22. Linear codes

22.1 Introduction

In this lecture, we will prove some properties of linear codes and describe Hamming's code that corrects single-bit errors.

22.2 Linear codes

A vector space L over the finite field $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ endowed with the opertations of vector addition (+) and scalar multiplication ($\cdot$) such that $(L, +)$ is an abelian group, and for any element $\alpha \in \mathbb{F}_q$, $\alpha \cdot v \in L$ for $v \in L$.
Span: The span of a set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ is the set $\{\sum \alpha_i \cdot \mathbf{v}_i \mid \alpha_i \in \mathbb{F}_q\}$.
Linear independence: A set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_k$ are linearly independent $\sum \alpha_i \cdot \mathbf{v}_i = 0$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$.
Basis:The basis of a linear space $L \subseteq \mathbb{F}_q^n$ is a set of linearly independent vectors in L that spans L. The number of elements in the basis is the *dimension* of L, denoted by $\dim(L)$.
Null space: The null space of a vector space L, denoted by $L^\perp$, is the set of vectors $\mathbf{w}$ such that $\langle \mathbf{w}, \mathbf{v} \rangle = 0$.

It can be shown that $L^\perp$ is also a linear space.

Proposition 22.1. *Let L be k-dimensional subspace of $\mathbb{F}_q^n$, and let $L^\perp$ be its null space. Then,* $\dim(L^\perp) = n - k$.

Let $L \subseteq \mathbb{F}_q^n$ be a subspace of dimension k and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be a basis for L. Then we can construct a matrix $G \in \mathbb{F}_q^{k \times n}$ where the i^{th} row of G is the vector $\mathbf{v}_i$. The matrix G generates the vector space L since $L = \{\mathbf{x}G \mid \mathbf{x} \in \mathbb{F}_q^k\}$. The number of linearly independent rows of a matrix is equal to the number of linearly independent columns of a matrix and this is known as the rank of the matrix G, denoted by $\mathrm{rk}(G)$. In this case $\mathrm{rk}(G) = k$.

An $[n, k, d]_q$ code $\mathcal{C}$ is a linear code is $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$ of dimension k. The matrix $G \in \mathbb{F}_q^{k \times n}$ where the rows form a basis for $\mathcal{C}$ is known as the generator matrix for the code $\mathcal{C}$ (we will refer to $\mathcal{C}$ as both a linear subspace and a code). Therefore $\mathcal{C} = \{\mathbf{x}G \mid \mathbf{x} \in \mathbb{F}_q^k\}$. For the code $\mathcal{C}$, the null space $\mathcal{C}^\perp$ is known as the dual code of $\mathcal{C}$. The linear space $\mathcal{C}^\perp$ has dimension $n - k$ and hence is generated by a matrix $H^T \in \mathbb{F}_q^{(n-k) \times n}$. Since H^T generates $\mathcal{C}^\perp$, we know that for every vector $\mathbf{x} \in \mathcal{C}$, $\mathbf{x}H = 0$. The matrix H is known as the parity-check matrix of the code $\mathcal{C}$.

For a codeword $\mathbf{x} \in \mathcal{C}$, let $\mathrm{wt}(\mathbf{x})$ denote the number of non-zero entries in the vector. This is known as the Hamming weight of the codeword $\mathbf{x}$. The minimum distance of a code $\mathcal{C}$ is connected to the parity-check matrix in the following way. First, we show that minimum distance of a linear code is equal to the minimum weight of the code.

Proposition 22.2. *The minimum distance of a linear code $\mathcal{C}$ is equal to the minimum weight of $\mathcal{C}$.*

Proof. Let d be the minimum distance of the code, and let w be the weight of the minimum weight codeword. Let $\mathbf{x}, \mathbf{y}$ be such that $\Delta(\mathbf{x}, \mathbf{y}) = d$. The vector $\mathbf{z} = \mathbf{x} - \mathbf{y}$ is also a codeword, and $\mathrm{wt}(\mathbf{z}) = \Delta(\mathbf{x}, \mathbf{y})$. Therefore, $w \leq d$. Let $\mathbf{w}$ be a codeword such that $\mathrm{wt}(\mathbf{w}) = w$. Therefore, $w = \Delta(\mathbf{w}, \mathbf{0}) \geq d$. Therefore, for any linear code $\mathcal{C}$, $w = d$. $\square$

Proposition 22.3. *The minimum distance of a k-dimensional linear code $\mathcal{C} \in \mathbb{F}_q^n$ with parity-check matrix H is equal to the smallest integer r such that there are r linearly dependent rows in H.*

Proof. Let d be the minimum distance of $\mathcal{C}$. Then, there exists a codeword $\mathbf{x}$ such that $\mathrm{wt}(\mathbf{x}) = d$. Since $\mathbf{x}H = 0$, there exists d rows $\mathbf{h}_1, \ldots, \mathbf{h}_d$ such that $\sum x_i \mathbf{h}_i = 0$. Similarly, if there exists r linearly dependent rows in H, then this gives a vector $\mathbf{x}$ of weight r such that $\mathbf{x}H = 0$. $\square$

Notice that permuting the rows of G does not change the linear space generated by G. Similarly, permuting the columns of G does not change the linear space generated by G since we are merely changing the coordinate names. Also, taking linear combinations of the rows of G does not change the space generated by G; we are merely changing the basis of the linear space. Thus we can convert the generator matrix G of linear code $\mathcal{C}$ to a form $[I_k \mid A]$ where I_k is the $k \times k$ identity matrix, and $A \in \mathbb{F}_q^{k \times n-k}$. Since H^T generates $\mathcal{C}^\perp$, we know that $H^T G^T = 0$. Therefore, we can express H^T as the matrix $[-A^T \mid I_{n-k}]$. We conclude the discussion above with the following proposition.

Proposition 22.4. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a k-dimensional linear space. Then the following holds:*

- *The generator matrix $G \in \mathbb{F}_q^{k \times n}$ can be expressed as $[I_k \mid A]$, where $A \in \mathbb{F}_q^{k \times n-k}$.*
- *The generator matrix $H^T \in \mathbb{F}_q^{n-k \times n}$ of $\mathcal{C}^\perp$ can be expressed as $[-A^T \mid I_{n-k}]$.*

When we have a generator matrix of the form $[I_k \mid A]$, then we can think of the encoding as sending the message symbols appended by the parity-check bits.

22.3 Hamming code

We will now see Hamming's construction of an error correcting code that can correct a single bit error. These are linear codes with minimum distance 3. For the rest of this discussion we will work over $\mathbb{F}_2$.

We want to construct an $[n, k, 3]_2$ code with parity check matrix $H \in \mathbb{F}_2^{n \times (n-k)}$. For any codeword $\mathbf{x}$ with $\mathrm{wt}(\mathbf{x}) = 1$, $\mathbf{x}H \neq 0$. This means that every row $\mathbf{h}_i$ of H is non-zero. Similarly, for every $\mathbf{x}$ with $\mathrm{wt}(\mathbf{x}) = 2$, $\mathbf{x}H \neq 0$. This implies that $\mathbf{h}_i \neq \mathbf{h}_j$ for $i \neq j$.

Let $l = n - k$. Hamming code is described by the parity check matrix H where each row is a binary string of length l. Since we want each row to be non-zero there are $2^l - 1$ many rows. From the discussion in the last paragraph we know that this code has distance at least 3. Thus we have the following theorem.

Theorem 22.5. *For every l, there is a $[2^l - 1, 2^l - l - 1, 3]_2$ code.*

22.3.1 Hamming $[7,4,3]_2$ code

The least for which we have Hamming code is $l = 3$, and for this value of l we have the $[7,4,3]_2$ Hamming code. Let's describe the parity check matrix and the generator matrix for this code. Recall that H consists of all strings of length l except the all 0 string. Therefore,

$$H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \text{ and } H^T = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Now, I can permute the columns of H^T to obtain the following matrix in the form $[-A^T \mid I_{n-k}]$.

$$H^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Since $G = [I_k \mid A]$, we can obtain the generator matrix for the $[7,4,3]_2$ code as below.

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

22.3.2 Decoding the Hamming code

Suppose $\mathbf{y}$ is a received message that we want to decode where $\mathbf{y} = \mathbf{x} + \mathbf{e}_i$. The word $\mathbf{x} \in \mathcal{C}$. Then, $(\mathbf{x} + \mathbf{e}_i)H = 0$, and this implies that $\mathbf{e}_i H = 0$. If H is arranged such that the i^{th} row is i written in binary, then $\mathbf{e}_i H$ gives you the location of the error (in binary).

22.3.3 Hamming's bound

Notice that to encode a k bit message to correct one bit of error, we needed $O(\log k)$ many parity check bits. Is this really necessary?

Theorem 22.6. *Let $\mathcal{C}$ be an $[n,k,3]_2$ code. Then $k \leq n - \log_2(n+1)$.*

Proof. For any two codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, we have $B(\mathbf{x},1) \cap B(\mathbf{y},1) = \emptyset$. Also $|\cup_{\mathbf{x}\in\mathcal{C}} B(\mathbf{x},1)| \leq 2^n$. Since the balls are disjoint, $|\cup_{\mathbf{x}\in\mathcal{C}} B(\mathbf{x},1)| = \sum_{\mathbf{x}\in\mathcal{C}} |B(\mathbf{x},1)| = 2^k(n+1)$. Therefore, $2^k(n+1) \leq 2^n$, and the bound follows from that. $\square$

The same argument for packing balls of radius $\lfloor (d-1)/2 \rfloor$ in $\{0,1\}^n$ can be used to prove the following more general form of the bound.

Theorem 22.7. *If an* $[n, k, d]_2$ *code exists, then*

$$2^k \operatorname{Vol}\left(\left\lfloor \frac{d-1}{2} \right\rfloor, n\right) \le 2^n.$$