Probability and Independence

Michael L. Littman

CS 0220 2021

July 14, 2021
Overview

Independence (17.6)
Alternative Formulation (17.6.1)
Mutual Independence (17.6.3)
Conditional probability

**Definition:** The conditional probability of event $A$ given event $B$ is:

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]}.$$ 

Conceptually, if we limit ourselves to the outcomes in $B$, how likely is an outcome in $A$?

**Example:**

- $A$: Die shows a number divisible by 3. $\Pr[A] = 1/3$. (3 and 6 from the six possibilities.)
- $B$: Die shows an odd number. $\Pr[B] = 1/2$.
- What does $\Pr[A \cap B]$ mean? Die shows an odd number divisible by 3. $\Pr[A \cap B] = 1/6$ (only 3).
- What does $\Pr[A|B]$ mean? Die shows a number divisible by 3 given that it’s odd. $\Pr[A|B] = 1/3$ (probability of picking 3 from 1, 3, 5). Also, $\frac{1/6}{1/2} = \frac{1}{6} \times 2 = \frac{1}{3}$. 
**Independence**

**Definition:** Event $A$ is *independent of* event $B$ iff

$$Pr[A|B] = Pr[A].$$

If $Pr[B] = 0$, we say it is independent of any other event including itself.

**Example:**

- $A$: Die shows the maximum or minimum number. $Pr[A] = 1/3$. (1, 6 from the six possibilities.)
- $B$: Die shows an odd number. $Pr[B] = 1/2$.
- $Pr[A|B] = 1/3$. (1 from 1,3,5.) So, $A$ and $B$ are independent.
- $C$: Die shows an even number. $Pr[C] = 1/2$.
- Are $B$ and $C$ independent? No, $Pr[C|B] = 0 \neq Pr[C]$.

Common misconception. Independent does not mean disjoint.
**Theorem:** A is independent of $B$ iff

$$ \Pr[A \cap B] = \Pr[A] \cdot \Pr[B]. $$

**Proof:** By cases.

- **Case 1:** If $\Pr[A] = 0$ or $\Pr[B] = 0$, then $\Pr[A \cap B] = 0$. Equality and independence are both achieved.

- **Case 2:** Otherwise, $A$ is independent of $B$ iff $\Pr[A|B] = \Pr[A]$ by definition. Substituting in the definition of conditional probability, we have $\Pr[A|B] = \Pr[A]$ iff

  $$ \frac{\Pr[A \cap B]}{\Pr[B]} = \Pr[A]. $$

  Multiplying both sides by $\Pr[B]$, we have $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$. QED.
Mutual Independence

**Definition:** A set of events $E_1, E_2, \ldots, E_n$ is *mutually independent* iff for all subsets $S \subseteq [1, n],$

$$\Pr \left[ \bigcap_{j \in S} E_j \right] = \prod_{j \in S} \Pr[E_j].$$

Example: If we toss $n$ fair coins, the tosses are mutually independent iff for every subset of $m$ coins, the probability that every coin in the subset comes up heads is $2^{-m}$. 
Independent missions

<table>
<thead>
<tr>
<th>Mission</th>
<th>Type</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mars</td>
<td>one-time</td>
<td>0.028</td>
</tr>
<tr>
<td>Mars</td>
<td>robot</td>
<td>0.042</td>
</tr>
<tr>
<td>Mars</td>
<td>reusable</td>
<td>0.252</td>
</tr>
<tr>
<td>Mars</td>
<td>robot</td>
<td>0.378</td>
</tr>
<tr>
<td>Moon</td>
<td>one-time</td>
<td>0.012</td>
</tr>
<tr>
<td>Moon</td>
<td>robot</td>
<td>0.018</td>
</tr>
<tr>
<td>Moon</td>
<td>reusable</td>
<td>0.108</td>
</tr>
<tr>
<td>Moon</td>
<td>robot</td>
<td>0.162</td>
</tr>
</tbody>
</table>

\[
\Pr[\text{Mars}] = 0.028 + 0.042 + 0.252 + 0.378 = 0.7
\]
\[
\Pr[\text{one-time}] = 0.028 + 0.042 + 0.012 + 0.018 = 0.1
\]
\[
\Pr[\text{person}] = 0.028 + 0.252 + 0.012 + 0.108 = 0.4
\]
\[
\Pr[\text{Mars AND one-time}] = 0.028 + 0.042 = 0.07 = 0.7 \times 0.1
\]
\[
\Pr[\text{Mars AND person}] = 0.028 + 0.252 = 0.28 = 0.7 \times 0.4
\]
\[
\Pr[\text{one-time AND person}] = 0.028 + 0.012 = 0.04 = 0.1 \times 0.4
\]
\[
\Pr[\text{Mars AND one-time AND person}] = 0.028 = 0.7 \times 0.1 \times 0.4
\]
Pairwise independence isn’t mutual independence

If $A$ is independent of $B$ and $C$, and $B$ and $C$ are independent of each other, how could $A$, $B$, and $C$ not be independent??

Example: Morley, Kyran, and Will each pick a bit 0/1 uniformly at random.

- $A$: Morley + Kyran $\equiv 1 \pmod{2}$
- $B$: Morley + Will $\equiv 1 \pmod{2}$
- $C$: Kyran + Will $\equiv 1 \pmod{2}$

Claim 1: These events are all pairwise independent.

For example, $\Pr[A] = 1/2$. $\Pr[A|B] = \frac{1}{4}/\frac{1}{2} = 1/2$.

Claim 2: These events are not mutually independent.

$\Pr[A \cap B \cap C] = 0$. Not $1/8$!

$k$-wise does not imply $(k + 1)$-wise mutual independence.