TUTORIAL I

1 Repetition code

1. Suppose that you have a disk drive where each bit gets flipped with probability $f = 0.1$ in a year. In order to be able to correct errors, we take a copy of the full drive $N - 1$ times so that we have N copies of the original data (N is odd). After one year, I would like to retrieve a given bit of the original drive. What should I do? Suppose I want the probability of error for this bit to be at most δ, how large should I take N as a function of δ? How large is this for $\delta = 10^{-10}$?

2. Let $X \in \mathbb{N}$ be a discrete random variable and $g : \mathbb{N} \to \mathbb{N}$. What can you say in general on the relation between $H(X)$ and $H(g(X))$? And in particular, if $g(n) = 2^n$?

2 Weighing problem

You are given 12 balls, all equal in weight except for one that is either heavier or lighter. You are also given a classical two-pan balance which allows you only to compare two subsets of balls (you are not given any reference weight). Your task is to design a strategy to determine which is the odd ball *and* whether it is heavier or lighter, using as few uses of the balance as possible.

1. What is the amount of uncertainty of a configuration?

2. How much information on average can a single use of the balance give? What is the minimum number of weighing one can hope to achieve?

3. Show that if we start by weighing balls 1-6 against 7-12, we don't get enough information to achieve the optimal solution.

4. Describe an optimal strategy.

5. Compute the exact information obtained during the process depending on the result of the second round (3 or 2 remaining situations).

3 Axiomatic approach to the Shannon entropy

If we require certain properties of our uncertainty measure, then it uniquely specifies the Shannon entropy. Let $\Delta_m = \{(p_1, \ldots, p_m) \in \mathbb{R}^m : p_i \geq 0, \sum_i p_i = 1\}$ be the set of distributions on m elements. Let our uncertainty measure $H_m : \Delta_m \to \mathbb{R}$ be a sequence of functions satisfying the following desirable properties

1. Symmetry: For any $m \geq 1$ and any permutation π of $\{1, \ldots, m\}$, $H_m(p_1, \ldots, p_m) = H_m(p_{\pi(1)}, \ldots, p_{\pi(m)})$

2. Normalization: $H_2(\frac{1}{2}, \frac{1}{2}) = 1$

3. Continuity: For any $m \geq 1$, H_m is a continuous function

4. Grouping: For any $m \geq 2$,

$$H_m(p_1, \ldots, p_m) = H_{m-1}(p_1 + p_2, p_3, \ldots, p_m) + (p_1 + p_2) H_2(\frac{p_1}{p_1 + p_2}, \frac{p_2}{p_1 + p_2})$$

5. Monotonicity: We have $H_m(\frac{1}{m}, \ldots, \frac{1}{m}) \leq H_{m+1}(\frac{1}{m+1}, \ldots, \frac{1}{m+1})$

Prove that $H_m(p_1, \ldots, p_m) = -\sum_{i=1}^{m} p_i \log_2 p_i$.

You can proceed in the following way. Let $g(m) = H_m(\frac{1}{m}, \ldots, \frac{1}{m})$.

1. Show that $g(n \cdot m) = g(n) + g(m)$.
2. Conclude that $g(m) = \log_2 m$. (Hint: for any n, let ℓ_n be such that $2^{\ell_n} \leq m^n \leq 2^{\ell_n + 1}$, show that $\frac{\ell_n}{n} \leq g(m) \leq \frac{\ell_n + 1}{n}$).
3. Use this to compute the value of $H_2(p, 1 - p)$.
4. Conclude with H_m.