Coding Theory : Endsem Exam

M Tech (CS), 2025-26

Exam Date: 26/11/2025 Time: 2:30 PM-5:30 PM 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. 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,

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

Let $n, \ell, \delta \in \mathbb{Z}_{\geq 1}$ with $\gcd(n,q) = 1$, $n \mid (q^m - 1)$, and $\delta \leq n$. Let $\beta \in \mathbb{F}_{q^m}$ be an n-th primitive root of unity in $\mathbb{F}_{q^m}$, that is, $\beta^n = 1$ but for any integer $0 < m < n$, $\beta^m \neq 1$. Then, the BCH code over the alphabet $\mathbb{F}_q$ is defined as follows:

$$\mathrm{BCH}(n,\delta,q,\ell) = \left\{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n \,\middle|\, \forall\, i \in \{0,1,2,\ldots,\delta-2\},\ \sum_{j=0}^{n-1} c_j \beta^{(\ell+i)j} = 0,\ \right\}.$$

   (a) (**20 marks**) Consider the code $\mathrm{RS}(E,k,q)^\perp$, that is, the dual of $\mathrm{RS}(E,k,q)$. Design an error-correction algorithm $\mathcal{A}$ for $\mathrm{RS}(E,k,q)^\perp$ that runs in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations and can correct less than $\frac{k+1}{2}$ many errors. More specifically, given a $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ as input to $\mathcal{A}$ with the promise that there exists a codeword $\mathbf{c} \in \mathrm{RS}(E,k,q)^\perp$ such that $\Delta(\mathbf{y},\mathbf{c}) < \frac{k+1}{2}$, it outputs $\mathbf{c}$ in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations.

   (b) (**10 marks**) Design an error-correction algorithm $\mathcal{B}$ for $\mathrm{BCH}(n,\delta,q,1)$ that runs in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations and can correct less than $\frac{\delta}{2}$ many errors. More specifically, given a $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ as input to $\mathcal{B}$ with the promise that there exists a codeword $\mathbf{c} \in \mathrm{BCH}(n,k,q)^\perp$ such that $\Delta(\mathbf{y},\mathbf{c}) < \frac{\delta}{2}$, it outputs $\mathbf{c}$ in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations.

2. 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,

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

3. (**10 marks**) Let q be a prime power. Let C_{in} be an $[n,k]_q$ code and C_{out} be an $[N,K]_Q$ with $Q = q^k$. Let $C = C_{\mathrm{in}} \circ C_{\mathrm{out}}$ be the concatenated code of C_{out} and C_{in}. As discussed in the class, C is an $[Nn, Kk]_q$ code. Let $k < n$. Then, show that

$$\mathrm{dist}\left(C^\perp\right) \leq k+1,$$

where $C^\perp$ is the dual code of C.