MA 5105 Coding Theory, IITB
Exercises and Problems

Prof. Sudhir Ghorpade

(1) Exercise. Let Q be a finite set, n a positive integer, and let d_H denote the Hamming distance on Q^n. Show that d_H satisfies the triangle inequality. Deduce that (Q^n, d_H) is a metric space.

(2) Exercise. Let $n, k \in \mathbb{Z}^+$, $k \leq n$ and q be a prime power. Find a formula for the number of $[n, k]_q$ codes.

(3) Problem. Let $n, k \in \mathbb{Z}^+$, $k \leq n$ and q be a prime power. Find a formula for the number of $[n, k]_q$ MDS codes.

(4) Exercise. Solve Problem (**??**) for $k = 1, 2$.

(5) Exercise. Let F be a field. Define when a $m \times n$ matrix with entries in F is said to be in (i) row echelon form, (ii) reduced row echelon form. Given any $A \in M_{m\times n}(\mathsf{F})$, show that A is row-equivalent to a unique $B \in M_{m\times n}(\mathsf{F})$ such that B is in reduced row echelon form. [Optional Question: Can you find an explicit formula for the entries of B in terms of the entries of A?]

(6) Exercise. Let F be a field and let $n, k \in \mathbb{Z}^+$, $k \leq n$. Define a relation $\sim$ on $M_{k\times n}(\mathsf{F})$ by

$$A \sim B \iff B = EA \text{ for some } E \in GL_k(\mathsf{F}).$$

Show that $\sim$ is an equivalence relation on $M_{k\times n}(\mathsf{F})$ as well as on the subset $M^0_{k\times n}(\mathsf{F})$ of $M_{k\times n}(\mathsf{F})$ defined by $M^0_{k\times n}(\mathsf{F}) = \{A \in M_{k\times n}(\mathsf{F}) : \text{rank}(A) = k\}$. Further, suppose $F = \mathbb{F}_q$ and let $\mathcal{C}^0 = M^0_{k\times n}(\mathbb{F}_q)/\sim$ and $\mathcal{C} = M_{k\times n}(\mathbb{F}_q)/\sim$ denote the set of equivalence classes in $M^0_{k\times n}(\mathbb{F}_q)$ and $M_{k\times n}(\mathbb{F}_q)$ with respect to the above equivalence relation. Determine the cardinalities $|\mathcal{C}^0|$ and $|\mathcal{C}|$. Compare the former with Exercise (**??**).

(7) Exercise. Let F be a field and let $n, k \in \mathbb{Z}^+$, $k \leq n$. Let $A, B \in M_{k\times n}(\mathsf{F})$. When will A and B have the same nullspace?

(8) Exercise. Let $n, k \in \mathbb{Z}^+$, $k \leq n$ and q be a prime power. Let C be an $[n, k]_q$ code. Show that $C^\perp$ is an $[n, n-k]_q$ code.

(9) Let C be an $[n, k]_q$ code. Show that

(a) $\dim C^\perp = n - k$.

(b) $(C^\perp)^\perp = C$.

(10) Let C be an $[n, k]_q$ code. Show that a matrix $H \in M_{k\times n}(\mathbb{F}_q)$ is a parity check matrix for C if and only if H is a generator matrix for $C^\perp$.

(11) Let C be an $[n,k]_q$ code. Show that C is self-dual (i.e., $C = C^\perp$) if and only if C is self-orthogonal (i.e., $C \subseteq C^\perp$) and $n = 2k$.

(12) Let C be an $[n,k]_q$ code. Show that C is MDS if and only if $C^\perp$ is MDS.

(13) Let $n, k \in \mathbb{Z}^+$, $k \leq n$ and q be a prime power. Show that the q-binomial coefficient (or Gaussian binomial coefficient) defined by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n - 1)\cdots(q^n - q^{k-1})}{(q^k - 1)\cdots(q^k - q^{k-1})}$$

is a polynomial in q of degree $k(n-k)$.

(14) Let $n, k \in \mathbb{Z}^+$, $k \leq n$. Consider the Gaussian binomial coefficient $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ as a function from $(-\infty, 1) \cup (1, \infty)$ to $[0, \infty)$ defined by

$$q \longmapsto \frac{(q^n - 1)\cdots(q^n - q^{k-1})}{(q^k - 1)\cdots(q^k - q^{k-1})}.$$

Find $\lim\limits_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q$.

(15) r be a positive integre and let $n := (q^r - 1)/(q-1)$ be the number of "lines" in $\mathbb{F}_q^r$, i.e., the number of 1-dimensional subspaces of $\mathbb{F}_q^r$. Let $\mathbf{H}_r(q)$ be a $r \times n$ matrix with entries in $\mathbb{F}_q$ such that any two columns of $\mathbf{H}_r(q)$ are linearly independent. Define $\mathscr{H}_r(q)$ to be $[n, n-r]$-code with $\mathbf{H}_r(q)$ as its parity check matrix and $\mathscr{S}_r(q)$ to be $[n, r]$-code with $\mathbf{H}_r(q)$ as its generator matrix. These are called *Hamming code* and *simplex code*, respectively. Find the minimum distance of $\mathscr{S}_r(q)$ and $\mathscr{H}_r(q)$.

(16) Determine the spectrum of the simplex code $\mathscr{S}_r(q)$ defined above.

(17) Let n, k be positive integers with $n \geq k$ and q be a prime power with $q \geq n$. Fix distinct elements $a_1, \cdots, a_n \in \mathbb{F}_q[x]$ and let

$$\mathrm{C} := \{c_f = (f(a_1), f(a_2), \cdots, f(a_n)) : f(x) \in \mathbb{F}_q[X] \text{ with } \deg f(x) < k\}.$$

This code C is known as *Reed-Solomon code.*

Find a parity check matrix for this code C.

(18) Let m, ν be integers with $m \geq 1$ and $v \geq 0$, and let q be a prime power. Also let $\mathbb{F}_q[X_1, X_2, \ldots, X_m]_{\leq \nu}$ denote the set of all polynomials in m variables $X_1, \ldots, X_m$ of deg $\leq \nu$ with coefficients in $\mathbb{F}_q$. Show that $\mathbb{F}_q[X_1, X_2, \ldots, X_m]_{\leq \nu}$ is a finite dimensional vector space over $\mathbb{F}_q$ and find a formula for $\dim_{\mathbb{F}_q} \mathbb{F}_q[X_1, X_2, \ldots, X_m]_{\leq \nu}$.

(19) Let $P_1, \ldots, P_{q^m}$ be a fixed ordering of the q^m points in $\mathbb{F}_{q^m}$. Consider the evaluation map

$$\mathrm{Ev} : \mathbb{F}_q[X_1, X_2, \ldots, X_m]_{\leq \nu} \longrightarrow \mathbb{F}_{q^m}$$

defined by $\mathrm{Ev}(f) = (f(P_1), \ldots, f(P_{q^m}))$. Show that if $\nu < q$, then the map Ev is injective. Note: The image of this map Ev is called *generalized Reed-Muller code* of order ν and length q^m, denoted by $\mathrm{RM}_q(\nu, m)$.

(20) Show that if $f \in \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ is a nonzero polynomial of degree d, then f has at most dq^{m-1} zeroes in $\mathbb{F}_q^m$. Deduce that if $\nu < q$, then $d(\mathrm{RM}_q(\nu, m)) = (q-\nu)q^{m-1}$. (Optional Question: Find a formula for $\dim_{\mathbb{F}_q} \mathrm{RM}_q(\nu, m)$ for any $\nu \leq m(q-1)$.)

(21) Let $\mathbf{C}$ be a $[n,k]_q$-code. Use the **MacWilliams Identity**:

$$\mathrm{W}_{\mathrm{C}^\perp}(X,Y) = \frac{1}{|C|}\mathrm{W}_{\mathrm{C}}(X+(q-1)Y, X-Y)$$

to show that, the spectrum $\{A_i : 0 \leq i \leq n\}$ of C and $\{B_i : 0 \leq i \leq n\}$ of $C^\perp$ are related by

$$B_j = \frac{1}{|\mathbf{C}|}\sum_{i=0}^{n} K_j(i)A_i \quad \text{for } j = 0, 1, \ldots, n,$$

where $K_j = K_j^{n,q}(X)$ is the j^{th} **Krawtchouk polynomial** defined by:

$$K_j(X) := \sum_{r=0}^{j}(-1)^r \binom{X}{r}\binom{n-X}{j-r}(q-1)^{j-r}.$$

where for any $r \in \mathbb{Z}$, and variable X,

$$\binom{X}{r} := \begin{cases} \dfrac{X(X-1)\cdots(X-r+1)}{r!} & \text{if } r \geq 0, \\ 0 & \text{if } r < 0. \end{cases}$$

(22) Let $\mathbf{C}$ be a $[n,k]_q$-code and let A_j, B_j be as in Q. **??**. Show that

$$\sum_{j=0}^{n}\binom{j}{\nu}A_j = q^k \sum_{j=0}^{\nu}(-1)^j\binom{n-j}{n-\nu}(q-1)^{\nu-j}B_j \quad \text{for } \nu = 0, 1, \ldots, n.$$

(23) Show that $\{X^j : j \geq 0\}$ and $\{\binom{X}{j} : j \geq 0\}$ form two bases of the polynomial ring over a field in one variable.

(24) Show that every $[n,k]_q$-code C is permutation equlvalent to a code whose generator matrix is in standard form.

(25) Show that the Hamming code $\mathscr{H}_r(q)$ is perfect for any prime power q.

(26) Let $\mathbf{C}$ is a (n,M) code over an alphabet set Q of size q and if $d = \mathrm{d}(\mathbf{C})$ and $qd > (q-1)n$, then $\mathrm{M} \leq \left\lfloor \dfrac{qd}{qd-(q-1)n} \right\rfloor$. This bound on size of $\mathbf{C}$ is called **Plotkin Bound**. Show that the equality holds if and only if $\mathbf{C}$ is an equidistant code with $\mathrm{d}(\mathbf{C}) = d$ and $M(q-1)n = (M-1)qd$.

(27) The q-ary entropy function is the function $H_q : [0,1] \longrightarrow \mathbb{R}$ defined by

$$H_q(x) := x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x) \quad \text{for } 0 < x < 1.$$

Show that

(i) $H_q(1-x) - H_q(x) = (1-2x)\log_q(q-1)$ for all $x \in [0,1]$.

(ii) H_q is continuous on [0,1], differentiable on (0,1) increasing on $\left[0, \frac{q-1}{q}\right]$ and decreasing on $\left[\frac{q-1}{q}, 1\right]$. It has absolute maximum at $\frac{q-1}{q}$ with value 1 and local minima at 0 and 1 with values 0 and $\log_q(q-1)$, respectively.

(iii) Draw the graph of H_q for $q = 2, q = 3$, show that H_q has vertical tangent at 0 & 1.

(28) Suppose $q \geq 2$ and $0 < \theta < 1 - \frac{1}{q}$. Use Stirling's Formula to show that

$$\lim_{n\to\infty} \frac{1}{n} \log_q \binom{n}{\lfloor \theta n \rfloor} = -\theta \log_q \theta - (1-\theta)\log_q(1-\theta).$$

(Stirling's formula or approximation for factorials: $\log n! \approx n \log n - n + \frac{1}{2}\log(2\pi n)$, where $f(n) \approx g(n)$ means the ratio $f(n)/g(n)$ tends to 1 as n tends to ∞)

(29) Show that $\binom{n}{j}(q-1)^j$ is increasing in j for $\frac{j}{n} \leq \frac{q-1}{q}$.

(30) (**Spoiling a code**) Suppose there exists a $[n,k,d]_q$-code C with $k \geq 2$, $d \geq 2$ & $n > d$. Then show that there exists q-ary linear codes with the following parameters:

(i) $[n+1, k, d]$

(ii) $[n, k, d-1]$

(iii) $[n-1, k, d-1]$

(iv) $[n, k-1, d]$

(v) $[n-1, k-1, d]$.

(31) Consider the binary Hamming code $C = \mathscr{H}_3(2)$ of length 7 and dimension 4. Show that a generator matrix of this code is given by

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Use this to show that C is not cyclic. On the other hand, if C' is the binary $[7,4]$-code with generator matrix given by

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

then show that C' is cyclc and C' is (permutation) equivalent to C. Further, consider the ring $R_7 := \mathbb{F}_2[x] = \mathbb{F}_2[X]/\langle X^7 - 1\rangle$ and the natural map $\pi : \mathbb{F}_2^7 \to R_7$ given by $\pi(c_0, c_1, \ldots, c_6) = c_0 + c_1 x + \cdots + c_6 x^6$ for $(c_0, c_1, \ldots, c_6) \in \mathbb{F}_2^7$. Compare the ideals generated by the elements of $\pi(C')$ corresponding to the rows of C'. Also find the generator polynomial for the cyclc code C'. Is this polynomial irreducible? Is it primitive?

(32) Suppose C is a q-ary cyclic code of length n and $g(X)$ is the generator polynomial of C. Suppose $c(X)$ is a polynomial in $\mathbb{F}_q[X]$ such that $c(x)$ generates the ideal $\pi(C)$ under the natural map $\pi : \mathbb{F}_q^n \to R_n$, where $R_n = \mathbb{F}_q[x] = \mathbb{F}_q[X]/\langle X^n - 1\rangle$. Show that

$$g(X) = \mathrm{GCD}(c(X), X^n - 1).$$

Deduce that if G ia a generator matrix of C and if $g_1(X), \ldots, g_k(X)$ denote polynomials of degree $< n$ corresponding to the k rows of G, then the generator polynomial of C is given by

$$g(X) = \mathrm{GCD}(g_1(X), \ldots, g_k(X), X^n - 1).$$

(33) Let C be a $[n, k]_q$ cyclic code, where $1 \le k \le n$, and let G be any generator matrix of C. Show that the $k \times k$ submatrix formed by the first k columns of G is nonsingular. Deduce that the reduced row echelon form (rref) of G is a matrix of the form $[I_k|A]$, i.e., in standard form. Further show that if the last row of the rref of G is $[0, \ldots, 0, 1, a_1, \ldots, a_{n-k}]$, then $a_{n-k} \neq 0$ and the generator polynomial of C is given by

$$\frac{1}{a_{n-k}}\left(1 + a_1 X + a_z X^2 + \cdots + a_{n-k} X^{n-k}\right).$$

(34) Consider the $[6, 3]$-code over $\mathbb{F}_7$ with generator matrix G defined by

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix},$$

Show that C is cyclic and determine the generator polynomial of C.

(35) Suppose C is a q-ary code of length n. Recall that the *reversed code* $\rho(C)$ is defined by

$$\rho(C) := \{\rho(c) : c \in C\}, \quad \text{where} \quad \rho(c_0, c_1, \ldots, c_{n-1}) := (c_{n-1}, c_{n-2}, \ldots, c_1, c_0).$$

Show that $\rho(C)$ is also a q-ary code of length n, and the codes C and $\rho(C)$ are (permutation) equivalent. Further show that if C is cyclic and $g(X)$ is the generator polynomial of C, then $\rho(C)$ is cyclic with the monic reciprocal of $g(X)$ as its generator polynomial. Deduce that if C is reversible, i.e., $\rho(C) = C$, and also C is cyclic, then the generator polynomial of C is equal to its monic reciprocal.

(36) Show that a cyclic code C is reversible iff it is complementary dual, i.e., $C \cap C^\perp = \{\mathbf{0}\}$.

(37) Suppose C is a binary cyclic code of length 7 such that the ideal $\pi(C)$ is generated by $1+x+x^5$. Determine the generator polynomial of C.

(38) Show that if q is a power of a prime p, then the binomial coefficient $\binom{q}{i}$ is divisible by p for $1 \le i < q$. Deduce that $(a+b)^q = a^q + b^q$ for all $a, b \in \mathbb{F}_q$.

(39) Use the formula

$$I_q(n) = \frac{1}{n}\sum_{d|n} \mu(n/d) q^d$$

for the number $I_q(n)$ of irreducible polynomials of degree n in $\mathbb{F}_q[X]$ to show that for every positive integer n, there exists at least one irreducible polynomial of degree n in $\mathbb{F}_q[X]$.

(40) Show that if q is a prime power and n a positive integer such that $\mathrm{GCD}(q, n) = 1$, then there exists a positive integer e such that $q^e \equiv 1 \pmod{n}$. Further show that $\mathbb{F}_{q^e}^*$ has exactly $\varphi(n)$ elements of order n. Find the least positive integer e such that the extension $\mathbb{F}_{3^e}$ of $\mathbb{F}_3$ has an element of order 11.

(41) Let q be a prime power and n a positive integer such that $\mathrm{GCD}(q, n) = 1$. Also let e be the least positive integer such that $q^e \equiv 1 \pmod{n}$, and $\alpha \in \mathbb{F}_{q^e}$ be an element of order n in $\mathbb{F}_{q^e}^*$. For $i \in \mathbb{Z}/n\mathbb{Z}$, let $m_i(X)$ be the minimal polynomial of α^i. Show that the monic reciprocal of $m_i(X)$ is $m_{-i}(X)$. Further

(42) With notations as in the previous question, compute the following. Suppose $q = 7$, $n = 6$, and $\alpha = 3$. Show that α is an element of order 6 in $\mathbb{F}_7$. Compute $m_i(X)$ for each $i \in \mathbb{Z}/6Z$.

(43) Let q, n, α and $m_i(X)$ be as in Q. (**??**). For $i \in \mathbb{Z}/n\mathbb{Z}$, let $C_q(i)$ denote the q-cyclotomy subset of $\mathbb{Z}/n\mathbb{Z}$ corresponding to i. Prove that

$$m_i(X) = \prod_{j \in C_q(i)} (X - \alpha^j).$$

(44) Let q be a prime power and n a positive integer such that $\mathrm{GCD}(q, n) = 1$. If $i_1, i_2 \in \mathbb{Z}/n\mathbb{Z}$ are such that $\mathrm{GCD}(i_1, n) = 1$ and $\mathrm{GCD}(i_1, n) = 1$. Show that the q-cyclotomy subsets $C_q(i_1)$ and $C_q(i_2)$ have the same cardinality. Deduce that the number of monic irreducible factors of the cyclotomic polynomial $\Phi_n(X)$ over $\mathbb{F}_q$ is equal to $\varphi(n)/|C_q(1)|$.

(45) Determine the number of monic irreducible factors and their degrees for the cyclotomic polynomials (i) $\Phi_{11}(X)$ in $\mathbb{F}_3[X]$, and (ii) $\Phi_{23}(X)$ in $\mathbb{F}_2[X]$.

(46) Consider the $[6, 3]_7$-cyclic code C of Q. (**??**). Take $\alpha = 3$ as the fixed element of order 6 in $\mathbb{F}_7$. Determine the zero-set $Z(C)$ of C and also the zero-set $Z(C^\perp)$ of its dual.

(47) Show that if a $[n, k]_q$-code C is r-MDS for some $r \in \{1, \ldots, k\}$, then it is s-MDS for each $s \in \mathbb{Z}$ with $r \le s \le k$. Deduce that a MDS code is r-MDS for each $r \in \{1, \ldots, k\}$, and in particular, it is nondegenerate.

(48) Let r be a positive integer and let $n = \frac{q^r - 1}{q - 1}$. Determine all the generalized Hamming weights of the q-ary simplex code $\mathscr{S}_r(q)$ of length n and dimension r.

(49) Show that the generalized Hamming weights $d_r = d_r(C)$ of a $[n, k]_q$-code C satisfy the Griesmer-Wei bound:

$$d_r \ge \sum_{i=0}^{r-1} \lceil \frac{d_1}{q^i} \rceil \quad \text{for each } r = 1, \ldots, k.$$

(Hint: Use the Griesmer bound for a r-dimensional subcode D of C such that $\mathrm{w}_H(D) = d_r(C)$.)

(50) Let $C = \mathrm{RM}_2(1, m)$ be the binary first order Reed-Muller code of order m. Determine all the generalized Hamming weights of C.