Veritasium combinatorics problem

Othman SLASSI

I. INTRODUCTION

We will find the probability p of success in the procedure explained in Veritasium for the general case: $2n$ boxes and $2n$ prisoners. I tried to be as thorough as possible by not omitting any detail but I did not present a proof of the number of cyclic permutations of p elements among N elements (equals to $\dfrac{A_N^p}{p}$) which is a will known result.

II. SOLUTION

A. Definitions

Definition 1 (Cycle) *Let $a \in \{1, 2 \cdots 2n\}$ the cycle of a is the set $C(a) = \{\sigma^k(a) \mid k \in \mathbb{N}\}$*
The number $l(a) = |C(a)|$ is the length of the cycle.

Definition 2 (Measure) *Let $\sigma \in S_{2n}$ the number $\mu(\sigma) = \max\limits_{1 \le a \le 2n}(|C(a)|)$ is the measure of permutation σ*

B. A better description

Every way of distributing the cards in the boxes is a permutation $\sigma \in S_{2n}$ so opening the box number a will show the card number $\sigma(a)$. The probability p that "the procedure described in Veritasium will work" is actually the number of permutations σ such that: $\mu(\sigma) \le n$ divided by $(2n)!$. The complement $q = 1 - p$, which is the probability of having at least an element a such that $l(a) \ge n+1$, is easier to calculate, we will call such an element **long**.

C. Lemmas

Lemma 1 *If a permutation σ has a long element a then it has $l(a)$ long elements and they have the same length.*
Proof: *If there exists a long element a then every element of the cycle $C(a)$ is long and has the same length. Furthermore the set $A := \overline{C(a)}$ has at most $n-1$ elements. So obviously: $\forall b \in A$ we have $l(b) \le n-1$ thus only the elements of $C(a)$ are long.*$\square$

Lemma 2 *let $1 \le k \le n$ and the set $E_k := \{\sigma \in S_{2n} \mid \mu(\sigma) = n+k\}$ We have : $|E_k| = \frac{(2n)!}{n+k}$*
Proof: *Let $\sigma_k \in E_k$ be permutation since it has a long element, then according to lemma 1 there is a unique cycle C_k with all the long elements (Note that: $|C_k| = n+k$ in this case).*
So every permutation in E_k determined by the choice of a cyclic permutation of $n+k$ elements (representing C_k) among $2n$ and a random permutation of the remaining $n-k$ elements. So: $|E_k| = (n-k)!\dfrac{A_{2n}^{n+k}}{n+k} = \dfrac{(2n)!}{n+k}$ $\square$

D. The final proof

$(E_k)_{1 \le k \le n}$ is a partition of the set E of permutations with at least one long element.

$$q = P(\sigma \in E) = \frac{|E|}{(2n)!} = \frac{1}{(2n)!}\sum_{k=1}^{n}|E_k| = \frac{1}{(2n)!}\sum_{k=1}^{n}\frac{(2n)!}{n+k} = \sum_{k=1}^{n}\frac{1}{n+k}$$

$$\boxed{p = 1 - \sum_{k=1}^{n}\frac{1}{n+k}}$$