EE 605: Error Correcting Codes

Assignment 1

Due: Thu, Oct 21st, 2021

General rules: I am ok if you discuss the homework with other students, but it is mandatory to write the answers on your own and mention at the start who all you have discussed the homework with. Failure to do so might lead to a straight rejection of the homework submission.

Question: 1. Prove that the following claims are equivalent:

1. A code $\mathcal{C}$ is MDS.
2. Every subset of k columns of the generator matrix G are linearly independent.
3. Every subset of $n-k$ columns of H are linearly independent.
4. If the generator matrix G is of the form $[I_k|A]$ ($k \times (n-k)$ matrix) where I_k is a $k \times k$ identity matrix, then A has the property that its every square submatrix has full rank.

Question: 2. Show that all binary (n,k,d) MDS codes are either of the form $(n,n,1)$ or $(n,1,n)$ or $(n,n-1,2)$. Also construct a binary MDS code of each form for any n.

Question: 3. Let $A(n,d)$ denote the largest number of codewords M in an (n,M,d) binary code.

1. Show that $A(n,d) \leq 2A(n-1,d)$.
2. Show that $A(2d,d) \leq 4d$. Hint: Use the above together with the Plotkin bound derived in class for $d < n/2$.
3. Show that the Reed-Muller code $RM(m,1)$ satisfies the above with equality.

Question: 4. We briefly mentioned the generator matrix of a Generalized Reed-Solomon (GRS) code. Consider $F = GF(q)$ for $q > n$, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote distinct non-zero elements of F and let $v_1, v_2, \ldots, v_n$ be non-zero elements of F. The generator matrix is given by

$$G_{GRS} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} v_1 & 0 & 0 & \ldots & 0 \\ 0 & v_2 & 0 & \ldots & 0 \\ 0 & 0 & v_3 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & v_n \end{pmatrix}$$

Show that the dual of a GRS code is also a GRS code with the same set of evaluation points.

Question: 5. Consider an $(n = 4, k = 2)$ Reed-Solomon code over $F = GF(5) = \{0, 1, 2, 3, 4\}$ with evaluation points comprising of all non-zero elements of F.

1. Find the generator matrix and the parity check matrix corresponding to this code.
2. Find the codeword corresponding to the message $(1, 1)$.
3. Suppose the received word is (2040). Demonstrate the working of the Berlekamp-Welch algorithm and find the output codeword.

Question: 6. (*singly extended* RS codes) Consider the following parity check matrix of a $[n = q, k, d]$ code over $GF(q)$:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{q-1}^2 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{q-k-1} & \alpha_2^{q-k-1} & \ldots & \alpha_{q-1}^{q-k-1} & 0 \end{pmatrix}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ are the non-zero elements of $GF(q)$. This corresponds to adding an overall parity check to an $[n = q - 1, k, d = q - k]$ GRS code with code multipliers $v_i = \alpha_i$. Show that the code is MDS and thus the additional parity check increases the minimum distance of the code by one.

Question: 7. (*doubly extended* RS codes) Consider the following parity check matrix of a $[n = q + 1, k, d]$ code over $GF(q)$:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} & 0 & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{q-1}^2 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{q-k} & \alpha_2^{q-k} & \ldots & \alpha_{q-1}^{q-k} & 0 & 1 \end{pmatrix}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ are the non-zero elements of $GF(q)$. Show that the code is MDS.

Question: 8. (*Wozencraft ensemble*): We showed the existence of a Wozencraft ensemble with rate $1/2$ in the class. Here we extend this to find a family of codes with rate in $(1/2, 1)$. Show that for any $1 \leq l \leq k$, there exists a family $\mathcal{F}$ of $[n = l + k, k]$ binary linear codes with the following properties:

1. The size of the family $|\mathcal{F}| = 2^k - 1$.
2. Most codes in the family have a relative distance of at least $H^{-1}\left(\frac{l}{l+k} - \epsilon\right)$, for any $\epsilon > 0$.

Hint: Consider the map $x \to (x, (\alpha x)_l)$ *where* $(y)_l$ *denotes the first* l *bits of* $y \in F_2^k$.