

ENCS 6161

# Probability and Random Processes

Fall 2004

X 1st. lecture, Sept. 8, 2004

- Course outline.
- Course Objective.

Applications of Probability & Random Processes:

- Digital Communications.
  - Communication Networks.
  - Signal Processing
  - Reliability
  - relative frequency  $\rightarrow$  Axiomatic approach
- Assume that we repeat a random experiment with  $K$  possible outcomes  $n$  times and record the number of times  $k=1, 2, \dots, K$  the outcome ~~event~~ occurs as  $N_k(n)$  then frequency of occurrence of  $k$  is  $\frac{N_k(n)}{n}$ . We expect that as the number of trials,  $n$ , tends to  $\infty$ , the ratio  $\frac{N_k(n)}{n} \rightarrow P_k$   $k=1, \dots, N$  where  $P_k$  is

the probability of  $k$ -th outcome. Note that  $P_k \leq 1$ .  
Note that for two disjoint outcomes  $k$  and  $l$ , we have  $N_{k,l}(n) = N_k(n) + N_l(n)$  and, therefore,

$$P_{k,l} = P_k + P_l.$$

Also, we have  $\sum_{k=1}^K N_k(n) = n$ . So,

$$\sum_{k=1}^K P_k = 1.$$

An approach, equivalent to the above, but more abstract is formulated based on the construction of the probabilistic model using a few axioms. This approach is called axiomatic probability theory.

The basic building blocks of the axiomatic probability are:  $\mathcal{S}$

- 1) A sample set <sup>$\mathcal{Y}$</sup> : A set of outcomes (basic, disjoint possible results of a random experiment,
- 2) A set of subsets of  $\mathcal{S}$  each called an event.

3) A probability measure: Assigning a value to each event.

examples of the sample space:

$S = \{H, T\}$  in tossing a coin

$S = \{1, 2, \dots, 6\}$  in throwing a dice.

$S = \{(1, 1), (1, 2), \dots, (6, 6)\}$  in throwing two ~~dice~~ die.

$S = \{2, 3, 4, \dots, 12\}$  the sum of two numbers when throwing two die.

$S = \{x: -V_p \leq x \leq V_p\}$  when sampling a voltage source with peak value  $V_p$ .

The sample space can be either finite, countable or uncountable.

Events: Each subset  $A \subseteq S$  constitutes an event take  $S = \{1, \dots, 6\}$

$A = \{1, 3, 5\}$  is the event of having an odd

number on the dice  $A = S = \{1, \dots, 6\}$  is the sure event and  $A = \Phi = \{\}$  is the null event.

similarly ~~the~~ for  $S = \{x: -V_p \leq x \leq V_p\}$

$A = \{x: 0 \leq x \leq V_p\}$  is the event that the sampled

value is positive and  $A = \{x: -\frac{V_p}{2} \leq x \leq \frac{V_p}{2}\}$

is the event that the voltage is between  $-\frac{V_p}{2}$  and  $+\frac{V_p}{2}$ .

A probability measure is a set function

$P(\cdot)$  with the following properties:

1)  $P(A) \geq 0$

2)  $P(S) = 1$  equivalently  $0 \leq P(A) \leq 1$   
(we will show this)

3) if  $A \cap B = \phi$  then  $P(A \cup B) = P(A) + P(B)$

3') if  $A_1, A_2, \dots$  are events such that  $A_i \cap A_j = \phi$

for all  $i \neq j$  then

$$P\left[\bigcup_{k=1}^{\infty} A_k\right] = \sum_{k=1}^{\infty} P(A_k)$$

Corollary 1:  $P(A^c) = 1 - P(A)$

~~from~~  $A^c \cap A = \phi \Rightarrow P(A^c \cup A) = P(A^c) + P(A)$

$$P(A^c \cup A) = P(S) = 1.$$

So,  $P(A^c) = 1 - P(A)$ .



Corollary 2:  $P(A) \leq 1 \quad \forall A$

$$P(A) = 1 - P(A^c) \leq 1 \quad \text{since } P(A^c) \geq 0.$$

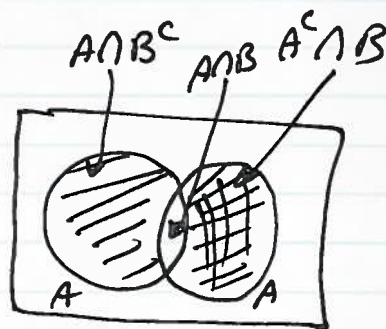
Corollary 3:  $P(\emptyset) = 0$

$$P(\emptyset) = 1 - P(\emptyset^c) = 1 - P(S) = 0$$

Corollary 4: if  $A_1, \dots, A_n$  are mutually exclusive events, i.e.,  ~~$A_i \cap A_j = \emptyset$~~   $A_i \cap A_j = \emptyset \quad \forall i \neq j$

then

$$P\left(\bigcup_{k=1}^n A_k\right) = \sum_{k=1}^n P(A_k)$$



Corollary 5:

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

$$\text{we have } A \cup B = (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B)$$

$$P(A \cup B) = P(A \cap B^c) + P(A^c \cap B) + P(A \cap B)$$

Similarly:

$$P(A) = P(A \cap B^c) + P(A \cap B)$$

$$P(B) = P(A^c \cap B) + P(A \cap B)$$

so,

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

$$\text{or } \boxed{P(A \cup B) = P(A) + P(B) - P(A \cap B)}$$

Union bound: ~~Assume that we have~~

$$P(A \cup B) \leq P(A) + P(B)$$

## Combinatorics:

1) Permutation: Assume that we have  $n$  objects.

In how many ways can we arrange them?

the first one, we can place in in any  $n$  locations, the second in any remaining location

etc. So  $P_n = n \times (n-1) \times (n-2) \times \dots \times 2 \times 1 = n!$

2) Permutation with order: In how many ways

we can select  $k$  objects from  $n \geq k$  objects?

For the 1st object we have  $n$  choices, for the

second  $n-1, \dots$  for the  $k$ th  $n-k+1$

$$\text{So } P_k^n = n \times (n-1) \times \dots \times (n-k+1) = \frac{n!}{(n-k)!}$$

3) Combination (selection without order):

In how many ways we can select  $k$  objects

from  $n \geq k$  objects (here order is not our concern)

Assume this number is  $C_k^n$ . That is, there are  $C_k^n$

ways in which  $k$  objects can be selected from

a set of  $n$  objects. Each<sup>one</sup> of these  $C_k^n$  sets can be arranged in  $k!$  ways so:

$k! C_k^n$  is the total number of ways  $k$  objects from a set of size  $n$  can be formed.

Or,

$$k! C_k^n = P_k^n = \frac{n!}{(n-k)!}$$

So

$$C_k^n = \frac{n!}{(n-k)! k!} = \binom{n}{k}$$

This is called  $n$ -choose- $k$ .

Example: Find the number of ways, one can select 2 objects from  $A = \{1, 2, 3, 4, 5\}$

$$\binom{5}{2} = \frac{5!}{2!3!} = 10$$

DTMF Signalling

---

## Conditional Probability

Take two events A and B

$$P[A \cap B] = P[A] P[B|A]$$

i.e., probability of A and B occurring is the probability of A occurring times the probability of B occurring given A has occurred.

$P(B|A)$  is called the conditional probability of B given A:

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

Similarly:

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

or

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

So,

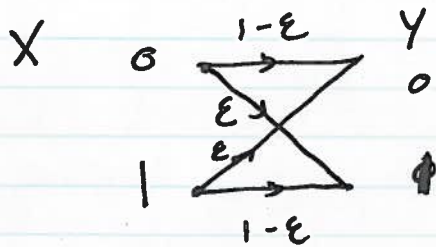
$$P(A|B) = \frac{P(A) P(B|A)}{P(B)}$$

This is called the Bayes Rule.



### Example:

Consider a communication channel transmitting binary data with probability of error  $\epsilon$ . Assume that bits at its input have  $P(0) = p$  and  $P(1) = 1 - p$ .



We have:

$$P(X=0, Y=0) = P(0,0) = p(1-\epsilon)$$

$$P(X=0, Y=1) = p\epsilon$$

$$P(X=1, Y=0) = (1-p)\epsilon$$

$$P(X=1, Y=1) = (1-p)(1-\epsilon)$$

$$P(X=0|Y=0) = \frac{P(X=0)P(Y=0|X=0)}{P(Y=0)}$$

$$= \frac{p(1-\epsilon)}{p(1-\epsilon) + (1-p)\epsilon}$$

$$P(X=1|Y=0) = \frac{P(X=1)P(Y=0|X=1)}{P(Y=0)} = \frac{(1-p)\epsilon}{p(1-\epsilon) + (1-p)\epsilon}$$

Upon observing  $Y$ , we form the a posteriori Probabilities  $P(X=0|Y=y)$  and  $P(X=1|Y=y)$  for  $Y=y \in \{0,1\}$  and decide in favour of the one being more probable (MAP detection). For  $Y=0$  for example, we ~~but~~ decide  $X=0$  if

$$P(X=0|Y=0) > P(X=1|Y=0)$$

or

$$P(X=0)P(Y=0|X=0) > P(X=1)P(Y=0|X=1)$$

or  $p(1-\epsilon) > (1-p)\epsilon$  else, we decide  $X=1$

( $p > \epsilon \rightarrow X=0$ )  
For  $Y=1$ , we decide  $X=0$  if

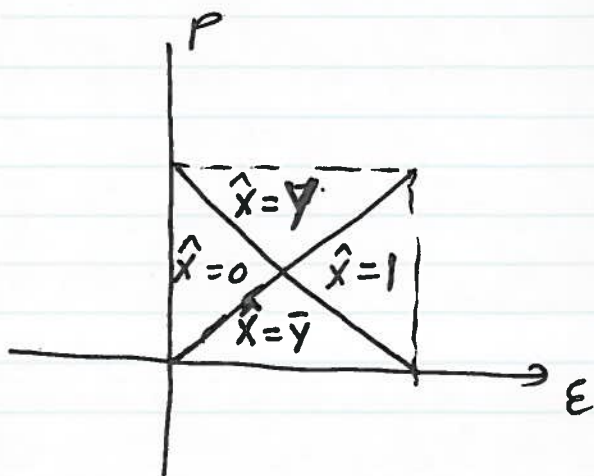
$$P(X=0)P(Y=1|X=0) > P(X=1)P(Y=1|X=1)$$

or

$$p\epsilon > (1-p)(1-\epsilon) \text{ else, we decide } X=1$$

$$[(p > 1-\epsilon) \rightarrow X=0]$$

or  $1-p < \epsilon$



## Example (Bayes Rule)

Assume that you are given the following information:

- 30% of the adults in a given city are smokers.
- Smokers die of lung cancer at a rate of 1 in 100,000.
- ~~no~~ fatality amongst non-smokers (of lung cancer) is 1 in 100 millions.

A person dies of lung cancer. You are asked to decide whether he has been a smoker or not.

a) What is your answer?

b) What is the probability that you are wrong?

$$P(S) = 0.3 \quad P(\bar{S}) = 0.7$$

$$P(L.C. | S) = 10^{-5} \quad P(L.C. | \bar{S}) = 10^{-8}$$

$$P(S | L.C.) = \frac{P(S)P(L.C. | S)}{P(L.C.)} = \frac{0.3 \times 10^{-5}}{0.3 \times 10^{-5} + 0.7 \times 10^{-8}}$$

$$P(S | L.C.) = 0.9977 \quad \text{and} \quad P(\bar{S} | L.C.) = 0.0023$$

a) He was smoker. b)  $P_e = 2.3 \times 10^{-3}$

## independence

two events  $A$  and  $B$  are said to be independent if knowing that  $B$  has occurred does not alter the probability of  $A$  happening i.e.,

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

For two independent events  $A$  and  $B$ , we have

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

For independent events  $A_1, A_2, \dots, A_n$

$$P(A_1 \cap A_2 \cap \dots \cap A_n) = \prod_{i=1}^n P(A_i)$$

~~Proof~~ In general, when events are not necessarily independent

$$\begin{aligned} P(A_1, \dots, A_n) &= P(A_1)P(A_2|A_1)P(A_3|A_1, A_2) \dots P(A_n|A_1, \dots, A_{n-1}) \\ &= \prod_{i=1}^n P(A_i|A_1, \dots, A_{i-1}) \end{aligned}$$