 11011101\}$$

Exercise 2 ($A(n, d)$, extending, puncturing, expurgating)**.** Define the intersection of length n binary vectors x and y to be the vector $x * y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$.

1. Show that
$$wt(x + y) = wt(x) + wt(y) - 2wt(x * y)$$
2. Show that $A(n, d) \leq A(n-1, d-1)$. Hint: consider 'puncturing', that is removing a common coordinate from every codeword.
3. Show that $A(n, 2r - 1) = A(n + 1, 2r)$ where $A(n, d)$ denotes the largest number of lenth n codewords with minimum distance d. Hint: consider 'extending' codewords by adding a parity check bit, i.e., $x_1, x_2, \ldots, x_n$ becomes $x_1, x_2, \ldots, x_n, \sum x_i$.
4. Show that $A(n, d) \leq 2A(n - 1, d)$. Hint: consider dividing codewords into two classes, those beginning with a 0 and those beginning with a 1.

Exercise 3. For each of the following codes

$$C_1 = \{00000, 01010, 00001, 01011, 01001\}$$

$$C_2 = \{000000, 101000, 001110, 100111\}$$

$$C_3 = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}.$$

tell if it is linear and evaluate the parameters (n, k, d).

Exercise 4. The dual of an $[n, k]_q$ code $\mathcal{C}$ is the set

$$\mathcal{C}^{\perp} = \{c \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in \mathcal{C}\}$$

($\langle \cdot, \cdot \rangle$ denotes the standard "scalar" product).

Show that if G and H are the generator and parity matrices, respectively, of $\mathcal{C}$, then H and G are the generator and parity matrices, respectively, of $\mathcal{C}^{\perp}$.

Exercise 5. Let C_1 and C_2 be an $[n, k_1, d_1]$ and an $[n, k_2, d_2]$ code, respectively. Let $C_1|C_2$ be the code consisting of all codewords of the form

$$(u, u + v) = (u_1, u_2, \ldots, u_n, u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

with $u = (u_1, u_2, \ldots, u_n) \in C_1$ and $v = (v_1, v_2, \ldots, v_n) \in C_2$. Show that $C_1|C_2$ is an $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ code. Hint. consider the cases $v = v'$ and $v \neq v'$. For the second case use the triangle inequality.

Exercise 6. In this exercise we show the existence of linear codes over $[q]$, $q \geq 2$, which achieve the Gilbert-Varshamov bound. To that aim we show the existence of a full rank generator matrix G of dimension $k \times n$ such that

$$k = (1 - H_q(\delta) - \varepsilon)n$$

and such that

$$wt(mG) \geq d$$

for any $m \in \mathbb{F}_q^k$.

1. Pick G randomly such that each of its elements is independently chosen with the uniform distribution over $[q]$. Fix $m \neq 0$. We first show that for such a random G, mG is a uniformly chosen vector over $[q]^n$.

   (a) Let X_i denote the i-th symbol of the n-vector mG. Show that X_i is independent of X_j for $i \neq j$.

   (b) Let $X_i = \sum_{j=1}^{k} m_j G_{ji}$. Since $m \neq 0$, at least one of its elements is non-zero. Say m_ℓ is the first non-zero element. Thus we can write $X_i = m_\ell G_{\ell i} + \sum_{j=\ell+1}^{k} m_j G_{ji}$. Using this, show that X_i is uniformly distributed over $[q]$ by conditioning over the possible realizations of $G_{\ell+1,i}, G_{\ell+2,i}, \ldots, G_{k,i}$.

2. Deduce that

$$Pr[wt(mG) < d] \leq \frac{q^{nH_q(\delta)}}{q^n}.$$

   Hint. $Vol_q(d-1, n) \leq q^{nH_q(\delta)}$.

3. Deduce that $Pr(\exists m : \ wt(mG) < d) \leq q^{-\varepsilon n}$ for some appropriate choice of k.

4. Conclude the proof.

Exercise 7. Is the code $C = \{000, 110, 011, 101\}$ MDS?

Exercise 8. Suppose we are in $\mathbb{F}_2$. Find

1. gcd$(x^4 + x^2 + 1, x^2 + 1)$
2. gcd$(x^6 + x^5 + x^3 + x + 1, x^4 + x^2 + 1)$
3. gcd$(x^6 + x^5 + x^3 + x + 1, x^4 + x^3 + x + 1)$

Exercise 9. Show that a Reed-Solomon code with 1 message symbol and n codeword symbols is an n times repetition code.