# ACT I: Exercises

## 1 Exercises on the basics of error-correcting codes

1. (Exercise 1.5 from Essential Coding Theory) Let $\Sigma$ be a finite set of alphabets. A function on $d : \Sigma^n \times \Sigma^n \to \mathbb{R}$ is called a *metric* (or, *distance function*) if the following conditions are satisfied: For all $\mathbf{u}, \mathbf{v} \in \Sigma^n$

   (a) $d(\mathbf{u}, \mathbf{v}) \geq 0$.

   (b) $d(\mathbf{u}, \mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$.

   (c) $d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u})$.

   (d) For any $\mathbf{w} \in \Sigma$, $d(\mathbf{u}, \mathbf{w}) \leq d(\mathbf{u}, \mathbf{v}) + d(\mathbf{v} + \mathbf{w})$ (Triangular Inequality).

   For any $\mathbf{u}, \mathbf{v} \in \Sigma^n$, the *Hamming distance* between $\mathbf{u}$ and $\mathbf{v}$, denoted by $\Delta(\mathbf{u}, \mathbf{V})$, is the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ. Show that Hamming distance is a metric.

2. (Exercise 1.4 from Essential Coding Theory) The parity code $C_{\oplus} : \{0,1\}^4 \to \{0,1\}^5$ is defined as follows: For all $(x_1, x_2, x_3, x_4) \in \{0,1\}^4$,

$$C_{\oplus}((x_1, x_2, x_3, x_4)) = (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_3 \oplus x_4).$$

   In the class, we have seen that $C_{\oplus}$ can detect one bit of error. Extending the same argument, show that $C_{\oplus}$ can detect any odd number of errors.

3. (Exercise 1.6 from Essential Coding Theory) Let $C$ be a code with distance $d$ for even $d$. Then argue that $C$ can correct up to $d/2 - 1$ many errors but cannot correct $d/2$ errors. Using this, show that if a code $C$ can correct at most $t$ errors then it has a distance $2t + 1$ or $2t + 2$.

4. (Exercise 1.7 from Essential Coding Theory) In the following, we will see that one can convert arbitrary codes into code with slightly different parameters:

   (a) Let $C$ be an $(n, k, d)_2$ code with $d$ odd. Then it can be converted into an $(n+1, k, d+1)_2$ code.

   (b) Let $C$ be an $(n, k, d)_{\Sigma}$ code. Then it can be converted into an $(n-1, k, d-1)_{\Sigma}$ code.

5. Let $C$ be code over the alphabet $\Sigma$. Then, prove the following.

   (a) If $C$ can detect at most $d - 1$ errors, then the distance of $C$ is $d$.

   (b) If $C$ can correct up to $d - 1$ erasures, then the distance of $C$ is $d$.

6. Let $C_H : \{0,1\}^4 \to \{0,1\}^7$ be a code defined as follows: For any $(x_1, x_2, x_3, x_4) \in \{0,1\}^4$,

$$C_H(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_4, x_1 \oplus x_3 \oplus x_4, x_2 \oplus x_3 \oplus x_4).$$

   Show that $C_H$ has a distance of 3.

## 2 Exercises on the basics of probability

1. Let $E_1, E_2, \ldots, E_n$ be $n$ events on a finite domain $D$ with the probability distribution $p$. Then, show the following.

   (a) (Inclusion-Exclusion principle)

$$\Pr[\cup_{i=1}^n E_i] = \sum_{i=1}^{n} \Pr[E_i] - \sum_{1 \le i < j \le n} \Pr[E_i \cap E_j] + \cdots + (-1)^{n-1} \Pr[\cap_{i=1}^n E_i].$$

   (b) (Union bound)

$$\Pr[\cup_{i=1}^n E_i] \le \sum_{i=1}^{n} \Pr[E_i].$$

2. Let $E_1, E_2$ be two events on a finite domain $D$ with the probability distribution $p$. Then show that

$$\Pr[E_1] = \Pr[E_1 \mid E_2] \cdot \Pr[E_2] + \Pr[E_1 \mid \overline{E_2}] \cdot \Pr[\overline{E_2}].$$

3. For a finite domain $D$, let $u_D$ denotes the *uniform* distribution on $D$, i.e., for all $x \in D$, $u_D(x) = 1/|D|$.

   Let $p_1$ and $p_2$ be two probability distributions on the finite domains $D_1$ and $D_2$, respectively. Then, $p_1 \times p_2$ is a probability distribution on the domain $D_1 \times D_2$ defined as follows: For all $x \in D_1$ and $y \in D_2$, $p_1 \times p_2(x, y)$ is the probability of picking $x$ from $D_1$ according to $p_1$ and picking $y$ independently from $D_2$ according to $p_2$.

   Two distributions $p_1$ and $p_2$ over a finite domain $D$ are called *identical* if for all $x \in D$, $p_1(x) = p_2(x)$.

   Then, show that for any positive integer $m$, the distribution $u_{D_1 \times D_2 \times \cdots \times D_m}$ is identical to the distribution $u_{D_1} \times u_{D_2} \times \cdots \times u_{D_m}$.

4. (Linearity of Expectation) Let $D$ be a finite domain with the probability distribution $p$. A *random variable* $X$ is a function $X : D \to \mathbb{R}$. The *expectation* of $X$ is defined as

$$\mathrm{E}[X] = \sum_{x \in D} p(x) \cdot X(x).$$

   Let $X_1, X_2, \ldots X_n$ be $n$ random variables over a finite domain $D$ with the probability distribution $p$. Then, show that

$$\mathrm{E}[X_1 + \cdots + X_n] = \sum_{i=1}^{n} \mathrm{E}[X_i].$$

5. (Indicator Random Variable) Let $D$ be a finite domain with the probability distribution $p$. A random variable $X : D \to \{0, 1\}$ is called *indicator random variable*. For any event $E$ on $D$, let $\mathbf{1}_E$ denotes the following indicator random variable: For all $x \in D$,

$$\mathbf{1}_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{otherwise} . \end{cases}$$

   Then for any event $E$, show that $\mathrm{E}[\mathbf{1}_E] = \Pr[E]$.

6. Let $x_1, x_2, \ldots x_k$ are $k$ random numbers picked uniformly and independently from the set $[n] = \{1, 2, \ldots, n\}$. What is the expected number of *collisions*, i.e., unordered pairs $\{i, j\}$ such that $x_i = x_j$?

7. Complete the proof of Markov Inequality and Chebyshev Inequality.

8. Let $G(V,E)$ be a random graph on $n$ vertices constructed as follows: For all $\{u,v\}$, with probability $1/2$, $\{u,v\} \in E$. Let $X$ be the random variable denoting the number of triangles in $G$. Compute the $\mathrm{E}[X]$ and $\mathrm{Var}[X]$. Calculate the best possible upper bound for $\Pr[X \geq (1+\epsilon)E[X]]$.

9. For a biased coin, let
$$|\Pr[\mathrm{HEAD}] - \Pr[\mathrm{TAIL}]| = \epsilon,$$
for some $\epsilon \in (0, 1/2)$. Using as minimum as possible coin tosses, design a random procedure such that it tells whether $\Pr[\mathrm{HEAD}] > \Pr[\mathrm{TAIL}]$ with probability $1/100$. Justify your answer.

10. Let $G(V,E)$ be an undirected graph $2n$ vertices and $m$ edges. Then the vertex $V$ can be partitioned into two sets $A$ and $B$ such that the number of edges across these two sets is at least
$$\frac{n}{2n-1}m.$$

11. A 3-CNF formula over variables $x_1, x_2, \ldots x_n$ is of the form
$$\Phi(x_1, x_2, \ldots, x_n) = \wedge_{i=1}^{m} \left(v_{i_1} \vee v_{i_1} \vee v_{i_3}\right),$$
where each $v_{i_j}$ is either a variable $x_i$ or its negation $\overline{x_i}$. The terms $(v_{i_1} \vee v_{i_1} \vee v_{i_3})$ in the formula $\Phi$ are called *clauses*. Show that given any such 3-CNF $\Phi$ over $n$-variables and $m$ cluases, there exists an assignment $\mathbf{a} \in \{0,1\}^n$ on the variables such that it *satisfies* at least $7m/8$ clauses of $\Phi$.

12. Let $C$ be a coin such that the probability of showing head is $p$. Suppose that $C$ is tossed $m$ times, and $\Delta_p$ is the probability of obtaining an odd number of heads. Then, show the following:
    (a) $\Delta_p = \frac{1}{2} \cdot (1 - (1-2p)^m)$.
    (b) If $m$ is odd, then $\Delta_p$ is a non-decreasing function of $p$.
    (c) Over $p \in [0, 1/2]$, $\Delta_p$ is a non-decreasing function of $p$.

## 3 Exercises on the basics of finite fields and linear spaces

1. This exercise aims to prove that the multiplicative group of a finite field is *cyclic*. We will prove this via the following sequence of exercises.
    (a) For every element $a$ in a finite group $G$, $a^{|G|} = 1$ [1].
    (b) Let $G$ be a finite commutative abelian group. Let $a$ and $b$ be two elements in $G$ such that the order[2] of $a$ and $b$ are $m$ and $n$, respectively. Then, show that $G$ has an element of order $\mathrm{lcm}(m,n)$.
    (c) Let $G$ be a finite commutative abelian group such that for every positive integer $n$, the number of elements $a$ with $a^n = 1$ is at most $n$. Then, $G$ is cyclic.
    (d) Prove that the multiplicative group of any finite field is cyclic. Hence, for any element $\alpha$ in finite field $\mathbb{F}_q$, $\alpha^q = \alpha$.

[1]Here, 1 denotes the identity element in $G$.
[2]The order of an element in $G$ is the smallest positive integer $i$ such that $a^i$ is the identity element in $G$

2. Let $\mathbb{F}$ be a field and let $f(x)$ be an irreducible polynomial in $\mathbb{F}[x]$ of degree $d$. Then, show that for every polynomial $g(x)$ of degree less than $d$, there exists a polynomial $h(x)$ of degree less than $d$ such that $g(x) \cdot h(x) = 1 \mod f(x)$. Using this, show that the set of all polynomials of degree less than $d$ forms a field under polynomial addition and multiplication modulo $f(x)$.

3. Let $S$ be a linear subspace of $\mathbb{F}_q^n$ of dimension of $k$. Then, show that there exists a full rank[3] $(n-k) \times n$ matrix $H$ such that
$$\{\mathbf{x} \in \mathbb{F}^n \mid H \cdot \mathbf{x} = 0\}.$$

4. Design an algorithm such that for a linear subspace $S$ of $\mathbb{F}_q^n$, given its generator matrix $G$, the algorithm computes its parity matrix in $\text{poly}(n)$ $\mathbb{F}_q$-operations.

5. Given a nonzero vector $\mathbf{u} \in \mathbb{F}_q^k$ and a uniformly random $k \times n$ matrix $G$ over $\mathbb{F}_q$, the vector $\mathbf{u} \cdot G$ is uniformly distributed over $\mathbb{F}_q^n$.

6. For any prime $q$ with $q \equiv 1 \mod 4$, show that $\mathbb{F}_q$ has an element $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$.

7. Over a finite field $\mathbb{F}_q$, an element $\alpha \in \mathbb{F}_q$ is called *quadratic residue* if $\alpha = \beta^2$ for some $\beta \in \mathbb{F}_q$. Otherwise, $\alpha$ is called *quadratic non-residue* in $\mathbb{F}_q$. Then, for any prime $q$ with $q \equiv 3 \mod 4$, show that there exists two quadratic residues $\alpha$ and $\beta$ in $\mathbb{F}_q$ such that $\alpha + \beta = -1$

8. Let $G$ be an $k \times n$ matrix over a $\mathbb{F}_q$. Let $G : \mathbb{F}^n \to \mathbb{F}^k$ be a mapping defined as $\mathbf{v} \mapsto G \cdot \mathbf{v}$. Then, for any $\mathbf{u} \in \mathbb{F}^k$ in the image of $G$, the size of the preimage of $\mathbf{u}$ is the size of the kernel of $G$.

9. Let $n$ be a positive integer and $\gcd(n, q) = 1$. Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$. Show that $\mathbb{F}_{q^m}$ contains an $n$-th *primitive root unity* [4] if and only if $n$ divides $q^m - 1$. Furthermore, show that for $m = \text{or}_n(q)$ [5], $\mathbb{F}_{q^m}$ is the smallest extension over $\mathbb{F}_q$ containing an $n$-th primitive root of unity.

10. Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$. Then, for any $\alpha \in \mathbb{F}_{q^m}$, show that there exists a polynomial $p(x) \in \mathbb{F}_q[x]$ such that $p(\alpha) = 0$. For any $\alpha \in \mathbb{F}_{q^m}$, let $p_\alpha(x)$ be a smallest degree polynomial such that $p_\alpha(\alpha) = 0$. Then, show that $p_\alpha(x)$ is an irreducible polynomial over $\mathbb{F}_q$ and for any polynomial $h(x)$ with $h(\alpha) = 0$, $p_\alpha(x)$ divides $h(x)$, that is, the set of all polynomials in $\mathbb{F}_q[x]$ with $\alpha$ is a root form a *principal ideal* in the ring $\mathbb{F}_q[x]$ and it is generated by $p_\alpha(x)$.

11. As we know, there exists a bijection $\Psi$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$ such that for any $\alpha, \beta \in \mathbb{F}_{q^m}$ and $a, b \in \mathbb{F}_q$,
$$\Psi(a\alpha + b\beta) = a \cdot \Psi(\alpha) + b \cdot \Psi(\beta).$$
Let $\alpha \in \mathbb{F}_{q^m}$, and $\Phi : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a mapping defined as follows: For all $\mathbf{u} \in \mathbb{F}_q^m$,
$$\Phi(\mathbf{u}) = \Psi\left(\alpha \cdot \Psi^{-1}(\mathbf{u})\right).$$
Then, show that $\Phi$ is a linear transformation. Furthermore, if $\alpha \neq 0$, $\Phi$ is invertible. Additionally, describe a matrix representing the linear transformation $\Phi$.

12. Show that $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ is a *principal ideal ring*, that is, every ideal $\mathcal{I}$ of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ is a principal ideal.

[3] An $m \times n$ matrix $M$ is called *full rank* if the rank of $M$ is $\min\{m, n\}$.

[4] An element in a field $\mathbb{F}$ is called $n$-th *primitive root of unity* if its order in the underlying multiplicative group of $\mathbb{F}$ is $n$.

[5] The $\text{or}_n(q)$ is the order of $q$ in the group formed by positive integers less than $n$ and relatively prime to $n$ and the group operation is the multiplication modulo $n$.

13. Over finite field $\mathbb{F}_q$, show that $x^n - 1$ can be decomposed as a product of distinct irreducible factors, that is,
$$x^n - 1 = f_1(x) f_2(x) \cdots f_t(x),$$
where all $f_i(x)$ are distinct irreducible polynomials.

14. For any two polynomials $f(x)$ and $g(x)$ over a finite field $\mathbb{F}_q$, the $\gcd(f,g)$ is the largest degree monic polynomial over $\mathbb{F}_q$ that divides both $f(x)$ and $g(x)$. Over a finite field $\mathbb{F}_q$, assume that for any two polynomials of degree less than $n$, we can compute $f+g$, $f \cdot g$, and $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg(r) < \deg(g)$, in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations. Then, show the following:
    (a) There is an algorithm such that given two polynomials $f(x)$ and $g(x)$ of degree less than $n$ as input, computes the $\gcd(f,g)$ in $\mathrm{poly}(n)$ $\mathbb{F}_q$-operations.
    (b) The ideal in $\mathbb{F}_q[x]$ generated by $f(x)$ and $g(x)$ is the same as the principal ideal generated by $\gcd(f,g)$.

# 4 Exercises on the basics of linear codes

1. Prove or disprove the following: For any $[n,k,d]_q$ linear code $C$, the dual code $C^\perp$ is an $[n, n-k, n-d]_q$ linear code.

2. For every positive integer $r$, compute the distance of $C_{H,r}^\perp$, where $C_{H,r}$ denotes the Hamming code defined in the class.

3. Let $C$ be an $[n,k]_q$ code. Define a function $f : C \to \mathbb{F}_q^{n^m}$ as follows: For $\mathbf{c} = (c_1, c_2, \ldots, c_n)$,
$$f(\mathbf{c}) = \left(c_{i_1} + c_{i_2} + \cdots + c_{i_m}\right)_{i_1, i_2, \ldots, i_m \in [n]}.$$
Then, show that
$$f(C) = \{f(\mathbf{c}) \mid \mathbf{c} \in C\}$$
is an $[n^m, k]_q$ code. Furthermore, given a generator matrix $G$, describe a generator matrix for $f(C)$.

# 5 Exercises on various bounds

1. Prove that for every positive integer $q \geq 2$, the $q$-ary entropy function $H_q(x)$ achieves maximum value at $1 - \frac{1}{q}$.

2. Read the proof of **Proposition 3.3.3** in Essential Coding Theory.

3. Let $q \geq 2$ be an positive integer. Let $\phi : [q] \to \mathbb{R}^q$ be a mapping defined as follows: For all $i \in [q]$,
$$\phi(i) = \Big(\frac{1}{q}, \frac{1}{q}, \ldots, \underbrace{\frac{-(q-1)}{q}}_{i^{\text{th}} \text{ position}}, \ldots, \frac{1}{q}\Big).$$
Let $C \subseteq [q]^n$ be a an $(n,k,d)_q$ code. Let $f : C \to \mathbb{R}^{nq}$ be a mapping defined as follows: For any $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$,
$$f(\mathbf{c}) = \sqrt{\frac{q}{n(q-1)}} \cdot (\phi(c_1), \phi(c_2), \ldots, \phi(c_n)).$$
Show that

(a) for all $\mathbf{c} \in C$, $f(\mathbf{c})$ is a unit vector.

(b) for all $\mathbf{c}_1 \neq \mathbf{c}_2 \in C$, $\langle f(\mathbf{c}_1), f(\mathbf{c}_2)\rangle = 1 - \left(\frac{q}{q-1}\right)\left(\frac{\Delta(\mathbf{c}_1,\mathbf{c}_2)}{n}\right)$.

4. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ be points in $\mathbb{R}^n$. Then, show that there exists a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ such that $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ where $\mathbf{v}_i = T(\mathbf{u}_i)$ satisfy the following property: $\mathbf{v}_m = (1, 0, 0, \ldots, 0)$ and for all $i \neq j \in [m]$, the angle between $\mathbf{u}_i$ and $\mathbf{u}_j$ is the same as the angle between $\mathbf{v}_i$ and $\mathbf{v}_j$. Hence, show that for all $i \neq j \in [m]$ if $\langle \mathbf{u}_i, \mathbf{u}_j\rangle \leq 0$ then $\langle \mathbf{v}_i, \mathbf{v}_j\rangle \leq 0$.

5. (**Cauchy-Schwartz Inequality**) Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. Then,

$$\langle \mathbf{u}, \mathbf{v}\rangle^2 = \langle \mathbf{u}, \mathbf{u}\rangle \cdot \langle \mathbf{v}, \mathbf{v}\rangle.$$

6. Read the proof of **Proposition 3.3.7** in Essential Coding Theory. Observe that it has been used to show that for any $\delta = \frac{1}{2} - \epsilon$, the rate we can get from GV bound is $\Omega(\epsilon^2)$ and the rate we get from Zybalov bound for code concatenation is $\Omega(\epsilon^3)$.

7. Solve **Exercise 4.6** in Essential Coding Theory. Observe that it was used to construct asymptotically good linear codes over alphabets of constant size via code concatenation.

# 6 Exercises on various explicit code families

1. (**Vandermonde matrix**) Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be $k$ elements from a field $\mathbb{F}$. Let

$$V(\alpha_1, \alpha_2, \ldots, \alpha_k) = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_k \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_k^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_k^{k-1} \end{bmatrix}.$$

Show that

$$\det(V(\alpha_1, \alpha_2, \ldots, \alpha_k)) = \prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j).$$

2. Let $C$ be an $[n, k]_q$ MDS code. Then, $C^\perp$ is an $[n, n-k]_q$ MDS code.

3. Let $C \subseteq \Sigma^n$ be an $(n, k, d)_q$ code. For any $S \subseteq [n]$ of $|S|$, let $C_S$ be the projection of the codewords in $C$ on the set $S$. Let $|C_S| = q^k$ for any subset $S$ of $[n]$ of $|S| = k$. Then, show that $C$ is an MDS code.

4. For all positive integer $k$, the Hadamard code $C_{\text{Had},k} : \mathbb{F}_2^k \to \mathbb{F}_2^{2^k}$ is defined via its generator matrix $G_k$ as follows: The columns of the generator matrix $G \in \mathbb{F}_2^{k \times 2^k}$ are indexed by the vectors in $\mathbb{F}_2^k$ and for a vector $\mathbf{x} \in \mathbb{F}_2^k$, the column of $G$ indexed by $\mathbf{x}$ is the vector $\mathbf{x}$. Describe a parity matrix for $C_{\text{Had},k}$.

5. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be $n$ distinct elements from the finite field $\mathbb{F}_q$. Let $\mathrm{RS}(n, k, q)$ be the Reed-Solomon code of block length $n$ with the evaluation points are $\alpha_1, \alpha_2, \ldots, \alpha_n$, dimension is $k$ and the alphabet is $\mathbb{F}_q$. Then, show the following:

(a) For $n = q$, $\mathrm{RS}(n, k, q)^\perp = \mathrm{RS}(n, n-k, q)$.

(b) For $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \mathbb{F}_q^*$, that is $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ where $\alpha$ is the generator of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$,

$$\mathrm{RS}(n,k,q)^\perp = \Big\{\big(c(1),\ \alpha c(\alpha),\ \alpha^2 c(\alpha^2),\ \ldots,\ \alpha^{q-2}c(\alpha^{q-2})\big) \mid c(x) \in \mathbb{F}_q[x] \text{ and } \deg(c) < n-k\Big\}.$$

6. Let $S$ be a set of $q$ distinct elements from a field $\mathbb{F}$. Let $M_{m,q}$ be the set of $m$-variate monomials with individual degree less than $q$, that is,

$$M_{m,q} = \Big\{x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m} \mid \forall\, i \in [m]\ e_i < q\Big\}.$$

Let $V$ be a $q^m \times q^m$ matrix whose rows are indexed by $S^m$ and columns are indexed by $M_{m,q}$ and for all $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in S^m$ and $\mathbf{x}^{\mathbf{e}} = x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m} \in M_{m,r}$, the entry of $V$ at $(\boldsymbol{\alpha}, \mathbf{x}^{\mathbf{e}})$ is $\alpha_1^{e_1}\alpha_2^{e_2}\cdots\alpha_m^{e_m}$. Show that $V$ is a full-rank matrix.

7. Let $f(x_1, x_2, \ldots, x_m)$ be a nonzero $m$-variate multilinear polynomial of degree $r$ over $\mathbb{F}_2$. Using a non-induction argument, show that

$$\#\{\boldsymbol{\alpha} \in \mathbb{F}_2^m \mid f(\boldsymbol{\alpha}) \neq 0\} \geq 2^{m-r}.$$

8. Read the proof of **Lemma 9.4.1** in Essential Coding Theory.

9. Show that there exists a nonzero $m$-variate polynomial $f(x_1, x_2, \ldots, x_m)$ over $\mathbb{F}_q$ with individual degree less than $q$ and total degree $r$ and

$$\#\Big\{\boldsymbol{\alpha} \in \mathbb{F}_q^m \mid f(\boldsymbol{\alpha}) = 0\Big\} = t \cdot q^{m-s-1},$$

where $s, t$ are nonnegative integers with $t < q-1$ and $r = s(q-1)+t$. It proves that **Lemma 9.4.1** in Essential Coding Theory is tight for all settings of parameters.

10. Read the proof of **Proposition 9.4.5** in Essential Coding Theory.

11. Consider the code $\mathrm{BCH}(n, \delta, 2, 0)$ with $n = 2^m - 1$, that is, the primitive BCH code over $\mathbb{F}_2$ with block length $n$, designed distance $\delta$ and any polynomial $c(x) \in \mathbb{F}_2[x]$ of degree less than $n$ is a codeword if and only if $c(1) = c(\beta) = c(\beta^2) = \cdots = c(\beta^{\delta-2}) = 0$ where $\beta$ is a primitive element of $\mathbb{F}_{2^m}$. Then, show the following:

(a) For a subspace $U \subseteq \mathbb{F}_{2^m}$ of dimension $\ell$ over $\mathbb{F}_2$ and for any $a \in \mathbb{Z}_{\geq 0}$ with less than $\ell$ ones in its binary representation,

$$\sum_{u \in U} u^a = 0.$$

**Hint:** Use induction on $\ell$.

(b) The distance of $\mathrm{BCH}(2^m - 1, 2^\ell - 1, 2, 0)$ is $2^\ell - 1$.

(c) The distance of $\mathrm{BCH}(2^m - 1, \delta, 2, 0)$ is at most $2\delta - 1$. Observe that it gives a better upper bound for the distance of primitive binary BCH codes than the upper bound we have seen in the class, which was $m \cdot \lfloor \frac{\delta-1}{2} \rfloor + 2$.

12. Let $\beta$ be an $n$-th primitive root of unity in $\mathbb{F}_{q^m}$. Then, for BCH codes, show the following

(a) $\mathrm{BCH}(n, \delta, q, 0) = \mathrm{RS}(n, \delta-1, q^m)^\perp \bigcap \mathbb{F}_q^n$, where the evaluation points of the RS code are $1, \beta, \beta^2, \ldots, \beta^{n-1}$.

(b) $\mathrm{BCH}(n, \delta, q, 1) = \mathrm{RS}(n, n-\delta+1, q^m) \bigcap \mathbb{F}_q^n$, where the evaluation points of the RS code are $1, \beta, \beta^2, \ldots, \beta^{n-1}$.

(c) The set of codewords of $\mathrm{BCH}(n, \delta, q, \ell)$ is

$$\Big\{\big(p(1), p(\beta), p(\beta^2), \ldots, p(\beta^{n-1})\ \mid\ p(x) \in \mathbb{F}_{q^m}[x] \text{ s.t. } p(x) = x^{n-\ell+1} \cdot c(x) \text{ with } \deg(c) \leq n-\delta\big)\Big\} \bigcap \mathbb{F}_q^n.$$

# 7 Exercises on Code Concatenation

1. If $C_{\text{out}}$ (Outer code) and $C_{\text{in}}$ (Inner code) both are linear, then show that the concatenation code $C_{\text{out}} \circ C_{\text{in}}$ is also a linear code. More specifically, prove it by constructing a generator matrix for $C_{\text{out}} \circ C_{\text{in}}$ from the generator matrices of $C_{\text{out}}$ and $C_{\text{in}}$.

2. Read the proof of **Theorem 10.3.1** in Essential Coding Theory.

3. Show that the *Justesen code* is a *strongly explicit code*. For the definition of Justesen code see **Section 10.3.1** in Essential Coding Theory, or you can look the Handwritten Note.

4. In the class, we have seen a natural decoding algorithm for concatenation codes that can correct less than $\frac{Dd}{4}$ many errors. Show that that decoding algorithm can be easily adapted to work for the case where the inner codes for each coordinate of the outer code are distinct just like the Justsen code.

5. Read the proof of **Lemma 14.3.1** and **Lemma 14.3.2** in Essential Coding Theory.