

Τόγιας Παναγιώτης

Στοιχεία Πιθανοτήτων & Στοχαστικές Ανελίξεις

Reprinted with corrections from The Boll System Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October, 1948.

### A Mathematical Theory of Communication

By C. E. SHANNON

### INTRODUCTION

The recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist¹ and Hartley² on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning, that is they refer to or are correlated according to some system with certain plysical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

- It is practically more useful. Parameters of engineering importance such as time, bandwidth, number of relays, etc., tend to vary linearly with the logarithm of the number of possibilities. For example, adding one relay to a group doubles the number of possible states of the relays. It adds 1 to the base 2 logarithm of this number. Doubling the time roughly squares the number of possible messages, or doubles the logarithm, etc.
- 2. It is nearer to our intuitive feeling as to the proper measure. This is closely related to (1) since we intuitively measures entities by linear compansion with common standards. One feels, for example, that two punched cards should have twice the capacity of one for information storage, and two identical channels twice the capacity of one for transmitting information.
- It is mathematically more suitable. Many of the limiting operations are simple in terms of the logarithm but would require clumsy restatement in terms of the number of possibilities.

The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly bits, a word suggested by J. W. Tukey. A device with two stable positions, such as a relay or a flip-flop circuit, can store one bit of information. N such devices can store N bits, since the total number of possible states is  $2^N$  and  $\log_2 2^N = N$ . If the base 10 is used the units may be called decimal digits. Since

 $log_2M = log_{10}M/log_{10}2$ = 3.32log<sub>10</sub>M,

¹Nyquist, H., "Certain Factors Affecting Telegraph Speed," Bell System Technical Journal, April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," A.I.E.E. Trans., v. 47, April 1928, p. 617.

<sup>2</sup>Hartley, R. V. L., "Transmission of Information," Bell System Technical Journal, July 1928, p. 535.

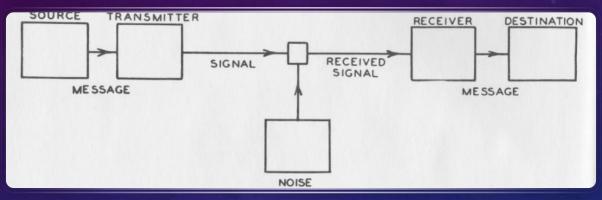
1

55 σελίδες | Βασικά στοιχεία επικοινωνίας, εντροπία & πλεονασμός πληροφορίας, πρόταση του όρου 'bit' (John Tukey)

Πρόθεσή του ήταν να παρουσιάσει ένα γενικό πλαίσιο επικοινωνίας με βάση τις αρχές των νέων, για την εποχή, ψηφιακών μέσων.

Δίνει απαντήσεις με μαθηματικούς όρους:

- Πως αναλογικά σήματα μπορούν να μετασχηματιστούν σε ψηφιακά
- ii. Πως ψηφιακά σήματα μπορούν να κωδικοποιηθούν με τέτοιο τρόπο ώστε ο θόρυβος και η παρεμβολή να μην βλάψουν το αρχικό μήνυμα που αντιπροσωπεύουν αυτά τα σήματα
- iii. Πως θα μπορούσε να εξασφαλιστεί η βέλτιστη χρησιμοποίηση ενός δεδομένου εύρους ζώνης ενός καναλιού επικοινωνίας



Ένα γενικό σύστημα επικοινωνιας, το οποίο δείχνει τη διαδικασία παραγωγής ενός μηνύματος

- Μία πηγή πληροφορίας παράγει ένα μήνυμα
- Ένας αναμεταδότης ο οποίος εφαρμόζεται στο μήνυμα, δημιουργεί ένα σήμα που μπορεί να διαμοιρασθεί μέσα σε ένα κανάλι
- Ένα κανάλι με ρόλο διαμεσολαβητή που χρησιμοποιείται από το σήμα το οποίο περιέχει τη πληροφορία που απαρτίζει το μήνυμα
- Ένας υποδοχέας ο οποίος αναδιαμορφώνει το σήμα πίσω στο αρχικό μήνυμα
- Ένας τελικός προορισμός (άνθρωπος ή μηχανή) για τον οποίο το μήνυμα προορίζεται

# MONTEΛΑ MARKOV ΣΕ ΦΥΣΙΚΗ ΓΛΩΣΣΑ ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΑΛΥΣΙΔΕΣ MARKOV ΓΙΑ ΤΗ ΣΤΑΤΙΣΤΙΚΗ ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΚΕΙΜΕΝΟΥ

# ΠΕΡΙ ΑΛΥΣΙΔΩΝ ΜΑRΚΟΥ & ΔΙΑΚΡΙΤΩΝ ΠΗΓΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

# Πηγή μίας διακριτής πληροφορίας

Αναπαράγει μηνύματα σύμβολο ανα σύμβολο και θα επιλέγει διαδοχικά σύμβολα σύμφωνα με ορισμένες πιθανότητες ανάλογα με προηγούμενες επιλογές καθώς και με τα συγκεκριμένα προκαθορισμένα σύμβολα

simulation .5 R

RRRSSSSS SRRRRS RRRRSSRS RRRSSRR

- Η πηγή μπορεί να αντιπροσωπευθεί απο μία στοχαστική διεργασία
- Οποιαδήποτε στοχαστική διεργασία η οποία παράγει μια διακριτή αλληλουχία συμβόλων που επιλέγεται από ένα πεπερασμένο σύνολο μπορεί να θεωρηθεί ως μια διακριτή πηγή

# ΠΕΡΙ ΑΛΥΣΙΔΩΝ ΜΑRΚΟΥ & ΔΙΑΚΡΙΤΩΝ ΠΗΓΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

## Εφαρμογή Αλυσίδας Markov

Όταν η αλυσίδα Markov είναι στη κατάσταση του μηνύματος R, έχει .9 πιθανότητα να παραμείνει ώς έχει και .1 πιθανότητα να αλλάξει σε S.

Στην κατάσταση που το μήνυμα είναι S, έχει .7 πιθανότητα να παραμείνει ως έχει και .3 πιθανότητα να αλλάξει σε R



$$P = \begin{bmatrix} .9 & .1 \\ .7 & .3 \end{bmatrix}$$

$$x^{0} = [1 \ 0]$$
  
 $x^{1} = x^{0}P = [1 \ 0]\begin{bmatrix} .9 & .1 \\ .7 & .3 \end{bmatrix} = [.9 \ .1]$   
 $x^{2} = x^{1}P = [.9 \ .1]\begin{bmatrix} .9 & .1 \\ .7 & .3 \end{bmatrix} = [.88 \ .12]$ 

Το μήνυμα αρχίζει ως R

Το δεύτερο μήνυμα κατά 90% θα είναι R και κατα 10% S

Το τρίτο μήνυμα κατά 88% θα είναι R και κατα 12% S Γενικά $x^n = x^{(n-1)}P$ 

### Οποιαδήποτε πηγή που μεταδίδει δεδομένα είναι μια διαδικασία Markov

Αυτή η υπόθεση οδηγεί στην ιδέα του εκ των προτέρων προσδιορισμού των πιθανοτήτων μετάβασης των συμβόλων επικοινωνίας

**Σε απλά ελληνικά:** στην πιθανότητα ενός συμβόλου να ακολουθείται απο άλλο σύμβολο ή ομάδα συμβόλων

Εάν, για παράδειγμα, η πηγή πληροφοριών αποτελείται από λέξεις της αγγλικής γλώσσας (εκτός απο ακρωνύμια), τότε η πιθανότητα μετάβασης του γράμματος "u" μετά το γράμμα "q" είναι 1



VIDEO QUIZZES QUOTES WORD FACTS TRENDS ABOUT THIS WORD V

Why does the letter Q almost always need to appear with a U in order to be useful?



siness Money Life & style Travel Environment TV Video Data Mo

Recent queries Send a query Crosswo lipAny answers? About Notes and Queries Sudoku

Stage and screen

Birds and the bees

### SEMANTIC ENIGMAS

Categories

Nocks and crannies

Yesteryear

The body beautiful

Why is the letter "Q" almost always followed by the letter "U" in some other languages? Can the combination "QU" be considered as a single letter in English, as "LL" and "CH" are in Spanish?

Peter Ford, Birmingham, United Kingdom

The letter "Q" is always followed by the letter "U" in Spanish too. In this language "LL" and "CH" are no longer considered as a single letter.

Antonio, Bariloche Argentina

Probably. There certainly are combinations which are, or have been, treated as single characters, in English. Older books will often have "ae" printed as a single, overlapped character, for example. Some, such as "th", kept their sound but were split up [...]stochastic processes can also be defined to produce a text consisting of a sequence of "words."

Προσεγγίσεις 1<sup>ης</sup> , 2<sup>ης</sup> και 3<sup>ης</sup> τάξης για γράμματα και λέξεις αντίστοιχα

"She said, Do you love me? I tell her, Only partly, I only love my bed and my momma, I'm sorry"

1<sup>n</sup> τάξη 2<sup>n</sup> τάξη 3<sup>n</sup> τάξη

### **Letter Frequency Analysis**

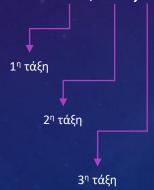
					4/
Use	Frequency				3/
E	0.12702	C	0.02782	J	0.001
T	0.09056	U	0.02758	х	0.001
A	0.08167	М	0.02406	Q	0.000
0	0.07507	w	0.02360	Z	0.000
I	0.06966	F	0.02228		3///
N	0.06749	G	0.02015		
S	0.06327	Y	0.01974		1/36
Н	0.06094	P	0.01929		
R	0.05987	В	0.01492		No. of Contracts
D	0.04253	V	0.00978		The same
L	0.04025	K	0.00772		- Uluca

11

[...]stochastic processes can also be defined to produce a text consisting of a sequence of "words."

Προσεγγίσεις 1<sup>ης</sup> , 2<sup>ης</sup> και 3<sup>ης</sup> τάξης για γράμματα και λέξεις αντίστοιχα

"She said, Do you love me? I tell her, Only partly, I only love my bed and my momma, I'm sorry"



1. Zero-order approximation (symbols independent and equiprobable).

XFOML RXKHRJFFJUJ ZLPWCFWKCYJ FFJEYVKCQSGHYD QPAAMKBZAACIBZL-HJQD.

2. First-order approximation (symbols independent but with frequencies of English text).

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

3. Second-order approximation (digram structure 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.

4. Third-order approximation (trigram structure as in English).

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

First-order word approximation. Rather than continue with tetragram, ..., n-gram structure it is easier
and better to jump at this point to word units. Here words are chosen independently but with their
appropriate frequencies.

REPRESENTING AND SPEEDILY IS AN GOOD APT OR COME CAN DIFFERENT NAT-URAL HERE HE THE A IN CAME THE TO OF TO EXPERT GRAY COME TO FURNISHES THE LINE MESSAGE HAD BE THESE.

Second-order word approximation. The word transition probabilities are correct but no further structure is included.

THE HEAD AND IN FRONTAL ATTACK ON AN ENGLISH WRITER THAT THE CHARACTER OF THIS POINT IS THEREFORE ANOTHER METHOD FOR THE LETTERS THAT THE TIME OF WHO EVER TOLD THE PROBLEM FOR AN UNEXPECTED.

# ΣΗΜΕΡΙΝΕΣ ΕΦΑΡΜΟΓΕΣ

Γονείς με ελεύθερο χρόνο (ή απόγνωση;)

Crying Babies and Markov Chains: How Much Sleep Will You Get Tonight? www.linkedin.com/pulse/crying-babies-markov-chains-how-much-sleep-you-get-tonight-daniel-lee/

Άλλοι τομείς



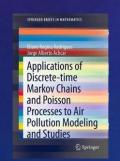
- 2. Text Prediction
- 3. AI
- 4. Machine Learning
- 5. Cryptography

Βήματα που κάνουμε (random walk) Σειρά σκέψεων (decision making, speech) Συμπεριφορά Ποωτεινών (math

Συμπεριφορά Πρωτεινών (math modeling)







6. Άνθρωπος



Τόγιας Παναγιώτης

Στοιχεία Πιθανοτήτων & Στοχαστικές Ανελίξεις