Exercise 5.27 from textbook

(The Monty Hall Problem) Monty Hall gives Dan the choice of three curtains. Behind one curtain is a car, while behind the other two curtains are goats. Dan chooses a curtain, but before it is opened, Monty Hall opens one of the other curtains and reveals a goat. He then offers Dan the option of keeping his original curtain or switching to the remaining closed curtain. The Monty Hall problem is to figure out Dan's best strategy: "To stick or to switch?"

(a) What is the probability that Dan wins the car if he always sticks to his first choice of curtain? What is the probability that Dan wins the car if he always switches curtains? Which is his best strategy? (If the answer seems counter-intuitive, suppose instead that there are 1000 curtains and that Monty Hall opens 998 goat curtains. Now what are the winning probabilities for the two strategies?)

Ans:

- **Probability of Winning if Dan Sticks to His First Choice:** Since there are three curtains and the car is behind one of them, Dan's initial choice has a $\frac{1}{3}$ probability of being correct. If he never switches, he wins the car $\frac{1}{3}$ of the time.
- **Probability of Winning if Dan Switches:** So, Monty Hall always reveals a goat, meaning the other closed curtain has the car whenever Dan initially chose a goat. Since Dan originally picks a goat $\frac{2}{3}$ of the time, switching guarantees a win in those cases. Thus, the probability of winning by switching is $\frac{2}{3}$
- If there are 1000 curtains, then Dan's initial probabilities of choosing the car and a goat are $\frac{1}{1000}$ and $\frac{999}{1000}$ respectively.

  Now, if Monty Hall opens 998 goat curtains, leaving only Dan's chosen curtain and one other curtain, then Dan has only $\frac{1}{1000}$ chances of winnig if he never switches. Otherwise, he has $\frac{999}{1000}$.

All all, the best strategy is to always switch.

(b) Suppose that we give Monty Hall another option, namely he's allowed to force Dan to stick with his first choice of curtain. Assuming that Monty Hall dislikes

giving away cars, now what is Dan's best strategy, and what is his probability of winning a car?

Ans:
If Monty Hall dislikes giving away cars and forces Dan to stick, then his probability of winning remains at $\frac{1}{3}$. In this case, Dan has no control over his odds, and Monty gets to keep more cars.

(c) More generally, suppose that there are N curtains and M cars, and suppose that Monty Hall opens K curtains that have goats behind them

- **Probability of winning if Dan sticks:**

$$Pr(\text{Dan wins a car} \mid \text{Dan sticks}) = \frac{M}{N}.$$

Since Dan chooses randomly among N curtains and M of them have cars, this remains his original probability.

- **Probability of winning if Dan switches:** The conditional probability is given by

$$Pr(\text{Dan wins a car} \mid \text{Dan switches}) = \frac{Pr(\text{Dan win a car} \cap \text{Dan switches})}{Pr(\text{Dan switches})}$$

Since Dan is guaranteed a switch atfer the initial pick, we can take

$$Pr(\text{Dan switches}) = 1$$

So the conditional probability reduces to

$$Pr(\text{Dan wins a car} \mid \text{Dan switches}) = Pr(\text{Dan win a car} \cap \text{Dan switches}).$$

So, we need to consider the following.

* Dan initially picks a goat
* Monty reveals K goat curtains
* Dan switches to a remaining unopened curtain that has a car

Since switching only helps when Dan's first pick was wrong, we need the probability that Dan's initial pick was a goat, and the probability that switching leads to a car.

The probability of initial pick is a goat is $Pr(\text{Goat}) = \frac{N-M}{N}$. After, Monty reveals K goats, there are now $N-K-1$ closed curtains, so the probability that switching leads to a car is $Pr(\text{switch leads to a car}) = \frac{M}{N-K-1}$ Mulltiplying the two probabilities give

$$\begin{aligned} Pr(\text{wins a car} \mid \text{switches}) &= Pr(\text{win a car} \cap \text{switches}) \\ &= Pr(\text{initial pick is a goat}) Pr(\text{switch leads to a car}) \\ &= \frac{M(N-M)}{N(N-K-1)}. \end{aligned}$$

In general, switching is the better strategy, the the probability in this case is alway higher.

Exercise 5.28 from textbook

Let S be a set, let A be a property of interest, and suppose that for $m \in S$, we have

$$Pr(m \text{ does not have property } A) = \delta.$$

Suppose further that a Monte Carlo algorithm applied to m and a random number r satisfy:

(1) If the algorithm returns Yes, then m definitely has property A.

(2) If m has property A, then the probability that the algorithm returns Yes is at least p.

Notice that we can restate (1) and (2) as conditional probabilities:

- $Pr(m \text{ has property } A \mid \text{algorithm returns } Yes) = 1$
- $Pr(\text{algorithm returns } Yes \mid m \text{ has property } A) \geq p$

Suppose that we run the algorithm N times on the number m, and suppose that the algorithm returns No every single time. Derive a lower bound, in terms of δ, p, and N, for the probability that m does not have property A.

Ans

Let

$$\begin{aligned} E &= \{\text{an integer in } S \text{ does not have property } A\} \\ F &= \{\text{the algorithm returns } No \ N \text{ times in a row}\}. \end{aligned}$$

Then, we want to find the probability that m does not have property A, given that the algorithm returned "No" every time. That is $Pr(E \mid F)$. The Bayesian formula says

$$\begin{aligned} Pr(E \mid F) &= \frac{Pr(F \mid E)Pr(E)}{P(F)} \\ &= \frac{Pr(F \mid E)Pr(E)}{Pr(F \mid E)Pr(E) + Pr(F \mid E^c)Pr(E^c)} \end{aligned} \tag{1}$$

We are given that $Pr(E^c) = 1 - \delta$ so, $Pr(E) = \delta$.

Consider $Pr(F \mid E)$. By property (1), we have

$$Pr(\text{returns } No \mid \text{does not have A}) = Pr(\text{has A} \mid \text{returns } Yes) = 1$$

. Since the experiment is run N times, if follows that

$$Pr(F \mid E) = Pr(\text{returns } No \mid \text{does not have A})^N = 1.$$

Next, we have

$$\begin{aligned} Pr(F \mid E^c) &= Pr(\text{returns } No \mid \text{has A})^N \\ &= (1 - Pr(\text{returns } Yes \mid \text{has A}))^N \\ &= \leq (1-p)^N \end{aligned}$$

Substituting everything in Equation (1), we have

$$\begin{aligned} Pr(E \mid F) &\geq \frac{1 \cdot \delta}{1 \cdot \delta + (1-p)^N \cdot (1-\delta)} \\ &= \frac{\delta}{\delta + (1-\delta)(1-p)^N} \end{aligned}$$

The lower bound is $\frac{\delta}{\delta+(1-\delta)(1-p)^N}$.

Exercise 5.30 from textbook

If an integer n is composite, then the Miller–Rabin test has at least a 75% chance of succeeding in proving that n is composite, while it never misidentifies a prime as being composite. Suppose that we run the Miller–Rabin test N times on the integer n and that it fails to prove that n is composite. Show that the probability that n is prime satisfies (approximately)

$$Pr(n \text{ is prime} \mid \text{the Miller–Rabin test fails } N \text{ times}) \geq 1 - \frac{\ln(n)}{4^N}$$

(Hint. Use Exercise 5.28 with appropriate choices of A, S, δ, and p. You may also use the estimate from Sect. 3.4.1 that the probability that n is prime is approximately $\frac{1}{\ln(n)}$).

Theorem 0.0.1 (The Prime Number Theorem [1]). *A randomly chosen number n has probability $\frac{1}{\ln(n)}$ of being prime.*

Answers

Let A be the property ***composite*** and let S be the set of integer. Choose $\delta = \frac{1}{\ln(n)}$ (The prime number theorem) and $p = 0.75$. Suppose a Monte Carlo algorithm applied to an integer $m \in S$ and a witness r satisfy

- $Pr(m \text{ is composite } A \mid \text{Miller-Rabin returns } Yes) = 1$
- $Pr(\text{Miller-Rabin returns } Yes \mid m \text{ is composite}) \geq 0.75$

From Exercise 5.28, we have

$$
\begin{aligned}
Pr(n \text{ is prime}|\text{fails } N \text{ times}) &= Pr(n \text{ is not composite} \mid \text{Miller-Rabin returns No } N \text{ times}) \\
&\geq \frac{1}{\ln(n)} \Big/ \left(\frac{1}{\ln(n)} + \left(1 - \frac{1}{\ln(n)}\right) \left(\frac{1}{4}\right)^N \right) \\
&= 1 - \frac{\ln(n) - 1}{4^N + \ln(n) - 1} \\
&\geq 1 - \frac{\ln(n)}{4^N}.
\end{aligned}
$$

Bibliography

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics. Springer, second edition, 2014. ISBN 978-1-4939-1710-5.