Slide #8. Proof that $d(C_{24}) = 8$. This can be carried out by "simply" listing all 2^{12} codewords of C_{24} and observing that the minimum non-zero weight equals 8. However, we will show an alternative proof of this (non brute force) using elementary concepts from linear codes.

Part 1: Show that the weight of any codeword in C_{24} is congruent to zero modulo 4. Let G be the generator matrix for C_{24} as displayed on slide #5. Let $\boldsymbol{g}_i$ denote the ith row of G for $i = 1, \ldots, 12$. Recall that any codeword in C_{24} is a linear combination of the rows of G. Thus, the idea for the proof is to show that $\mathrm{wt}(\boldsymbol{g}_i) \equiv 0 \pmod 4$, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j) \equiv 0 \pmod 4$, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j + \boldsymbol{g}_k) \equiv 0 \pmod 4$ for all $i, j, k \in [1..12]$, etc.

- By direct inspection, $\mathrm{wt}(\boldsymbol{g}_i) \equiv 0 \pmod 4$.
- $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j) = \mathrm{wt}(\boldsymbol{g}_i) + \mathrm{wt}(\boldsymbol{g}_j) - 2 \cdot \mathrm{wt}(\boldsymbol{g}_i * \boldsymbol{g}_j)$. Since C_{24} is self-dual, one has $\mathrm{wt}(\boldsymbol{g}_i * \boldsymbol{g}_j) \equiv 0 \pmod 2$, whence $2 \cdot \mathrm{wt}(\boldsymbol{g}_i * \boldsymbol{g}_j) \equiv 0 \pmod 4$. In conclusion, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j)$ is the summation of three terms, each a multiple of 4. Thus, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j) \equiv 0 \pmod 4$.
- $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j + \boldsymbol{g}_k) = \mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j) + \mathrm{wt}(\boldsymbol{g}_k) - 2 \cdot \mathrm{wt}((\boldsymbol{g}_i + \boldsymbol{g}_j) * \boldsymbol{g}_k)$. In the previous bullets, we showed that $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j)$ and $\mathrm{wt}(\boldsymbol{g}_k)$ are both multiples of 4. Again, since C_{24} is self-dual, one has $\mathrm{wt}((\boldsymbol{g}_i + \boldsymbol{g}_j) * \boldsymbol{g}_k) \equiv 0 \pmod 2$, whence $2 \cdot \mathrm{wt}(\boldsymbol{g}_i * \boldsymbol{g}_j) \equiv 0 \pmod 4$. In conclusion, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j + \boldsymbol{g}_k)$ is the summation of three terms, each a multiple of 4. Thus, $\mathrm{wt}(\boldsymbol{g}_i + \boldsymbol{g}_j + \boldsymbol{g}_k) \equiv 0 \pmod 4$.
- We can now proceed iteratively and show that the weight of any sum of 4, 5, ..., 12 rows of G is always a multiple of 4.

Part 2: Show that there is no word of weight 4. By way of contradiction, suppose $\boldsymbol{c} \in C_{24}$ has weight equal to 4. Write $\boldsymbol{c} = (\boldsymbol{c}_L | \boldsymbol{c}_R)$ where $\boldsymbol{c}_L$ consists of the first 12 bits of $\boldsymbol{c}$ (in other words, $\boldsymbol{c}_L$ is the left half of $\boldsymbol{c}$). Similarly, $\boldsymbol{c}_R$ is the right half of $\boldsymbol{c}$. Observe that

$$\boldsymbol{c} = (\boldsymbol{c}_L \mid \boldsymbol{c}_R) = \boldsymbol{u} \cdot [I_{12} \mid B] = [\boldsymbol{u} \mid \boldsymbol{u} \cdot B]$$

for some information vector $\boldsymbol{u}$. Since $[B \mid I_{12}]$ is another generator matrix for C_{24}, we also have

$$\boldsymbol{c} = (\boldsymbol{c}_L \mid \boldsymbol{c}_R) = \boldsymbol{u}' \cdot [B \mid I_{12}] = [\boldsymbol{u}' \cdot B \mid \boldsymbol{u}']$$

for some information vector $\boldsymbol{u}'$. We then have five possibilities:

- $\mathrm{wt}(\boldsymbol{c}_L) = 0$ and $\mathrm{wt}(\boldsymbol{c}_R) = 4$. This implies $\boldsymbol{u} = \boldsymbol{0}$ and $\mathrm{wt}(\boldsymbol{u} \cdot B) = 4$, a contradiction.
- $\mathrm{wt}(\boldsymbol{c}_L) = 4$ and $\mathrm{wt}(\boldsymbol{c}_R) = 0$. This implies $\boldsymbol{u}' = \boldsymbol{0}$ and $\mathrm{wt}(\boldsymbol{u}' \cdot B) = 4$, a contradiction.
- $\mathrm{wt}(\boldsymbol{c}_L) = 1$ and $\mathrm{wt}(\boldsymbol{c}_R) = 3$. This implies $\mathrm{wt}(\boldsymbol{u}) = 1$ and $\mathrm{wt}(\boldsymbol{u} \cdot B) = \mathrm{wt}(\text{some row of } B) = 3$. But this is impossible since no row of B has weight equal to 3.
- $\mathrm{wt}(\boldsymbol{c}_L) = 3$ and $\mathrm{wt}(\boldsymbol{c}_R) = 1$. This implies $\mathrm{wt}(\boldsymbol{u}') = 1$ and $\mathrm{wt}(\boldsymbol{u}' \cdot B) = \mathrm{wt}(\text{some row of } B) = 3$. But this is impossible since no row of B has weight equal to 3.
- $\mathrm{wt}(\boldsymbol{c}_L) = 2$ and $\mathrm{wt}(\boldsymbol{c}_R) = 2$. This implies $\mathrm{wt}(\boldsymbol{u}) = 2$ and $\mathrm{wt}(\boldsymbol{u} \cdot B) = \mathrm{wt}(\text{sum of 2 rows of } B) = 2$. But this does not happen either.

In conclusion, no codeword in C_{24} has weight equal to 4. $\square$

Slide #9. Justification for the decoding algorithm for C_{24}. As usual, the main part of the decoding algorithm is to determine the error pattern $\boldsymbol{u}$. Since the error-correcting capability of C_{24} equals 3, we shall assume that $\mathrm{wt}(\boldsymbol{u}) \le 3$. The syndrome of any such error pattern uniquely identifies it (no two such error patterns have the same syndrome).

Recall that $s = \mathrm{syn}\,\boldsymbol{r} = \mathrm{syn}\,\boldsymbol{u}$. Let $\boldsymbol{u} = [\boldsymbol{u}_1 \mid \boldsymbol{u}_2]$. Since

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

one has $s = \boldsymbol{u}_1 + \boldsymbol{u}_2 \cdot B$. Observe that either $\mathrm{wt}(\boldsymbol{u}_1) \le 1$ or $\mathrm{wt}(\boldsymbol{u}_2) \le 1$.

Notation: In what follows, $\boldsymbol{e}_i$ denotes the word or vector having a 1 in position i (for some $i \in [1..12]$) and 0s in the other positions.

- If $\mathrm{wt}(\boldsymbol{u}_2) = 0$, then $s = \boldsymbol{u}_1$, whence $\mathrm{wt}(s) \le 3$. In this case, $\boldsymbol{u} = [s \mid \mathbf{0}]$.
- If $\mathrm{wt}(\boldsymbol{u}_2) = 1$, then $s = \boldsymbol{u}_1 + \boldsymbol{b}_i$ for some $i \in [1..12]$. Recall that $\boldsymbol{b}_i$ denotes the ith row of B. One has $\mathrm{wt}(\boldsymbol{u}_1) = \mathrm{wt}(s + \boldsymbol{b}_i) \le 2$. In this case, $\boldsymbol{u} = [s + \boldsymbol{b}_i \mid \boldsymbol{e}_i]$.

Note that $s \cdot B = \boldsymbol{u}_1 \cdot B + \boldsymbol{u}_2$.

- If $\mathrm{wt}(\boldsymbol{u}_1) = 0$, then $sB = \boldsymbol{u}_2$, whence $\mathrm{wt}(sB) \le 3$. In this case, $\boldsymbol{u} = [\mathbf{0} \mid sB]$.
- If $\mathrm{wt}(\boldsymbol{u}_1) = 1$, then $sB = \boldsymbol{b}_i + \boldsymbol{u}_2$ for some $i \in [1..12]$. One has $\mathrm{wt}(\boldsymbol{u}_2) = \mathrm{wt}(sB + \boldsymbol{b}_i) \le 2$. In this case, $\boldsymbol{u} = [\boldsymbol{e}_i \mid sB + \boldsymbol{b}_i]$.