2. Linear Codes

Linear Codes

- Assume the code alphabet $\mathbb{F}$ can be given a *field* structure.
  - What is a *field*? A set with *addition* and *multiplication* operations $\{+, *\}$ with all the properties we're used to (e.g., $\mathbb{Q}, \mathbb{R}, \mathbb{C}$).
    - A *finite field* is a field with a finite number of elements. In our case, $\mathbb{F}$ is a finite field, of, say, $|\mathbb{F}| = q$ elements.
    - We will see that $q = p^m$ for some prime number p and integer $m \geq 1$. We denote such a field by $\mathbb{F}_q$ or $\mathrm{GF}(q)$.
    - Example: $\mathbb{F}_2 = \{0,\ 1\}$ with $\textsc{xor}, \textsc{and}$ operations.
    - Much more about finite fields later!
  - $\mathbb{F}^n$ is a *linear space* over $\mathbb{F}$ (the field of *scalars*). All the usual notions and properties apply: bases, sub-spaces, matrices, linear transforms, etc.
- A code $\mathcal{C} : (n, M, d)$ over $\mathbb{F}$ is a *subset* of $\mathbb{F}^n$.
  $\mathcal{C}$ is called a *linear code* if it is a *linear sub-space* of $\mathbb{F}^n$ over $\mathbb{F}$.
  - $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C},\ a_1, a_2 \in \mathbb{F} \quad \Rightarrow \quad a_1\mathbf{c}_1 + a_2\mathbf{c}_2 \in \mathcal{C}$

Parameters of a Linear Code

- $\mathcal{C}$ is a linear sub-space of $\mathbb{F}^n$ over $\mathbb{F}$. Let $k \leq n$ be the dimension of this linear sub-space, and let $q = |\mathbb{F}|$.
- $\mathcal{C}$ has a *basis* $\{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{k-1}\}$ such that every $\mathbf{c} \in \mathcal{C}$ can be written as

$$\mathbf{c} = \sum_{i=0}^{k-1} a_i \mathbf{c}_i, \quad a_i \in \mathbb{F},\ 0 \leq i \leq k-1\,,$$

  and every distinct vector of coefficients $[a_0, a_1, \ldots, a_{k-1}]$ corresponds to a different codeword. There are q^k such vectors.
- Therefore, $\mathcal{C}$ has $M = q^k$ codewords, which explains why we called $k = \log_q M$ the *dimension* of $\mathcal{C}$ (even when $\mathcal{C}$ was not linear).
- $r = n - k$ is the *redundancy* of $\mathcal{C}$, $R = k/n$ its *rate*.
- We use the notation $[n, k, d]$ to denote the parameters of a linear code. An $[n, k, d]$ code over $\mathbb{F}$ is an (n, q^k, d) code over $\mathbb{F}$.

Generator Matrix

- A *generator matrix* for a linear code $\mathcal{C}$ is a $k \times n$ matrix G whose rows form a basis of $\mathcal{C}$.
- **Example:** $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \hat{G} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$
  are *both* generators of the $[3, 2, 2]$ parity code over $\mathbb{F}_2$.
- In general, the $[n, n-1, 2]$ parity code over any F is generated by

$$G = \left(\begin{array}{c|c} & -1 \\ & -1 \\ I_{n-1} & \vdots \\ & -1 \end{array} \right),$$

  where I_{n-1} is the $(n-1) \times (n-1)$ identity matrix.
- What's G for the repetition code?

$$G = (1\ 1\ \ldots\ 1).$$

Minimum Weight

- For an $[n, k, d]$ code $\mathcal{C}$,

$$\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \implies \mathbf{c}_1 - \mathbf{c}_2 \in \mathcal{C}\,, \text{ and } \mathsf{d}(\mathbf{c}_1, \mathbf{c}_2) = \mathsf{wt}(\mathbf{c}_1 - \mathbf{c}_2)\,.$$

  Therefore,

$$d = \min_{\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \,:\, \mathbf{c}_1 \neq \mathbf{c}_2} \mathsf{d}(\mathbf{c}_1, \mathbf{c}_2) = \min_{\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C} \,:\, \mathbf{c}_1 \neq \mathbf{c}_2} \mathsf{wt}(\mathbf{c}_1 - \mathbf{c}_2) = \min_{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}} \mathsf{wt}(\mathbf{c})\,.$$

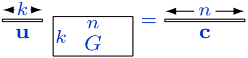
  $\Rightarrow$ *minimum distance is the same as minimum weight for linear codes*.

- Recall also that $\mathbf{0} \in \mathcal{C}$ and $\mathsf{d}(\mathbf{c}, \mathbf{0}) = \mathsf{wt}(\mathbf{c})$.

Encoding Linear Codes

- Since $\mathrm{rank}(G) = k$, the map $\mathcal{E} : \mathbb{F}^k \to \mathcal{C}$ defined by

$$\mathcal{E} : \mathbf{u} \mapsto \mathbf{c} = \mathbf{u}\, G\,, \quad \mathbf{u} \in \mathbb{F}^k$$



  is 1-1, and can serve as an encoding mechanism for $\mathcal{C}$.

- Applying elementary row operations and possibly reordering coordinates (columns), we can bring G to the form

$$G = \left(\; I_k \;\middle|\; A \;\right) \qquad \textit{systematic generator matrix,}$$

  where I_k is a $k \times k$ identity matrix, and A is a $k \times (n-k)$ matrix.

$$\mathbf{u} \mapsto \mathbf{c} = \mathbf{u}\, G = (\, \mathbf{u} \mid \mathbf{u}\, A\,) \qquad \textit{systematic encoding.}$$

- In a systematic encoding, the k *information symbols* from $\mathbf{u}$ are transmitted ‘as is’, and $n-k$ *check symbols* (or *redundancy* symbols, or *parity* symbols) are appended.

Parity Check Matrix

- Let $\mathcal{C} : [n, k, d]$. A *parity-check matrix (PCM)* of $\mathcal{C}$ is an $r \times n$ matrix H such that for all $\mathbf{c} \in \mathbb{F}^n$,

$$\mathbf{c} \in \mathcal{C} \quad \Longleftrightarrow \quad H\mathbf{c}^T = \mathbf{0}\,.$$

  - $\mathcal{C}$ is the (right) kernel of H in $\mathbb{F}^n$. Therefore,

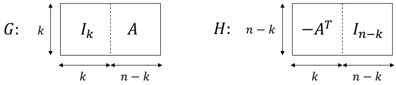
$$\operatorname{rank}(H) = n - \dim\ker(H) = n - k$$

  - We will usually have $r = \operatorname{rank}(H) = n - k$ (no superfluous rows)

- For a generator matrix G of $\mathcal{C}$, we have

$$HG^T = 0 \Rightarrow GH^T = 0, \;\; \textbf{and} \;\; \dim\ker(G) = n - \operatorname{rank}(G) = n - k = r$$

- If $G = (\ I_k \mid A\ )$, then $H = (-A^T \mid I_{n-k}\ )$ is a (systematic) parity-check matrix.



Dual Code

- The *dual* code of $\mathcal{C} : [n, k, d]$ is

$$\mathcal{C}^{\perp} = \{\, \mathbf{x} \in \mathbb{F}^n \,:\, \mathbf{x}\,\mathbf{c}^T = 0 \;\; \forall \mathbf{c} \in \mathcal{C} \,\},$$

  or, equivalently

$$\mathcal{C}^{\perp} = \{\, \mathbf{x} \in \mathbb{F}^n \,:\, \mathbf{x}\,G^T = \mathbf{0} \,\}.$$

- $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$
- G and H of $\mathcal{C}$ reverse roles for $\mathcal{C}^{\perp}$:

$$\mathcal{C} : \; \left\{ \begin{array}{ccc} G & = & H^{\perp} \\ H & = & G^{\perp} \end{array} \right\} \; : \mathcal{C}^{\perp}\,.$$

- $\mathcal{C}^{\perp}$ is an $[n, n-k, d^{\perp}]$ code over $\mathbb{F}$.

Examples

- $H = (1\,1\,\ldots\,1)$ is a PCM for the $[n, n-1, 2]$ parity code, which has generator matrix

$$G = \left(\begin{array}{c|c} & -1 \\ & -1 \\ I & \vdots \\ & -1 \end{array}\right).$$

  On the other hand, H generates the $[n, 1, n]$ repetition code, and G is a check matrix for it $\Rightarrow$ *parity and repetition codes are dual*.

- $[7, 4, 3]$ *Hamming code* over $\mathbb{F}_2$ is defined by

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

- $GH^T = 0$ can be verified by direct inspection

Minimum Distance and H

Theorem

Let H be a PCM of $\mathcal{C} \neq \{\mathbf{0}\}$. The minimum distance of $\mathcal{C}$ is the largest integer d such that every subset of $d-1$ columns in H is linearly independent.

- **Proof.** There is a codeword $\mathbf{c}$ of weight t in $\mathcal{C}$ if and only if there are t l.d. columns in H (those columns that correspond to non-zero coordinates of $\mathbf{c}$). □
- **Example:** Code $\mathcal{C}$ with

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

All the columns are different $\Rightarrow$ every 2 columns are linearly independent $\Rightarrow$ $d \geq 3$.
On the other hand, $H \cdot [1\,1\,1\,0\,0\,0\,0]^T = \mathbf{0} \;\Rightarrow\; d = 3$.

The Binary Hamming Code

- The m-th *order Hamming code* $\mathcal{H}_m$ over $\mathbb{F}_2$ is defined by the $m \times (2^m - 1)$ PCM

$$H_m = [\, \mathbf{h}_1 \; \mathbf{h}_2 \; \ldots \; \mathbf{h}_{2^m-1} \,],$$

  where $\mathbf{h}_i$ is the length-m (column) binary representation of i.

$$m \left\{ \begin{bmatrix} 1 & 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & 1 \end{bmatrix} \right.$$

- Clearly, H_m has full rank m.

Theorem

$\mathcal{H}_m$ is a $[2^m - 1,\, 2^m - 1 - m,\, 3]$ linear code.

Proof. $[n, k]$ parameters are immediate. No two columns of H_m are l.d. $\Rightarrow$ $d \geq 3$. On the other hand, $\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 = \mathbf{0}$ for all m.

The q-ary Hamming Code

- The m-th order Hamming code $\mathcal{H}_{q,m}$ over $\mathbb{F} = \mathbb{F}_q,\ q \geq 2,$ has PCM $H_{q,m}$ consisting of all distinct nonzero m-columns $\mathbf{h} \in \mathbb{F}_q^m$ *up to scalar multiples*, e.g.

$$\mathbf{h} \in H_{q,m} \implies a\mathbf{h} \notin H_{q,m}\ \forall a \in \mathbb{F}_q \backslash \{1\}.$$

Example: $q = 3$

$$m \left\{ \begin{bmatrix} 1 & 0 & 1 & 2 & \cdots & \cdots & 2 \\ 0 & 1 & 1 & 1 & \cdots & \cdots & 2 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & 2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \cdots & 1 \end{bmatrix} \right.$$

Theorem

$\mathcal{H}_{q,m}$ *is an* $[n, n-m, 3]$ *code with*

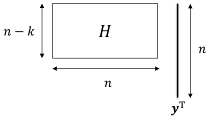
$$n = \frac{q^m - 1}{q - 1}$$

Proof. As before, no two columns of $H_{q,m}$ are multiples of each other, i.e. dependent. One the other hand, there are l.d. triplets of columns.

Cosets and Syndromes

- Let $\mathbf{y} \in \mathbb{F}^n$. The *syndrome* of $\mathbf{y}$ (with respect to an $(n-k) \times n$ PCM H of $\mathcal{C}$) is defined by

$$\mathbf{s} = H\mathbf{y}^T \in \mathbb{F}^{n-k}.$$



- The set

$$\mathbf{y} + \mathcal{C} \triangleq \{\mathbf{y} + \mathbf{c} \; : \; \mathbf{c} \in \mathcal{C}\}$$

  is a *coset* of $\mathcal{C}$ (as an additive subgroup) in $\mathbb{F}^n$.
  - Since $\mathbf{0} \in \mathcal{C}$, we have $\mathbf{y} \in \mathbf{y} + \mathcal{C}$; also $\mathcal{C} = \mathbf{0} + \mathcal{C}$ is a coset itself.
- Let $\bar{\mathbf{y}} \in \mathbb{F}^n$. If $\bar{\mathbf{y}} \in \mathbf{y} + \mathcal{C}$, then $\bar{\mathbf{y}} - \mathbf{y} \in \mathcal{C}$, and
  - $\bar{\mathbf{y}} + \mathcal{C} = \mathbf{y} + (\bar{\mathbf{y}} - \mathbf{y}) + \mathcal{C} = \mathbf{y} + \mathcal{C}$,
  - $H(\bar{\mathbf{y}} - \mathbf{y})^T = \mathbf{0} \implies H\bar{\mathbf{y}}^T = H\mathbf{y}^T$

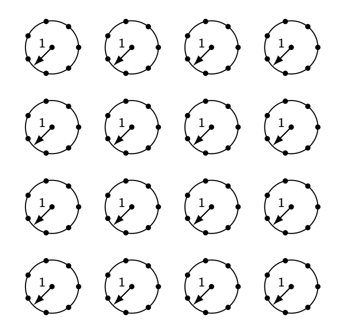
    $\implies$ *The syndrome is invariant for all* $\bar{\mathbf{y}} \in \mathbf{y} + \mathcal{C}$.
- If $\bar{\mathbf{y}} - \mathbf{y} \notin \mathcal{C}$ then $(\bar{\mathbf{y}} + \mathcal{C}) \cap (\mathbf{y} + \mathcal{C}) = \phi$.
- Let $\mathbb{F} = \mathbb{F}_q$. There are q^{n-k} distinct, disjoint cosets of $\mathcal{C}$ in $\mathbb{F}^n$. Cosets form a *partition* of $\mathbb{F}^n$.
- Given a PCM H, there is a 1-1 correspondence between the q^{n-k} cosets of $\mathcal{C}$ in $\mathbb{F}^n$ and the q^{n-k} possible syndrome values.

Syndrome Decoding of Linear Codes

- $\mathbf{c} \in \mathcal{C}$ is sent and $\mathbf{y} = \mathbf{c} + \mathbf{e}$ is received on an additive channel
- $\mathbf{y}$ and $\mathbf{e}$ are in the same coset of $\mathcal{C}$.
- Nearest-neighbor decoding of $\mathbf{y}$ calls for finding the closest codeword $\mathbf{c}$ to $\mathbf{y} \implies$ find a vector $\mathbf{e}$ of *lowest weight* in $\mathbf{y}+\mathcal{C}$: a *coset leader*.
  - *coset leaders need not be unique* (when are they?)
- Decoding algorithm: upon receiving $\mathbf{y}$
  - compute the syndrome $\mathbf{s} = H\mathbf{y}^T$
  - find a coset leader $\mathbf{e}$ in the coset corresponding to $\mathbf{s}$
  - decode $\mathbf{y}$ into $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$
- If $n - k$ is (very) small, a table containing one leader per coset can be pre-computed. The table is indexed by $\mathbf{s}$. On the other hand, if k is (very) small, we can go over $\mathbf{y} + \mathcal{C}$ exhaustively, and find a coset leader.
- In general, however, all known algorithms for syndrome decoding are *exponential* in $\min(k, n-k)$. In fact, the problem has been shown to be NP-hard.

Decoding the Hamming Code

1. Consider $\mathcal{H}_m$ over $\mathbb{F}_2$. We have
   $n = 2^m - 1, \quad m = n - k.$
   Given a received $\mathbf{y}$,
   $$\mathbf{s} = H_m \mathbf{y}^T$$
   is an m-tuple in $\mathbb{F}_2^m$.
2. if $\mathbf{s} = \mathbf{0}$ then $\mathbf{y} \in \mathcal{C} \implies \mathbf{0}$ is the coset leader of $\mathbf{y} + \mathcal{C}$
3. if $\mathbf{s} \neq \mathbf{0}$ then $\mathbf{s} = \mathbf{h}_i$ for some $i \implies$
   $$\mathbf{e}_i = [0, \quad 0, \quad \ldots, \quad 0, \quad \underset{\substack{\uparrow \\ i}}{1}, \quad 0, \quad \ldots, \quad 0]$$
   is the coset leader of $\mathbf{y} + \mathcal{C}$, since
   $H_m \mathbf{y}^T = \mathbf{s} = \mathbf{h}_i = H_m \mathbf{e}_i \,, \quad \mathbf{y} \notin \mathcal{C},$ and $\mathrm{wt}(\mathbf{e}_i) = 1.$
   - Every word in $\mathbb{F}_2^n$ is at distance at most 1 from a codeword.
   - Spheres of radius 1 around codewords are disjoint and cover $\mathbb{F}_2^n$: *perfect code*.



steps 1–3 above describe a *complete decoding algorithm* for $\mathcal{H}_m, \quad \forall m$.

Deriving Codes from Other Codes

- *Adding an overall parity check.* Let $\mathcal{C}$ be a binary $[n, k, d]$ code with some odd-weight codewords. We form a new code $\hat{\mathcal{C}}$ by appending a 0 at the end of even-weight codewords, and a 1 at the end of odd-weight ones.
  - Every codeword in $\hat{\mathcal{C}}$ has even weight.
  - $\hat{\mathcal{C}}$ is an $[n+1, k, 2\lceil d/2 \rceil]$ code. If d is odd, $\hat{d} = d + 1$.
  - **Example:** The $[7, 4, 3]$ binary Hamming code can be extended to an $[8, 4, 4]$ code with PCM

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

corrects any pattern of 1 error, and detects any pattern of 2.

Deriving Codes from Other Codes (cont.)

- *Expurgate by throwing away codewords.* E.g., select subset of codewords satisfying an independent parity check.
  - **Example:** Selecting the even-weight sub-code of the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code yields a $[2^m - 1, 2^m - 2 - m, 4]$ code.

- *Shortening by taking a cross-section.* Select all codewords $\mathbf{c}$ with, say, $c_1 = 0$, and eliminate that coordinate (can be repeated for more coordinates). An $[n, k, d]$ code yields an $[n - 1, k - 1, \geq d]$ code.