

# Information Theory

## Lecture notes 2015-2016

## Introduction

# Organization

Professors:

- ▶ Lectures: Nicolae Cleju (nikcleju@etti.tuiasi.ro)
- ▶ Laboratories: Daniel Matasaru (..@etti.tuiasi.ro)

# Grades

$$\text{Final grade} = 0.75 \text{ Exam} + 0.25 \text{ Lab}$$

# Time schedule

- ▶ 14 weeks of lectures (3h each)
- ▶ 14 weeks of laboratories (2h each)

# Course structure

1. Chapter I: Discrete Information Sources
2. Chapter II: Discrete Transmission Channels
3. Chapter III: Source Coding
4. Chapter IV: Channel Coding

# Bibliography

1. ***Elements of Information Theory*, Valeriu Munteanu, Daniela Tarniceriu, Ed. CERM I 2007**
2. *Elements of Information Theory*, Thomas M. Cover, Joy A. Thomas, 2nd Edition, Wiley 2006
3. *Information and Coding Theory*, Gareth A. Jones, J. Mary Jones, Springer 2000
4. *Transmisia si codarea informatiei*, lectures at ETTI (Romanian)



## Introduction to probabilities

# Basic notions of probability

- ▶ Random variable = the outcome of an experiment
- ▶ Distribution (probability mass function)
- ▶ Discrete distribution
- ▶ Alphabet

# Basic properties

- ▶ Two independent events:

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

## Chapter I: Discrete information sources

# Block diagram of a communication system

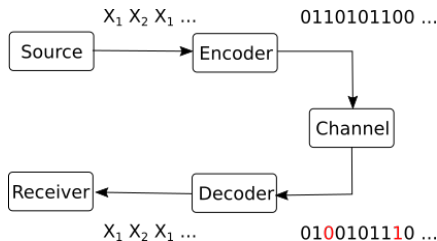


Figure 1: Block diagram of a communication system

# What is information?

## Example:

- ▶ I tell you the following sentence: “your favorite football team lost the last match”.
- ▶ Does this message carry information? How, why, how much?
- ▶ Consider the following facts:
  - ▶ the message carries information only because you didn't already know the result.
  - ▶ if you already known the result, the message is useless (brings no information)
  - ▶ since you didn't know the result, there were multiple results possible (win, equal or lose)
  - ▶ the actual information in the message is that *lost* happened, and not *win* or *equal*
  - ▶ if the result was to be expected, there is little information. If the result is highly unusual, there is more information in this message

# Information source

- ▶ We will always consider information in a context similar to the above example.
- ▶ We will use terminology from probability theory to define information:
  - ▶ there is a *probabilistic source* that can produce a number of different *events*.
  - ▶ each event has a certain probability. We know all the probabilities beforehand.
  - ▶ at one time, an event is randomly selected according to its probability.
  - ▶ afterwards, a new message can be selected, and so on ==> a stream of messages is produced.
- ▶ The source is called an *information source* and the selected event is a *message*.
- ▶ A message carries the information that **it** happened, and not the other possible message events that could have been selected.
- ▶ The quantity of information is dependent in its probability.

# Discrete memoryless source

- ▶ A discrete memoryless source (DMS) is an information source where the messages are **independent** , i.e. the choice of a message at one time does not depend on what were the previous messages
- ▶ Each message has a fixed probability. The set of probabilities is the *distribution* of the source.

$$S : \begin{pmatrix} s_1 & s_2 & s_3 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

- ▶ Properties:
  - ▶ Discrete: it can take a value from a discrete set (alphabet)
  - ▶ Complete:  $\sum p(s_i) = 1$
  - ▶ Memoryless: successive values are independent of previous values (e.g. successive throws of a coin)
- ▶ A message from a DMS is also called a *random variable* in probabilistics.



# Examples

- ▶ A coin is a discrete memoryless source (DMS) with two messages:

$$S : \begin{pmatrix} \textit{coin\_head} & \textit{coin\_tail} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

- ▶ A dice is a discrete memoryless source (DMS) with six messages:

$$S : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}$$

- ▶ Playing the lottery can be modeled as DMS:

$$S : \begin{pmatrix} s_1 & s_2 \\ 0.9999 & 0.0001 \end{pmatrix}$$

# Examples

- ▶ An extreme type of DMS containing the certain event:

$$S : \begin{pmatrix} s_1 & s_2 \\ 1 & 0 \end{pmatrix}$$

- ▶ Receiving an unknown *bit* (0 or 1) with equal probabilities:

$$S : \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

- ▶ When a DMS provides a new message, it gives out some new information, i.e. the information that a particular message took place.
- ▶ The information attached to a particular event (message) is rigorously defined as:

$$i(s_i) = -\log_2(p(s_i))$$

- ▶ Properties:
  - ▶  $i(s_i) \geq 0$
  - ▶ lower probability (rare events) means higher information
  - ▶ higher probability (frequent events) means lower information
  - ▶ a certain event brings no information:  $-\log(1) = 0$
  - ▶ an event with probability 0 brings infinite information (but it never happens..)

# Entropy of a DMS

- ▶ We usually don't care about a single message. We are interested in a large number of them (think millions of bits of data).
- ▶ We are interested in the *average* information of a message from a DMS.
- ▶ Definition: the entropy of a DMS source  $S$  is **the average information of a message**:

$$H(S) = \sum_k p_k i(s_k) = - \sum_k p_k \log_2(p_k)$$

where  $p_k = p(s_k)$  is the probability of message  $k$ .

# The choice of logarithm

- ▶ Any base of logarithm can be used in the definition.
- ▶ Usual convention: use binary logarithm  $\log_2()$ .  $H(S)$  measured in *bits* (*bits / message*)
- ▶ If using natural logarithm  $\ln()$ ,  $H(S)$  is measured in *nats*.
- ▶ Logarithm bases can be converted to/from one another:

$$\log_b(x) = \frac{\log_a(x)}{\log_a(b)}$$

- ▶ Entropies using different logarithms differ only in scaling:

$$H_b(S) = \frac{H_a(S)}{\log_a(b)}$$

# Examples

- ▶ Coin:  $H(S) = 1 \text{ bit/message}$
- ▶ Dice:  $H(S) = \log(6) \text{ bits/message}$
- ▶ Lottery:  $H(S) = -0.9999 \log(0.9999) - 0.0001 \log(0.0001)$
- ▶ Receiving 1 bit:  $H(S) = 1 \text{ bit/message}$  (hence the name!)

# Interpretation of the entropy

All the following interpretations of entropy are true:

- ▶  $H(S)$  is the *average uncertainty* of the source  $S$
- ▶  $H(S)$  is the *average information* of messages from source  $S$
- ▶ A long sequence of  $N$  messages from  $S$  has total information  $\approx N \cdot H(S)$
- ▶  $H(S)$  is the minimum number of bits (0,1) required to uniquely represent an average message from source  $S$

# Properties of entropy

We prove the following **properties of entropy**:

1.  $H(S) \geq 0$  (non-negative)
2.  $H(S)$  is maximum when all  $n$  messages have equal probability  $\frac{1}{n}$ .  
The maximum value is  $\max H(S) = \log(n)$ .
3. *Diversification* of the source always increases the entropy



## Example - Game

Game: I think of a number between 1 and 8. You have to guess it by asking yes/no questions.

- ▶ How much uncertainty does the problem have?
- ▶ How is the best way to ask questions? Why?
- ▶ What if the questions are not asked in the best way?
- ▶ On average, what is the number of questions required to find the number?

## Example - Game v2

- ▶ Suppose I choose a number according to the following distribution:

$$S : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}$$

- ▶ On average, what is the number of questions required to find the number?
  - ▶ What questions would you ask?
- ▶ What if the distribution is:

$$S : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ 0.14 & 0.29 & 0.4 & 0.17 \end{pmatrix}$$

- ▶ In general:
  - ▶ What distribution makes guessing the number the most difficult?
  - ▶ What distribution makes guessing the number the easiest?

# Information flow of a DMS

- ▶ Suppose that message  $s_i$  takes time  $t_i$  to be transmitted via some channel.
- ▶ Definition: the information flow of a DMS  $S$  is **the average information transmitted per unit of time**:

$$H_\tau(S) = \frac{H(S)}{\bar{t}}$$

where  $\bar{t}$  is the average duration of transmitting a message:

$$H(S) = \sum_i p_i t_i$$

# Extended DMS

- ▶ Definition: the  $n$ -th order extension of a DMS  $S$ ,  $S^n$  is the source with messages has as messages all the combinations of  $n$  messages of  $S$ :

$$\sigma_i = \underbrace{s_j s_k \dots s_l}_n$$

- ▶ If  $S$  has  $k$  messages,  $S^n$  has  $k^n$  messages
- ▶ Since  $S$  is DMS

$$p(\sigma_i) = p(s_j) \cdot p(s_k) \cdot \dots \cdot p(s_l)$$

# Extended DMS - Example

► Examples:

$$S : \begin{pmatrix} s_1 & s_2 \\ \frac{1}{4} & \frac{3}{4} \end{pmatrix}$$

$$S^2 : \begin{pmatrix} \sigma_1 = s_1 s_1 & \sigma_2 = s_1 s_2 & \sigma_3 = s_2 s_1 & \sigma_4 = s_2 s_2 \\ \frac{1}{16} & \frac{3}{16} & \frac{3}{16} & \frac{9}{16} \end{pmatrix}$$

$$S^3 : \begin{pmatrix} s_1 s_1 s_1 & s_1 s_1 s_2 & s_1 s_2 s_1 & s_1 s_2 s_2 & s_2 s_1 s_1 & s_2 s_1 s_2 & s_2 s_2 s_1 & s_2 s_2 s_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

# Extended DMS - Another example

- ▶ Long sequence of binary messages:

010011001110010100...

- ▶ Can be grouped in bits, half-bytes, bytes, 16-bit words, 32-bit long words, and so on.

# Property of DMS

- ▶ Theorem: The entropy of a  $n$ -th order extension is  $n$  times larger than the entropy of the original DMS

$$H(S^n) = nH(S)$$

- ▶ Interpretation: grouping messages from a long sequence in blocks of  $n$  does not change total information (e.g. groups of 8 bits = 1 byte)

# An example [memoryless is not enough]

- The distribution (frequencies) of letters in English:

letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

- Text from a memoryless source with these probabilities:

OCRO HLI RGWR NMIELWIS EU LL NBNESEBYA TH EEI  
ALHENHTTPA OOBTTVA NAH BRL

(taken from *Elements of Information Theory*, Cover, Thomas)

- What's wrong? **Memoryless**



# Sources with memory

- ▶ **Definition:** A source has memory of order  $m$  if the probability of a message depends on the last  $m$  messages.
- ▶ The last  $m$  messages = the **state** of the source ( $S_i$ ).
- ▶ A source with  $n$  messages and memory  $m \Rightarrow n^m$  states in all.
- ▶ For every state, messages can have a different set of probabilities.  
Notation:  $p(s_i|S_k) = \text{"probability of } s_i \text{ in state } S_k \text{"}$ .
- ▶ Also known as *Markov sources*.

# Example

- ▶ A source with  $n = 4$  messages and memory  $m = 1$ 
  - ▶ if last message was  $s_1$ , choose next message with distribution

$$S_1 : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ 0.4 & 0.3 & 0.2 & 0.1 \end{pmatrix}$$

- ▶ if last message was  $s_2$ , choose next message with distribution

$$S_2 : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ 0.33 & 0.37 & 0.15 & 0.15 \end{pmatrix}$$

- ▶ if last message was  $s_3$ , choose next message with distribution

$$S_3 : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ 0.2 & 0.35 & 0.41 & 0.04 \end{pmatrix}$$

- ▶ if last message was  $s_4$ , choose next message with distribution

$$S_4 : \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ 0.1 & 0.2 & 0.3 & 0.4 \end{pmatrix}$$

# Transitions

- ▶ When a new message is provided, the source **transitions** to a new state:

$$\begin{array}{c} s_i s_j s_k \quad s_l \\ \underbrace{\hspace{1.5cm}} \\ \text{old state} \end{array}$$
$$\begin{array}{c} s_i \quad s_j s_k s_l \\ \underbrace{\hspace{1.5cm}} \\ \text{new state} \end{array}$$

- ▶ The message probabilities = the probabilities of transitions from some state  $S_u$  to another state  $S_v$

# Transition matrix

- ▶ The transition probabilities are organized in a **transition matrix**  $[T]$

$$[T] = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1N} \\ p_{21} & p_{22} & \dots & p_{2N} \\ \dots & \dots & \dots & \dots \\ p_{N1} & p_{N2} & \dots & p_{NN} \end{bmatrix}$$

- ▶  $p_{ij}$  is the transition probability from state  $S_i$  to state  $S_j$
- ▶  $N$  is the total number of states

# Graphical representation

Example here

# Entropy of sources with memory

- ▶ Each state  $S_k$  has a different distribution  $\rightarrow$  each state has a different entropy  $H(S_k)$

$$H(S_k) = - \sum_i p(s_i|S_k) \cdot \log(p(s_i|S_k))$$

- ▶ Global entropy = average entropy

$$H(S) = \sum_k p_k H(S_k)$$

where  $p_k$  = probability that the source is in state  $S_i$  (i.e. after a very long sequence of messages, how many times the source was in state  $S_k$ )

# Ergodic sources

- ▶ Let  $p_i^{(t)}$  = the probability that source  $S$  is in state  $S_i$  at time  $t$ .
- ▶ In what state will it be at time  $t + 1$ ? (after one more message)  
(probabilities)

$$[p_1^{(t)}, p_2^{(t)}, \dots, p_N^{(t)}] \cdot [T] = [p_1^{(t+1)}, p_2^{(t+1)}, \dots, p_N^{(t+1)}]$$

- ▶ After one more message:

$$[p_1^{(t)}, p_2^{(t)}, \dots, p_N^{(t)}] \cdot [T] \cdot [T] = [p_1^{(t+2)}, p_2^{(t+2)}, \dots, p_N^{(t+2)}]$$

- ▶ In general, after  $n$  messages the probabilities that the source is in a certain state are:

$$[p_1^{(0)}, p_2^{(0)}, \dots, p_N^{(0)}] \cdot [T]^n = [p_1^{(n)}, p_2^{(n)}, \dots, p_N^{(n)}]$$

- ▶ A source is called **ergodic** if every state can be reached from every state, in a finite number of steps.

## Property of ergodic sources:

- ▶ After many messages, the probabilities of the states *become stationary* (converge to some fixed values), irrespective of the initial probabilities.

$$\lim_{n \rightarrow \infty} [p_1^{(n)}, p_2^{(n)}, \dots, p_N^{(n)}] = [p_1, p_2, \dots, p_N]$$



# Finding the stationary probabilities

- ▶ After  $n$  messages and after  $n + 1$  messages, the probabilities are the same:

$$[p_1, p_2, \dots, p_N] \cdot [T] = [p_1, p_2, \dots, p_N]$$

- ▶ Also  $p_1 + p_2 + \dots + p_N = 1$ .

$\Rightarrow$  solve system of equations, find values.

# Entropy of ergodic sources with memory

- ▶ The entropy of an ergodic source with memory is

$$H(S) = \sum_k p_k H(S_k) = - \sum_k p_k \sum_i p(s_i | S_k) \cdot \log(p(s_i | S_k))$$

# Example English text as sources with memory

(taken from *Elements of Information Theory*, Cover, Thomas)

- ▶ Memoryless source, equal probabilities:

XFOML RXKHRJFFJUJ ZLPWCFWKCYJ  
FFJEYVKCQSGXYD QPAAMKBZAACIBZLHJQD

- ▶ Memoryless source, probabilities of each letter as in English:

OCRO HLI RGWR NMIELWIS EU LL NBNESBYA TH EEI  
ALHENHTTPA OOBTTVA NAH BRL

- ▶ Source with memory  $m = 1$ , frequency of pairs as in English:

ON IE ANTSOUTINYS ARE T INCTORE ST BE S DEAMY  
ACHIN D ILONASIVE TU COOWE AT TEASONARE FUSO  
TIZIN ANDY TOBE SEACE CTISBE

- ▶ Source with memory  $m = 2$ , frequency of triplets as in English:

IN NO IST LAT WHEY CRATICT FROURE BERS GROCID  
PONDENOME OF DEMONSTURES OF THE REPTAGIN IS  
REGOACTIONA OF CRE

- ▶ Source with memory  $m = 3$ , frequency of 4-plets as in English:

THE GENERATED JOB PROVIDUAL BETTER TRAND THE DISPLAYED  
CODE, ABOVERY UPONDULTS WELL THE CODERST IN THESTICAL  
IT DO HOCK BOTHE MERG. (INSTATES CONS ERATION. NEVER  
ANY OF PUBLE AND TO THEORY. EVENTIAL CALLEGAND TO ELAST  
BENERATED IN WITH PIES AS IS WITH THE )

# Chapter summary

- ▶ Information of a message:  $i(s_i) = -\log_2(p(s_i))$
- ▶ Entropy of a memoryless source:  
 $H(S) = \sum_k p_k i(s_k) = -\sum_k p_k \log_2(p_k)$
- ▶ Properties of entropy:
  1.  $H(S) \geq 0$
  2. Is maximum when all messages have equal probability  
( $H_{\max}(S) = \log(n)$ )
  3. *Diversification* of the source always increases the entropy
- ▶ Sources with memory: definition, transitions
- ▶ Stationary probabilities of ergodic sources with memory:  
 $[p_1, p_2, \dots, p_N] \cdot [T] = [p_1, p_2, \dots, p_N], \sum_i p_i = 1.$
- ▶ Entropy of sources with memory:

$$H(S) = \sum_k p_k H(S_k) = -\sum_k p_k \sum_i p(s_i|S_k) \cdot \log(p(s_i|S_k))$$

## Chapter II: Discrete Transmission Channels

# What are they?

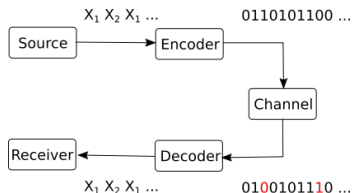


Figure 2: Communication system

- ▶ A system of two related random variables
- ▶ Input random variable  $X = x_1, x_2, \dots$ , output random variable  $Y = y_1, y_2, \dots$
- ▶  $X$  and  $Y$  are *related*, but still *random* (usually because of *noise*)

# Nomenclature

- ▶ Discrete: the input alphabet and the output alphabet are finite
- ▶ Memoryless: the output symbol depends only on the current input symbol
- ▶ Stationary: the noise arising on the channel is time invariant (i.e. its statistics do not vary in time)

# Systems of two random variables

- ▶ Two random variables:  $X = x_1, x_2, \dots$ ,  $Y = y_1, y_2, \dots$
- ▶ Example: throw a dice (X) and a coin (Y) simultaneously
- ▶ How to describe this system?

A single joint information source:

$$X \cap Y : \begin{pmatrix} x_1 \cap y_1 & x_1 \cap y_2 & \dots & x_i \cap y_j \\ p(x_1 \cap y_1) & p(x_1 \cap y_2) & \dots & p(x_i \cap y_j) \end{pmatrix}$$

Arrange in a nicer form (table):

	$y_1$	$y_2$	$y_3$
$x_1$	...	...	...
$x_2$	...	...	...
$x_3$	...	...	...

- ▶ Elements of the table:  $p(x_i \cap y_j)$



# Joint probability matrix

The table constitutes the **joint probability matrix**:

$$P(X, Y) = \begin{bmatrix} p(x_1 \cap y_1) & p(x_1 \cap y_2) & \cdots & p(x_1 \cap y_M) \\ p(x_2 \cap y_1) & p(x_2 \cap y_2) & \cdots & p(x_2 \cap y_M) \\ \vdots & \vdots & \cdots & \vdots \\ p(x_N \cap y_1) & p(x_N \cap y_2) & \cdots & p(x_N \cap y_M) \end{bmatrix}$$

$$\sum_i \sum_j p(x_i \cap y_j) = 1$$

- ▶ This matrix completely defines the two-variable system
- ▶ This matrix completely defines the communication process

- ▶ The distribution  $X \cap Y$  determines the **joint entropy**:

$$H(X, Y) = - \sum_i \sum_j p(x_i \cap y_j) \cdot \log(p(x_i \cap y_j))$$

- ▶ This is the global entropy of the system (knowing the input and the output)

# Marginal distributions

- ▶  $p(x_i) = \sum_j p(x_i \cap y_j) =$  sum of row  $i$  from  $P(X,Y)$
- ▶  $p(y_j) = \sum_i p(x_i \cap y_j) =$  sum of column  $j$  from  $P(X,Y)$
- ▶ The distributions  $p(x)$  and  $p(y)$  are called **marginal distributions** (“summed along the margins”)

## Examples [marginal distributions not enough]

- ▶ Example 1:

$$P(X, Y) = \begin{bmatrix} 0.3 & 0 \\ 0 & 0.7 \end{bmatrix}$$

- ▶ Example 2:

$$P(X, Y) = \begin{bmatrix} 0.15 & 0.15 \\ 0.15 & 0.55 \end{bmatrix}$$

- ▶ Both have identical  $p(x)$  and  $p(y)$ , but are completely different
- ▶ Which one is better for a transmission?
- ▶ Marginal distribution are useful, but not enough. Essential is the *relation* between  $X$  and  $Y$ .

$$p(A \cap B) = p(A) \cdot p(B|A)$$

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

- ▶ “The conditional probability of B **given A**” (i.e. given that event A happened)
- ▶ Examples. . .
- ▶ Independence:

$$p(A \cap B) = p(A)p(B)$$

$$p(B \cap A) = p(B)$$

# Channel matrix

Noise (or channel) matrix:

$$P(Y|X) = \begin{bmatrix} p(y_1|x_1) & p(y_2|x_1) & \cdots & p(y_M|x_1) \\ p(y_1|x_2) & p(y_2|x_2) & \cdots & p(y_M|x_2) \\ \vdots & \vdots & \cdots & \vdots \\ p(y_1|x_N) & p(y_2|x_N) & \cdots & p(y_M|x_N) \end{bmatrix}$$

- ▶ Defines the probability of an output **given an input**
- ▶ Each row = a separate distribution ...

# Three examples

Three examples to help you remember conditional probabilities

- ▶ Play and win the lottery
- ▶ Gambler's paradox
- ▶ CNN: Crippled cruise ship returns; passengers happy to be back