
TUTORIAL X

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

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

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

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

2 Codes Achieving the Gilbert-Varshamov Bound

The purpose of this exercise is to use the probabilistic method to show that a random linear code lies on the Gilbert-Varshamov bound, with high probability.

1. Given a non-zero vector $\mathbf{m} \in \mathbb{F}_q^k$ and a uniformly random $k \times n$ matrix \mathbf{G} over \mathbb{F}_q , show that the vector \mathbf{mG} is uniformly distributed over \mathbb{F}_q^n .
2. For $k = (1 - H_q(\delta) - \varepsilon)n$, show that there exists a $k \times n$ matrix \mathbf{G} such that

$$\text{for every } \mathbf{m} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}, \text{wt}(\mathbf{mG}) \geq d$$

3. Show that \mathbf{G} has full rank (i.e., it has dimension at least $k = (1 - H_q(\delta) - \varepsilon)n$)

3 Singleton Bound

For every $[n, k, d]$ -linear code, show that $k \leq n - d + 1$.

4 Weights of Codewords

Let C be an $[n, k, d]$ -linear code over \mathbb{F}_q . Prove the following.

1. For $q = 2$, either all the codewords have even weight or exactly half have even weight and the rest have odd weight.
2. For any q , either all the codewords begin with 0 or exactly a fraction $1/q$ of the codewords begin with 0. In general, for a given position $1 \leq i \leq n$, either all codewords contain 0 at the i -th position or each $\alpha \in \mathbb{F}_q$ appears at the i -th position of exactly $1/q$ of the codewords in C .

3. The following inequality holds for the minimum distance d of C .

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}$$