## Question 1.

**(a)** Find generator matrix G.

From the given information we can deduce $n = 7$ and $k = 4$. So, we have a $(7, 3)$ code, so we are looking for matrix of size $(3x7)$. We also know that $g(x) = 1 + x^2 + x^3 + x^4$. From this, we can construct a generator matrix $G$ using steps described in the tutorial video.

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

**(b)** Find parity check matrix H.

To find the parity-check matrix, I need to divide $x^7 - 1$ by $g(x)$. When using only binary alphabet I can calculate $(x^7 + 1) : (x^4 + x^3 + x^2 + 1)$. This gives me $h(x)$, which is $h(x) = x^3 + x^2 + 1$.

From this we can construct a parity-check matrix $H$, again using steps from tutorial.

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

**(c)** Using polynomials encode the message 101.

To encode the message $m = 101$ I calculate the respresentation of $m$ in polynomial, giving me $m(x) = 1 + x^2$. Then I multiply $m(x) * g(x)$ to get the encoded polynomial codeword $c(x)$ and then turn it into binary representation $c$.

$c(x) = m(x) * g(x) = x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 1$

$c(x) = x^6 + x^5 + x^3 + 1$

$c = 1001011.$

**Question 2.**

---

**(a)** First we have to factorize $x^6 + 1$ as the length is 6 and we are in $\mathbb{F}_2$.

$x^6 + 1 = (x+1)^2(x^2+x+1)^2$

All binary cyclic codes are in form:

$(x+1)^{a_1}(x^2+x+1)^{a_2}, a_1 \in \{0,1,2\}, a_2 \in \{0,1,2\}$

We have $3^2$ possibilities, therefore there are 9 binary cyclic codes of length 6.

**(b)** First we have to factorize $x^6 + 4$ as the length is 6 and we are in $\mathbb{F}_2$.

$x^6 + 4 = (x+1)(x+4)(x^2+4x+1)(x^2+x+1)$

All quinary cyclic codes are in form:

$(x+1)^{a_1}(x+4)^{a_2}(x^2+4x+1)^{a_3}(x^2+x+1)^{a_4}, \forall i \in \{1,2,3,4\}, a_i \in \{0,1\}$

We have $2^4$ possibilities, therefore there are 16 quinary cyclic codes of length 6.

## Question 3.

The code is not equivalent to a cyclic code.

*Proof.* A binary cyclic code on $\mathbb{F}_2^8$ must be generated by a factor of $x^8 - 1$.
$x^8 - 1 = (x+1)^8 \implies$ there are 8 factors of $x^8 - 1 \pmod 2$: $(x+1)^i$ for $i \in \{0, \dots, 7\}$.
The degree of the $i$-th factor is $i$, therefore the only factor which generates an $[8,4]$-code is $(x+1)^4$.

$$\begin{aligned} k &= n - \deg g(x) \\ 4 &= 8 - \deg g(x) \\ \deg(g(x)) &= 4 \end{aligned}$$

The generator matrix of $\langle (x+1)^4 \rangle$ is:

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

As $G'$ generates a linear code, the Hamming distance of the generated code is the minimal of $G'$ row weights (number of 1s). Hamming distance of code generated by $G$ is also the minimal weight of a row in $G$:

$$\begin{aligned} \text{Ham}(C_{G'}) &= 2 \\ \text{Ham}(C_G) &= 4 \end{aligned}$$

The code generated by $G$ cannot be equivalent to the only possible $[8,4]$ cyclic code generated by $G'$, as the Hamming distance is preserved between equivalent codes.

Thus, the $[8,4]$ extended binary Hamming code is not equivalent to a cyclic code.

## Question 4.

We can write every code polynomial generated by $g(x)$ as $w(x) = u(x)g(x)$. Since $x + 1$ is a factor of $g(x)$ and $g(x), u(x)$ are not factors of each other, $x + 1$ is also a factor of every code polynomial $w(x)$. Hence $w(1) = 0$. It also holds that

$$w(1) = 0 \iff w_0 + w_1 + ... + w_{n-1} = 0.$$

And thus

$$w(1) = 0 \iff w \text{ has even weight.}$$

That means that if $1 + x|g(x)$, then every $w$ generated by $g(x)$ has even weight.

**Question 5.**

---

For the polynomial $g(x) = \sum_{i=0}^{n} x^{2i}$ to be a generating polynomial of a $q$-ary cyclic code of length $2n+2$ for any integer $n$ and prime $q$, the $g(x)$ needs to divide the polynomial $x^{2n+2} - 1$ in $\mathbb{F}_q$.

Therefore we have to find a polynomial $h(x)$ such that $x^{2n+2} - 1 = g(x) \cdot h(x) \pmod{q}$ for any integer $n$ and prime $q$.

The polynomial $h(x)$ we are looking for is $h(x) = x^2 - 1 \pmod{q}$.

Let us write the polynomial $g(x)$ in the following form:

$$g(x) = \sum_{i=0}^{n} x^{2i} = 1 + x^2 + x^4 + \ldots + x^{2n-2} + x^{2n} \pmod{q}$$

Then obviously for any integer $n$ and prime $q$ the following product holds:

$$\begin{array}{r} x^{2n} + x^{2n-2} + \ldots + x^4 + x^2 + 1 \\ \cdot \qquad\qquad\qquad\qquad\qquad x^2 - 1 \\ \hline -x^{2n} - x^{2n-2} - \ldots - x^4 - x^2 - 1 \\ x^{2n+2} + x^{2n} + x^{2n-2} + \ldots + x^4 + x^2 \qquad \\ \hline x^{2n+2} \qquad\qquad\qquad\qquad\qquad\qquad - 1 \end{array}$$

Therefore $g(x) \mid x^{2n+2} - 1$ for any integer $n$ and prime $q$, which implies that the polynomial $g(x) = \sum_{i=0}^{n} x^{2i}$ is a generating polynomial of a $q$-ary cyclic code of length $2n+2$ for any integer $n$ and prime $q$.

**Question 6.**

---

**(a)**

- $s = w \cdot H^T = (000100001010100000000001) \cdot [I|B]^T = 001100110001$
- $w(s) \nleq 3$
- $w(s + b_i) = w(s + b_{10}) = w(100001000000) = 2 \leq 2$
- $e = [s + b_{10}, e_{10}] = [100001000000, 000000000100] = 100001000000000000000100$
- $c = w + e = 100101001010100000000101$, $c_1 \ldots c_{12} = b_1 + b_{10} + b_{12}$
- $c = 100101001010100000000101$

**(b)**

- $s = w \cdot H^T = (110100110100010111100000) \cdot [I|B]^T = 110100010001$
- $w(s) \nleq 3$
- $w(s + b_i) \nleq 2, \forall i \in \{1, \ldots, 12\}$
- $s \cdot G = 010101000000$
- $w(010101000000) = 3 \leq 3$
- $e = [000000000000, 010101000000] = 000000000000010101000000$
- $c = w + e = 110100110100000010100000$, $c_1 \ldots c_{12} = b_5 + b_7$
- $c = 110100110100000010100000$