Dr. Maurice Cochand and Humberto Naves

Problem Sheet 4

1. In coding theory, a *linear code* of length n is a linear subspace C of the vector space $\mathbb{F}^n$ over the finite field $\mathbb{F}$. The elements of C are called *codewords*. The *weight* of a codeword v is the number of nonzero coordinates in v. The *Hamming distance* between two codewords u and v is the number of coordinates in which they differ. The *distance* of the code C is the minimum Hamming distance between any two distinct codewords in C. Prove that the distance of the code C is equal to the minimum weight of nonzero codewords in C.

2. Given a binary message $x \in \{0,1\}^n$ of length n, the *Hadamard code* encodes the message into a codeword $\text{Had}(x)$, using an encoding function $\text{Had} : \{0,1\}^n \to \{0,1\}^{2^n}$. This function is defined as follows

$$\text{Had}(x) = \Big(\langle x, y \rangle\Big)_{y \in \{0,1\}^n},$$

where $\langle x, y \rangle$ denotes the *inner product* of two vectors $x, y \in \{0,1\}^n$ modulo 2, i.e.,

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \pmod 2.$$

Prove that the Hadamard code is a linear code and compute its distance.

3. Let p be a prime number and n be a positive integer. One way to explicitly compute the multiplicative inverse of an element $\overline{a}$ in a finite field $\mathbb{F}$ of size p^n is as follows. We know that $\mathbb{F}$ is isomorphic to the quotient ring $\mathbb{F}_p[X]/(q(X))$, where $\mathbb{F}_p[X]$ denotes the polynomial ring over the field $\mathbb{F}_p$ of integers modulo p, and $q(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree n. Let $a(X) \in \mathbb{F}_p[X]$ be such that $\overline{a} \equiv a(X) \pmod{q(X)}$. Because $\overline{a} \neq 0$, the polynomial $a(X)$ is not divisible by $q(X)$, and since $q(X)$ is irreducible, we have $\gcd\{a(X), q(X)\} = 1$. By the Euclidean algorithm, there exist two polynomials $r(X)$ and $s(X)$ such that

$$a(X)r(X) + q(X)s(X) = 1. \tag{1}$$

In particular, $a(X) \cdot r(X) \equiv 1 \pmod{q(X)}$, so $(\overline{a})^{-1} \equiv r(X) \pmod{q(X)}$. Using this algorithm, compute the inverse of the elements $\overline{X} + 1$ and $\overline{X}^2 + 1$ in the field $\mathbb{F}_2[X]/(X^3 + X + 1)$.

Bitte wenden!

4. Let $\mathbb{F}_q$ denote the unique field of size $q = 2^n$, where $n \geq 1$ is an integer number. Let $F : \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$ be defined as $F(x) = (x, x^3)$.

(i) Show that if $F(x_1) + F(x_2) = F(y_1) + F(y_2)$, where $x_1 \neq x_2$ and $y_1 \neq y_2$, then $\{x_1, x_2\} = \{y_1, y_2\}$.

(ii) Compute explicitly the map F for $n = 3$ in the finite field $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$.

(iii) Using the map F computed above, construct an error-correcting code $C \subseteq \{0,1\}^8$ having 4 codewords that is able to correct at least 2 faulty bits.