1 Monty Hall Challenge

Let us take on the challenge posed in lecture, and formally analyze the Monty Hall Problem.

(a) Assume that the corgi (the prize) and two goats were placed uniformly at random behind the three doors. What is the probability space $(\Omega, \mathbb{P})$?

(b) If our contestant chose door 1 in the first round, and decides to switch to another door after being shown a goat behind door 2 or 3, what are the events C_1 ="They win the corgi" and $\overline{C_1}$ ="They win a goat"? What are their probabilities $\mathbb{P}(C_1)$ and $\mathbb{P}(\overline{C_1})$?

(c) If the contestant does not switch doors, what are the events $C_2, \overline{C_2}$ of winning the corgi and goats, and their respective probabilities now?

(d) If instead of choosing door 1 in the beginning, they chose a door uniformly at random, how do your $\Omega, \mathbb{P}, C_i, \overline{C_i}$ from above change?

Solution:

(a) The randomness here lies in how the animals were distributed behind the doors. The possible outcomes are collected in the sample space $\Omega = \{CGG, GCG, GGC\}$, where each sequence encodes what animal hides behind which door, e.g. CGG means the corgi is behind door 1, and the goats behind doors 2 and 3. Since we are placing animals uniformly, the probability $\mathbb{P}(\omega)$ of each outcome ω is $1/|\Omega| = 1/3$.

(b) If the corgi sleeps behind door 1, then the contestant can only win a goat after switching. If, however, a goat is behind door 1, then the contestant will always win the corgi after switching, since Carol shows him the other goat! So $C_1 = \{GCG, GGC\}$, while $\overline{C_1} = \Omega \setminus C_1 = \{CGG\}$. As a result, the associated probabilites are $\mathbb{P}(C_1) = 2/3, \mathbb{P}(\overline{C_1}) = 1/3$.

(c) Now the roles of C_1 and $\overline{C_1}$ invert: If the contestant does not switch doors, they can only win if the corgi is behind door 1, i.e. $C_2 = \{CGG\}$ and $\overline{C_2} = \{GCG, GGC\}$. So $\mathbb{P}(C_2) = 1/3, \mathbb{P}(\overline{C_2}) = 2/3$.

(d) Our new sample space Ω' now becomes bigger since the outcomes include the choice of our contestant: $\Omega' = \{1,2,3\} \times \Omega$, where for any element $(i,s) \in \Omega'$, i indicates the choice of door, and s is a sequence of animals as before. Since everything is equally likely, individual probabilites are now $\mathbb{P}(\omega) = 1/|\Omega'| = 1/9$. Regardless of the choice i however, there are still two outcomes in which the contestant wins if he switches, and only one if he doesn't switch. So $|C_1| = 2 \cdot 3 = 6$ and $|C_2| = 1 \cdot 3 = 3$, yielding overall probabilities $\mathbb{P}(C_1) = 2/3, \mathbb{P}(C_2) = 1/3$.

2 Probability Warm-Up

(a) Suppose that we have a bucket of 30 red balls and 70 blue balls. If we pick 20 balls out of the bucket, what is the probability of getting exactly k red balls (assuming $0 \le k \le 20$) if the sampling is done with replacement?

(b) Same as part (a), but the sampling is without replacement.

(c) If we roll a regular, 6-sided die 5 times. What is the probability that at least one value is observed more than once?

Solution:

(a) Since there is replacement, each time we sample, the probability of choosing a red ball is $30/100$. We repeat this sampling independently 20 times. So

$$\mathbb{P}(k \text{ red balls}) = \binom{20}{k}(0.3)^k(0.7)^{20-k}.$$

(b) Let A be the event of getting exactly k red balls. We note that the size of the sample space is $\binom{100}{20}$, since we are choosing 20 balls out of a total of 100. To find $|A|$, we need to be able to find out how many ways we can choose k red balls and $20-k$ blue balls. So we have that $|A| = \binom{30}{k}\binom{70}{20-k}$. So

$$\mathbb{P}(A) = \frac{\binom{30}{k}\binom{70}{20-k}}{\binom{100}{20}}.$$

(c) Let B be the event that at least one value is observed more than once. We see that $\mathbb{P}(B) = 1 - \mathbb{P}(\overline{B})$. So we need to find out the probability that the values of the 5 rolls are distinct. We see that $\mathbb{P}(\overline{B})$ simply the number of ways to choose 5 numbers (order matters) divided by the sample space (which is 6^5). So

$$\mathbb{P}(\overline{B}) = \frac{6!}{6^5} = \frac{5!}{6^4}.$$

So,

$$\mathbb{P}(B) = 1 - \frac{5!}{6^4}.$$

3 Polynomial Probabilities

(a) Let us pick a degree $< p$ polynomial f over $\mathrm{GF}(p)$ uniformly at random. What is the probability space $(\Omega, \mathbb{P})$?

(b) What is the probability that $f(0) = a$ for some fixed $a \in \mathrm{GF}(p)$?

(c) Assume Alice shared a secret with $\text{Bob}_1, \text{Bob}_2$ and Bob_3. That is, she constructed a polynomial g of degree at most 2 with $p(0) = s$. If Bob_1 and Bob_2 got together and made a (uniform) random guess at what Bob_3's value was, what is the probability that they recover s correctly?

Solution:

(a) The outcome of our experiment is a polynomial of degree at most $p-1$, so Ω is simply the set of all such polynomials. Each polynomial $\omega \in \Omega$ has equal chances of being sampled, and so $\mathbb{P}(\omega) = 1/|\Omega| = 1/p^p$ for all $\omega \in \Omega$.

(b) There are exactly p^{p-1} degree $< p$ polynomials whose value at 0 is a. Let us call the set of such polynomials A, then $\mathbb{P}(A) = p^{p-1}/p^p = 1/p$.

(c) There are exactly p degree < 2 polynomials with two points fixed. Each of them has a different value at $x = 0$, since for each $a \in \text{GF}(p)$, we can find a polynomial passing through Bob_1's, Bob_2's points and $(0, a)$. Bob_1 and Bob_2 randomly guessing Bob_3's value is tantamount to choosing one of these polynomials uniformly at random. Hence the probability that $f(0) = s$ is $1/p$. That is, Bob_1 and Bob_2 might as well have tried to guess s directly.