ERROR CORRECTING CODES

Definition (Alphabet) An alphabet is a finite set of symbols.

Example: A simple example of an alphabet is the set $\mathcal{A} := \{B, \#, 17, P, \$, 0, u\}$.

Definition (Codeword) A codeword is a string of symbols in an alphabet.

Example: In the alphabet $\mathcal{A} := \{B, \#, 17, P, \$, 0, u\}$, some examples of codewords of length 4 are:

$P17u$, $0B\$, $uBuB$, $0000$.

Definition (Code) A code is a set of codewords in an alphabet.

Example: In the alphabet $\mathcal{A} := \{B, \#, 17, P, \$, 0, u\}$, an example of a code is the set of 5 words: $\{P17u, 0B\$, $uBuB, 0000, PP\}$.

If all the codewords are known and recorded in some dictionary then it is possible to transmit messages (strings of codewords) to another entity over a noisy channel and detect and possibly correct errors. For example in the code $C := \{P17u, 0B\$, $uBuB, 0000, PP\}$ if the word $0B\$ is sent and received as $PB\$, then if we knew that only one error was made it can be determined that the letter $P$ was an error which can be corrected by changing $P$ to 0.

Definition (Linear Code) A linear code is a code where the codewords form a finite abelian group under addition.

Main Problem of Coding Theory: To construct an alphabet and a code in that alphabet so it is as easy as possible to detect and correct errors in transmissions of codewords. A key idea for solving this problem is the notion of Hamming distance.

Definition (Hamming distance $d_H$) Let $C$ be a code and let

$w = w_1w_2\ldots w_n, \quad w' = w'_1w'_2\ldots w'_n,$

be two codewords in $C$ where $w_i, w'_j$ are elements of the alphabet of $C$. Then $d_H(w, w')$ is defined to be the number of $1 \leq i \leq n$ where $w_i \neq w'_i$.

Definition (Minimum Hamming distance $d_H(C)$ of a code $C$) Let $C$ be a code. We define

$$d_H(C) = \min_{w, w' \in C, w \neq w'} d_H(w, w').$$

LINEAR CODES OVER FINITE FIELDS

A linear code over a finite field is a linear code where the alphabet is a finite field.

Definition ([n, k]-code) Let $1 \leq k < n$ be integers. An $[n, k]$-code over a finite field $\mathbb{F}$ is a code with alphabet $\mathbb{F}$ which is a $k$-dimensional subspace of $\mathbb{F}^n$. 
Definition ([n, k, d]-code) Let 1 ≤ k < n be integers. An [n, k, d]-code is an [n, k]-code over a finite field \( \mathbb{F} \) (denoted \( C \)) where \( d_H(C) = d \).

**CONSTRUCTING BINARY LINEAR (n, k) CODES**

Definition (Binary linear code) A binary linear code is a linear code with alphabet the finite field of two elements: \( \mathbb{F}_2 := \{0, 1\} \).

Binary linear \((n, k)\) codes can be constructed using a generating matrix \( G \) of the form:

\[
G = (I_k, P)
\]

where \( I_k \) is the \( k \times k \) identity matrix and \( P \) is a \( k \times (n - k) \) matrix with entries in \( \mathbb{F}_2 \). We create a binary \((n, k)\) code by defining the codewords to be all possible row vectors of the form

\[
x \cdot G
\]

where \( x = (x_1, x_2, \ldots, x_k) \) with \( x_i \in \mathbb{F}_2 \) for \( i = 1, 2, \ldots, k \).

**HAMMING DISTANCE \( d_H \) AND WEIGHT \( w_H \) FOR BINARY LINEAR CODES**

Lemma 1: The Hamming distance for a bilinear code \( C \) is translation invariant, i.e.,

\[
d_H(x, x') = d_H(x + y, x' + y)
\]

for all codewords \( x, x', y \in C \). This is easily proved and is left as an exercise. An important consequence is that for a bilinear code we can conclude that

\[
d_H(x, x') = d_H(x - x', x' - x') = d_H(x - x', 0) = d_H(x + x', 0).
\]

Definition (Hamming weight \( w_H \)) Let \( C \) be a bilinear code. The Hamming weight \( w_H(x) \) of a codeword \( x \in C \) is defined to be the number of “ones” in \( x \).

Examples: \( w_H(1, 0, 0, 1, 1, 0, 1) = 4 \), \( w_H(0, 1, 0, 1, 0, 0, 0) = 2 \).

Lemma 1 tells us that the minimal Hamming distance (between distinct codewords) of a bilinear code \( C \) has to be the same as the minimal Hamming weight of all non-zero codewords.

**EXAMPLES OF BINARY LINEAR (n, k) CODES**

Example (Repetition Code): Let \( k = 1 \) and \( n > k \). Define the generator matrix

\[
G = (1, 1, \ldots, 1).
\]

Since \( k = 1 \), the only \( k \times k \) matrices \( x \in \mathbb{F}_2 \) are \((0)\) or \((1)\). So the only codewords generated by \( x \cdot G \) are

\[
(0, 0, \ldots, 0), \quad (1, 1, \ldots, 1).
\]

Exercise: Show that the binary repetition code \( C \) above has Hamming distance \( d_H(C) = n \).
**Example (Parity Check Code):** Let $n > 1$ and $k = n - 1$. A generator matrix for the Parity Check $[n, n - 1]$-code is

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

with one’s in the last column. The codewords are all of the form $x \cdot G$ where $x = (x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$. Note that every codeword will be of the form:

$$(x_1, x_2, \ldots, x_{n-1}, x_1 + x_2 + \cdots + x_{n-1}),$$

so the last bit in the codeword gives the parity check.

**Exercise:** Show that the parity check code $C$ above has Hamming distance $d_H(C) = 2$.

**Example (Hamming (7,4) code):** Here the generator matrix is

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

Here are some examples of codewords:

$$(1, 1, 0, 0) \cdot G = (1, 1, 0, 0, 0, 1, 1)$$

$$(1, 1, 1, 1) \cdot G = (1, 1, 1, 1, 1, 1, 1)$$

$$(0, 0, 0, 0) \cdot G = (0, 0, 0, 0, 0, 0, 0).$$

**Exercise:** Show that the Hamming $[7,4]$-code $C$ above has Hamming distance $d_H(C) = 3$.

**PARITY CHECK MATRIX**

A parity check matrix for a bilinear $[n, k]$-code with generator matrix

$$G = (I_k, P)$$

where $I_k$ is the $k \times k$ identity matrix and and $P$ is a $k \times (n - k)$ matrix with entries in $\mathbb{F}_2$ is the matrix

$$H = (-P^T, I_{n-k}).$$

Here $P^T$ is the transpose of the matrix $P$ and $I_{n-k}$ is the $(n - k) \times (n - k)$ identity matrix.

**Theorem:** We have: $G \cdot H^T = 0$.

**Proof:** See p. 411 in "Introduction to Cryptography with Coding Theory." □

**Theorem:** We have $c \cdot H^T = 0$ for any codeword $c$.

**Proof:** Every codeword $c$ is of the form $c = x \cdot G$ with $x \in \mathbb{F}_2^k$. It follows that we have $c \cdot H^T = x \cdot G \cdot H^T = 0$. □
EXAMPLES OF PARITY CHECK MATRICES

EXAMPLE 1: ([6,2]-code) Let $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} = (I_2, P)$ with

\[ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}. \]

Then we form

\[-P^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad I_{6-2} = I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \]

\[H = (-P^T, I_4) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad H^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.\]

It is easy to see that $G \cdot H^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 0$.

Remark: Rather than write out a long zero matrix we abbreviate it by 0.

EXAMPLE 2: ([7,3]-code) Let $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} = (I_3, P)$ with

\[ I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \]

Then we form

\[-P^T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad I_{7-3} = I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \]

\[H = (-P^T, I_4) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad H^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \]

Again, we have: $G \cdot H^T = 0$. 

4