Číslo cvičení: 3
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. (a) $x^6 - 1 = (1 - x + x^2)(1 + x + x^3 + x^4) \implies h(x) = x^2 - x + 1$
   (b) $(x^2 - x + 1)(x^5 + x^4 + x^3) = x(-1 + x^6) + (x + x^3 + x^5), (x^2 - x + 1)(x^5 + x^4 + x^3 + x) = x(-1 + x^6) + (2x - x^2 + 2x^3 + x^5) \implies$ the words do not belong to C.

2. (a) Not linear $\implies$ not cyclic, not equivalent to a cyclic code.
   (b) Not a cyclic code, not equivalent to a cyclic code.
   (c) Is a cyclic code.
   (d) Not a cyclic code, not equivalent to a cyclic code.

3.

4. MDS $\iff M = q^{n-d+1}$. $\mathrm{Ham}(r, 2)$ has a $(r \times (2^r - 1)) = ((n - k) \times n)$ parity check matrix $\implies n = 2^r - 1, n - k = r, d = 3$. $M = q^k = 2^{n-r}$.

$$2^{2^r-1-3+1} = 2^{2^r-1-r}$$
$$2^r - 3 = 2^r - 1 - r$$
$$r = 2$$

5. $(x^7 - 1)/(x^3 + x + 1) = x^4 + x^2 + x + 1 = h(x)$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}, \bar{h}(x) = x^4 + x^3 + x^2 + 1$$

6. $x^6 - 1 = (x - 1)(x + 1)(x^2 - x + 1)(x^2 + x + 1)$. There are $2^4 = 16$ such codes. Their generator polynomials are: $1, (x - 1), (x + 1), (x^2 - x + 1), (x^2 + x + 1), (x^2 - 1), (x^3 - 2x^2 + 2x - 1), (x^3 - 1), (x^3 + 1), (x^3 + 2x^2 + 2x + 1), (x^4 + x^2 + 1), (x^4 + x^3 - x + 1), (x^4 - x^3 + x - 1), (x^5 - x^4 + x^3 - x^2 + x - 1), (x^5 + x^4 + x^3 + x^2 + x + 1), (x^6 - 1) = 0$

Polynomial	Matrix
1	I_6
$x + 1$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$
$x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$
$x^3 + 1$	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$
$x^4 + x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$
$(x^5 + x^4 + x^3 + x^2 + x + 1)$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

7. (a) Let C_1 be a repetition code of length n, C_2 a no-parity code of length $n \implies \neg C_1 = C_1, C_1 \cap C_2 = C_1 = C_3$.
   (b) C_3 does not exist. There must be at least one non-zero codeword in C_1. If C_3 were to be cyclic, that non-zero bit would have to be shifted to all positions including the last one.
   (c) Let C_1 and C_2 be the same as in (a) $\implies C_1 \cup C_2 = C_2 = C_3$.