TUTORIAL IX

1 Isoperimetric inequality for the discrete hypercube

Let $V = \{0,1\}^n$ and let $G = (V, E)$ be the hypercube graph (i.e., we have $(u, v) \in E$ if u and v differ at exactly one coordinate). We define the *boundary* of $S \subset V$ as the set of all edges that go from the inside of S to the outside of S, i.e., $\partial S = \{(u, v) \in E \colon u \in S, v \notin S\}$. Furthermore, we call $|S|$ the *volume* of S, and we denote by $\delta(S) = |\partial S|$ the size of the boundary of S.

1. Show that for any S we have $\delta(S) = n|S| - 2e(S)$, where $e(S) = |\{(u, v) \in E \colon u, v \in S\}|$ is the number of edges in the subgraph induced by S.
2. Let $X = (X_1, \dots, X_n)$ be a uniform random variable on S. Compute $\sum_{i=1}^n H(X_i|X_{-i})$.
3. Prove the entropy chain rule: for arbitrary random variables $X_1, \dots, X_n$ we have $H(X_1, \dots, X_n) = \sum_{i=1}^n H(X_i|X_1, \dots, X_{i-1})$.
4. Prove that $\delta(S) \geq |S|(n - \log|S|)$.
5. A k-dimensional subcube is a subset of G obtained by fixing $n - k$ coordinates to some values and allowing the remaining k coordinates to take any value. Show that among the sets of volume 2^k subcubes minimize the size of the boundary.

2 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)

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 $\mathbb{F}_q$.