Assignment 1 - ACT1

Nirjhar Nath
nirjhar@cmi.ac.in
BMC202239

Problem 1:

Let C be an $[n, k, d]_q$ code over a finite field $\mathbb{F}_q$ with the generator matrix G. If G does not have a column containing all zeros, then show that

$$\sum_{\mathbf{c} \in C} \mathrm{wt}(\mathbf{c}) = n(q-1)q^{k-1},$$

where $\mathrm{wt}(\mathbf{c})$ denotes the number of nonzero coordinates in $\mathbf{c} \in \mathbb{F}_q^n$.

Solution 1:

Let C be an $[n, k, d]_q$ linear code over the finite field $\mathbb{F}_q$ with the generator matrix G. The code has length n, dimension k, and minimum distance d. Since C is a linear code, it is generated by a $k \times n$ generator matrix G, which we denote as:

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}.$$

Each codeword $\mathbf{c}$ in C can be expressed as a linear combination of the rows of G. Let $\mathbf{v} = (v_1, v_2, \ldots, v_k) \in \mathbb{F}_q^k$ be a vector representing the coefficients of this linear combination. Then, the codeword corresponding to $\mathbf{v}$ is:

$$\mathbf{c} = \mathbf{v}G = (v_1, v_2, \ldots, v_k) \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}.$$

This gives us a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ where each coordinate c_j is computed as:

$$c_j = v_1 g_{1j} + v_2 g_{2j} + \cdots + v_k g_{kj}.$$

Since we are given that G does not have any column that contains all zeros, for each column j in G, at least one of the elements $g_{1j}, g_{2j}, \ldots, g_{kj}$ is non-zero. This implies that it is possible to select coefficients $v_1, v_2, \ldots, v_k$ such that the sum $v_1 g_{1j} + v_2 g_{2j} + \cdots + v_k g_{kj}$ is non-zero.

For a fixed coordinate j (where $1 \leq j \leq n$), we consider how many choices of the vector $\mathbf{v} = (v_1, v_2, \ldots, v_k)$ result in $c_j \neq 0$. Since the sum $v_1 g_{1j} + v_2 g_{2j} + \cdots + v_k g_{kj}$ forms a linear combination over the field $\mathbb{F}_q$, for each possible choice of values for $v_2, v_3, \ldots, v_k$, there are exactly $q - 1$ non-zero choices for v_1 that result in a non-zero sum. Since there are q^{k-1} possible ways to choose the remaining coefficients $v_2, \ldots, v_k$, the total number of ways to choose $(v_1, v_2, \ldots, v_k)$ such that $c_j \neq 0$ is $(q-1)q^{k-1}$.

This argument holds for each coordinate $j = 1, 2, \ldots, n$ because none of the columns of G are all zeros. Therefore, each of the n coordinates contributes $(q-1)q^{k-1}$ non-zero entries when summed over all codewords. Therefore,

$$\sum_{\mathbf{c} \in C} \mathrm{wt}(\mathbf{c}) = n \cdot (q-1)q^{k-1},$$

which completes the proof. ■

Problem 2:

Let C be an $[n, k]_q$ code where the block length and the dimension of C are n and k, respectively. The code C is called self-dual if $C = C^{\perp}$, that is, the code C is the same as its dual. For any prime q, is there an $[8, 4]_q$ *self-dual* code over $\mathbb{F}_q$?

Solution 2:

A self-dual code C of length n and dimension k over $\mathbb{F}_q$ satisfies $C = C^{\perp}$. For an $[8, 4]_q$ self-dual code, the parity-check matrix H must satisfy $HH^T = 0$. We consider two cases based on the properties of the finite field $\mathbb{F}_q$.

Case 1: $q = 2$ or $q \equiv 1 \pmod 4$

In this case, there exists an element $a \in \mathbb{F}_q$ such that $a^2 + 1 = 0$. For $q = 2$, $a = 1$ works. For $q \equiv 1 \pmod 4$, the existence of such an element a follows from number theory.

Consider the matrix:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & a \end{bmatrix}.$$

Clearly, H is full-rank. Also,

$$HH^T = \begin{bmatrix} 1 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{bmatrix}$$

$$= \begin{bmatrix} 1 + a^2 & 0 & 0 & 0 \\ 0 & 1 + a^2 & 0 & 0 \\ 0 & 0 & 1 + a^2 & 0 \\ 0 & 0 & 0 & 1 + a^2 \end{bmatrix}.$$

Since $a^2 + 1 = 0$, so we have, $HH^T = 0$, i.e., the code is self-dual.

Case 2: $q \equiv 3 \pmod 4$

In this case, there exist elements $a, b \in \mathbb{F}_q$ such that $a^2 + b^2 + 1 = 0$ (by Problem 3.7 of the Practice Problem Set). Consider the matrix:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & a & b & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & a & b & 0 \\ 0 & 0 & 1 & 0 & b & -a & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & b & -a & 0 \end{bmatrix}.$$

Here also, H is clearly full rank. We have,

$$HH^T = \begin{bmatrix} 1 & 0 & 0 & 0 & a & b & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & a & b & 0 \\ 0 & 0 & 1 & 0 & b & -a & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & b & -a & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & 0 & b & 0 \\ b & a & -a & b \\ 0 & b & 0 & -a \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1+a^2+b^2 & 0 & 0 & 0 \\ 0 & 1+a^2+b^2 & 0 & 0 \\ 0 & 0 & 1+a^2+b^2 & 0 \\ 0 & 0 & 0 & 1+a^2+b^2 \end{bmatrix}.$$

Since $a^2 + b^2 + 1 = 0$, we get $HH^T = 0$, i.e., the code is self-dual.

Therefore, for any prime q, there exists an $[8, 4]_q$ self-dual code over the finite field $\mathbb{F}_q$. The structure of the parity-check matrix depends on whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$, but in both cases, a self-dual code can be constructed, as shown above. ■

Problem 3:

The set of all $n_2 \times n_1$ matrices over $\mathbb{F}_2$ forms a vector space V of dimension $n_1 n_2$. 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 V 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. The code C is called the *direct product* of C_1 and C_2.

Solution 3:

Here, V is the vector space of all $n_2 \times n_1$ matrices over the finite field $\mathbb{F}_2$. The dimension of V is $n_1 n_2$ since each matrix has $n_1 n_2$ entries and each entry can independently take a value in $\mathbb{F}_2$.

First, we need to show that C is a subspace of V. Consider any two matrices $A, B \in C$. By definition, every column of A and B is a codeword in C_1, and every row of A and B is a codeword in C_2. Since C_1 and C_2 are linear codes, the sum of any two codewords in these codes is also a codeword in the same code. Therefore, for the sum $A + B$, each column remains a codeword in C_1 and each row remains a codeword in C_2, implying that $A + B \in C$. Closure under scalar multiplication is trivial since the scalars in $\mathbb{F}_2$ are 0 and 1, so multiplying by a scalar either results in the zero matrix or leaves the matrix unchanged. Thus, C is closed under both addition and scalar multiplication, making it a subspace of V and hence a linear code.

Next, we determine the dimension of C. Each matrix in C has n_1 columns, each of which must be a codeword in the $[n_1, k_1, d_1]_2$ code C_1. There are k_1 degrees of freedom in choosing these columns since C_1 has dimension k_1. Similarly, each matrix in C has n_2 rows, each of which must be a codeword in the $[n_2, k_2, d_2]_2$ code C_2, giving k_2 degrees of freedom in choosing these rows. Therefore, the total number of independent choices for constructing the matrix is $k_1 k_2$. Consequently, the dimension of C is $k_1 k_2$.

Now, we compute the minimum distance of C. Consider a non-zero matrix $A \in C$. Since each column of A is a codeword in C_1, if at least one column is non-zero, it must contain at least d_1 non-zero entries, as the minimum distance of C_1 is d_1. Similarly, since each row of A is a codeword in C_2, if at least one row is non-zero, it must contain at least d_2 non-zero entries, as the minimum distance of C_2 is d_2. To satisfy both conditions simultaneously, the matrix must have at least $d_1 d_2$ non-zero entries. Therefore, the minimum distance of the code C is $d_1 d_2$.

Thus, C is a linear code of length $n_1 n_2$, dimension $k_1 k_2$, and minimum distance $d_1 d_2$. Hence, C is an $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ code. ■

Problem 4:

Show that $[15, 8, 5]_2$ code does not exist.

Solution 4:

Let $\mathcal{L}(k, d)$ be the minimum length of a binary code with Hamming distance $\geq d$ and dimension k. Let C be an $[n, k, d]_2$ code. Then, from Problem 5(a), we have, there exists an $[n - d, k - 1, d']_q$ code with $d' \geq \lceil d/2 \rceil$. Therefore, the length of such a code is $\geq \mathcal{L}\left(k - 1, \left\lceil \frac{d}{2} \right\rceil\right)$. Therefore,

$$\mathcal{L}(k, d) = d + \mathcal{L}\left(k - 1, \left\lceil \frac{d}{2} \right\rceil\right).$$

Putting $k = 8$ and $d = 5$, we get:

$$\mathcal{L}(8, 5) \geq 5 + \mathcal{L}(7, 3). \tag{1}$$

The generalized Hamming bound is the following:

$$n - k \geq \log_q \left(\sum_{i=0}^{\lceil \frac{d-1}{2} \rceil} \binom{n}{i} (q-1)^i \right).$$

Putting $q = 2, k = 7$ and $d = 2$, we have

$$n - 7 \geq \log_2 \left(\sum_{i=0}^{1} \binom{n}{i} \right) \geq \log_2(1 + n). \tag{2}$$

Clearly, $n = 11$ is the smallest value of n which satisfies equation (2), i.e.,

$$\mathcal{L}(7, 3) \geq 11.$$

Using this in equation (1), we get:

$$\mathcal{L}(8, 5) \geq 16.$$

Therefore, $[15, 8, 5]_2$ code does not exist. ■

Problem 5:

(a) If there exists an $[n,k,d]_q$ code, then there exists an $[n-d,k-1,d']_q$ code with $d' \geq \lceil d/q \rceil$.

(b) For any $[n,k,d]_q$-code,

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

It is known as *Griesmer Bound.*

Solution 5:

(a) Let C be an $[n,k,d]_q$-code. Let G be a generator matrix of C. We can always assume, without loss of generality, that the first row vector of G is of the form $v = (1,\dots,1,0,\dots,0)$, with weight d. Then, G can be written as:

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

where G' is a $(k-1)\times(n-d)$ matrix.

Now, consider the code C' generated by G'. The code C' has length $n-d$ and dimension $k-1$. Let d' be the minimum distance of C'. Let $\mathbf{u} \in C'$ such that $\mathrm{wt}(\mathbf{u}) = d'$. Then, $\exists$ some $\mathbf{w} = (w_1, w_2, \dots, w_d) \in \mathbb{F}_q^d$ such that $(\mathbf{w} \mid \mathbf{u}) \in C$, where $(\mathbf{w} \mid \mathbf{u})$ represents the concatenation of $\mathbf{w}$ and $\mathbf{u}$.

By the Pigeonhole Principle, there exists some $\alpha \in \mathbb{F}_q$ such that at least $\lceil \frac{d}{q} \rceil$ of $w_1, w_2, \dots, w_d$ are equal to α. Since $(\mathbf{w} \mid \mathbf{u}) - \alpha\mathbf{v} \in C$, we have:

$$\begin{aligned} d &\leq \mathrm{wt}((\mathbf{w} \mid \mathbf{u}) - \alpha\mathbf{v}) \\ &= \mathrm{wt}((\mathbf{w} - (\alpha,\dots,\alpha)) \mid \mathbf{u}) \\ &= \mathrm{wt}(\mathbf{w} - (\alpha,\dots,\alpha)) + \mathrm{wt}(\mathbf{u}) \\ &\leq \left(d - \left\lceil \frac{d}{q} \right\rceil\right) + d'. \end{aligned}$$

Thus, we obtain:

$$d' \geq \left\lceil \frac{d}{q} \right\rceil,$$

which proves the result.

(b) For a given k and d, let $N_{k,d}$ be the minimum value of n for which there exists an $[n,k,d]_q$-code. We shall prove this result by induction on k.

Base Case: When $k = 0$, the result is clear.

Inductive Step: Assume that the result is true for $k = k_0 - 1$. Let C be an $[N_{k_0,d}, k_0, d]_q$-code. By part (a), there exists an $[N_{k_0,d} - d, k_0 - 1, d']_q$-code with $d' \geq \lceil d/q \rceil$.

By the induction hypothesis, we have:

$$N_{k_0-1,d'} \geq \sum_{i=0}^{k_0-2} \left\lceil \frac{d'}{q^i} \right\rceil .$$

Since $d' \geq \lceil d/q \rceil$, it follows that:

$$N_{k_0,d} - d \geq \sum_{i=0}^{k_0-2} \left\lceil \frac{\lceil d/q \rceil}{q^i} \right\rceil.$$

Thus,

$$N_{k_0,d} \geq d + \sum_{i=0}^{k_0-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil = \sum_{i=0}^{k_0-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

which completes the proof.

■

Problem 6:

Let $q \geq 2$ be an integer. Let $\delta \in \left(0, 1 - \frac{1}{q}\right)$. Let $\epsilon \in [0, 1 - H_q(\delta)]$ and n be a positive integer. Let $k = (1 - H_q(\delta) - \epsilon)n$. Let H be an $(n-k) \times n$ matrix over $\mathbb{F}_q$ picked uniformly and randomly. Then, show that H is a parity-check matrix of a code of block length n, rate $1 - H_q(\delta) - \epsilon$, and relative distance at least δ with probability at least $1 - q^{-\epsilon n}$.

Solution 6:

Let $q \geq 2$ be an integer and let $\mathbb{F}_q$ be the finite field with q elements. Given $\delta \in \left(0, 1 - \frac{1}{q}\right)$ and $\epsilon \in [0, 1 - H_q(\delta)]$, let n be a positive integer, and define $k = (1 - H_q(\delta) - \epsilon)n$. Let H be an $(n-k) \times n$ matrix over $\mathbb{F}_q$ chosen uniformly at random. We want to show that the matrix H is the parity-check matrix of a code with block length n, rate $1 - H_q(\delta) - \epsilon$, and relative distance at least δ with probability at least $1 - q^{-\epsilon n}$.

The rate of the code is given by $R = \frac{k}{n}$. Since $k = (1 - H_q(\delta) - \epsilon)n$, we have $R = 1 - H_q(\delta) - \epsilon$. Therefore, the code will have the desired rate provided the parity-check matrix H has full rank, i.e., rank $n - k$. The probability that a random matrix H does not have full rank is negligible for large n, so the rate condition is satisfied with high probability.

Next, we consider the relative distance of the code. The relative distance of a linear code is determined by the minimum Hamming weight of its non-zero codewords. Codewords correspond to vectors in the null space of H. To show that the code has a relative distance at least δ, we need to bound the probability that there exists a non-zero vector c in the null space of H with Hamming weight less than or equal to δn.

Since H is chosen uniformly at random, for any fixed non-zero vector $c \in \mathbb{F}_q^n$, the probability that c belongs to the null space of H and has Hamming weight at most δn is given by:

$$\frac{\mathrm{Vol}_q(n, \delta n)}{q^n} \leq q^{(H_q(\delta)-1)n},$$

where $\mathrm{Vol}_q(n, \delta n)$ represents the volume of a Hamming ball of radius δn in the space $\mathbb{F}_q^n$.

The null space of H contains q^k vectors. The probability that there exists at least one non-zero codeword in this space with weight less than or equal to δn can be bounded by applying the union bound:

$$q^k \cdot q^{(H_q(\delta)-1)n} = q^{(1-H_q(\delta)-\epsilon)n} \cdot q^{(H_q(\delta)-1)n} = q \cdot q^{-\epsilon n} = q^{1-\epsilon n}.$$

The probability that no non-zero codeword in the null space of H has weight less than or equal to δn is the complement of the above probability, which is $1 - q^{1-\epsilon n}$. Since $q^{1-\epsilon n}$ becomes extremely small for large n (as $\epsilon > 0$), this probability approaches 1. Thus, we can conclude that with probability at least $1 - q^{-\epsilon n}$, the random parity-check matrix H defines a linear code with rate $1 - H_q(\delta) - \epsilon$ and relative distance at least δ. ■