Question 1.

(a) $1000 \in C_1$, but $1000 + 1000 = 0000$ and $0000 \notin C_1$. Therefore C_1 is not linear code.

(b) Let's consider $w_1 = x_1x_2x_3x_4x_5, w_2 = y_1y_2y_3y_4y_5 \in C_2, w = w_1 + w_2$. Symbol at position i in codeword w can be written as $x_i + y_i$ and number of ones in w can be written as $\sum_{i=1}^{5} x_i + y_i$. There can happen two cases when adding x_i and y_i:

(a) x_i and y_i are different values. Then there is only one symbol of one among them, which is odd, and result of addition is one, which is also odd.

(b) x_i and y_i are same values. Then number of ones among them is even, and result is zero, which is also even.

Because sum of number of ones in w_1 and w_2 is even, the resulting number of ones in w is also even. Therefore $w \in C_2$.

Now, let's consider $g \in C_2$ and $k \in 0, 1$. During $k \cdot g$, two cases can happen:

(a) k is 1. Then $k \cdot g = g$, which belongs in C_2.

(b) k is 0. Then $k \cdot g = 00000$, which belongs in C_2.

This all means, that $\forall w_1, w_2 \in C_2 : w_1 + w_2 \in C_2$ and $\forall w \in C_2, \forall k \in 0, 1 : k \cdot w \in C_2$. Therefore C_2 is linear code.

(c) $021 \in C_3$, but $2 \cdot 021 = 012$ and $012 \notin C_3$. Therefore C_3 is not linear code.

Question 2.

By the definition of hamming codes the parity check matrix H has to be of size $r \times 2^r - 1$ where columns are all non-zero distinct words from $\mathbb{F}_2^r$.

(a) First we calculate parity matrix H_1 from generator matrix G_1.

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = [\mathbb{I}_k | A]$$

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} = [-A^\top | \mathbb{I}_{n-k}]$$

From there H_1 has $r = 1$ rows. For code generated by generator matrix G_1 to be equivalent with hamming code, matrix H_1 has to have $2^r - 1$ columns, but $2^1 - 1 \neq 4$ and therefore code generated by G_1 is not equivalent with hamming code.

(b) First we calculate parity matrix H_2 from generator matrix G_2.

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = [\mathbb{I}_k | A]$$

$$H_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = [-A^\top | \mathbb{I}_{n-k}]$$

H_2 has $r = 3$ rows and $2^3 - 1 = 7$ columns where each column contains non-zero distinct word. Therefore code generated by G_2 is equivalent with hamming code.

Question 3.

By definition, all Hamming codes have minimum distance 3. $[n, k]$-Hamming code is thus a $(n = \frac{q^k-1}{q-1}, M = q^{n-k}, 3)$ code. We plug this into the Hamming bound equation and get:

$$q^{n-k}\left(\binom{n}{0} + \binom{n}{1}(q-1)\right) \leq q^n$$
$$q^{n-k}(1 + n(q-1)) \leq q^n$$
$$q^{n-k}\left(1 + \frac{q^k-1}{q-1}(q-1)\right) \leq q^n$$
$$q^{n-k}(1 + q^k - 1) \leq q^n$$
$$q^{n-k}q^k \leq q^n$$
$$q^n \leq q^n$$

Equality holds, so all Hamming codes are perfect.

Question 4.

(a)

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow \left[\begin{array}{cc|ccc} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$H = [A^T | I_3]$$

$$G = [I_2 | A]$$

$$G = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

(b) Let C be a linear code and let weight of C, notation $w(C)$, be the smallest of the weights of non-zero code words of C. Then $h(C) = w(C)$.

$$C = \{00000, 10011, 01101, 11110\}$$

$$h(C) = w(C) = 3$$

(c)

coset leaders $(l(z))$	syndromes(z)
00000	000
10000	101
01000	010
00100	$\underline{100}$
00010	011
00001	110
11000	111
10100	001

y = 10111

Step 1: Given y compute $S(y) = yH^T$

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

Step 2: Locate $z = S(y)$ in the syndrome column

$$l(100) = 00100$$

Step 3: Decode y as $y - l(z)$

$$y - l(z) = 10111 - 00100 = \underline{\underline{10011}}$$

Question 5.

Binary code C is self-dual iff $C = C^{\perp}$. $G = [I_k|A] \implies H = [A^T|I_{n-k}]$ (for binary code).

(a)

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

$\sim$ (exchanging second and third row)

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

$\Longrightarrow$

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Definition from lecture 2, slide 32: A parity check matrix H for an $[n, k]$-code C is any generator matrix of $C^{\perp}$. We can see that $G_1 = H_1$ and therefore, code generated by G_1 is self-dual.

(b) Matrix G_2 generates a $[5, 2]$-code. Let's assume it is self-dual. Then, according to the theorem in lecture 2, slide 32, it is a $[5, 3]$-code. We have reached a contradiction, therefore the initial assumption was false and that means code generated by G_2 is not self-dual.

Question 6.

To prove $(C+D)^{\perp} = C^{\perp} \cap D^{\perp}$ it is necessary to prove $(C+D)^{\perp} \subseteq C^{\perp} \cap D^{\perp}$ and $C^{\perp} \cap D^{\perp} \subseteq (C+D)^{\perp}$

I. $(C + D)^{\perp} \subseteq C^{\perp} \cap D^{\perp}$
Let $x \in (C + D)^{\perp}$ and $x \cdot y = 0$, for all $y \in (C + D)$.
Let $c \in C$ and then for all $c \in C$, $c = c + 0 \in (C + D)$, so $x \cdot c = 0$, which means that $x \in C^{\perp}$.
Let $d \in D$ and then $\forall d \in D$, $d = 0 + d \in (C + D)$, so $x \cdot d = 0$, which means that $x \in D^{\perp}$.

II. $C^{\perp} \cap D^{\perp} \subseteq (C + D)^{\perp}$
For all $y \in (C^{\perp} \cap D^{\perp}) : y \cdot c = 0$ and $v \cdot d = 0$, which means that $v \cdot (c + d) = 0$, so $v \in (C + D)^{\perp}$.

Question 7.

Let the code be C an $[n, k, d]$ linear code, then we know $B(n, d) = q^k$. We want to get an $[n-1, k*, d]$ code, what we can achieve with code shortening. If we have a full 0 column(special case, this position is useless), we can shorten the code without loosing any base code words, and we get an $[n-1, k, d]$ code, and the equality clearly holds(this gives the most possible k). More generally(no all 0 column), we can transform the codes generator matrix to have only one 1bit in its last column. With shortening we receive an $[n-1, k-1, \geq d]$ code, which has q^{k-1} code words. Substituting into the non-equivalence we get:

$$\begin{aligned} B_q(n, d) &\leq q\,\mathrm{B}_{\mathrm{q}}(n-1, d) \\ q^k &\leq q \cdot q^{k-1} \\ q^k &\leq q^k \end{aligned}$$

which is true.