SIM Global Education

UOW AUSTRALIA

# CSCI262 – SYSTEM SECURITY

## Bayesian Probability

14 October 2022

# Bayesian Probability

**Bayesian inference** is a method of statistical inference in which Bayes' theorem is used to update the probability for a hypothesis as more evidence or information becomes available.

Bayesian inference is an important technique in statistics, and especially in mathematical statistics.

Bayesian updating is particularly important in the dynamic analysis of a sequence of data.

Bayesian inference has found application in a wide range of activities, including science, engineering, philosophy, medicine, sport, and law.

In the philosophy of decision theory, Bayesian inference is closely related to subjective probability, often called "Bayesian probability".

Source: https://en.wikipedia.org/wiki/Bayesian_inference, Referenced on 22 Jan 2018

# Bayesian Probability – Example

Some example:

The accuracy of a malware checker is 95%, meaning the malware checker will correctly identify a message as viral 95% of the time and the malware checker will correctly identify a message as non-viral 95% of the time. The incidence of malware attachments in email messages is 0.125%, that is 1 in 800 email messages is a malware. This is the base-rate. The malware checker has just flagged a message as being a malware. What is the probability that the message is actually clean (not a malware)? Justify your answer.

# Bayesian Probability – Example

- According to Baye’s theorem, the probability of event A occurs given that event B has already occurred is given by the formula:

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

- Let A be the event that the message is clean, and
- Let B be the event that the message is flagged as malware.

# Bayesian Probability – Example

- The probability that the message is clean $P(A) = 100\% - 0.125\%\ (the\ base\ rate)$, that is,

$$P(A) = P(Message\ is\ clean) = 1 - 0.00125 = 0.99875.$$

- The probability that the message is **flagged** as malware given that the message is actually clean $P(B|A)$ is 100% - 95%, this is because the malware checker is able to correctly flag a malware 95% of the time, that is,

$$P(B|A) \\ = P(Message\ is\ flagged\ as\ malware\ given\ that\ message\ is\ clean) \\ = 1 - 0.95 = 0.05.$$

# Bayesian Probability – Example

- The probability that the message is malware $P(B)$ is the sum of:
  1. The probability the message is flagged as malware when the message is actually malware (that is, the message is correctly flagged); that is $P(B|\bar{A})P(\bar{A})$
  2. The probability the message is flagged as malware when the message is actually clean (that is, the message is incorrectly flagged); that is $P(B|A)P(A)$.

# Bayesian Probability – Example

- Hence, P(B) the probability that the message is flagged as malware is

$$P(B)$$

$$= P\begin{pmatrix} the\ message\ is\ flagged\ as\ malware\ when \\ the\ message\ is\ malware \end{pmatrix} +$$

$$P\begin{pmatrix} the\ message\ is\ flagged\ as\ malware\ when \\ the\ message\ is\ clean \end{pmatrix}$$

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

# Bayesian Probability – Example

- The probability that a message is a malware is 0.125%, hence $P(\bar{A}) = P(message\ is\ malware) = 0.125\% = 0.00125$.

- The probability that a message is flagged as malware given the message is a malware is $P(B|\bar{A}) = P\begin{pmatrix} message\ is\ flagged\ as\ malware\ given \\ the\ message\ is\ malware \end{pmatrix}$
$= 95\% = 0.95$

# Bayesian Probability – Example

- Hence,

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

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

$$= \frac{0.05 \times 0.99875}{(0.95 \times 0.00125) + (0.05 \times 0.99875)}$$

$$= \frac{0.0499375}{0.0011875 + 0.04375}$$

$$= 0.97677 \approx 97.68\%$$

Hence, there is 97.68% chance that the email attachment clean.

# Bayesian Probability – Example

- From the above example, what do you think of Baye’s theorem being used in intrusion detection system?

Intrusion detection systems don’t cope very well with this type of problem.

The relevance of the Base-Rate Fallacy to intrusion detection systems is that, from Stallings and Brown:

> In general, if the actual numbers of intrusions is low compared to the number of legitimate uses of a system, then the false alarm rate will be high unless the test is extremely discriminating.

The fallacy is a feature of Bayes' theorem. This theorem relates to conditional probability and tells you the probability of some outcome in the context of known information.