TUTORIAL X

1 Finite fields

In this exercise, we will prove some properties of finite fields. In the following, we will denote by $\mathbb{F}_q$ a finite field of cardinality q (we will see that there exists a unique field of cardinality q so $\mathbb{F}_q$ is in fact "the" finite field of cardinality q).
We recall that a field K is a ring, with a neutral element 0 for the addition and a neutral element 1 for the multiplication ($0 \neq 1$), and such that every non zero element in K has an inverse for the multiplication. We also want that the multiplication is commutative in K (and of course also the addition is commutative but this is always the case in a ring).

1. Let $n \geq 2$, show that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.
2. Prove that there exists a prime p such that $\mathbb{F}_q$ contains $\mathbb{Z}/p\mathbb{Z}$.
3. Prove that there is an $n \geq 1$ such that $q = p^n$.

   So far, we have proven that if $\mathbb{F}_q$ is a finite field of cardinality q, then q is a prime power. Now we prove the converse. Assume that $q = p^n$ for some prime n, we will construct a finite field of cardinality q.
4. Let K be a field and $P \in K[X]$ a polynomial with coefficients in K. Show that $K[X]/(P)$ is a field if and only if P is irreducible in $K[X]$.
5. We admit that, in $(\mathbb{Z}/p\mathbb{Z})[X]$, there exist irreducible polynomials of any degree. Construct a finite field of cardinality q.

   So far, we have proven that there exist finite field of cardinality p^n for any prime p and $n \geq 1$ and that there are the unique possible cardinality for finite fields. We will now show that for a given $q = p^n$ there is a unique field of cardinality q up to isomorphism (and then we can call it $\mathbb{F}_q$ without ambiguity).
6. (Optional) We admit that for any prime p, there exist an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$, that is a field $\overline{\mathbb{F}_p}$ that contains $\mathbb{Z}/p\mathbb{Z}$ and such that any polynomial in $\overline{\mathbb{F}_p}[X]$ has a root in $\overline{\mathbb{F}_p}$ (we also want that all elements of $\overline{\mathbb{F}_p}$ are algebraic on $\mathbb{Z}/p\mathbb{Z}$ but this is not important here). Show that $\mathbb{F}_q = \{a \in \overline{\mathbb{F}_p}, a^q = a\}$.

   This proves the unicity of $\mathbb{F}_q$.

2 Error-correcting VS error-detecting codes

Show that the following statements are equivalent for a code C:

1. C has minimum distance $d \geq 2$.
2. If d is odd, C can correct $(d-1)/2$ errors.
3. If d is even, C can correct $d/2 - 1$ errors.
4. C can detect $d - 1$ errors.
5. C can correct $d - 1$ erasures (in the erasure model, the receiver knows where the errors have occurred).

3 Generalized Hamming bound

Prove the following bound: for any $(n,k,d)_q$ code $C \subseteq (\Sigma)^n$ with $|\Sigma| = q$,

$$k \leq n - \log_q \left(\sum_{i=0}^{\lfloor \frac{(d-1)}{2} \rfloor} \binom{n}{i} (q-1)^i \right)$$

4 Parity check matrix

Let C be a $[n,k,d]_q$-linear code and $G \in \mathbb{F}_q^{k\times n}$ be a generator matrix. That is, $C = \{xG, x \in \mathbb{F}_q^k\}$. We call a parity check matrix of the code C a matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ such that for all $c \in \mathbb{F}_q^n$ we have $cH^T = 0$ if and only if $c \in C$. The objective of this exercise is to show how to construct a parity check matrix from a generator matrix.

1. Show that H is a parity check matrix if and only if $GH^T = 0$ and rank$(H) = n - k$.
2. Show that, from G we can construct a generator matrix G' of the form $G' = [I_k|P]$ for some $P \in \mathbb{F}_q^{k\times(n-k)}$. (If n is not optimal, we may have to permute the coefficients of the vectors).
3. Construct a parity check matrix from G'.
4. Construct a parity check matrix of the code given by the generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ in $\mathbb{F}_2$.

5 (Optional) Almost-universal hash-functions: link between almost-universal hash-functions and codes with a good distance

A hash function is generally a function from a large space to a small one. A desirable property for a hash function is that there are few collisions. A family of functions $\{f_y\}_{y\in\mathcal{Y}}$ from $f_y : \mathcal{X} \to \mathcal{Z}$ is called ϵ-almost universal if for any $x \neq x'$, we have $\underset{y}{\mathbf{P}} \{f_y(x) = f_y(x')\} \leq \epsilon$ for a uniformly chosen $y \in \mathcal{Y}$. In other words, for any $x \neq x'$,

$$|\{y \in \mathcal{Y} : f_y(x) = f_y(x')\}| \leq \epsilon|\mathcal{Y}| \,. \tag{1}$$

The objective of the exercise is to show that almost-universal hash-functions and codes with a good distance are equivalent: from one you can construct the other efficiently.

Definition 5.1. *Let $\mathcal{H} = \{f_1, \ldots, f_n\}$ be a family of hash-functions, where for each $1 \leq i \leq n$, $f_i : \mathcal{X} \to \mathcal{Z}$. We define the code $C_{\mathcal{H}} = \mathcal{X} \to \mathcal{Z}^n$ by*

$$C_{\mathcal{H}}(x) = (f_1(x), \ldots, f_n(x))$$

for all $x \in \mathcal{X}$.

On the contrary, given a code $C : \mathcal{X} \to \mathcal{Z}^n$, we define the family of hash-functions $\mathcal{H}_C = \{f_1, \ldots, f_n\}$, from $\mathcal{X}$ to $\mathcal{Z}$ by

$$f_i(x) = C(x)_i$$

where $x \in \mathcal{X}$ and $C(x)_i$ is the i-th letter of $C(x)$ in the alphabet $\mathcal{Z}$.

1. Let $\mathcal{H} = \{f_1, \ldots, f_n\}$ be a family of ϵ-almost universal hash-functions. Prove that $C_{\mathcal{H}}$ has minimum distance $(1-\epsilon)n$.
2. On the other way, let C be a code from $\mathcal{X}$ to $\mathcal{Z}^n$ with minimum distance δn, prove that $\mathcal{H}_C$ is a family of $(1-\delta)$-almost universal hash-functions.