Solutions 4

1. Let $\omega(v)$ denote the weight of a codeword $v \in C$, and let $d_H(u, v)$ denote the Hamming distance between u and v. Additionally, let

$$d = \min\{d_H(u, v) : u, v \in C, u \neq v\},$$

denote the distance of the code C, and let

$$d' = \min\{\omega(v) : v \in C, v \neq 0\}$$

denote the minimum weight of a nonzero codeword. Our goal is to show that $d = d'$. Since C is a linear subspace of $\mathbb{F}^n$, the vector 0 belongs to C and C is closed under vector addition, i.e., and for all $u, v \in C$, the vector $u - v$ also belongs to C. It is straightforward to check that $\omega(v) = d_H(v, 0)$ and $d_H(u, v) = d_H(u - v, 0)$ for all $u, v \in C$. This implies that

$$\begin{aligned} d &= \min\{d_H(u, v) : u, v \in C, u \neq v\} \\ &= \min\{d_H(u - v, 0) : u, v \in C, u \neq v\} \\ &= \min\{d_H(v, 0) : v \in C, v \neq 0\} \\ &= \min\{\omega(v) : v \in C, v \neq 0\} = d', \end{aligned}$$

concluding the proof.

2. The Hadamard code is the image of the function Had. In order to prove that the Hadamard code is a linear code, it suffices to prove that

$$\text{Had}(x) + \text{Had}(y) = \text{Had}(x + y)$$

for all $x, y \in \{0, 1\}^n$, i.e, Had is a linear function. But it is straightforward to check that Had is linear, since

$$\langle x, z\rangle + \langle y, z\rangle = \langle x + y, z\rangle$$

for all $z \in \{0, 1\}^n$. We now turn to compute the distance of the Hadamard code. Let $x, y \in \{0, 1\}^n$ be two distinct messages. We claim that the Hamming distance between $\text{Had}(x)$ and $\text{Had}(y)$ is exactly 2^{n-1}. Let i be an index such the coordinates x_i and y_i are different, and let $e \in \{0, 1\}^n$ denote the vector having coordinates $e_j = 0$ if $j \neq i$ and $e_i = 1$. For any $z \in \{0, 1\}^n$, we have

$$\langle x, z\rangle = \langle y, z\rangle \iff \langle x, z + e\rangle \neq \langle y, z + e\rangle,$$

hence $\text{Had}(x)$ and $\text{Had}(y)$ differ in exactly 2^{n-1} coordinates, finishing the proof of the claim.

Bitte wenden!

3. Using the Euclidean algorithm to compute the greatest common divisor of X^3+X+1 and $X+1$ in $\mathbb{F}_2[X]$, we obtain

$$1 \cdot (X^3 + X + 1) + (X^2 + X) \cdot (X + 1) = 1,$$

thus the inverse of $\overline{X}+1$ in $\mathbb{F}_2[X]/(X^3+X+1)$ is $\overline{X}^2+\overline{X}$. Similarly, if we apply the same algorithm to compute the greatest common divisor of $X^3 + X + 1$ and $X^2 + 1$, we get

$$1 \cdot (X^3 + X + 1) + X \cdot (X^2 + 1) = 1,$$

therefore the inverse of $\overline{X}^2 + 1$ in $\mathbb{F}_2[X]/(X^3 + X + 1)$ is $\overline{X}$.

4. (i) Suppose, towards contradiction, there exist two pairs $x_1 \neq x_2$ and $y_1 \neq y_2$ such that $F(x_1) + F(x_2) = F(y_1) + F(y_2)$. By the definition of F, this implies that

$$\begin{aligned} x_1 + x_2 &= y_1 + y_2 \neq 0 \\ x_1^3 + x_2^3 &= y_1^3 + y_2^3. \end{aligned}$$

Because we are working in a field of characteristic 2, we have

$$x_1^2 + x_2^2 = (x_1 + x_2)^2 = (y_1 + y_2)^2 = y_1^2 + y_2^2.$$

Moreover,

$$\begin{aligned} x_1^3 + x_2^3 &= (x_1 + x_2)(x_1^2 + x_2^2 - x_1x_2) \\ y_1^3 + y_2^3 &= (y_1 + y_2)(y_1^2 + y_2^2 - y_1y_2), \end{aligned}$$

hence

$$\begin{aligned} x_1 + x_2 &= y_1 + y_2 \\ x_1x_2 &= y_1y_2. \end{aligned}$$

Therefore, the two polynomials $(X - x_1)(X - x_2)$ and $(X - y_1)(X - y_2)$ are identical, and thus they have the same set of roots, i.e., $\{x_1, x_2\} = \{y_1, y_2\}$, concluding the proof.

(ii) Let $a \in \mathbb{F}_8$ be an element such that $a^3 + a + 1 = 0$ (such element exists by exercise 3). We think of $\mathbb{F}_8$ as a vector space over $\mathbb{F}_2$ with basis $\{1, a, a^2\}$. Then $\mathbb{F}_8 \simeq \mathbb{F}_2^3$ and the map F can be written as

$$\begin{array}{lcllcl} (0,0,0) & \mapsto & (0,0,0,0,0,0) & (1,0,0) & \mapsto & (1,0,0,1,0,1) \\ (0,0,1) & \mapsto & (0,0,1,0,0,1) & (1,0,1) & \mapsto & (1,0,1,1,1,0) \\ (0,1,0) & \mapsto & (0,1,0,0,1,1) & (1,1,0) & \mapsto & (1,1,0,1,1,1) \\ (0,1,1) & \mapsto & (0,1,1,1,0,0) & (1,1,1) & \mapsto & (1,1,1,0,1,0). \end{array}$$

Siehe nächstes Blatt!

(iii) Let M be the matrix whose columns are the 8 vectors in the image of F, i.e.,

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

The codes in $C \subseteq \mathbb{F}_2^8$ are all the vectors $v \in \mathbb{F}_2^8$ such that $M \cdot v = 0$. Since the rank of M in $\mathbb{F}_2$ is 6, there are exactly four such vectors v. Moreover, since the pairwise sums of any two columns in M are all distinct, the code C can correct at least 2 faulty bits.