Encoding/Decoding Framework

\[ 0 < k \leq n \]

Message space \( \mathcal{E}_0,13^k = \{ b_1, \ldots, b_k \mid b_i \in \begin{array}{c} \mathbb{Z}_2 \end{array} \} \)

Codeword space \( \mathcal{E}_0,13^n = \{ c_1, \ldots, c_n \mid c_i \in \begin{array}{c} \mathbb{Z}_2 \end{array} \} \)

- Original message: \( b_1, b_2, \ldots, b_k \)
- Decoded message: \( b'_1, b'_2, \ldots, b'_k \)

**Encoder**: \( f : \mathcal{E}_0,13^k \to \mathcal{E}_0,13^n \) is a 1-1 function that typically adds **redundancy**

**Noise**: a model assumption is made, such as

(i) at most one error, \( \varepsilon_1, \ldots, \varepsilon_n = 0 \cdots 010 \cdots 0 \)
(ii) small independent chance of error in each position.

**Decoder**: a well-defined function

\( g : \mathcal{E}_0,13^n \to \mathcal{E}_0,13^k \) U "resend" U "unrecoverable failure"
Example a repetition code.

Set $k = 1$, $n = 3$.

$\mathbb{Z}_2$, $\mathbb{Z}_2^3$.

$f(0) = 000$, $f(1) = 111$.

decoding function depends on noise assumption.

assumption 1 $\leq 1$ error.

$g(000) = g(100) = g(010) = g(001) = 0$
$g(111) = g(110) = g(101) = g(011) = 1$

assumption 2 $\leq 2$ errors

$g(000) = 0$ otherwise, $g(b_1b_2b_3) = "resend"$
$g(111) = 1$

assumption 3 probability of error in any bit is independent with probability .05.

Using $g$ from assumption 1, what is the probability of successful decoding?
Linear Transformation encoders

Any matrix over a field provides an encoding function.

\[ M: \mathbb{F}_2, 13^k \rightarrow \mathbb{F}_2, 13^n \]

\[ b M = c \]

where \( M \) is a \( k \times n \) matrix over \( \mathbb{Z}_2 \).

\[ G: \mathbb{F}_2, 13^4 \rightarrow \mathbb{F}_2, 13^7 \]

\[ G = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 \\
d_1 & d_2 & d_3 & d_4 & p_1 & p_2 & p_3
\end{bmatrix} \]

Idea: "data" bits are \( d_1, d_2, d_3, d_4 \)

"redundancy" parity check bits are \( p_1, p_2, p_3 \)

\[ b = b_1 b_2 b_3 b_4 \]

\[ bG = c_1 g_1 \ldots c_7 \]

<table>
<thead>
<tr>
<th>( b )</th>
<th>( bG )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0001</td>
<td>0001</td>
</tr>
<tr>
<td>0010</td>
<td>0010</td>
</tr>
<tr>
<td>0100</td>
<td>0100</td>
</tr>
<tr>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>1001</td>
<td>1001</td>
</tr>
<tr>
<td>1010</td>
<td>1010</td>
</tr>
</tbody>
</table>
Parity bit $p_i$ is assigned to the data bits in its circle, so that sum = 0.

Every data bit is covered by
1. At least 2 parity bits
2. A unique subset of parity bits.

Up to 1 error can be corrected.
Up to 2 errors can be detected.
Hypercube viewpoint

$\mathbb{E}_0,13^4 \xrightarrow{f} \mathbb{E}_0,13^7$

0 errors codeword

1 error

Radius 1 Hamming ball in $\mathbb{E}_0,13^7$ with center 0001011

message space

codeword space

\[
\{0001011, 1001011, 0101011, 0011011, 0000011, 0001111, 0001011, 0001001, 0001010\}
\]
Definition (Linear Code)

An \((n,k)\) linear code over a finite field \(F\) is a \(k\)-dimensional subspace \(V\) of the vector space \(F^n = F \oplus F \oplus \cdots \oplus F\) (\(n\) copies) over \(F\). Elements of \(V\) are called codewords. When \(F = \mathbb{Z}_2\), \(V\) is a binary code.

\((n,k)\) linear code \(\iff\) generator matrix \(G : F^k \rightarrow F^n\) via basis of \(V\)

\[
G = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & \| \\
0 & 0 & 1 & 0 & 1 & 1 & \| \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{bmatrix} = \begin{bmatrix}
I_{k \times n} \\
A_{k \times (n-k)}
\end{bmatrix}
\]

Generator matrix of a \((7,4)\) linear code.
**Parity-Check Matrix Decoding (PCMD)**

\[ G = [I_r | A_{r \times n-r}] \iff H = \begin{bmatrix} -A_{r \times n-r} \\ I_{n-r} \end{bmatrix} \]

**generator matrix**

**parity-check matrix**

**Example**

\[ G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ \hline \\ d_1 & d_2 & d_3 & p_1 & p_2 & p_3 \end{bmatrix} \]

\[ H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \]

**PCMD algorithm**

1. received word = \( w \). Find \( wH \).
2. \( wH = 0 \) \( \Rightarrow \) decode as \( w \) itself.
3. \( wH = i^{th} \) row of \( H \) \( \Rightarrow \) decode as \( w + e_i \) (and no other)
4. Otherwise \( \geq 2 \) errors. Do not decode.

\[ wH = [q_1, q_2, \ldots, q_{n-r}] \]

\( q_i = 0 \) iff \( i^{th} \) parity relation holds for \( w \).

**Exercise** Decode 101011, 111010, 110000
\[ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \end{bmatrix} H = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} = 5^{th} \text{ row of } H, \text{ so decode as } 101001. \]
\[ \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} H = \begin{bmatrix} 1 & 1 \end{bmatrix} = 1^{st} \text{ row of } H, \text{ so decode as } 011010 \]
\[ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} H = \begin{bmatrix} 0 & 1 \end{bmatrix} \text{ not a row of } H. \text{ 2 \text{ errors, do not decode.} } \]

**Lemma (Orthogonality Relation)**

Let \( C \) be an \((n, k)\) linear code over \( F \) with generator matrix \( G \) and parity-check matrix \( H \). Then, for any \( v \in F^n \),

\[ vH = 0 \quad \text{iff} \quad v \in C. \]

**Proof**

\( H \) is \( n \times (n-k) \), \( H \) contains \( I_{n-k} \) and so ranks \((H) + \dim(\ker H) = n \)

\[ (n-k) + k = n. \]

\( \dim C = k \), so we just show \( C \subseteq \ker H \).

Let \( v \in C \), and let \( m \) satisfy \( v = mg \).

Then \( vH = mGH \)

\[ = m \begin{bmatrix} I_k \mid A \end{bmatrix} \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix} \]

\[ = m(I_k(-A) + A I_{n-k}) = m \cdot 0 = 0. \]

\( \square \)
Exercise. Given \( r \geq 2 \) parity bits, what is the maximum number of data bits
\[
\mathcal{C} = \{ d_1, \ldots, d_k, p_1, \ldots, p_r \}
\]
in a \((r + \ell, k)\) linear code for which 1 error can be corrected?
(Hint: Look at rows of \( H \).)

Theorem 31.3 (Parity-check Matrix Decoding)

PCMD will correct any single error iff rows of \( H \) are nonzero and no two rows are dependent.

Proof (binary case) independent rows \( \iff \) distinct rows

(\( \Leftarrow \)) Assume rows of \( H \) are nonzero and distinct.
Assume \( w \) is transmitted but received as \( w + e_i \).
\[
(w + e_i) H = wH + e_i H = e_i H \quad \text{(Orthog. Lemma)}
\]
\[= i^{th} \text{ row of } H.\]
The \( i^{th} \) row is distinct, and so the error is identified.

(\( \Rightarrow \)) No row of \( H \) can be the zero row. Otherwise an error-free code word \( w \) yields \( wH = \mathbf{0} \), and an error is reported in the position of the \( 0 \) row of \( H \).
No two rows \( i \neq j \) of \( H \) are the same. Otherwise if \( w \) is a code word received as \( w + e_i \),
\[
(w + e_i) H = wH + e_i H = i^{th} \text{ row of } H
\]
\[= j^{th} \text{ row of } H.\]
The decoding algorithm reports 2 errors and does not decode.\( \square \)