«Calcul formel avancé et applications». Brief lecture notes.

12.09.2024. Lecture 1.

1. The game guess a number : one players chooses an integer number between 1 and n, another player should find this number by asking questions with answers *yes* or *no*. There is a simple strategy that allows to find the chosen number in $\lceil \log_2 n \rceil$ questions (bisection). Moreover, there is a non-adaptive strategy with the same number of questions (the second player asks bits of the binary expansion of the chosen number ; all questions are formulated in advance, before the first response).

These strategies are optimal : no strategy helps to reveal the chosen number in less than $\lceil \log_2 n \rceil$ questions (in the worst case). Indeed, every guessing strategy can be represented as a binary tree (with questions in the internal nodes and the guessed numbers in a leave). Since such a tree must have at least n leaves (one leave for each possible answer), the depth of the tree must be at least $\lceil \log_2 n \rceil$.

2. Weighing problems (finding a counterfeit coin). In the class we discussed several variations of the classic problem of finding a counterfeit coin. In all these problems we assume that there are several identical-looking coins, one of which differs from the others in weight (all other coins have the same weight). We have at our disposal a scale without supplementary weights. With this scale we can compare any two groups of coins and find out whether they differ in weight or not (and if they differ, which group is lighter and which one s heavier).

Example 1. We are given $n = 12$ coins and one if them is fake. It is known that the fake coin is lighter than the genuine ones. How many weighings does it take to find a genuine coin ? It is not hard to see that this requires 3 weighings : there exists a strategy that finds the fake coin in *three* operations, and there is no strategy which does the same in only *two* operations.

Example 2. We are given $n = 12$ coins and one of them is fake. This time the fake coin can be heavier or lighter than the genuine ones. How many weighings does it take to find a genuine coin ? In the class we found out that the fake one can be found in *four* weighings, and that *two* operations is not enough.

Exercise 1. What is the number of weighings required to find among 12 coins the fake one (which can be heavier or lighter than the genuine ones) ? *Hint :* improve the lower bound 3 or the upper bound 4 proven in the class.

Example 3. We are given $n = 14$ coins, and again one fake coin can be heavier or lighter than the genuine ones. How many weighings does it take to find a genuine coin ? In the class we proved that there exists a strategy that finds the fake coin in *four* operations.

Exercise 2. Prove that there is no strategy which finds among 14 coins the fake one in *three* operations. *Hint :* Use the notion of entropy, see the next section.

3. Shannon's entropy. For a random variable α with n possible values $a_1, \ldots, a_n$ such that for $i = 1 \ldots n$ $\mathrm{Prob}[\alpha = a_i] = p_i$, we define its Shannon's entropy as

$$H(\alpha) := \sum_{i=1}^{n} p_i \log \frac{1}{p_i}$$

(with the usual convention $0 \cdot \log \frac{1}{0} = 0$).

In the class we proved :

Proposition 1. *For every random variable α distributed on a set of n values*

$$H(\alpha) \geq 0$$

Moreover, $H(\alpha) = 0$ *if and only if the distribution is concentrated at one point* (*one probability* p_i *is equal to* 1*, and the other* p_j *for* $j \neq i$ *are equal to* 0).

Proposition 2. *For every random variable* α *distributed on a set of* n *values*

$$H(\alpha) \leq \log n.$$

Moreover, $H(\alpha) = \log n$ *if and only if the distribution is uniform* ($p_1 = \ldots = p_n = \frac{1}{n}$).

4. The game guess a number revisited : one players chooses an integer number between 1 and n with known probabilities $p_1, \ldots, p_n$, another player should find this number by asking questions with answers *yes* or *no*. We need to estimate the *average* number of questions needed to identify the number.

In the class we discussed a bisection strategy that requires *on average* $\approx \sum\limits_{i=1}^{n} p_i \log \frac{1}{p_i}$ questions (but a more precise statement and a formal proof is postponed).

Theorem 1. Every strategy of guessing a number with yes-or-no questions requires *at least*

$$\sum_{i=1}^{n} p_i \log \frac{1}{p_i}$$

questions on average.

Idea of the proof : concavity of the logarithm and Jensen's inequality (more details in the class).

Theorem 2. For every distribution of probabilities $(p_1, \ldots, p_n)$ there exists a strategy of guessing a number with yes-or-no questions with *less than*

$$\sum_{i=1}^{n} p_i \log \frac{1}{p_i} + 1$$

questions on average.

Idea of the proof : We let $\ell_i := \left\lceil \log \frac{1}{p_i} \right\rceil$ and construct a strategy which requires ℓ_i questions to reveal that the chosen number is i. At first we show that

$$\sum 2^{\ell_i} \leq 1. \qquad (*)$$

Then we use Ineq. (*) to prove that there exists a binary tree with n leaves where the path from the root to the leaf no. i is of length ℓ_i. A combination of these two facts implies the theorem.

Exercise 3 (optional)**.** Show that for some distributions $(p_1, \ldots, p_n)$ the expression

$$\sum_{i=1}^{n} p_i \left\lceil \log \frac{1}{p_i} \right\rceil$$

is strictly greater than the optimal average number of questions in a strategy of guessing a number with yes-or-no questions.