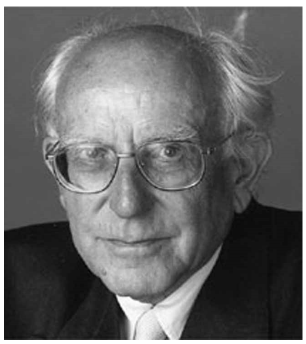
MATH 525
Section 3.5: The Extended Golay Code

October 24, 2020

The Extended Golay Code



Marcel Golay

- In 1949 Marcel Golay noticed that

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11},$$

so he started to look for a perfect $(23, 12, 7)$-linear code, and succeeded. We will study this code, now known as the Golay code, in the next section.

- The *extended* Golay code, C_{24}, is the linear code of length 24, dimension 12, and distance 8, whose generator matrix is:

$$G = [I_{12}|B]$$

where B is the 12×12 matrix

$$B = \left[\begin{array}{c|c} B_1 & j^T \\ \hline j & 0 \end{array}\right] \text{ where } j = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$$

and B_1 is displayed on the next slide.

- The following concept will be used on the next slide: The *left-cyclic shift* of the vector $(v_1, v_2, v_3, \ldots, v_n) \in K^n$ is the vector

$$(v_2, v_3, \ldots, v_n, v_1).$$

For example, the left-cyclic shift of 1011 is 0111.

$$B = \left[\begin{array}{ccccccccccc|c}
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}\right]$$

Each row of the 11×11 submatrix B_1 is a left-cyclic shift of the previous row.

The generator matrix $G = [I_{12}|B]$ of C_{24}:

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

$$
B = \begin{array}{c}
\mathbf{b}_1\\ \mathbf{b}_2\\ \mathbf{b}_3\\ \mathbf{b}_4\\ \mathbf{b}_5\\ \mathbf{b}_6\\ \mathbf{b}_7\\ \mathbf{b}_8\\ \mathbf{b}_9\\ \mathbf{b}_{10}\\ \mathbf{b}_{11}\\ \mathbf{b}_{12}
\end{array}
\left[\begin{array}{cccc|cccc|cccc}
1&1&0&1&1&1&0&0&0&1&0&1\\
1&0&1&1&1&0&0&0&1&0&1&1\\
0&1&1&1&0&0&0&1&0&1&1&1\\
1&1&1&0&0&0&1&0&1&1&0&1\\
1&1&0&0&0&1&0&1&1&0&1&1\\
1&0&0&0&1&0&1&1&0&1&1&1\\
0&0&0&1&0&1&1&0&1&1&1&1\\
0&0&1&0&1&1&0&1&1&1&0&1\\
0&1&0&1&1&0&1&1&1&0&0&1\\
1&0&1&1&0&1&1&1&0&0&0&1\\
0&1&1&0&1&1&1&0&0&0&1&1\\
1&1&1&1&1&1&1&1&1&1&1&0
\end{array}\right]
\begin{array}{c}
\mathbf{b}_1\\ \mathbf{b}_2\\ \mathbf{b}_3\\ \mathbf{b}_4\\ \mathbf{b}_5\\ \mathbf{b}_6\\ \mathbf{b}_7\\ \mathbf{b}_8\\ \mathbf{b}_9\\ \mathbf{b}_{10}\\ \mathbf{b}_{11}\\ \mathbf{b}_{12}
\end{array}
$$

Properties of C_{24}

1. $|C| = 2^{12} = 4096$.
2. A parity-check matrix for C_{24} is $\begin{bmatrix} B \\ I_{12} \end{bmatrix}$.
3. Another parity-check matrix is $H = \begin{bmatrix} I_{12} \\ B \end{bmatrix}$.

Proof.

This follows from the observation that

$$G \cdot H = [I_{12}|B] \cdot \left[\frac{I_{12}}{B}\right] = I_{12} + B^2 = I_{12} + BB^T$$

(because $B = B^T$). By direct inspection, $\mathbf{b}_1 \cdot \mathbf{b}_1 = 1$ and $\mathbf{b}_1 \cdot \mathbf{b}_i = 0$ for all $i > 1$. From the cyclic structure of B_1, it follows that $\mathbf{b}_i \cdot \mathbf{b}_j = 0$ whenever $i \neq j$ (note that if $j > i$, then $\mathbf{b}_i \cdot \mathbf{b}_j = \mathbf{b}_1 \cdot \mathbf{b}_{j-i}$). Therefore, $I_{12} + BB^T = I_{12} + I_{12} = \mathbf{0}$, i.e., $G \cdot H = \mathbf{0}$. □

4. C_{24} is self-dual, i.e., $C_{24}^{\perp} = C_{24}$.
5. $d(C_{24}) = 8$.

Proof.

The proof of the last statement is divided into two parts:

Part 1) Show that the weight of any codeword in C_{24} is congruent to zero modulo 4.

Part 2) Show that there is no word of weight 4.

□

Set $H = \left[\begin{array}{c} I_{12} \\ \hline B \end{array}\right]$ as the parity-check matrix for C_{24}.

Algorithm for Decoding the Extended Golay Code C_{24}:

- Input: The received vector $r = (r_1, r_2, \ldots, r_{24}) \in K^{24}$.
- The output will be u, the estimated error vector.

1) Compute $s = r \cdot H$.
2) If $\mathrm{wt}(s) \leq 3$ then $u = [s, 0]$. EXIT.
3) If $\mathrm{wt}(s + b_i) \leq 2$ for row i of B then $u = [s + b_i, e_i]$. EXIT.
4) Compute sB.
5) If $\mathrm{wt}(sB) \leq 3$ then $u = [0, sB]$. EXIT.
6) If $\mathrm{wt}(sB + b_i) \leq 2$ for row i of B then $u = [e_i, sB + b_i]$. EXIT.
7) Request retransmission or declare failure.

Example

Decode the following received words, assuming the code being used is C_{24}:

(a) $r = (0000\ 0100\ 0101\ 1000\ 1111\ 0001)$.

(b) $r = (1000\ 0100\ 1010\ 1100\ 1100\ 1000)$.

(c) $r = (1000\ 0110\ 1010\ 1000\ 1100\ 1000)$.

Helpful calculations:
In (a), $s_1 = rH = (0101\ 0010\ 0000)$.
In (b), $s_1 = rH = (1111\ 0101\ 0001)$.
In (c), $s_1 = rH = (0100\ 1111\ 1010)$ and $s_2 = s_1 B = (1111\ 1000\ 1111)$.

To see an example of how syndromes are calculated, turn to the next slide.

Example

Calculate the syndrome of $r = (\underbrace{0000\ 0100\ 0101}_{\text{left half}}\ \ \underbrace{1000\ 1111\ 0001}_{\text{right half}})$ in part (a) of the previous example. Recall:

$$s = r \cdot H = r \cdot \left[\frac{I_{12}}{B} \right],$$

and observe that the right half of r has 1s in positions 1, 5, 6, 7, 8, and 12. It follows that s is equal to:

$$\begin{array}{rr@{\quad}c}
 & \text{left half of } r \rightarrow & 0000\ 0100\ 0101 \\
 & \boldsymbol{b}_1 \rightarrow & 1101\ 1100\ 0101 \\
 & \boldsymbol{b}_5 \rightarrow & 1100\ 0101\ 1011 \\
+ & \boldsymbol{b}_6 \rightarrow & 1000\ 1011\ 0111 \\
 & \boldsymbol{b}_7 \rightarrow & 0001\ 0110\ 1111 \\
 & \boldsymbol{b}_8 \rightarrow & 0010\ 1101\ 1101 \\
 & \boldsymbol{b}_{12} \rightarrow & 1111\ 1111\ 1110 \\
\hline
 & s \rightarrow & 0101\ 0010\ 0000
\end{array}$$