

3rd homework assignment - Error correcting codes

turn in by April 24, 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)

$$(G_1 \ G_2)$$

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. Consider an undirected graph $G = (V, E)$ with m vertices and n edges. Each subset of the edges of G can be represented by a vector $\{0, 1\}^n$, where each coordinate corresponds to an edge of G and indicates whether the edge is present in the subset. Define a code $C_{\text{cut}} \subseteq \{0, 1\}^n$ of vectors that represent cuts in G , that is subsets of edges $F \subseteq E$ such that for some subset $S \subseteq V$, $F = \{\{u, v\}, u \in S \ \& \ v \notin S\}$.

a) Show that C_{cut} is a linear code.

b) Show that if we can efficiently find for each $x \in \{0, 1\}^n$ the closest codeword from C_{cut} , then we can efficiently find the largest cut in G . Finding the largest cut in G is so called MAX-CUT problem that is known to be NP-complete.

Problem 3. In Reed-Solomon code we interpret each message $m = m_1m_2 \cdots m_k \in GF[q]$ as the coefficients of a polynomial $p_m(x)$, and the codeword corresponding to m is $(p_m(\alpha_1), \dots, p_m(\alpha_n))$. Consider a different code, where to each m we assign a polynomial $p'_m(x)$ of degree at most $k - 1$ such that $p'_m(\alpha_i) = m_i$, for $i = 1, \dots, k$, and $(p'_m(\alpha_1), p'_m(\alpha_2), \dots, p'_m(\alpha_n))$ will be the codeword of m . Show that this code is again Reed-Solomon code. Find the generating matrix of this code.

Problem 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.)