Edgar
Kaziakhmedov

Assignment 2

Information Theory
05.03.2019

Problem 1

a. $\boldsymbol{n}$ (length) $= 9$,
$\boldsymbol{k}$ (dim) $=$ rank(G) $= 3$ (obtained after Gaussian elimination),
$\boldsymbol{d}$ (distance) $= 3$ (obtained from parity check matrix)

b.

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \sim \left[\begin{array}{ccc|cccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] = \left[\begin{array}{c|c} I_k & P \end{array}\right]$$

c.

$$H = \left[\begin{array}{c|c} -P^T & I_{n-k} \end{array}\right] = \left[\begin{array}{ccc|cccccc} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

d. C is a [n,k]-code (in out case [9,3])
$C^{\perp}$ (dual) is a [9,6] code [Th. 7.3 p. 68 Hill]
parity check matrix H of [9,3]-code C is a generator matrix of $C^{\perp}$
$d_{C^{\perp}} = 2$

Problem 2

Basically we need to consider two-dimensional single parity check code size of $n_1 \times n_2$ (look at the picture bellow with example)

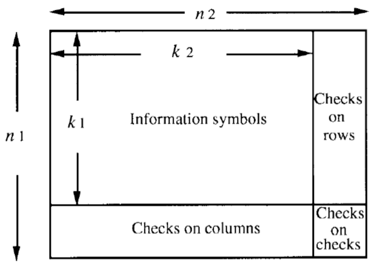

Figure 1: Two-dimensional single parity check code

So, to obtain codeword weight of 4 we need to put 4 bits in a following way (outlined boxes are parity bits):

....	....	....	....	....	....	....	....
....	....	....	....	....	....	....	....
....	....	1	....	....	1	....	....
....	....	....	....	....	....	....	....
....	....	....	....	....	....	....	....
....	....	1	....	....	1	....	....
....	....	....	....	....	....	....	....
....	....	....	....	....	....	....	....

So, first of all, we need to select two different columns, then select two different rows in those columns, therefore the number of all possible 4 bit positions (in accordance with aforementioned pattern):

$$\boxed{N_4 = C_{n_1}^2 C_{n_2}^2}$$

In case of codeword weight of 6 the idea is the same, so we simply place 6 bits in following way:

....	....	....	....	....	....	....	....
....	1	....	1	....	....	....	....
....	....	....	....	....	....	....	....
....	....	....	1	....	1	....	....
....	....	....	....	....	....	....	....
....	1	....	....	....	1	....	....
....	....	....	....	....	....	....	....
....	....	....	....	....	....	....	....

At the first glance everything looks similar, we select 3 rows randomly and then 3 columns in the same manner, but the difference is that the pattern is not symmetric, so we can permute it and have to take this fact into account (3! possible permutations):

$$\boxed{N_6 = 3! C_{n_1}^3 C_{n_2}^3}$$

Problem 3

Let's look at [8, 4] extended Hamming code.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Notice that weights of all codewords $\in \{0, 4, 8\}$

Now, assume that all extended Hamming code is cyclic with $g(x)$:

$$g(x) | x^8 - 1$$

$$deg(g(x)) = 4 \quad (1)$$

$$x^8 - 1 = (x^4 - 1)^2 \quad (2)$$

From (1) and (2) $\Rightarrow g(x) = x^4 - 1$, consider $u(x) = 1$, polynomial for code-word is equal to $v(x) = 1g(x)$. Vector corresponding to $v(x)$ has weight 2. It's a contradiction $\Rightarrow$ extended Hamming code isn't cyclic.

Problem 4

$\mathcal{C}$ is a cyclic code with $g(x)$:

$$g(x) | x^n - 1$$

$$x + 1 \not| g(x) \quad (1)$$

$$x^n - 1 = (x + 1) \underbrace{(x^{n-1} + ... + 1)}_{\text{all coefficients} = 1} \quad (2)$$

From (1) and (2) $\Rightarrow g(x) | x^{n-1} + ... + 1 \Rightarrow \underbrace{(11...1)}_{\text{all ones}}$ - code-word

Answer doesn't depend on n.

Problem 5

a) $GF(2^3)$, $\phi(x) = x^3 + x + 1$:

$$\alpha^0 = 1,$$

$$\alpha^1 = \alpha,$$

$$\alpha^2 = \alpha^2,$$

$$\alpha^3 = \alpha + 1,$$

$$\alpha^4 = \alpha^2 + \alpha,$$

$$\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1,$$

$$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1,$$

$$\alpha^7 = \alpha^3 + \alpha = 1$$

b) $n = 7$, $k = 5$, $d = n - k + 1 = 3$

c)

$$F_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} & \alpha^{24} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^{18} & \alpha^{24} & \alpha^{30} & \alpha^{36} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}$$

$$V = u_{ext}F$$

$$W_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$$

$$\hat{u} = \hat{V}W$$

$$\hat{u} = \begin{bmatrix} \alpha & 0 & \alpha & 1 & \alpha^6 & \alpha^3 & \alpha^2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$$

$$\hat{u} = \begin{bmatrix} \alpha + 1 & 1 & \alpha^2 + \alpha & 0 & \alpha & \alpha^2 + 1 & 1 \end{bmatrix}^T$$

$$\sigma(x) = \sigma_1 x + 1$$

$$\sigma_1 = \frac{1}{\alpha^2 + 1} = \alpha$$

Recursively calculate errors:

$$e_4 = \frac{e_5}{\sigma_1} = \frac{\alpha^6}{\alpha} = \alpha^5$$

$$e_3 = \frac{e_4}{\sigma_1} = \frac{\alpha^5}{\alpha} = \alpha^4$$

$$e_2 = \alpha^3$$

$$e_1 = \alpha^2$$

$$e_0 = \alpha$$

Correct occurred errors: $u = \hat{u} + \mathbf{e}$

$$u = \left[\begin{array}{ccccc} 1 & \alpha^6 & \alpha^6 & \alpha^4 & \alpha^6 \end{array}\right]$$

Problem 6

The MaxWilliams identity is the following:

$$W(C, x, y) = \frac{1}{|C_\perp|} W(C_\perp; y - x; y + x)$$

$$W(C_\perp, x, y) = \sum_{w=0}^{n} A_w x^w y^{n-w}$$

Where A_w is a number of codewords in dual code weight of w.
Let's do an estimate on cardinal of $C_\perp$. We can consider subtraction of two info vectors:

$$(u_1 - u_2)G_\perp = (u_1 - u_2)H$$

Let's consider conditions when those two vectors correspond to the codeword, we can say that, the following equation,

$$(u_1 - u_2)H = 0$$

holds true if $(u_1 - u_2)$ is equal to all ones or all zeros (case with zeros is clear and we don't consider it), but let's consider then it equal to all ones. As H iterates of all possible combinations with two ones, for final vector to be zero we need $u_1 - u_2$ to be of all ones (to work out ones in H). Hence, for each vector we have inverted version. Therefore:

$$|C_\perp| = \frac{2^m}{2}$$

For particular position in codeword to be one, we have to have 1 and 0 on the same positions as in H but in info vector, so the number of 1s in codevector is equal to the number of pairs 1 and 0 in infovector or $k(m - k)$, where k is number of ones in infovectors, so:

$$W(C_\perp, x, y) = \sum_{w=0}^{n} C_m^k x^{k(m-k)} y^{C_m^k - k(m-k)}$$

And finally:

$$\boxed{W(C,x,y) = \frac{1}{2^{m-1}} \sum_{w=0}^{n} C_m^k (y-x)^{k(m-k)} (y+x)^{C_m^k - k(m-k)}}$$

Problem 7

Let's define the states of the trellis as follows: Let s_r be the label of the state at time r, then

$$s_{r+1} = s_r + x_{r+1}\boldsymbol{h}_{r+1} = \sum_{l=1}^{r} x_l \boldsymbol{h}_l$$

where x_{r+1} runs through all permissible code symbols at time $r+1$. The state at the end of time interval $r+1$, s_{r+1} is calculated form the preceding state s_r. We see that this equation simply implements the parity check equation $\boldsymbol{H}x = 0$ in a recursive fashion, since the final zero-state $s_{n+1} = \sum_{l=1}^{n} x_l \boldsymbol{h})_l = \boldsymbol{H}x$ is the complete parity check equation.

a. There can be at most $\boxed{2^{n-k}}$ distinct states at time r, since that is the maximum number of distinct binary vectors of length $n-k$.

b. The maximum number of outgoing edges is 2. The maximum number of incoming edges is 2 as well.

c. Before we start, let's represent given parity check matrix in a systematic way:

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \sim \left[\begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Let us construct the trellis of the given code (Fig.2):
The states s_r are labeled as ternary vectors $(\sigma_1, \sigma_2, \sigma_3)^T$. All the path extensions which lead to states $s_{n+1} \neq (000)^T$ are not shown, since $s_i^{(i)}$ is the final syndrome and must equal $(000)^T$ for x to be a code word. The red lines of the trellis are such that a "0" causes a horizontal transition and a "1" causes a sloped transition. This follows from initial formula for states. ($x_{r+1} = 0$ causes $s_{r+1} = s_r$).

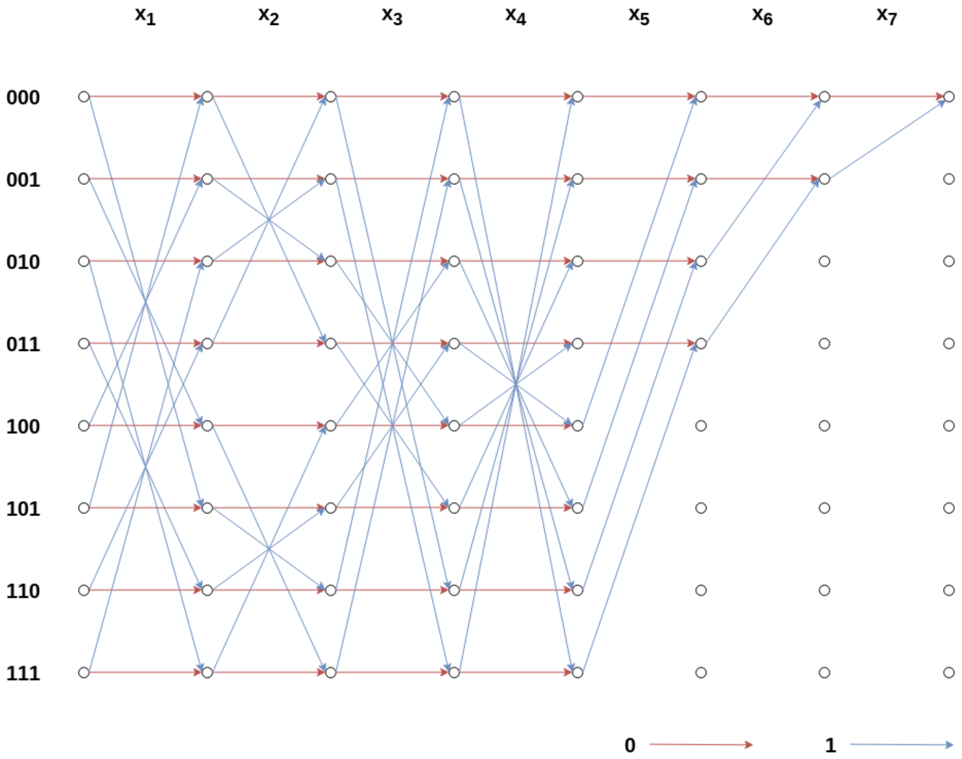

Figure 2: Trellis diagram