System Security Group | Lancaster University

What Are Events?

System Security Group | Lancaster University

Sample Space S={}

- The sample space defines everything that can happen:
- Discrete:
  - Written as a list $S = \{a, b, c\}$
- Continuous:
  - Measurement of a continuous variable i.e. height
  - Written as $S = (0,10)$ for open interval $0 < x < 10$
  - Written as $S = [0,10]$ for closed interval $0 \le x \le 10$

Events

- Events are what we observe and are subsets of S.
- The event is said to occur if an element of the event is measured.
- As events are sets then set operations apply to them
  - $A \cup B$: A or B occurs
  - $A \cap B$: A and B occur
  - $S - A$ or $\bar{A}$: not A occurs
  - $A = \emptyset$: The impossible event
  - $A = S$: The certain event

Axioms of Probability

- $P(A)$ is the probability of the event $A \subseteq S$
- This assigns a probability to an event
- Axioms
  1. The certain event S has probability = 1: $P(S) = 1$
  2. All probabilities are positive: $P(A) \geq 0$
  3. Additional rule: if A and B are disjointed such that $A \cap B = \emptyset$ then: $P(A \cup B) = P(A) + P(B)$

Axioms of Probability

4. Complement rule: $P(S - A) = 1 - P(A)$
5. $P(\emptyset) = 0$
6. If $A \subseteq B$ then $P(A) \leq P(B)$
7. General Addition Rule:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Consider this through a Venn diagram. The overlap cannot count twice.

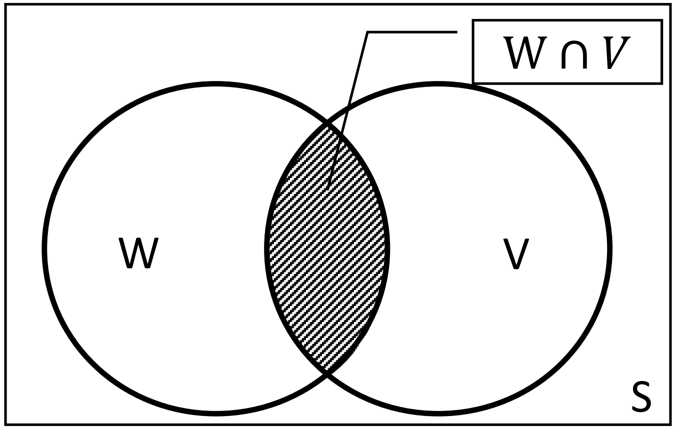
Example Problem

- During an analysis of machines on a network it is found that 80% of them were infected with a worm, 50% infected with a virus and that 40% infected with both. Find the probabilities of:
  1. A machine has either a worm OR a virus
  2. A machine has a worm but NOT a virus
  3. A machine is not infected.

Example Solution 1

Let W and V denote worm and virus infection respectively.

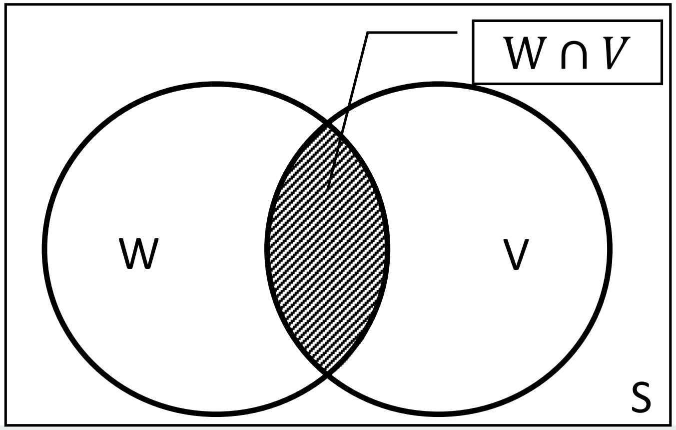
1. This is relatively easy as we can use the General addition rule. Therefore,
   $P(W \cup V) = P(W) + P(V) - P(W \cap V)$
   $= 0.8 + 0.5 - 0.4 = 0.9$



Example Solution 2

2. The group of machines with a worm includes those that have both and those with just a worm. Therefore, to find event where there are just those with a worm and no virus we need to know: $E = \{x : x \in (W \cap \bar{V})\}$

$$P(W \cap \bar{V}) = \mathrm{P(W)} - \mathrm{P(W} \cap V) = 0.8 - 0.4 = 0.4$$



Example Solution 3

3. Use De Morgan's Law and the answer from 1.

$$P(\overline{W} \cap \overline{V}) = P(\overline{W \cup V})$$
$$P(\overline{W \cup V}) = 1 - P(W \cup V)$$
$$= 1 - \left(P(W) + P(V) - P(W \cap V)\right)$$
$$= 1 - 0.8 - 0.5 + 0.4 = 0.1$$

System Security Group | Lancaster University

Questions?

System Security Group | Lancaster University

Conditional Probabilities

System Security Group | Lancaster University

Conditional Probability

- This allows us to deal with a probability if we know an event has already occurred
- What is the probability of event A GIVEN that event B has already occurred. $P(A|B)$
- We effectively have to scale the sample space to B, therefore:

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

Where $B \neq \emptyset \ \therefore P(B) > 0$

Conditional Probability Flipping

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

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

Therefore

$$P(B|A)P(A) = P(A|B)P(B) = P(A \cap B)$$

Simple Example

- Probability that a fair dice role is even given that the result is less than 4.

$$R = \{1,2,3,4,5,6\}, P(R) = \tfrac{1}{6}$$

$$P(Even| < 4) = \frac{P(even \; \& < 4)}{P(< 4)}$$

$$E_{even\&<4} = \{x: x \in R, x < 4, x \; is \; even\} = \{2\}$$

$$E_{<4} = \{x: x \in R, x < 4\} = \{1,2,3\}$$

$$= \frac{P(\{2\})}{P(1,2,3\})} = \frac{\frac{1}{6}}{3 \times \frac{1}{6}} = \frac{1}{3}$$

Another Example

The probability of a machine being on the Internet is $P(I) = 0.92$. The probability it has a virus is $P(V) = 0.82$. The probability it has a virus and is on the Internet is $P(V \cap I) = 0.78$

1. Probability it has a virus given it is on the Internet, $P(V|I)$
2. Probability it does not have a virus given it is not on the Internet, $P(\bar{V}|\bar{I})$

Another Example Solution 1

1. Simple conditional probability:

$$P(V|I) = \frac{P(V \cap I)}{P(I)}$$

$$= \frac{0.78}{0.92} = 0.85$$

Another Example Solution 2

2. A bit more complicated!

$$P(\bar{V}|\bar{I}) = \frac{P(\bar{V} \cap \bar{I})}{P(\bar{I})}$$

$$P(\bar{V} \cap \bar{I}) = P(\overline{V \cup I})$$

$$P(\overline{V \cup I}) = 1 - \mathrm{P}(\mathrm{V} \cup I)$$

$$P(V \cup I) = P(V) + P(I) - P(V \cap I)$$

$$\therefore \; P(\bar{V}|\bar{I}) = \frac{1 - P(V) - P(I) + P(V \cap I)}{1 - P(I)}$$

$$= \frac{1 - 0.83 - 0.92 + 0.78}{1 - 0.92} = \frac{0.03}{0.08} = 0.38$$

Independence

- The probability of event B may be raised, lowered or stay the same, given A has occurred.
- If it stays the same they are independent
  - $P(B|A) = P(B)$
  - $P(A|B) = P(A)$
- Independence is symmetric between two events

Bayes and Bayesian Theory

- Bayes’ theorem gives the relationship between P(A) and P(B), and P(A|B) and P(B|A).
- Enables us to update a probability given an observation.
  - The *prior probability*, is what we have before
  - The *posterior probability*, is what we get afterwards

Bayesian Example

- Example: 10% of all hosts have a security flaw. A screening procedure positively identifies security flaws 80% of the time and 10% of unflawed machines are incorrectly identified.
- Identify the probability that a machine has a flaw given the machine has tested positive for a flaw.

Bayesian Example Solution

- Consider the probabilities as frequencies:
  - Consider a sample space of 1000 machines
  - $P(F) = 0.1$ have flaws, therefore 100 machines
  - $P(\bar{F}) = 0.9$ are unflawed, therefore 900 machines
  - $P(+T|F) = 0.8$, 80 out of 100 flawed machines test positive.
  - $P(+T|\bar{F}) = 0.1$, 90 out of 900 unflawed machines test positive.
  - 170 Positive tests
  - Therefore $P(F|T) = \frac{80}{170} = 47\%$

Bayes Theorem

- The general theorem is:

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

- Applying the law of total probability:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|\bar{A})P(\bar{A})}$$

Suggest you read: http://arbital.com/p/bayes_rule_guide

System Security Group | Lancaster University

Questions?