# MATH 525
## Section 3.7: The Golay Code

October 26, 2020



- Marcel Golay introduced his $(23, 12, 7)$ code (now known as the Golay code) in the one-page paper "Notes on digital coding," published in the *Proceedings of the I.R.E.* in 1949.
- The Golay code, denoted by $C_{23}$, is perfect because

$$|C| = \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{t}}, \quad \text{that is, } 2^{12} = \frac{2^{23}}{\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}}$$

  where $t = 3$ is the error-correction capability of the code. From this, it follows that any word $w \in K^{23}$ is at distance at most 3 from exactly one codeword in $C_{23}$.
- One generator matrix is $G = [I_{12}|\widehat{B}]$ where $\widehat{B}$ is the $12 \times 11$ matrix obtained from $B$ (on p. 77) by deleting its last column.
- We also say that $C_{23}$ is obtained from $C_{24}$ by *puncturing* it, that is, by removing the last bit from every codeword in $C_{24}$.

**Decoding Algorithm for $C_{23}$:**

- Input: The received vector $r = (r_1, r_2, \ldots, r_{23}) \in K^{23}$.
- The output will be the codeword $\widehat{c} \in C_{23}$, closest to $r$.

1) Append a digit $i \in \{0, 1\}$ to $r$ so that $ri$ has odd weight.
2) Decode $ri$ using the decoding algorithm for $C_{24}$, obtaining $c$.
3) Remove the last digit from $c$, obtaining $\widehat{c} \in C_{23}$.

* * *

**Question**: Why does the above algorithm work?



*Partial Proof*: Let $r = v + u$ where $v \in C_{23}$ is the sent codeword and $u \in K^{23}$ is the error pattern. We will do the proof in the case where $\mathrm{wt}(u) = 3$.

Case 1: $\mathrm{wt}(r) =$ odd, $\mathrm{wt}(v) =$ even. In this case, the decoder will append 0 to $r$, obtaining $r0$. The codeword $v0 \in C_{24}$ is at distance 3 from $r0$. The output is $v$, as desired.

Case 2: $\mathrm{wt}(r) =$ even, $\mathrm{wt}(v) =$ odd. In this case, the decoder will append 1 to $r$, obtaining $r1$. The codeword $v1 \in C_{24}$ is at distance 3 from $r1$. The output is $v$, as desired.

The cases where $\mathrm{wt}(u) \in \{0, 1, 2\}$ are left as an exercise. $\square$

**Remark**: If $\mathrm{wt}(u) = 0$, then $ri$ is never a codeword of $C_{24}$ (because $ri$ has odd weight). However, $r = v$ and so $ri = vi$. It follows that:

1. If $\mathrm{wt}(v) =$ odd, then $i = 0$ and $ri = v0$. Thus,

$$\mathrm{syn}(ri) = \mathrm{syn}(v0) = \mathrm{syn}(v1 + \mathbf{0}1) = \mathbf{b}_{12}$$

   where $\mathbf{0} \in K^{23}$ is the all-zero vector and $\mathbf{b}_{12}$ is the 12th row of $B$.

2. If $\mathrm{wt}(v) =$ even, then $i = 1$ and $ri = v1$. Thus,

$$\mathrm{syn}(ri) = \mathrm{syn}(v1) = \mathrm{syn}(v0 + \mathbf{0}1) = \mathbf{b}_{12}.$$

In either case, $\mathrm{syn}(ri) = \mathbf{b}_{12}$ when there are no errors. This can be used to make decoding more efficient: If $\mathrm{syn}(ri) = \mathbf{b}_{12}$, then the decoder does not need to run the algorithm described on slide 3; it can directly conclude that $r \in C_{23}$ is the sent codeword.