TUTORIAL IX

1 q-ary Entropy and Volume of Hamming Balls

q-ary entropy function: Let q be an integer and x be a real number such that $q \geq 2$ and $0 \leq x \leq 1$. Then the q-ary entropy function is defined as follows:

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x).$$

Volume of a Hamming ball: Let $q \geq 2$ and $n \geq r \geq 1$ be integers. The volume of a Hamming ball of radius r is given by

$$\mathrm{Vol}_q(r, n) = |B_q(\mathbf{0}, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

For $0 \leq p \leq 1 - \frac{1}{q}$ real, show that the following bounds hold for large enough n.

1. $\mathrm{Vol}_q(pn, n) \leq q^{nH_q(p)}$.
2. $\mathrm{Vol}_q(pn, n) \geq q^{nH_q(p) - o(n)}$. (Hint: Use Stirling's approximation)

2 Hamming riddle

There are n people in a room, each of whom is given a black/white hat chosen uniformly at random (and independent of the choices of all other people). Each person can see the hat color of all other people, but not their own. Each person is asked if (s)he wishes to guess their own hat color. They can either guess, or abstain. Each person makes their choice without knowledge of what the other people are doing. They either win collectively, or lose collectively. They win if all the people who don't abstain guess their hat color correctly and at least one person does not abstain. They lose if all people abstain, or if some person guesses their color incorrectly. The goal below is to come up with a strategy that will allow the n people to win with pretty high probability

1. Argue that the n people can win with probability at least $\frac{1}{2}$
2. Lets say that a directed graph G is a subgraph of the n-dimensional hypercube if its vertex set is $\{0,1\}^n$ and if $u \to v$ is an edge in G, then u and v differ in at most one coordinate. Let $K(G)$ be the number of vertices of G with in-degree at least one, and out-degree zero. Show that the probability of winning the hat problem equals the maximum, over directed subgraphs G of the n-dimensional hypercube, of $K(G)/2^n$
3. Using the fact that the out-degree of any vertex is at most n,show that $K(G)/2^n$ is at most $\frac{n}{n+1}$ for any directed subgraph G of the n-dimensional hypercube.
4. Show that if $n = 2^r - 1$, then there exists a directed subgraph G of the n-dimensional hypercube with $K(G)/2^n = \frac{n}{n+1}$.
   Hint:This is where the Hamming code comes in.

3 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 $\mathbb{F}_q$.