Encryption Theory

§2.1 Probability

Dfn: A probability space

1) a set Ω sample space

2) a set $\mathcal{F}$ of subsets of Ω
event space

3) fn $P: \mathcal{F} \to [0,1]$
satisfies some rules.

Ex: roll 6-sided die

$\Omega = \{1, 2, 3, 4, 5, 6\}$

'get an even #' $= \{2, 4, 6\} \subseteq \Omega$

'higher than 2' $= \{3, 4, 5, 6\}$

$$P(F) = \frac{\# F}{6}$$

Abuse of notation:

$$P(2) = P(\{2\})$$

We assume

Ω finite

$\mathcal{F} = 2^{\Omega}$ the power set

all the subsets of Ω

Ex: Roll a die, flip a coin

$$\Omega = \{(n,m) \mid n \in \{h,t\}, m \in \{1,2,3,4,5,6\}\}$$

$$E = \{(h,2),(h,4),(h,6)\}$$

$$P(E) = 1/4$$

Ex: Roll 2 dice

don't care which is which

$$\Omega = \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,2),(2,3),(2,4),(2,5),(2,6),$$
$$(3,3),(3,4),(3,5),(3,6),(4,4),(4,5),(4,6),(5,5),(5,6),(6,6)\}$$

$$\#\Omega = 21$$

$$P(\{(1,1)\}) = 1/36$$

$$P(\{(1,2)\}) = 1/18$$

Probability axioms ω Ω omega o O omicron

1) $\forall\ \omega \in \Omega,\ 0 \leq P(\omega) \leq 1.$

2) $P(\Omega) = \sum_{\omega \in \Omega} P(\omega) = 1.$

$P(\{\omega_1, \omega_2\}) = P(\omega_1) + P(\omega_2)$

It's not true that

$P(E \cup F) = P(E) + P(F)$

$E = \{1, 2, 3\}$ $P(E) = 1/2$

$F = \{2, 4, 6\}$ $P(F) = 1/2$

$E \cup F = \{1, 2, 3, 4, 6\}$ $P(E \cup F) = 5/6$

Dfn: E and F are disjoint if

$E \cap F = \emptyset$

3) If $E \cap F = \emptyset$, then

$P(E \cup F) = P(E) + P(F).$

Dfn: The complement of E is

$E^c = \{\omega \in \Omega \mid \omega \notin E\}$

4) $P(E^c) = 1 - P(E)$

Ex: $E = \{2,4,6\}$

$F = \{1,3,5\}$

E, F disjoint,

$F = E^c$.

$G = \{1,3\}$

E, G disjoint.

$\emptyset = \{\}$ disjoint from E, F.

$E = \{2,4,6\}$, $F = \{1,2\}$ die

$P(E) = 3/6 = 1/2$ $\quad P(F) = 1/3$

$P(E \cap F) = P(\{2\}) = 1/6$

$G = \{1,3\}$ $\quad P(G) = 1/3$

$P(E \cap G) = P(\emptyset) = 0$

Dfn: E, F are <u>independent</u> if $P(E \cap F) = P(E)P(F)$.

Ω = Roll 2 dice in order

$\#\Omega = 36$

E = first die is even $\qquad$ F = second die is 3

$P(E) = 1/2$ $\qquad$ $P(F) = 1/6$

$P(E \cap F) = P(E)P(F) = 1/12$.

Conditional Probability

Dfn: $P(F \mid E) = \dfrac{P(F \cap E)}{P(E)}$

"If E happens how likely is F?"

$E = \{1,2,3\}$, $F = \{1,2,5,6\}$

$$P(F/E) = \frac{P(E \cap F)}{P(E)} = \frac{2/6}{3/6} = \frac{2}{3}$$

---

2 dice, forgetting order

E = contains a 1 $\qquad$ F = contains a 2

$P(E) = \dfrac{11}{36}$ $\qquad$ $P(F) = \dfrac{11}{36}$

$$P(F \mid E) = \frac{2/36}{11/36} = \frac{2}{11}$$

Note: different from roll one die, then the other!

$$P(F|E) = \frac{P(F\cap E)}{P(E)}$$

$$P(F|E)\,P(E) = P(F\cap E) = P(E\cap F) = P(E|F)\,P(F)$$

Thm (Bayes): $$P(F|E) = \frac{P(E|F)\,P(F)}{P(E)}.$$

Prop:

1) $P(E) = P(E|F)\,P(F) + P(E|F^c)\,P(F^c)$

Pf/ $P(E|F)\,P(F) + P(E|F^c)\,P(F^c) = P(E\cap F) + P(E\cap F^c) = P\big((E\cap F)\cup(E\cap F^c)\big)$

$= P(E)$

2) $P(E|F) = \dfrac{P(F|E)\,P(E)}{P(F|E)\,P(E) + P(F|E^c)\,P(E^c)}$ (Bayes's Thm)

Ex: test 80% accuracy

and 2% of ppl have covid

you test positive, how likely is it you have covid.

$$P(C|+) = \frac{P(+|C)\,P(C)}{P(+|C)\,P(C) + P(+|\neg C)\,P(\neg C)} = \frac{.8 \cdot .02}{.8 \cdot .02 + .2 \cdot .98} \approx .075$$

Random Variables

Dfn: a random variable is a fn $X: \Omega \to \mathbb{R}$

Can define an event: fix $x \in \mathbb{R}$

$\{\omega \in \Omega \mid X(\omega) \le x\}$

$\{\omega \in \Omega \mid X(\omega) = x\}$

$\{\omega \in \Omega \mid X(\omega) \ge x\}$

Dfn: $X: \Omega \to \mathbb{R}$

The <u>probability density fn</u> of X is

$f_X(x) = P(X = x)$

If rolling and totaling 2 dice

$f_X(1) = 0$

$f_X(2) = \frac{1}{36}$

$f_X(5) = \frac{4}{36}$

$f_X(3.5) = 0$

~~The cumulative distribution fn~~

$\cancel{F_X(x) = P(X \le x)}$.

~~important if~~ $\cancel{\#\Omega = \infty}$