Information and coding theory HW#2

Evgeny Marshakov

Problem 1

Obviously, as codes C_1 and C_2 are of the same dimension k with lengths n_1 and n_2, then the code with generator matrix $G = [G_1|G_2]$ has the same number of rows, hence have the same dimension and has the length $n_1 + n_2$.

Let c_1, c_2 be the codewords s.t.

$$\|c_i\|_H = d(C_i) = d_i$$

Then it is obvious that if we have the row $(c_1|c_2)$ in the generating matrix then $d(C) = d(C_1)+d(C_2) = d_1+d_2$. Also it is obvious that in general $d(C) \geq d_1 + d_2$. So the code with generator matrix G has the parameters $(n_1 + n_2, k, \geq d_1 + d_2)$

Problem 2

If we can realize the extended [8, 4] Hamming code as a cyclic code then it is an ideal in the ring $\mathbb{F}_2[x]/(x^8-1)$. As we are working over field of characteristic 2, then we have the following

$$x^8 - 1 = x^8 + 1 = (x + 1)^8 \tag{1}$$

We know that the generating polynomial is a factor of $x^8 - 1$. Due to (1) we obtain that $g(x) = (x + 1)^i$, for $1 \leq i \leq 7$. We know that the hamming code is 4-dimensional code, so the generating polynomial $g(x) = (x + 1)^4$. It can be easily seen that

$$\|g(x)\|_H = \|(x + 1)^4\|_H = \|1 + x^4\|_H = 2 \tag{2}$$

So we have a contradiction with the fact that the distance of the extended [8, 4] Hamming code is 4.

Problem 3

We know that the generating polynomial $g(x)$ is a factor of $x^n - 1$. So

$$g(x)m(x) = x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1) = (x+1)(x^{n-1} + x^{n-2} + \ldots + x + 1) \quad (3)$$

The last equality is true due to the characteristic of our field. As $(x+1) \nmid g(x)$ then $m(x) = (x+1)p(x)$ and we obtain

$$g(x)m(x) = (x+1)g(x)p(x) = x^n - 1 \Rightarrow g(x)p(x) = 1 + x + \ldots + x^{n-2} + x^{n-1} \quad (4)$$

Hence, our code contains the all-one codeword.

Problem 4

Let us construct a finite field

$$GF(2^4) = \mathbb{F}_2[x]/(x^4 + x^3 + 1) \quad (5)$$

Let α be a primitive element of this field. Then

$$\alpha^0 = 1 \tag{6}$$

$$\alpha^1 = \alpha \tag{7}$$

$$\alpha^2 = \alpha^2 \tag{8}$$

$$\alpha^3 = \alpha^3 \tag{9}$$

$$\alpha^4 = \alpha^3 + 1 \tag{10}$$

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^4 + \alpha = 1 + \alpha + \alpha^3 \tag{11}$$

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha + \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3 \tag{12}$$

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^2 \tag{13}$$

$$\alpha^8 = \alpha + \alpha^2 + \alpha^3 \tag{14}$$

$$\alpha^9 = \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha^2 \tag{15}$$

$$\alpha^{10} = \alpha + \alpha^3 \tag{16}$$

$$\alpha^{11} = \alpha^2 + \alpha^4 = 1 + \alpha^2 + \alpha^3 \tag{17}$$

$$\alpha^{12} = \alpha + \alpha^3 + \alpha^4 = 1 + \alpha \tag{18}$$

$$\alpha^{13} = \alpha + \alpha^2 \tag{19}$$

$$\alpha^{14} = \alpha^2 + \alpha^3 \tag{20}$$

$$\alpha^{15} = \alpha^3 + \alpha^4 = 1 \tag{21}$$

To construct primitive [15, 7] BCH code that can correct two errors we need to find polynomial with roots $\alpha, \alpha^2, \alpha^3, \alpha^4$ that divides $x^n - 1$. We know that ff α is a root of irreducible polynomial over the field $GF(2^4)$ then $\alpha^2, \alpha^4, \alpha^8$ are also the roots of the this polynomial. The same is true for α^3 and $\alpha^6, \alpha^9, \alpha^{12}$. It can be easily checked that

$$p_1 = (x)(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x^3 + 1 \tag{22}$$

$$p_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = x^4 + x^3 + x^2 + x + 1 \tag{23}$$

hence

$$g(x) = p_1(x)p_3(x) = x^8 + x^4 + x^2 + x + 1 \tag{24}$$

As we are working with cyclic code then the generator matrix is the following

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{25}$$

We received a vector

$$f = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{26}$$

We know from Sagalovich that syndrome can be calculated as follows

$$S_1 = 1 + \alpha^1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6 + \alpha^7 + \alpha^1 4 = \alpha \tag{27}$$

$$S_2 = 1 + \alpha^2 + \alpha^4 + \alpha^6 + \alpha^8 + \alpha^{12} + \alpha^{14} + \alpha^{13} = \alpha^2 \tag{28}$$

$$S_3 = 1 + \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^3 + \alpha^6 + \alpha^{12} = \alpha^2 \tag{29}$$

and that an equation for locators has the following form

$$x^2 + S_1 x + S_1^2 + \frac{S_3}{S_1} = x^2 + \alpha x + \alpha^2 + \alpha = 0 \tag{30}$$

It can be easily checked that α^3, α^{10} are the roots of this equation. So the correct code vector is the following

$$\tilde{f} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{31}$$

It can be easily checked that

$$g(x)(1+x^6) = \tilde{f}(x) \tag{32}$$

So the message is

$$m = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{33}$$

Problem 5

Let us construct a finite field

$$GF(2^3) = \mathbb{F}_2[x]/(x^3+x^2+1) \tag{34}$$

Let α be a primitive element of this field. Then

$$\alpha^0 = 1 \tag{35}$$

$$\alpha^1 = \alpha \tag{36}$$

$$\alpha^2 = \alpha^2 \tag{37}$$

$$\alpha^3 = \alpha^2 + 1 \tag{38}$$

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha^3 + \alpha = 1 + \alpha + \alpha^2 \tag{39}$$

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha + \alpha^2 + \alpha^3 = 1 + \alpha \tag{40}$$

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha + \alpha^2 \tag{41}$$

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha^2 + \alpha^3 = 1 \tag{42}$$

We know that Reed-Solomon's code achieve an equality in Singleton's bound, so $d = n - k + 1 = 5$. From lectures we know that the generating polynomial is the following

$$g(x) = (x-\alpha)\dots(x-\alpha^{d-1}) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 + \alpha^2 x^3 + \alpha^3 x^2 + x + \alpha^3 \tag{43}$$

The parity check matrix of our code is the following

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{bmatrix} \tag{44}$$

We can find the syndrome of our message $f^T = [\alpha^4, \alpha^2, \alpha^4, 0, 0, \alpha, \alpha^6]$

$$S = Hf = \begin{bmatrix} 1 \\ \alpha \\ 0 \\ \alpha^4 \end{bmatrix} \tag{45}$$

So we can easily obtain the system on coefficients of error locator polynomial

$$\begin{bmatrix} S_2 & S_1 \\ S_3 & S_2 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} \tag{46}$$

Substituting S_i we obtain the following system

$$\begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^4 \end{bmatrix} \tag{47}$$

from which we can find that $\sigma_1 = \alpha^2, \sigma_2 = \alpha^3$. So we find the error locator polynomial

$$\sigma(z) = \alpha^3 z^2 + \alpha^2 z + 1 \tag{48}$$

This polynomial has the following roots

$$z_1 = \alpha^{-3} \tag{49}$$

$$z_2 = \alpha^0 \tag{50}$$

Now we know that we have errors on the first and the fourth places. Now from the system

$$\begin{cases} Y_1 + Y_2\alpha^3 = S_2 = \alpha \\ Y_1 + Y_2\alpha^5 = S_4 = \alpha^4 \end{cases} \tag{51}$$

we can find that $Y_1 = \alpha^2, Y_2 = 1$, so received message is the following

$$\tilde{f} = \begin{bmatrix} \alpha^5 & \alpha^2 & \alpha^4 & 1 & 0 & \alpha & \alpha^2 \end{bmatrix} \tag{52}$$

It can be easily seen that

$$(\alpha^6 x^2 + \alpha^2) \cdot g(x) = \tilde{f} \tag{53}$$

So the message is the following

$$m(x) = \alpha^2 + \alpha^6 x^2 \tag{54}$$

or

$$m = \begin{bmatrix} \alpha^2 & 0 & \alpha^6 \end{bmatrix} \tag{55}$$

Problem 6

Let us see on the matrix H as on the matrix that determined the graph in the following way: number of rows correspond to number of verticies , number of columns corresponds to number of edges. If $H_{ij} = 1$ then the i-th vertex belongs to the j-th edge. It can be easily seen that the matrix H determines a complete graph on n verticies. So any codeword in the dual code can be described as follows: we choose any set of verticies $W \subset V$ and put 1 on the places corresponding to edges that connect W and $V \backslash W$. Indeed, if we choose two verticies i, j that connect with the edge e then in the corresponding rows we find ones on the places (ie) and (je), so in the sum we find 0 on e-th place.

Thus, if we choose k verticies we obtain a codeword with $(m-k)k$ ones. So the weight enumerator of the

dual code is the following

$$W_{C^\perp}(x,y) = \sum_{k=0}^{m} \binom{m}{k} x^{\binom{m}{2}-(m-k)k} y^{(m-k)k} \tag{56}$$

Applying MacWilliam's identities we can find that

$$W_C(x,y) = \frac{1}{|C^\perp|} W_{C^\perp}(x+y, x-y) = \frac{1}{2^m} \sum_{k=0}^{m} \binom{m}{k} (x+y)^{\binom{m}{2}-(m-k)k} (x-y)^{(m-k)k} \tag{57}$$

Problem 7

Any element c of our code is determined by the following equation

$$\begin{bmatrix} \mathbf{h}_1 & \mathbf{h}_2 & \dots & \mathbf{h}_n \end{bmatrix} \cdot c = 0 \tag{58}$$

Any state S can be described as follows

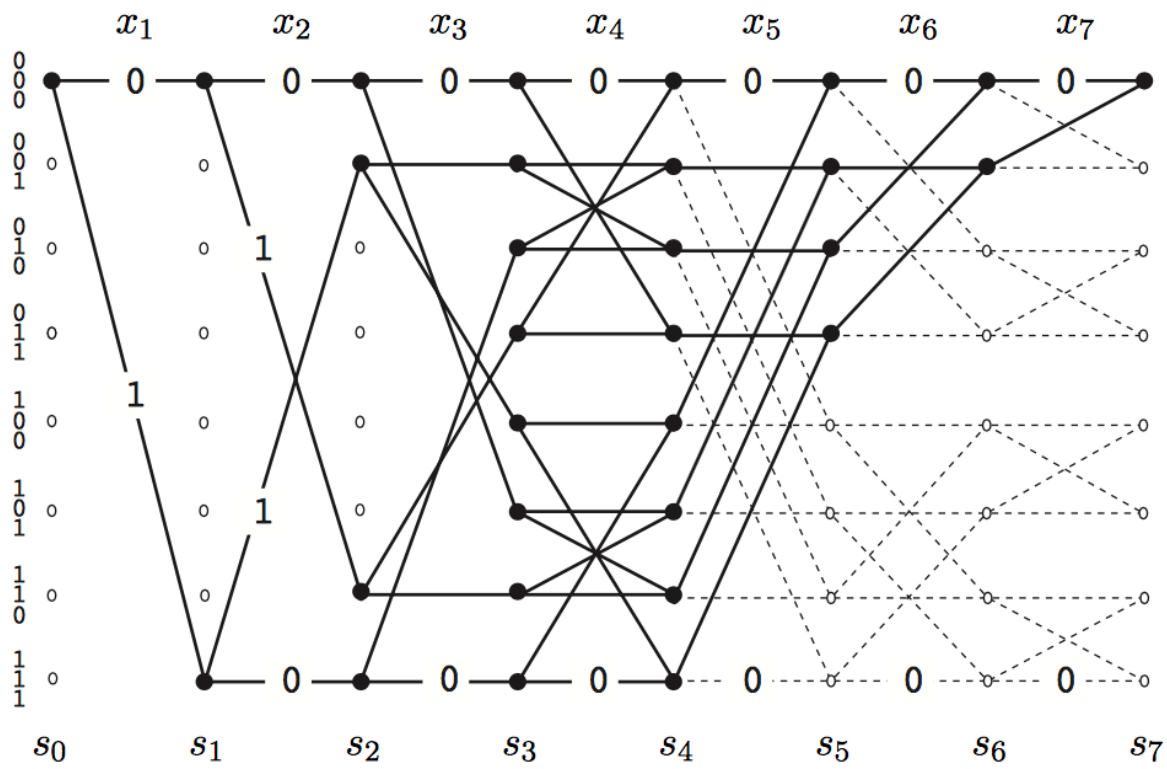
$$S = \left\{ \sum_{i=0}^{n} x_i \mathbf{h}_i \middle| x_i \in \{0,1\} \right\} \tag{59}$$

Note that there are 2^n different sets of the coefficients $\{x_i^{(t)}\}$, but all $\mathbf{h}_i$ lie in $(n-k)$-dimensional space, so there are $2^{(n-k)}$ different states.

Let $S^k, 0 \le k \le n$ be a layer of the trellis, i.e.

$$S^k = \left\{ \sum_{i=0}^{k} x_i \mathbf{h}_i \middle| x_i \in \{0,1\} \right\} \tag{60}$$

So our trellis consists of $n+1$ layers. To get from the k-th layer to $k+1$-th we add to our state $\mathbf{h}_{k+1}$ with some coefficient (zero or one). Thus, there are two edges incoming and two edges outcoming from each state. Here is trellis for the Hamming code with another parity check matrix. They are isomorphic, so it's not a problem.


x_1 x_2 x_3 x_4 x_5 x_6 x_7
0000
0001
0010
0011
1000
1001
1100
1111
s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7