Learners' Space 2025 – Coding Theory
Week 2 Handout

Nirav Bhattad & Aryan Prakash, MnP Club, IIT Bombay

July 2025

Contents

§1. Vector Spaces and subspaces

Before we move on to one of the main topics of discussion of this handout, linear codes, we first need the definition vector spaces and linear subspaces. While, this has been covered in the MA110 course, of your first year, we reiterate it here for clarity.

Definition 1.1 (Vector Space)**.** A vector space V over a field $\mathbb{F}$ is given by a triple $(T, +, \cdot)$ such that $(T, +)$ form a commutative group and $\cdot$, referred to as the scalar product, is a function $\mathbb{F} \times T \to T$ such that for every $a, b \in \mathbb{F}$ and $\mathbf{u}, \mathbf{u} \in T$ we have $(a + b) \cdot \mathbf{u} = a \cdot \mathbf{u} + b \cdot \mathbf{u}$ and $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$

Definition 1.2 (Linear Subspace)**.** (Linear Subspace). A non-empty subset $S \subseteq \mathbb{F}^n$ is a linear subspace if the following properties hold:

1. For every $\mathbf{x}, \mathbf{y} \in S$, $\mathbf{x} + \mathbf{y} \in S$, where the addition is vector addition over $\mathbb{F}$ (that is, do addition component-wise over $\mathbb{F}$).
2. For every $a \in \mathbb{F}$ and $\mathbf{x} \in S$, $a \cdot \mathbf{x} \in S$, where the multiplication is done component-wise over $\mathbb{F}$.

We assume that everybody is familiar with the span of a set and the definition if linear independence after solving question 6 of the first assignment. We will also be using some results from the proved results in question 6, so please keep them in mind to.

§2. Linear codes

Definition 2.1 (Linear Codes)**.** Let q be a prime power (i.e., $q = p^s$ for some prime p and integer $s \geqslant 1$). $C \subseteq \mathbb{F}_q^n$ is a linear code if it is a linear subspace of $\mathbb{F}_q^n$. If C has dimension k and distance d, then it will be referred to as an $[n, k, d]_q$ or just an $[n, k]_q$ code.

Definition 2.2 (Generator and Parity Check Matrix)**.** If C is an $[n, k]_q$ linear code then there exists a matrix $G \in \mathbb{F}_q^{k \times n}$ of rank k satisfying

$$C = \{\mathbf{x} \cdot G \mid \mathbf{x} \in \mathbb{F}_q^k\}$$

G is referred to as a generator matrix of C. In other words, the code C is the set of all possible linear combinators of rows of G.

If C is an $[n, k]_q$ linear code, then there exists a matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ of rank $n - k$ satisfying

$$C = \{\mathbf{y} \in \mathbb{F}_q^n \mid H \cdot \mathbf{y}^T = \mathbf{0}\}$$

Now from results proved in question 6 on linear subspaces, we have 2 alternate characterizations of an $[n, k]_q$ linear code C.

1. C is generated be a $k \times n$ generator matrix G.
2. C is defined by a $(n - k) \times n$ parity check matrix H.

We require G and H to have full row rank. Also note that the generator matrix G and the parity check matrix H are not unique for a given code. However, all generator matrices and parity check matrices have the same dimensions.

Proposition 2.3. Any $[n, k]_q$ linear code can be represented with $\min(nk, n(n - k))$ symbols from $\mathbb{F}_q$.

Proof. We have that the generator matrix G has nk symbols and the parity check matrix H has $n(n - k)$ symbols. □

Definition 2.4 (Hamming Code (for $r = 3$))**.** The *Hamming Code* (for $r = 3$) is a binary code of block length $n = 7$ and dimension $k = 4$ with minimum distance $\Delta(C_H) = 3$. Given a message $(x_1, x_2, x_3, x_4) \in \{0, 1\}^4$, the corresponding codeword is given by

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

§3. On the Distance of a Linear Code

Proposition 3.1. For every $[n, k, d]_q$ code C, we have

$$d = \min_{\substack{c \in C \\ c \neq 0}} \mathrm{wt}(c)$$

Proof. First, we show that d is no more than the minimum weight. We can see this by considering $\Delta(0, c')$ where c' is the non-zero codeword in C with minimum weight; its distance from 0 is equal to its weight. Thus, we have $d \leqslant \mathrm{wt}(c')$, as desired.

Now, to show that d is no less than the minimum weight, consider $c_1 \neq c_2 \in C$ such that $\Delta(c_1, c_2) = d$. Note that $c_1 - c_2 \in C$ (this is because $-c_2 = -1 \cdot c_2 \in C$, where -1 is the additive inverse of 1 in F_q and $c_1 - c_2 = c_1 + (-c_2)$, which is in C by the definition of linear codes). Now note that $\mathrm{wt}(c_1 - c_2) = \Delta(c_1, c_2) = d$, since the non-zero symbols in $c_1 - c_2$ occur exactly in the positions where the two codewords differ. Further, since $c_1 \neq c_2, c_1 - c_2 \neq 0$, which implies that the minimum Hamming weight of any non-zero codeword in C is at most d. □

Proposition 3.2. For every $[n, k, d]_q$ code C with parity check matrix H, d equals the size of the smallest subset of columns of H that are linearly dependent.

Proof. By Proposition 3.1, we need to show that the minimum weight of a non-zero codeword in C is the minimum number of linearly dependent columns. Let t be the minimum number of linearly dependent columns in H.

For one first direction, let $c \neq 0 \in C$ be a codeword with $\mathrm{wt}(c) = d$. Now note that, by the definition of the parity check matrix, $H \cdot c^T = 0$. We check that $\sum_{i=1}^{n} c_i H^i = 0$, where

$$H = \begin{pmatrix} \uparrow & \uparrow & & \uparrow & & \uparrow \\ H^1 & H^2 & \dots & H^i & \dots & H^n \\ \downarrow & \downarrow & & \downarrow & & \downarrow \end{pmatrix}$$

and $c = (c_1, \cdots, c_n)$. So for $H \cdot c^T$ to be zero, those H^i with $c_i \neq 0$ are linearly dependent. This means that $d \geqslant t$, as the columns corresponding to non-zero entries in c are one instance of linearly dependent columns.

For the other direction, consider the minimum set of columns from $H, H^{i_1}, H^{i_2}, \cdots, H^{i_t}$ that are linearly dependent. This implies that there exist non-zero elements $c'_{i_1}, \cdots, c'_{i_t} \in F_q$ such that $c'_{i_1} H^{i_1} + \cdots + c'_{i_t} H^{i_t} = 0$. (Note that all the c'_{i_j} are non-zero as no set of fewer than t columns are linearly dependent.) Now extend $c'_{i_1}, \cdots, c'_{i_t}$ to the vector c' such that $c'_j = 0$ for $j \notin \{i_1, \cdots, i_t\}$. Note that we have $H \cdot (c')^T = 0$ and thus, we have $c' \in C$. This in turn implies that $d \leqslant \mathrm{wt}(c') = t$ (where recall t is the minimum number of linearly independent columns in H). □

§4. Hamming Codes

We have seen a particular example of Hamming Code as the $[7, 4, 3]_2$ Hamming Code. In general, for any $r \geqslant 2$, there is a $[2^r - 1, 2^r - r - 1, 3]_2$ Hamming Code.

Definition 4.1 (Binary Hamming Code)**.** For any positive integer r, define the matrix $H_r \in \mathbb{F}_2^{r \times (2^r - 1)}$ to be the $r \times (2^r - 1)$ matrix whose i^{th} column H_r^i is the binary representation of i, for $1 \leqslant i \leqslant 2^r - 1$ (as a vector in $0, 1^r$).

The $[2^r - 1, 2^r - r - 1]_2$ Hamming Code, denoted by $C_{H,r}$, is the code with parity check matrix H_r.
As we have seen for the $r = 3$ case, H_3 is given by:

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Proposition 4.2. The Hamming Code $[2^r - 1, 2^r - r - 1]_2$ has distance $d = 3$.

Proof. No two columns in H_r are linearly dependent. Thus, by proposition 3.2, we have that the distance is at least 3. It is at most 3, since, for example, $H_r^1 + H_r^2 + H_r^3 = \mathbf{0}$ □

Now, by definition of a perfect code given in the week 1 handout, since under the Hamming Bound for $d = 3$, as every Hamming Code satisfies the bound, we have that the Hamming Code is a perfect code.

§5. Dual of a Linear Code

Definition 5.1 (Dual of a Code)**.** Let H be a parity check matrix of a code C, then the code generated by H is called the *dual* of C. The dual of C is denoted by $C^\perp$.

Proposition 5.2. If C is a $[n, k]_q$ code, then:

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

Definition 5.3 (Simplex and Hadamard Codes)**.** For any positive integer r, the *Simplex Code* $C_{\text{Sim},r}$ is the code generated by H_r. Equivalently, $C_{\text{Sim},r} = C_{H,r}^\perp$.

For any positive integer r, the *Hadamard Code* $C_{\text{Had},r}$ is the $[2^r, r]_2$ is the code generated by the $r \times 2^r$ matrix H_r' obtained by adding the all zero column to (say in front of the columns) in H_r.

Proposition 5.4. $C_{\text{Sim},r}$ and $C_{\text{Had},r}$ both have distances 2^{r-1}.

Proof. We first show the result for $C_{\text{Had},r}$. In fact, we will show something stronger: every non-zero codeword in $C_{\text{Had},r}$ has weight exactly equal to 2^{r-1} (the claimed distance follows from Proposition 3.1). Consider a message $x \neq 0$. Let its i^{th} entry be $x_i = 1$. x is encoded as

$$c = (x_1, x_2, \ldots, x_r)(H_r^0, H_r^1, \ldots, H_r^{2^r-1}),$$

where H_r^j is the binary representation of $0 \leqslant j \leqslant 2^r - 1$ (that is, the set of vectors H_r^j is exactly the set of all the vectors in $\{0, 1\}^r$). Further note that the j^{th} bit of the codeword c is $\langle x, H_r^j \rangle$. Group all the columns of the generator matrix into pairs (u, v) such that $v = u + e_i$ (i.e., v and u are the same except in the ith position). For example, for $r = 3$ and $i = 2$, the paired up columns are marked with the same color below:

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

Notice that this partitions all the columns into 2^{r-1} disjoint pairs. Then,

$$\langle x, v \rangle = \langle x, u + e_i \rangle = \langle x, u \rangle + \langle x, e_i \rangle = \langle x, u \rangle + x_i = \langle x, u \rangle + 1.$$

Thus, we have that $\langle x, v \rangle$ is the negation of $\langle x, u \rangle$, i.e., exactly one of $\langle x, v \rangle$ and $\langle x, u \rangle$ is 1. As the choice of the pair (u, v) was arbitrary, we have proved that for any non-zero codeword c such that $c \in C_{\text{Had},r}$, $\text{wt}(c) = 2^{r-1}$.

For the simplex code, we observe that all codewords of $C_{\text{Had},r}$ are obtained by padding a 0 to the beginning of the codewords in $C_{\text{Sim},r}$, which implies that all non-zero codewords in $C_{\text{Sim},r}$ also have a weight of 2^{r-1}, which completes the proof. □

Let r be a positive integer and let $n = \frac{q^r-1}{q-1} = |\mathbb{P}^{r-1}(\mathbb{F}_q)|$ (where $\mathbb{P}^{r-1}(\mathbb{F}_q)$ is the projective space of dimension $r - 1$ over $\mathbb{F}_q$). Let $H_r(q)$ be an $r \times n$ matrix with entries in $\mathbb{F}_q$ such that any two columns are linearly independent. In effect, the columns of $H_r(q)$ are obtained by representatives in $\mathbb{F}_q^r$ of distinct points of $\mathbb{P}^{r-1}(\mathbb{F}_q)$. Observe that the columns of $H_r(q)$ include some nonzero scalar multiples of the standard basis vectors of $\mathbb{F}_q^r$, and hence the rank of $H_r(q)$ is r.

Definition 5.5 (q-ary Hamming, Simplex and HadamardCodes)**.** Define $\mathscr{H}_r(q)$ to be an $[n, n-r]_q$-code with $H_r(q)$ as its parity-check matrix and $\mathscr{S}_r(q)$ to be an $[n, r]_q$-code with $H_r(q)$ as its generator matrix. These are called q-ary *Hamming code* and q-ary *simplex code*, respectively.

The q-ary *Hadamard code* is defined as the $[q^r, r]_q$ code with generator matrix defined by the $r \times q^r$ matrix $H'_r(q)$ with columns as the q-ary representations of the elements of $\mathbb{F}_q^r$. This code is denoted by $\mathscr{H}'_r(q)$.

Proposition 5.6. $d(\mathscr{H}_r(q)) = 3$ and $d(\mathscr{S}_r(q)) = q^{r-1}$. Also we have that $\mathscr{H}_r(q)^\perp = \mathscr{S}_r(q)$

Proof. $d(\mathscr{H}_r(q)) = 3$ is trivial from Proposition 3.2. For $d(\mathscr{S}_r(q)) = q^{r-1}$, we use a similar approach as we used for Proposition 5.4. Note that there are q^r points in $\mathbb{F}_q^r$, and q^{r-1} have i^{th} coordinate 0 for some i such that $x_i \neq 0$. Thus, the number of matrices with i^{th} coordinate not 0 is $q^{r-1}(q-1)$, and normalizing them (basically seeing them in $\mathbb{P}^{r-1}(\mathbb{F}_q)$), we have their weight will be q^{r-1}.

For the last part, note that the dual of $\mathscr{H}_r(q)$ is $\mathscr{S}_r(q)$, since the generator matrix of $\mathscr{S}_r(q)$ is the parity check matrix of $\mathscr{H}_r(q)$. □

§6. Reed-Solomon Codes

Reed-Solomon codes are a group of codes which allow you to choose how many errors and erasures you wish to correct. It utilizes the uniqueness of polynomial interpolation. We first discuss how Reed-Solomon codes actually encode a message.

Definition 6.1 (Reed Solomon Codes)**.** Let $\mathbb{F}_q$ be a finite field, and choose n and k satisfying $k \leqslant n \leqslant q$. Fix a sequence $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ of n distinct elements (also called *evaluation points*) from $\mathbb{F}_q$. We define an encoding function for Reed-Solomon code $\text{RS}_q[\alpha, k] : \mathbb{F}_q^k \to \mathbb{F}_q^n$ as follows. Map a message $\mathbf{m} = (m_0, m_1, \ldots, m_{k-1})$ with $m_i \in \mathbb{F}_q$ to the degree $k-1$ polynomial.

$$\mathbf{m} \mapsto f_{\mathbf{m}}(X),$$

where

$$f_{\mathbf{m}}(X) = \sum_{i=0}^{k-1} m_i X^i. \quad (5.1)$$

Note that $f_{\mathbf{m}}(X) \in \mathbb{F}_q[X]$ is a polynomial of degree at most $k-1$. The encoding of $\mathbf{m}$ is the evaluation of $f_{\mathbf{m}}(X)$ at all the α_i's:

$$\text{RS}_q[\alpha, k](\mathbf{m}) = \left(f_{\mathbf{m}}(\alpha_1), f_{\mathbf{m}}(\alpha_2), \ldots, f_{\mathbf{m}}(\alpha_n)\right).$$

When q, α and k are known from context, we suppress them in the notation and simply refer to the map as RS. We call the image of this map, i.e., the set $\{\text{RS}[\mathbf{m}] \mid \mathbf{m} \in \mathbb{F}_q^k\}$, the *Reed-Solomon* code or RS code. A common special case is $n = q-1$ with the set of evaluation points being $\mathbb{F}^* \coloneqq \mathbb{F} \setminus \{0\}$.

The above definition is heavy, so read it again if you don't understand in one go. We now discuss some interesting properties of the RS code.

Proposition 6.2. RS Codes are linear codes.

The proof of this fact is quite elementary, and therefore left as an exercise to the reader. In fact, you may see it almost it immediately from the way the code is defined. Before an interesting result on the distance of a RS code, we present a theorem, without proof which we use to prove the result that follows it.

Theorem 6.3 (Singleton Bound)**.** For every $(n, k, d)_q$ code, the following holds:

$$k \leqslant n - d + 1$$

Proposition 6.4. The minimum distance of RS is $n - k + 1$.

Proof. Fix arbitrary $\mathbf{m_1} \neq \mathbf{m_2} \in \mathbb{F}_q^k$. Note that $f_{\mathbf{m_1}}(X), f_{\mathbf{m_2}}(X) \in \mathbb{F}_q[X]$ are distinct polynomials of degree at most $k-1$ since $\mathbf{m_1} \neq \mathbf{m_2} \in \mathbb{F}_q^k$. Then $f_{\mathbf{m_1}}(X) - f_{\mathbf{m_2}}(X) \neq 0$ also has degree at most $k-1$. Note that $\text{wt}(\text{RS}(\mathbf{m_2}) - \text{RS}(\mathbf{m_1})) =$

$\Delta(\text{RS}(\mathbf{m_1}), \text{RS}(\mathbf{m_2}))$. The weight of $\text{RS}(\mathbf{m_2}) - \text{RS}(\mathbf{m_1})$ is n minus the number of zeroes in $\text{RS}(\mathbf{m_2}) - \text{RS}(\mathbf{m_1})$, which is equal to n minus the number of roots that $f_{\mathbf{m_1}}(X) - f_{\mathbf{m_2}}(X)$ has among $\{\alpha_1, \ldots, \alpha_n\}$. That is,

$$\Delta(\text{RS}(\mathbf{m_1}), \text{RS}(\mathbf{m_2})) = n - |\{\alpha_i \mid f_{\mathbf{m_1}}(\alpha_i) = f_{\mathbf{m_2}}(\alpha_i)\}|.$$

Now, $f_{\mathbf{m_1}}(X) - f_{\mathbf{m_2}}(X)$ has at most $k-1$ roots. Thus, the weight of $\text{RS}(\mathbf{m_2}) - \text{RS}(\mathbf{m_1})$ is at least $n-(k-1) = n-k+1$. Therefore $d \geqslant n - k + 1$, and since the Singleton bound implies that $d \leqslant n - k + 1$, we have $d = n - k + 1$. The argument above also shows that distinct polynomials $f_{\mathbf{m_1}}(X), f_{\mathbf{m_2}}(X) \in \mathbb{F}_q[X]$ are mapped to distinct codewords. (This is because the Hamming distance between any two codewords is at least $n - k + 1 \geqslant 1$, where the last inequality follows as $k \leqslant n$.) Therefore, the code contains q^k codewords and has dimension k. The claim on linearity of the code follows from Proposition 6.2. □

Theorem 6.5. RS is a $[n, k, n - k + 1]_q$ code, i.e., RS matches the Singleton Bound.

Finally, we describe a generator matrix for RS codes. Such a matrix is guaranteed to exist by Proposition 6.2, but now we give an explicit one. By Definition 6.1, any basis $f_{\mathbf{m_1}}, ..., f_{\mathbf{m_k}}$ of polynomials of degree at most $k-1$ gives rise to a basis $\text{RS}(\mathbf{m_1}), ..., \text{RS}(\mathbf{m_k})$ of the code. A particularly nice polynomial basis is the set of monomials $1, X, ..., X^i, ..., X^{k-1}$. The corresponding generator matrix, whose ith row (numbering rows from 0 to $k-1$) is

$$(\alpha_1^i, \alpha_2^i, ..., \alpha_j^i, ..., \alpha_n^i)$$

and this generator matrix is called the *Vandermonde matrix* of size $k \times n$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_j & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_j^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \alpha_1^i & \alpha_2^i & \cdots & \alpha_j^i & \cdots & \alpha_n^i \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_j^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$