Brandon Szeto
Professor Kenneth Zeger
ECE 109

Week 3, Lecture 01-24-23

Example: Flip a coin twice

$$S = \{HH, HT, TH, TT\}$$

Let us define the events:

$$E = \text{"First flip is heads"} = \{HH, HT\}$$
$$F = \text{"Flips are different"} = \{HT, TH\}$$
$$P(E) = \frac{2}{4} = \frac{1}{2}$$
$$P(E|F) = \frac{P(EF)}{P(F)} = \frac{P(\{HT\})}{P(\{HT, TH\})}$$
$$= \frac{\frac{1}{4}}{\frac{2}{4}} = \frac{1}{2}$$

So, in this case,

$$P(E) = P(E|F) = \frac{1}{2}$$
$$\rightarrow E, F \text{ are independent}$$

Let's multiply both sides by $P(F)$:

$$P(E)P(F) = P(E|F)P(F) = P(EF)$$

i.e. $P(EF)$ factors into $P(E)P(F)$. If $P(F) \neq 0$, then this implies $P(E|F) = P(E)$.

Definition: Events E, F are independent if $P(EF) = P(E)P(F)$.

Consequences: If E, F are independent, then

1. E, F^c are independent
2. E^c, F are independent
3. E^c, F^c are independent

Proof of 1: Assume $P(E) \neq 0$.

$$P(EF^c) = P(E)P(F^c|E)$$
$$= P(E)(1 - P(F|E))$$
$$= P(E)(1 - P(F))$$
$$= P(E)P(F^c)$$
$$\rightarrow E, F^c \text{ are independent}$$

Disjoint versus Independence

Suppose E, F are disjoint and $P(E) \neq 0$ and $P(F) \neq 0$.

$$\therefore EF = 0$$
$$P(EF) = P(0) = 0$$
$$P(E)P(F) \neq 0$$
$$\therefore P(EF) \neq P(E)P(F)$$
$$\rightarrow P(E) \neq 0 \text{ but } P(E|F) = 0$$

.

Example: Given two inputs x and y, the output of an XOR gate z is 1 if and only if $x \neq y$

$$x, y, z \in \{0, 1\}$$

Suppose x and y are chosen with equal probability $\frac{1}{2}$ and independently. Let us define the events:

$$\begin{aligned} A &== x = 1 \\ B &== y = 1 \\ C &== z = 1 \end{aligned}$$

By assumption A, B are independent events.

$$\begin{aligned} P(A) = P(B) &= \frac{1}{2} \\ C &= AB^c \cup A^cB \\ P(C) &= P(AB^c \cup A^cB) \\ &= P(AB^c) + P(A^cB) \\ &= P(A)P(B^c) + P(A^c)P(B) \\ &= \frac{1}{2} * \frac{1}{2} + \frac{1}{2} * \frac{1}{2} \\ AC &== x = 1 \text{ and } z = 1 \\ &== x = 1, y = 0, z = 1 \\ &== x = 1, y = 0 \\ &== AB^c \\ P(AC) &= P(AB^c) = P(A)P(B^c) = \frac{1}{2} * \frac{1}{2} = \frac{1}{4} \\ \therefore P(AC) &= P(A)P(C) \\ &\rightarrow A, C \text{ are independent} \end{aligned}$$

Also by symmetry, B, C are independent. But A, C (also B, C) are **not** physically indepent. It is very clear that they are part of the same XOR gate.

> **Definition:** Events A, B, C are **independent** if all of the following are true:
> 1) A, B are independent
> 2) B, C are independent
> 3) A, C are independent
> 4) $P(ABC) = P(A)P(B)P(C)$

Note: If A, B, C are pairwise independent, then

$$P(ABC) = P(A)P(B)P(C)$$

is equivalent to $P(A|BC) = P(A)$ since:

$$\begin{aligned} P(A|BC)P(BC) &= P(A)P(BC) \\ P(ABC) &= P(A)P(B)P(C) \end{aligned}$$

It is possible to satisfy pairwise independence (conditions numbers 1, 2, and 3), but not condition number 4. Consider the XOR example.

$$\begin{aligned} ABC &== x = 1, y = 1, z = 1 = 0 \\ P(ABC) &= P(0) = 0 \end{aligned}$$

But $P(A)P(B)P(C) = \frac{1}{2} * \frac{1}{2} * \frac{1}{2} = \frac{1}{8} \neq 0$

$$\therefore \text{ condition number 4 is not satisfied.}$$

$$\therefore A, B, C \text{ are pairwise independent but } A, B, C \text{ are } \textbf{not} \text{ independent}$$

> **Definition:** Events A, B are **conditionally independent given event C**, if:
> $$P(AB|C) = P(A|C)P(B|C)$$
> assuming $P(C) \neq 0$

Note: If A, B are independent given C, then:

$$P(A|BC) = \frac{P(ABC)}{P(BC)} = \frac{P(AB|C)P(C)}{P(B|C)P(C)}$$
$$= P(A|C)$$

This is similar to $P(A|B) = P(A)$ but with the extra "given C".

Example: Flip 2 coins

Let us define the events:

$$A = \text{"First coin is heads"}$$
$$B = \text{"Second coin is heads"}$$
$$C = \text{"First and second coin are both heads"}$$

Note: $C = AB$

1. A, B are independent (by assumption)

   $$P(A|C) = \frac{P(AC)}{P(C)} = \frac{P(AAB)}{P(C)} = \frac{P(AB)}{P(C)} = \frac{P(C)}{P(C)} = 1$$

2. $$P(A|BC) = \frac{P(ABC)}{P(BC)} = \frac{P(C)}{P(C)} = 1$$

   $\therefore P(A|C) = P(A|BC) = 1$

   $\rightarrow A, B$ are independent given C.

   $$P(A|C^c) = \frac{P(AC^c)}{P(C^c)} = \frac{P(HT)}{1 - P(HH)} = \frac{\frac{1}{4}}{1 - \frac{1}{4}} = \frac{1}{3} \frac{P(C)}{P(C)} = 1$$

3. $$P(A|BC^c) = \frac{P(ABC^c)}{P(BC^c)} = \frac{P(0)}{P(TH)} = 0$$

   $\therefore P(A|C^c) \neq P(A|BC^c)$

   $\rightarrow A, B$ are **not** independent given C^c.

Example: Let a sample space of equiprobable outcomes be:

$$S = \{1, 2, 3, 4, 5\}$$

Let us define the events:

$$A = \{1, 2, 5\}$$
$$B = \{1, 3, 5\}$$
$$C = \{1, 2, 3, 4\}$$

1. We know $P(A)$ and $P(B)$ are not independent from the following:

$$\begin{aligned}
P(AB) &= P(\{1,5\}) = \frac{2}{5} \\
P(A) &= P(B) = \frac{3}{5} \\
P(AB) &\neq P(A)P(B) \\
&\rightarrow A, B \textbf{ not } \text{independent}
\end{aligned}$$

2. However, given C, this changes

$$\begin{aligned}
P(AB|C) &= P(\{1,5\}|\{1,2,3,4\}) = \frac{1}{4} \\
P(A|C) &= P(\{1,2,5\}|\{1,2,3,4\}) = \frac{2}{4} = \frac{1}{2} \\
P(B|C) &= P(\{1,3,5\}|\{1,2,3,4\}) = \frac{2}{4} = \frac{1}{2} \\
\therefore P(AB|C) &= P(A|C) * P(B|C) \\
&\rightarrow A, B \text{ are independent given } C.
\end{aligned}$$