1 Problem List 1

Задача 1.1. Show that a code with minimal distance d can fix up to $d-1$ erasures - unknown bits at fixed positions.

Доказательство. The decoder needs to fill in $d-1$ (known) coordinates in order to recover the transmitted codeword. Suppose that there are two different possible ways of filling in these $d-1$ coordinates and these give us two different codewords c and $\hat{c}$. Hamming distance between c and $\hat{c}$ can't be $d-1$ or smaller, because it contradicts the assumption that any two distinct codewords must differ in at least d places. (this argument can be applied iff the locations of the errors are known) □

Задача 1.2. Are there exists $(n, k, d)_q$-codes as follows (recall that q is alphabet size, n is block size, k is number of information symbols, d is the minimal distance):

(a) $[n, n, 1]_q$

(b) $[n, n-1, 2]_q$

(c) $[11, 5, 5]_2$

(d) $[20, 7, 5]_2$

(e) $[22, 15, 3]_2$

Доказательство. (a) input = output

(b) binary parity check code of length n

(c) $d=5$ means all patterns of up to two bit errors can be corrected, but $2^{11-5} = 64 < \binom{11}{2} + 11 + 1 = 67$

(d)

(e)

□

Задача 1.3. Find $(n, k, d)_q$ satisfying Hamming condition but with $d > n-k+1$

Доказательство. Singleton bound If C is a linear code with block length n, dimension k and minimum distance d over the finite field with q elements, then the maximum number of codewords is q^k and the Singleton bound implies:

$$q^k \leq q^{n-d+1}$$
$$k \leq n-d+1$$
$$d \leq n-k+1$$

□

Задача 1.4. Propose a $(n, n-1, 2)_q$-code that can detect transposition of any pair of symbols (when symbols exchange their places).

Доказательство. □

Задача 1.5. Suppose $C \subset V = \mathbb{F}_q^n$ be a linear code. By dual code denote $C^* = \operatorname{Ann}(C) \subset V^*$. So if C is $(n, k, d)_q$ - code, then C^* is $(n, n-k, d')_q$ - code for some d'.

(a) Show that for natural dual bases we have generator and parity check matrices for C^* coincide with parity check and generator matrices for C respectively.

(b) Show that group of repeating symbol corresponds to check sum of this group in the dual code.

(c) Find a minimal distance for the code, dual to Hamming code. code generated by a polynomial $x^k h\left(x^{-1}\right)$, where $h(t) = \left(t^n - 1\right)/g(x)$.

(d) Suppose that C is a cyclic polynomial $(n, k, d)_q$ - code generated by polynomial $g(x)$. Show that $C*$ is a cyclic code generated by a polynomial $x^k h(x^{-1})$, where $h(t) = (t^n - 1)/g(x)$

(e) Is dual to polynomial code always polynomial?

Доказательство. (a)

(b)

(c)

(d)

(e)

□

Задача 1.6. For a given graph with m vertices and n edges we associate $(n, n - m, d)_q$ code as follows. Bits are enumerated by edges, a vector is a code word iff sum of bits for all edges with a common vertex is zero.

(a) Find a graph associated with repeating code.

(b) Find minimal distance of the code associated with n-gone.

(c) Find minimal distance of the code associated with a simplex on m vertices.

(d) Find minimal distance of the code associated with Petersen graph

Доказательство. (a)

(b)

(c)

(d)

□