Coding Theory : Endsem Exam (Back Paper)

M Tech (CS), 2025-26

Date: 17.12.2025 Time: Total Marks: 60

---

1. All the statements proven in the class can be assumed without proofs.
2. To solve a sub-problem of a particular problem in the question paper, you can assume all its previous sub-problems without proof.
3. Other than that, anything you use needs to be proven.
4. During examination, *only* handwritten notes are allowed, printouts/electronic notes are *not* allowed. Calculators are also *not* allowed during the examination.

---

1. (4 marks) Let G be a generator matrix of an $[n,k,d]_2$ code. Then, show that G has at least kd ones in it.

2. **(6 marks)** For any $[n,k,d]_2$ code, either all of the codewords begin with a zero or exactly half of the codewords begin with a zero.

3. **(10 marks)** For $i = 1,2$, let C_i be an $[n_i,k_i,d_i]_2$ linear code over $\mathbb{F}_2$. Let C be the subsets of $\mathbb{F}_2^{n_1 \times n_2}$ consisting of those matrices for which every column, respectively every row, is a codeword in C_1, respectively C_2. Show that C is an $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ code.

4. **(10 marks)** Let q be a prime power. Then, show that an $[n,k]_q$ code C is an MDS code if and only if for any generator matrix G of it, the following holds: any set of k columns of G are linearly independent.

5. **(10 marks)** Let $\mathbb{F}_q$ be the finite field of size q. Let $E = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_q$, that is, $n \leq q$. Let $k \in \mathbb{Z}_{\geq 1}$ such that $k \leq n$. Let $\mathrm{RS}(E,k,q)$ be the set of Reed-Solomon codes of block length n, dimension k, and alphabet $\mathbb{F}_q$, defined using E as the evaluation points. That is,

$$\mathrm{RS}(E,k,q) = \Big\{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f(x) \in \mathbb{F}_q[x] \text{ such that } \deg(f) < k\Big\}.$$

For $E = \mathbb{F}_q$, show that $\mathrm{RS}(E,k,q)^{\perp} = \mathrm{RS}(E,q-k,q)$.

6. Let $G = (L,R,E)$ be a c-left-regular and d-right-regular bipartite graph with the left vertex set $L = [n]$, the right vertex set $R = [m]$, and the set of edges $E \subseteq L \times R$. For any $r \in R$ and $j \in [d]$, let $N_j(r)$ denote the j-th smallest neighbor of r, that is, if $\{i_1, i_2, i_3, \ldots, i_d\} \subset L$ be the set of neighbors of r with $i_1 < i_2 < \cdots < i_d$, then $N_j(r) = i_j$. Let $\Sigma = \{0,1\}^d$. For all $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \{0,1\}^n$, define $G(\mathbf{u}) \in \Sigma^m$ as follows: For all $r \in [m]$, $G(\mathbf{u})_r$, the r-th coordinate of $G(\mathbf{u})$, is

$$G(\mathbf{u})_r = \left(u_{N_1(r)}, u_{N_2(r)}, \ldots, u_{N_d(r)}\right).$$

Let $C \subseteq \{0,1\}^n$ be a binary code of block length n. Let $G(C) \subseteq \Sigma^m$ be a code over the alphabet Σ, defined as follows:

$$G(C) = \Big\{G(\mathbf{c}) \Big| \mathbf{c} \in C\Big\}.$$

Now show the following.

   (a) **(10 marks)** $R(G(C)) = \frac{1}{c} \cdot R(C)$, where $R(C)$ and $R(G(C))$ are the rates of C and $G(C)$, respectively.

   (b) **(10 marks)** Suppose that G and C satisfies the following property: For some $\gamma, \epsilon \in (0,1)$, let $\mathrm{dist}(C) \geq \gamma n$, and for every $S \subseteq L$ with $|S| \geq \gamma n$, let $|N(S)| \geq (1-\epsilon)m$, where $N(S)$ denotes the set of neighbors of S. Then,

$$\mathrm{dist}(G(C)) \geq (1-\epsilon)m.$$