Lab 8: Probability & Number Theory

CSCI104

Definitions

- We have a fair coin. We flip it 2 times. What is the probability of getting at least one head?
- **Trial:** flipping a coin 2 times
- **Sample space:** set of all possible outcomes for any trial
- **Size of out sample space:** $|H,T|^2 = 4.$
- **Event:** any subset of the sample space

- HH
- HT
- TH
- TT

$$3/4.$$

Definitions Continued

- S = sample space of equally likely outcomes
- E = event of S
- THEN, the probability of E is:

$$\boxed{P(E) = \frac{|E|}{|S|}}$$

Complements

- **Complement:** probability the event DOESN'T occur
  - Event = E
  - Complement = $\bar{E}$,
- **Complement rule:** the probability of an event and its complement should add up to 1 $$P(\bar{E}) = 1 - P(E)$$
- Sometimes easier to first compute complement
  - What is the probability of at least one head?
  - $1 - 1/4 = 3/4.$

- HH
- HT
- TH
- TT

Complement

Sum Rule

- Given a sequence of pairwise disjoint (mutually exclusive) events E1, E2, E3, the probability of these events occurring is the sum of the probability of each event: $P(E_1 \cup E_2 \cup E_3 \cup \ldots) = P(E_1) + P(E_2) + P(E_3) + \ldots$

Events $\boldsymbol{E}_i$ and $\boldsymbol{E}_j$ are mutually exclusive if $\boldsymbol{E}_i \cap \boldsymbol{E}_j = \emptyset$. In other words, they cannot occur at the same time.

Sum Rule Example

- Suppose we draw a card from a standard deck of cards
- What is the probability that the card we draw is a **king** or **queen**?

Solution: let event E_1 be the event of getting a Queen, and event E_2 be the event of getting a King. There are 4 Queens and 4 Kings in a standard deck of 52 cards, so $P(E_1) = 4/52$, and $P(E_2) = 4/52$. Thus, the probability of drawing a Queen or King is $4/52 + 4/52 = 8/52$.

Subtraction Rule

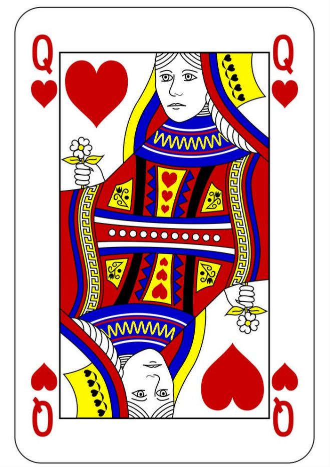
- Also called the inclusion-exclusion principle
- Used when we want to compute the probability of union of events that are not mutually exclusive

$$\boxed{P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)}$$

Subtraction Rule Example

- Suppose we draw a card from a standard deck of cards
- What is the probability that the card we draw is a **queen** or **heart**?

Solution: let event E_1 be the event of getting a Queen, and event E_2 be the event of getting a Heart. These two events are no longer mutually exclusive: both events can occur simultaneously if we draw a Queen of hearts. There are 4 Queens, 13 Hearts, and 1 Queen of hearts in a standard deck of 52 cards. Thus, $P(E_1) = 4/52$, $P(E_2) = 13/52$, and $P(E_1 \cap E_2) = 1/52$. Thus, the probability of drawing a Queen or Heart is $4/52 + 13/52 - 1/52 = 16/52$.



Conditional Probability

- Means the probability of an event occurring, given another event
- "The probability of B given A"

$$\boxed{P(B|A) = \frac{P(A \cap B)}{P(A)}}$$

INDEPENDENCE

- If likelihood of B occurring does not depend on A $\boxed{P(B \mid A) = P(B).}$

Conditional Probability Example

"The probability of B given A"

- We draw a card from deck
- We know card is face (A)
- What is the probability the card is a king? (B)

First, let's compute P(A). There are 52 cards in a deck. Each deck has 13 ranks, 3 of which have "faces" (Jack, Queen, King). Each rank comes in 4 suits, yielding a total of 3 * 4 = 12 face cards in a deck. Thus, assuming a well shuffled deck where all outcomes are equally likely, the probability of event A is 12/52.

Next, we need to compute P(A ∩ B). Of the 12 possible face cards one can draw, 4 are Ks. P(A ∩ B), the probability of drawing a face card AND a K, is 4/52.

Finally, we can compute P(B): (4/52)/(12/52) = 4/12 = 1/3

Random Variables

- A mapping from the sample space to set of real numbers
- Flipping 2 coins
  - Sample space has 4 elements
  - Random variable X denotes the number of heads in each outcome

- $X(HH) = 2$
- $X(HT) = 1$
- $X(TH) = 1$
- $X(TT) = 0$

Probability distribution of random variable X

- $P(X = 0) = 1/4$
- $P(X = 1) = 2/4$
- $P(X = 2) = 1/4$

Expectation

- Random variable X
- **Expected value** of X is E(X), the weighted average of X

$$E(X) = \sum_{s \in S} P(s) \cdot X(s)$$

- Linearity of expectation: to calculate the expectation of a sum of random variables

$$E(X_1 + \cdots + X_n) = E(X_1) + \cdots + E(X_n)$$

- Multiplying a random variable by a scalar constant multiplies its expected value by that constant
- Adding a constant to a random variable adds that constant to its expected value

value. For random variable $\boldsymbol{X}$ and constants $\boldsymbol{a}$ and $\boldsymbol{b}$:

$$E(aX + b) = a \cdot E(X) + b$$

Both of the above holds even if random variables are not independent!

Expectation Example

- We roll 2 fair dice. Let X be the sum of each roll. What is E(X)?

Solution: the probability distribution of X is:

- $P(X=2)=1/36$
- $P(X=3)=2/36$
- $P(X=4)=3/36$
- $P(X=5)=4/36$
- $P(X=6)=5/36$
- $P(X=7)=6/36$
- $P(X=8)=5/36$
- $P(X=9)=4/36$
- $P(X=10)=3/36$
- $P(X=11)=2/36$
- $P(X=12)=1/36$

But there is really a simpler way to solve this:

Let X_1, X_2 be random variables that denote the value on the first and second die, respectively. We can see that $X = X_1 + X_2$, therefore by the linearity of expectation, $E(X) = E(X_1 + X_2) = E(X_1) + E(X_2)$.

We know that $E(X_1) = E(X_2) = \frac{1}{6}(1+2+3+4+5+6)$, hence $E(X) = 7$.

Thus:

$E(X) = 2 \times (1/36) + 3 \times (2/36) + \ldots + 12 \times (1/36) = 7$.

Basic Number Theory

- **$m \mid n$**
  - Reads as "m divides n," which means that there exists a number k such that $n = km$
- **$a \equiv b \pmod{m}$**
  - "a is congruent to b modulo m," which means that

    $m \mid a - b$

Basic Number Theory, pt. 2

- **If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,**
  - $ac \equiv bd \pmod{m}$
    - $m \mid ac - bd$
  - $a + c \equiv b + d \pmod{m}$
    - $m \mid a + c - b - d$
- **gcd(a, b)**
  - "Greatest common divisor between a and b," which is *d* such that $d \mid a$ and $d \mid b$
  - If $d = 1$, then a and b are "co-prime" or relatively prime to each other

Fermant Little Theorem

- Fermat's little theorem states that given a prime number p, and another number a which is NOT a multiple of p, we have:
$$a^{(p-1)} \equiv 1 \pmod{p}$$
- This basically means that if we are given a number n, and we can find an a such that $a^{(p-1)} \; ! \equiv 1 \pmod{n}$, then n is NOT prime
- If we test a lot of numbers and they all come out ≡ 1 (meaning it can only be divided by 1), we can have high confidence that the number is prime, (but we won't be 100% certain!)

Check Off

1. Start with probability questions (4)
2. Next, move to number theory coding exercise about Fermat Theorem (skeleton available on GitHub)
3. Show answer to probability questions and passing coding tests