Coding Theory: Golay Codes

Good Codes

Codes seen so far

$(n,k,d_H)_q$	k/n	name
$(n,1,n)_q$	$\frac{1}{n}$	repetition
$(n,n-1,2)_q$	$\frac{n-1}{n}$	parity check
$[(7,4,3)_2$	$\frac{4}{7}$	Hamming]
$[(4,2,3)_3$	$\frac{1}{2}$	tetracode]
$(\frac{q^r-1}{q-1}, n-r, 3)_q$	$\frac{n-r}{n}$	Hamming

Golay Codes

4 codes named Golay codes: $\mathcal{G}_{24}$, $\mathcal{G}_{23}$, $\mathcal{G}_{12}$, $\mathcal{G}_{11}$

ref: `https://ethw.org/Marcel_J._E._Golay`

Binary $(24, 12)$ code, with generator matrix $G = [\mathbf{I}_{12}, A]$ and

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

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

row 2: mod 11, we have $0 \equiv 0^2$, $1 \equiv 1^2$, $3 \equiv 5^2$, $4 \equiv 2^2$, $5 \equiv 4^2$, $9 \equiv 3^2$

row $i+1$ is a shift on the left of row i for $i \geq 2$ (bordered reverse circulant matrix).

Rows of the generator matrix have weights 8 and 12 $\Rightarrow$ the inner product of any row with itself is $0 \mod 2$.

Rows of the generator matrix have weights 8 and 12 $\Rightarrow$ the inner product of any row with itself is $0 \mod 2$.

Row i for $i \geq 2$ has weight 6+2 (they are shifts of row 2), thus the inner product of row 1 and row i is $6 \equiv 0 \mod 2$.

Rows of the generator matrix have weights 8 and 12 $\Rightarrow$ the inner product of any row with itself is $0 \mod 2$.

Row i for $i \geq 2$ has weight 6+2 (they are shifts of row 2), thus the inner product of row 1 and row i is $6 \equiv 0 \mod 2$.

The inner product of row 2 with row $i \geq 3$ is $4 \equiv 0 \mod 2$ by direct inspection.

Rows of the generator matrix have weights 8 and 12 $\Rightarrow$ the inner product of any row with itself is $0 \mod 2$.

Row i for $i \geq 2$ has weight 6+2 (they are shifts of row 2), thus the inner product of row 1 and row i is $6 \equiv 0 \mod 2$.

The inner product of row 2 with row $i \geq 3$ is $4 \equiv 0 \mod 2$ by direct inspection.

For rows i and j, $i, j \geq 3$, since both rows are shifts of row 2, shift both rows so row i is mapped to row 2, and use the previous argument.

For $\mathbf{g}_i$ a row of G, we showed that $\mathbf{g}_i \cdot \mathbf{g}_j^T = 0$ for all i, j.

For $\mathbf{c}$ a codeword in $\mathcal{G}_{24}$, $\mathbf{c} = \sum_{i=1}^{k} x_i \mathbf{g}_i$.

For $\mathbf{g}_i$ a row of G, we showed that $\mathbf{g}_i \cdot \mathbf{g}_j^T = 0$ for all i, j.

For $\mathbf{c}$ a codeword in $\mathcal{G}_{24}$, $\mathbf{c} = \sum_{i=1}^{k} x_i \mathbf{g}_i$.

By definition $\mathcal{G}_{24}^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^{24},\ \mathbf{x} \cdot \mathbf{c}^T = 0 \text{ for all } \mathbf{c} \in \mathcal{G}_{24}\}$.

$$\underbrace{(\sum_{i=1}^{k} x_i' \mathbf{g}_i)}_{\mathbf{c}' \in \mathcal{G}_{24}} \cdot \underbrace{(\sum_{j=1}^{k} x_j \mathbf{g}_j)^T}_{\mathbf{c}^T \in \mathcal{G}_{24}} = 0 \text{ thus } \mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}.$$

For $\mathbf{g}_i$ a row of G, we showed that $\mathbf{g}_i \cdot \mathbf{g}_j^T = 0$ for all i, j.

For $\mathbf{c}$ a codeword in $\mathcal{G}_{24}$, $\mathbf{c} = \sum_{i=1}^{k} x_i \mathbf{g}_i$.

By definition $\mathcal{G}_{24}^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^{24},\ \mathbf{x} \cdot \mathbf{c}^T = 0 \text{ for all } \mathbf{c} \in \mathcal{G}_{24}\}$.

$$\underbrace{(\sum_{i=1}^{k} x_i' \mathbf{g}_i)}_{\mathbf{c}' \in \mathcal{G}_{24}} \cdot \underbrace{(\sum_{j=1}^{k} x_j \mathbf{g}_j)^T}_{\mathbf{c}^T \in \mathcal{G}_{24}} = 0 \text{ thus } \mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}.$$

- Since $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}$ and $\dim(\mathcal{G}_{24}) = \dim(\mathcal{G}_{24}^{\perp}) = 12$, we have $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

Since $\mathcal{G}_{24}$ is self-dual and rows of G have weights 8 or 12, codewords of $\mathcal{G}_{24}$ have weights divisible by 4 (see HW).

Since $\mathcal{G}_{24}$ is self-dual and rows of G have weights 8 or 12, codewords of $\mathcal{G}_{24}$ have weights divisible by 4 (see HW).

Thus the Hamming distance is either 4 or 8.

Since $\mathcal{G}_{24}$ is self-dual and rows of G have weights 8 or 12, codewords of $\mathcal{G}_{24}$ have weights divisible by 4 (see HW).

Thus the Hamming distance is either 4 or 8.

Suppose $wt(\mathbf{c}) = 4$. Write $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$, $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_2^{12}$.

1. $wt(\mathbf{c}_1) = 0$, $wt(\mathbf{c}_2) = 4$: $wt(\mathbf{c}_1) = 0$ implies that the data symbols are all 0.
2. $wt(\mathbf{c}_1) = 1$, $wt(\mathbf{c}_2) = 3$: $wt(\mathbf{c}_1) = 1$ implies $\mathbf{c}$ is a row of G.
3. $wt(\mathbf{c}_1) = 2$, $wt(\mathbf{c}_2) = 2$: $\mathbf{c}$ is the sum of two rows of G.

Since $\mathcal{G}_{24}$ is self-dual and rows of G have weights 8 or 12, codewords of $\mathcal{G}_{24}$ have weights divisible by 4 (see HW).

Thus the Hamming distance is either 4 or 8.

Suppose $wt(\mathbf{c}) = 4$. Write $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$, $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_2^{12}$.

1. $wt(\mathbf{c}_1) = 0$, $wt(\mathbf{c}_2) = 4$: $wt(\mathbf{c}_1) = 0$ implies that the data symbols are all 0.
2. $wt(\mathbf{c}_1) = 1$, $wt(\mathbf{c}_2) = 3$: $wt(\mathbf{c}_1) = 1$ implies $\mathbf{c}$ is a row of G.
3. $wt(\mathbf{c}_1) = 2$, $wt(\mathbf{c}_2) = 2$: $\mathbf{c}$ is the sum of two rows of G.
4. $A = A^T$ and since $\mathcal{G}_{24}$ is self-dual, $H = [A|\mathbf{I}_{12}]$ is a generator matrix. Thus if $(\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{G}_{12}$, so is $(\mathbf{c}_2, \mathbf{c}_1)$.

Since $\mathcal{G}_{24}$ is self-dual and rows of G have weights 8 or 12, codewords of $\mathcal{G}_{24}$ have weights divisible by 4 (see HW).

Thus the Hamming distance is either 4 or 8.

Suppose $wt(\mathbf{c}) = 4$. Write $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2)$, $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_2^{12}$.

1. $wt(\mathbf{c}_1) = 0$, $wt(\mathbf{c}_2) = 4$: $wt(\mathbf{c}_1) = 0$ implies that the data symbols are all 0.
2. $wt(\mathbf{c}_1) = 1$, $wt(\mathbf{c}_2) = 3$: $wt(\mathbf{c}_1) = 1$ implies $\mathbf{c}$ is a row of G.
3. $wt(\mathbf{c}_1) = 2$, $wt(\mathbf{c}_2) = 2$: $\mathbf{c}$ is the sum of two rows of G.
4. $A = A^T$ and since $\mathcal{G}_{24}$ is self-dual, $H = [A|\mathbf{I}_{12}]$ is a generator matrix. Thus if $(\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{G}_{12}$, so is $(\mathbf{c}_2, \mathbf{c}_1)$.

- $d_H(\mathcal{G}_{24}) = 8$.

Puncturing

For a linear $(n,k,d)_q$ code $\mathcal{C}$, puncturing means deleting the same coordinate i in each codeword. The resulting code is denoted by $\mathcal{C}^*$.
(1) $\mathcal{C}^*$ has length $n-1$.
(2) Delete column i from the generator matrix (so $\mathcal{C}^*$ is linear).

Consider the tetracode $\mathcal{C}$ over $\mathbb{F}_3$, $(x_1,x_2) \mapsto (x_1,x_2,x_1+x_2,x_1-x_2)$:

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

Puncture in coordinate 3 to get (x_1,x_2,x_1-x_2), puncture in coordinate 4 to get (x_1,x_2,x_1+x_2).

Dimension after puncturing.

Puncturing does not increase the number of codewords. Can it reduce it?

Dimension after puncturing.

Puncturing does not increase the number of codewords. Can it reduce it?

To have less codewords, we would need two codewords of $\mathcal{C}$ that agree in all coordinates but i, then when i is punctured, both codewords become the same and the number reduces, but that would mean that the Hamming distance of $\mathcal{C}$ is 1.

Minimum distance after puncturing.

Puncturing does not increase the minimum distance. Can it reduce it?

Minimum distance after puncturing.

Puncturing does not increase the minimum distance. Can it reduce it?

The minimum Hamming distance will decrease by 1 only if a codeword with minimum weight has a nonzero ith coordinate.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (1) if $d > 1$, $\mathcal{C}^*$ is an $(n-1, k, d^*)$ code where $d^* = d - 1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero ith coordinate and $d^* = d$ otherwise.

For the $(5, 2, 2)_2$ code given by

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

puncture in coordinate 1:

$$G_1^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

since G has distance 2 and the codeword $(1, 1, 0, 0, 0)$ of weight 2 which is punctured in 1, the new minimum distance is 1.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (1) if $d > 1$, $\mathcal{C}^*$ is an $(n-1, k, d^*)$ code where $d^* = d - 1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero ith coordinate and $d^* = d$ otherwise.

For the $(5, 2, 2)_2$ code given by

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

puncture in coordinate 5:

$$G_5^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Since $\mathcal{C}$ contains $(0,0,0,0,0)$, $(0,0,1,1,1)$, $(1,1,0,0,0)$, $(1,1,1,1,1)$, $wt(1,1,0,0,0) = 2$ with a 0 in the 5th coordinate, so the minimum distance is 2.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (2) if $d = 1$, $\mathcal{C}^*$ is an $(n-1, k, 1)$ code if $\mathcal{C}$ has no codeword of weight 1 whose nonzero entry is in coordinate i, otherwise, if $k > 1$, $\mathcal{C}^*$ is an $(n-1, k-1, d^*)$ code with $d^* \geq 1$.

For the $(4, 2, 1)_2$ code given by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

puncture in coordinate 4:

$$G_4^* = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

since $\mathcal{C}$ has a codeword of weight 1 but its nonzero entry is in coordinate 1, the distance is still 1.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (2) if $d = 1$, $\mathcal{C}^*$ is an $(n-1, k, 1)$ code if $\mathcal{C}$ has no codeword of weight 1 whose nonzero entry is in coordinate i, otherwise, if $k > 1$, $\mathcal{C}^*$ is an $(n-1, k-1, d^*)$ code with $d^* \geq 1$.

For the $(4, 2, 1)_2$ code given by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

puncture in coordinate 1:

$$G_1^* = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix},$$

the dimension drops. Since $\mathcal{C}$ has a unique codeword of weight 1 and its nonzero entry is in coordinate 1, this codeword disappears and the new distance is actually 3.

Binary $(23, 12)$ code, with generator matrix $G^* = [\mathbf{I}_{12}, A^*]$ and

$$A^* = \left[\begin{array}{c|cccccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}\right]$$

This is $\mathcal{G}_{24}^*$, that is $\mathcal{G}_{24}$ punctured in the last coordinate.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (1) if $d > 1$, $\mathcal{C}^*$ is an $(n-1, k, d^*)$ code where $d^* = d - 1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero ith coordinate and $d^* = d$ otherwise.

Puncturing.

For $\mathcal{C}^*$ the code punctured on the ith coordinate: (1) if $d > 1$, $\mathcal{C}^*$ is an $(n-1, k, d^*)$ code where $d^* = d - 1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero ith coordinate and $d^* = d$ otherwise.

Several rows of G have weight 8, and a 1 in the last coordinate, after puncturing the last column, they will yield codewords of weight 7.

- $d_H(\mathcal{G}_{23}) = 7$.

Ternary $(12, 6)$ code, with generator matrix $G = [\mathbf{I}_6, A]$ and

$$A = \left[\begin{array}{c|ccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{array}\right]$$

This code is a $(12, 6, 6)$ self-dual ternary code (see HW).

Ternary $(11, 6)$ code, with generator matrix $G^* = [\mathbf{I}_6, A^*]$ and

$$A^* = \left[\begin{array}{c|cccc} 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 & 2 \\ 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 \end{array}\right]$$

This is $\mathcal{G}_{12}^*$, that is $\mathcal{G}_{12}$ punctured in the last coordinate.

Binary Golay codes

$$SPB = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Binary Golay codes

$$SPB = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Both codes contain 2^{12} codewords, $t = 3$ ($d_H = 7, 8$) and

$$SPB = \begin{cases} \frac{2^{24}}{\sum_{i=0}^{3} \binom{24}{i}} = \frac{2^{24}}{1+24+276+2024} = \frac{2^{24}}{2325} & n = 24 \\ \frac{2^{23}}{\sum_{i=0}^{3} \binom{23}{i}} = \frac{2^{23}}{1+23+253+1771} = \frac{2^{23}}{2^{11}} & n = 23 \end{cases}$$

so $\mathcal{G}_{23}$ is perfect.

Ternary Golay codes

$$SPB = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Ternary Golay codes

$$SPB = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

Both codes contain 3^6 codewords, $t = 2$ ($d_H = 6, 5$) and

$$SPB = \begin{cases} \frac{3^{12}}{\sum_{i=0}^{2} \binom{12}{i} 2^i} = \frac{3^{12}}{1+24+264} = \frac{3^{12}}{289} & n = 12 \\ \frac{3^{11}}{\sum_{i=0}^{2} \binom{11}{i} 2^i} = \frac{3^{11}}{1+22+220} = \frac{3^{11}}{243} & n = 11 \end{cases}$$

so $\mathcal{G}_{11}$ is perfect.

Extending.

If $\mathcal{C}$ is an $(n, k, d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1, \ldots, x_n) \in \mathcal{C},\ x_1 + \cdots + x_{n+1} = 0\}$

Extending.

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

A generator matrix $\hat{G}$ for $\hat{\mathcal{C}}$ can be obtained from G by adding an extra column to G, so that the sum of the coordinates of each row of $\hat{G}$ is 0.

Thus the code $\hat{\mathcal{C}}$ is linear.

Extending.

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

Extending.

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

Parity check matrix:

Extending.

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

Parity check matrix: For H a parity check matrix of $\mathcal{C}$,

$$\hat{H} = \left[\begin{array}{ccc|c} 1 & \ldots & 1 & 1 \\ \hline & & & 0 \\ & H & & \vdots \\ & & & 0 \end{array}\right]$$

- Minimum distance:

Extending.

If $\mathcal{C}$ is an $(n,k,d)_q$ code, the extended code $\hat{\mathcal{C}}$ is the code $\{(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{F}_q^{n+1},\ (x_1,\ldots,x_n) \in \mathcal{C},\ x_1+\cdots+x_{n+1}=0\}$

Parity check matrix: For H a parity check matrix of $\mathcal{C}$,

$$\hat{H} = \left[\begin{array}{ccc|c} 1 & \ldots & 1 & 1 \\ \hline & & & 0 \\ & H & & \vdots \\ & & & 0 \end{array}\right]$$

- Minimum distance: $d_H(\hat{\mathcal{C}}) = d_H(\mathcal{C})$ or $d_H(\mathcal{C})+1$.

Extended tetracode over $\mathbb{F}_3$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \to \hat{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{bmatrix}$$

Extended tetracode over $\mathbb{F}_3$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix} \to \hat{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & -1 \end{bmatrix}$$

In $\mathcal{C}$, $(1,0,1,1)$ has weight 3, it is extended to $(1,0,1,1,0)$ which still has weight 3, so $\hat{d} = 3$.

Puncturing/Extending.

If we extend $\mathcal{C}$ and then puncture the new coordinate, we get $\mathcal{C}$. If we puncture $\mathcal{C}$ in its last coordinate and extend it, we may not get $\mathcal{C}$ back.

Puncturing/Extending.

If we extend $\mathcal{C}$ and then puncture the new coordinate, we get $\mathcal{C}$. If we puncture $\mathcal{C}$ in its last coordinate and extend it, we may not get $\mathcal{C}$ back.

Puncture in the last coordinate

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

to get

$$G^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

then extend

$$\hat{G}^* = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

to find a different code.

Codes seen so far

$(n,k,d_H)_q$	k/n	name	perfect
$(n,1,n)_q$	$\frac{1}{n}$	repetition	
$(n,n-1,2)_q$	$\frac{n-1}{n}$	parity check	
$(\frac{q^r-1}{q-1},n-r,3)_q$	$\frac{n-r}{n}$	Hamming	yes
$(24,12,8)_2$	$\frac{1}{2}$	$\mathcal{G}_{24}$	no
$(23,12,7)_2$	$\frac{12}{23}$	$\mathcal{G}_{23}$	yes
$(12,6,6)_3$	$\frac{1}{2}$	$\mathcal{G}_{12}$	no
$(11,6,5)_3$	$\frac{6}{11}$	$\mathcal{G}_{11}$	yes

Golay codes

Puncturing

Extending