NTIN 100 Intro to Info Transmission and Processing summer 2016/2017

3nd homework assignment - Error correcting codes

turn in by May 4, 2017.

Problem 1. Let G_1 and G_2 be generating matrices of codes with parameters $[n_1, k, d_1]_q$ and $[n_2, k, d_2]_q$. Find the parameters of the codes generated by the following matrices.

a)

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

b)

$$\begin{pmatrix} G_1 & G_2 \end{pmatrix}$$

c)

$$G_1 \otimes G_2 = \begin{pmatrix} a_{1,1}G_2 & a_{1,2}G_2 & \cdots & a_{1,n_1}G_2 \\ a_{2,1}G_2 & a_{2,2}G_2 & \cdots & a_{2,n_1}G_2 \\ \cdots & \cdots & \cdots & \cdots \\ a_{k,1}G_2 & a_{k,2}G_2 & \cdots & a_{k,n_1}G_2 \end{pmatrix}.$$

Here

$$G_1 = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n_1} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n_1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k,1} & a_{k,2} & \cdots & a_{k,n_1} \end{pmatrix}$$

and $a_{i,j}G_2$ is the matrix G_2 with every entry multiplied by $a_{i,j}$.

Problem 2. In Reed-Solomon code we interpret each message $m = m_1 m_2 \cdots m_k \in GF[q]$ as the coefficients of a polynomial $p_m(x)$, and the codeword corresponding to m is $(p_m(\alpha_1), \ldots, p_m(\alpha_n))$. Consider a different code, where to each m we assign a polynomial $p'_m(x)$ of degree at most $k-1$ such that $p'_m(\alpha_i) = m_i$, pro $i = 1, \ldots, k$, and $(p'_m(\alpha_1), p'_m(\alpha_2), \ldots, p'_m(\alpha_n))$ will be the codeword of m. Show that this code is again Reed-Solomon code. Find the generating matrix of this code.

Problem 3. Let n be a positive integer. Consider the following code: each message is a matrix M from $GF[2]^{n\times n}$. The codeword of M consists of M together with parities of each row, each column, and the parity of the parities, i.e., a codeword is from $GF[2]^{(n+1)\times(n+1)}$. How many errors can this code correct? How do you correct the errors?

Problem 4. Let H be the parity check matrix of a linear code C over $GF[2]$, where C is generated by a $k \times n$ matrix G. (That is $C = \{bG,\, b \in \{0,1\}^k\} = \{y \in \{0,1\}^n,\, yH = 0\}$.) Show that the minimum distance of C is d if and only if every $d-1$ rows of the matrix H are linearly independent and there are d rows in H, that are linearly dependent. Does the claim hold also over fields other than $GF[2]$? ($GF[2]$ is the field with elements 0 and 1 and computing mod 2.)

Problem 5. Let p be a prime. Using uniqueness of prime factorization of each integer show, that for each $m \in \{1, \dots, p-1\}$, the function $f_m(x) = m \cdot x \bmod p$ is a bijection from $\{1, \dots, p-1\}$ to $\{1, \dots, p-1\}$ (it is *one-to-one* and *onto*). Conclude that $\{0, \dots, p-1\}$ with counting mod p is a field, in particular, show that there are inverses for multiplication.