Probability Review Before we define perfect secrecy, we will review some Probability

- Random variable - A function X from sample space S to $\mathbb{R}$ numbers

---

<u>Example</u>. I toss a coin 3 times. The sample space is

$$\{HHH, \underbrace{HHT, HTH, THH}, HTT, THT, TTH, TTT\}$$

$X: S \to \mathbb{R}$ let $X(s) := \#$ of heads in S

$X(HTH) = 2$ X is a discrete random variable

- Probability Distribution - A function $P_r: \text{Range}(X) \to [0,1]$ that gives ~~possible~~ values of probabilities for a random variable

---

<u>Example</u>: Let X be defined as above then

$$P_X: \text{Range}(X) \to [0,1]$$

$P_X(HHH) = P_r(HHH) = \frac{1}{8}$ $P_X(TTT) = P_r(TTT) = 1/8$

$P_X(HHT) = P_r(\{HHT \cup HTH \cup THH\}) = 3/8$

$P_X(1\ \text{Head}) = 3/8$

Note probabilities are between 0, 1

Probabilities in distribution must sum to Zovo.

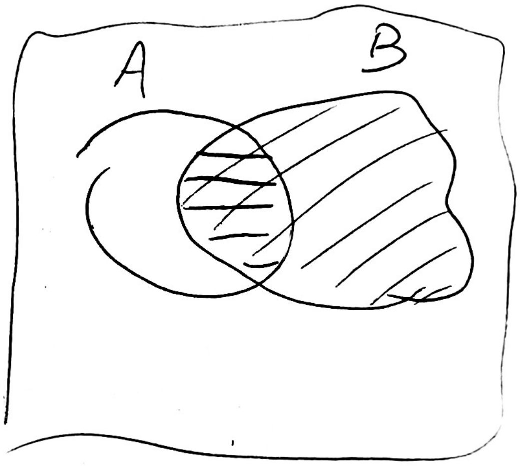
- Event: a particular occurence in some experiment. (some subset of S)

  Ex. How many ways could I land on heads 2 with 3 coin flips

  $\{HTH, HHT, THH\}$

- Conditional probability: Probability that an event occurs given that another event already occured.

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



- X, Y are independent if for all $x, y \in X, Y$ then

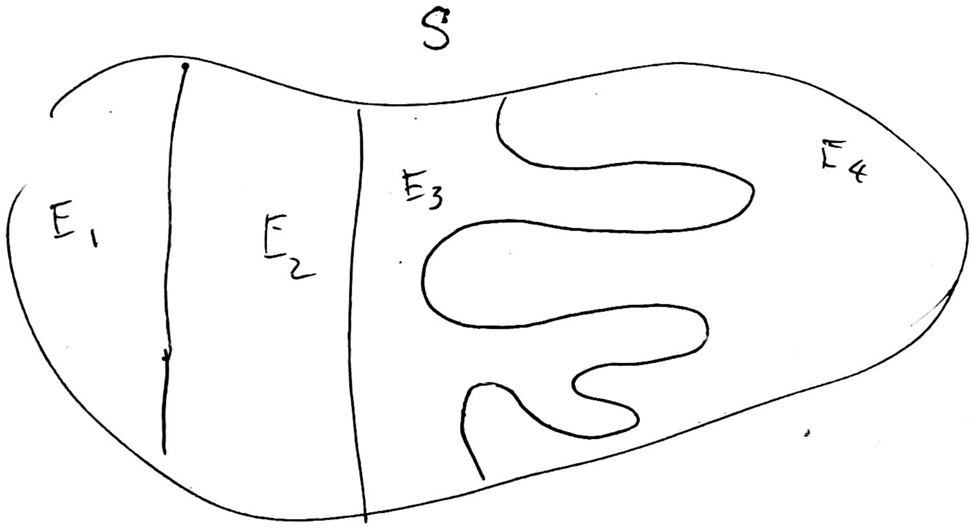
$$\Pr[X=x \mid Y=y] = \Pr[X=x] \quad \text{or} \quad P(X=x \cap Y=y] = \Pr(X=x)P(Y=y)$$

$$= \frac{\Pr(X=x \cap Y=y)}{P(Y=y)} = \frac{P(X=x)\,P(Y=y)}{P(Y=y)}$$

Thm. Law of total probability: Suppose events $E_1, \ldots, E_n$ form a partition of S. Then for any event A:

$$Pr[A] = \sum_{i=1}^{n} Pr[A \cap E_i] = \sum_{i=1}^{n} Pr[A \mid E_i] \, Pr[E_i].$$

A partition is $\bigcup E_i = S$ s.t. $E_i \cap E_j = \emptyset$ for all i, j



Thm: Bayes Thm. For any event A, B where $Pr(A) \neq 0$ then

$$P(B \mid A) = \frac{P(A \mid B)\, P(B)}{P(A)}$$

Example. Consider the shift cipher, and the distribution

$Pr[M = \text{'one'}] = 1/2$, $Pr[M = \text{'ten'}] = 1/2$.

What is $Pr[C = \text{'rqh'}]$?

law of total probability

$$Pr[C = \text{'rqh'}] = Pr[C = \text{'rqh'} \mid M = \text{'one'}] \cdot Pr[M = \text{'one'}]$$
$$+ Pr[C = \text{'rqh'} \mid M = \text{'ten'}]\ Pr[M = \text{'ten'}]$$

shift 3

$$[C = \text{'rqh'} \mid M = \text{'one'}] = 1/26$$

-3

$$[C = \text{'rqh} \mid M = \text{'ten'}] = 0$$

$\cancel{-3}$

$$= 1/26 \cdot 1/2 + 0 \cdot 1/2 = 1/52$$

Example

Consider the shift cipher. $(\mathcal{K} = \{0, \ldots, 25\})$

Suppose $\Pr[M = \text{'a'}] = .8$ $\Pr[M = \text{'z'}] = .2$. $\mathcal{M} = \{a, z\}$

What is the probability $\Pr[C = \text{'b'}]$ $\mathcal{C} = \{a, \ldots z\}$

$Enc_K(\text{'a'}) = b$ when $K = 1$

$Enc_K(\text{'z'}) = b$ when $K = 2$

law of total probability

$$\Pr[C = \text{"b"}] = \Pr[M = \text{'a'}] \Pr(K = 1) + \Pr[M = z] \cdot \Pr[K = 2]$$

$$= .8 \cdot 1/26 + .2\ (1/26)$$

$P(M = z \wedge P\ K = 2)$

$M \wedge K$ independent

- Distributions over K and M are independent

- Distribution over K is fixed by Gen

- Distribution over M varies on parties who are using the scheme

- Distribution = Probability Measure = probability mass function

roughly

Lets now define perfect Secrecy

Actual definition

1. Imagine an adversary who knows the distribution over M.

2. The adversary observes a ciphertext.

3. Observing the ciphertext should have no effect on the knowledge of the adversary.

Def.

An encryption scheme (Gen, Enc, Dec) over a message space $\mathcal{M}$ is perfectly secret if

for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C=c] > 0$:

$$\Pr[M=m \mid C=c] = \Pr[M=m].$$

- Note Key space/message space is always independent
- Perfectly secret says Ciphers/messages are independent

Lemma. The shift cipher is not perfectly secret.

Counter example

(1.) Consider $Pr[M = \text{'one'}] = 1/2$ and $Pr[M = \text{'ten'}] = 1/2$

$m = \text{'ten'}$ $c = \text{'rqh'}$

(2) $Pr[M = \text{'ten'} \mid C = \text{'rqh'}] = 0 \neq Pr[M = \text{'ten'}]$

(3.) Therefore not perfectly secret.

Ciphertext leaks info. I.E. tells us what our

plain text can't be!

Lemma 2.2

An encryption scheme (Gen, Enc, Dec) over a message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$Pr[C = c \mid M = m] = Pr[C = c]$$

Proof. $\Rightarrow$ If (Gen, Enc, DEC) are perfectly secret $\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$

then $P(M=m \mid C=c] = P[m=m]$. Let's Apply Bayes Thm:

$$\frac{P[C=c \mid M=m] \frac{P(M=m)}{P[M=c]} =}{P(C=c)} = P[M=m]$$

$$P(M=m \mid \cancel{C=c}) = \frac{P(C=c \mid M=m) \cancel{P(C=c)}}{\cancel{P(M=m)}}$$

$$P[C=c \mid M=m] = P[C=c]$$

$$P(M=m \mid C=c) = P(m)$$

$$= \frac{P(C=c \mid M=m) P(m)}{P(C=c)}$$

$P_m =$

$$P(M=m \mid C=c) = \frac{P(c \mid m) P(m)}{P(c)}$$

Note. Assumption $Pr[C=c] > 0$

$Pr(M=m) > 0$

Perfectly indistinguishability - states that the probability distribution over C is independent of the plaintext. I.E $\forall m_1, m_2 \in M$, $C(m_1) = C(m_2)$ are identical.

Lemma 2.3

M is perfectly secret iff every distribution over M every $m_0, m_1 \in M$ and every $c \in C$:

$$P_r[C=c \mid M=m_0] = P_r[C=c \mid M=m_1]$$

$\boxed{\text{Proof both ways}}$

- "it is impossible to distinguish an encryption of m_0 from an encryption of m_1"

- We call this perfect indistinguishability b/c it is impossible to distinguish an encryption of m_0 to m_1.