Lecture for 9-15-2016

Hai Tran

Conditional Probability

Suppose you study how weather in the morning compare to weather in the afternoon, you find that the frequency of event occurring are :

Morning	sunny	rainy	snowy
Afternoon			
sunny	1/5	1/10	0
rainy	1/10	1/5	1/10
snowy	0	1/10	1/10

Today: Rainy this morning, what is the probability it will be sunny this afternoon?

$P(\text{sunny this afternoon}|\text{rainy this morning}) = \frac{1}{4}$

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

$P(\text{rainy in morning}) = \frac{4}{10}$

$P(\text{rainy morning and sunny afternoon}) = \frac{1}{10}$

Thus $P(A|B) = \frac{\frac{1}{10}}{\frac{4}{10}} = \frac{1}{4}$

Perfect Secrecy

A system has perfect secrecy if for any message m and any key k, P(original message was m | ciphertext Eve capture is C) = P(original message was m)

Suppose that Alice and Bob are exchanging messages that are either a or b and they have 3 possible keys k1,k2 and k3All 3 keys are equally likely of the time Bob sends a of the time Bob sends b

Encryption system

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

Suppose Eve intercepts the ciphertext C=2 Eve wants to compute: $P(m = a|C = 2)$ Thus

$$\begin{aligned}\frac{P(m = a \text{ and } c = 2)}{P(c = 2)} &= \frac{P(\text{key was } k_2 \text{ and the message was } a)}{P(\text{key is } k_1 \text{ and } m = b) + P(\text{key is } k_2 \text{ and } m = a)} \\ &= \frac{P(\text{key was } k_2) \times P(m = a)}{P(\text{key was } k_1) \times P(m = b) + P(\text{key was } k_2) \times P(m = a)} \\ &= \frac{\frac{1}{3} \times \frac{1}{4}}{\frac{1}{3} \times \frac{3}{4} + \frac{1}{3} \times \frac{1}{4}} = \frac{\frac{1}{12}}{\frac{3}{12} + \frac{1}{12}} = \frac{\frac{1}{12}}{\frac{4}{12}} = \frac{1}{4} = P(m = a)\end{aligned}$$

Eve didnt learn anything

Suppose Eve intercepts the cipher text C=1 P(m=a—C=1):

$$\frac{P(m = a \text{ and } C = 1)}{P(C = 1)} = \frac{P(m = a) \times P(\text{key was } k_1)}{P(m = a) \times P(\text{key was } k_1)} = \frac{\frac{1}{4} \times \frac{1}{3}}{\frac{1}{4} \times \frac{1}{3}} = 1 \neq P(m = a).$$

Thus Eve learned something about the message so the system doesnt have perfect secrecy.

Theorem: the one time pad has perfect secrecy

Key to proof: Any massage can be encoded to any ciphertext by exactly one keyIssue with one time pad: Need to transmit a key.Impractical since keys can only be used once.

Facts from number theory

How do you compute GCDs? Greatest common divisor GCD(4,26) = Factor both numbers and use that to find the greatest factor

GCD(1317, 56) = Try dividing both numbers by things until you find something

Euclidean Algorithm:

- compute GCD (1317,56)
- Do division with remainderGCD (1317,56) = GCD(56,29) = GCD(29,27) = GCD(27,2) = GCD(2,1) = 1

Idea: Keep doing division with remainder until the first time we get a remainder 0.

If GCD(a,b) = dthen there exsist x,y such that xa+yb = d

29 = 1317 23(56)27 = 561(29)2 = 29 1(27) 1 = 27 -13(2)

1 = 27 13(2) = 27-13(29-27) = -12(27)-13(29)= ... = 645(56) 27(1317) (work backward)