



Θεωρία της Πληροφορίας (Θ)

Ενότητα 1: Θεωρία της Πληροφορίας

ΔΙΔΑΣΚΩΝ: Δρ. Αναστάσιος Πολίτης

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕ



Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.



Ενότητα 1

Θεωρία της Πληροφορίας

ΔΙΔΑΣΚΩΝ: Δρ. Αναστάσιος Πολίτης

Θεωρία της Πληροφορίας 3^ο Εξάμηνο

Τομέας Τηλεπικοινωνιών και Δικτύων

Δρ. Αναστάσιος Πολίτης

- **Διεξαγωγή του Μαθήματος**

- Κάθε πότε?
 - Βλέπε πρόγραμμα εξαμήνου.
- Πού?
 - ΑΜΦ Τμήματος Μηχανικών Πληροφορικής Τ.Ε.
- Πώς?
 - 13 Διαλέξεις (περιλαμβάνουν και τις Ασκήσεις Πράξης)

- **Εξέταση**

- Γραπτή στο τέλος του εξαμήνου.
- Κλειστές σημειώσεις (δίνεται τυπολόγιο).

- **Επικοινωνία και ενημέρωση**

- Ιστοσελίδα Μαθήματος:

<http://www.teiser.gr/icd/staff/politis/mathimata.htm>

- Επικοινωνία με τον διδάσκοντα

anpol@teiser.gr (αποστολές μηνυμάτων που είναι ανώνυμα δεν θα απαντώνται)

- Ώρες γραφείου: βλέπε ιστοσελίδα.

• Βασική βιβλιογραφία μαθήματος

- Εγχειρίδιο Δρ. Ι. Ρέκανου «Θεωρία της Πληροφορίας», Οκτώβριος 2003 (βρίσκεται στη σελίδα του μαθήματος και στο εκπαιδευτικό υλικό).
- Ότι ειπωθεί κατά την διάρκεια των διαλέξεων (παραδείγματα, ασκήσεις)
- Οι διαφάνειες του μαθήματος (μόνο ως βοήθημα).

• Συμπληρωματική βιβλιογραφία

- «Εισαγωγή στη θεωρία πληροφορίας», Αφράτη Φώτω.



- «Θεωρία πληροφοριών – Κώδικες», Βούκαλης Δημήτρης.



• 20^{ος} Αιώνας

- Αιώνας Πληροφορικής και Επικοινωνιών.
- Ανάπτυξη μέσων
 - καταγραφής
 - αποθήκευσης
 - επεξεργασίας
 - μετάδοσης (επικοινωνία)

της πληροφορίας.

- Ραγδαία εξέλιξη τεχνολογικών επιτευγμάτων

Τηλέφωνο



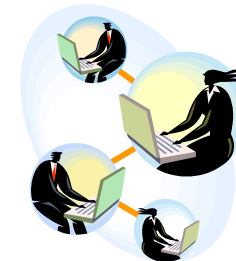
Τηλεόραση



Ραδιόφωνο



Δίκτυα Υπολογιστών



- **Τι είναι όμως η Πληροφορία**
 - Γνώση
 - Ενημέρωση
 - Συμβουλή
 - Δεδομένα
- Παράδειγμα Χρηματιστή-Επενδυτή
 - Ο επενδυτής χρειάζεται **πληροφορίες** από τον χρηματιστή (**Συμβουλή**).
 - Ο χρηματιστής τις δίνει βασιζόμενος σε **πληροφορίες** που κατέχει (**Γνώση**).
 - Ο χρηματιστής **πληροφορεί** τον επενδυτή για τις μετοχές μιας εταιρίας (**Ενημέρωση**).
 - Ο επενδυτής αξιολογεί τις **πληροφορίες** για να πουλήσει/αγοράσει (**Δεδομένα**).
- Η πληροφορία είναι **Μέτρο της Αβεβαιότητας** (ή της βεβαιότητας)
 - Ο επενδυτής μειώνει την **αβεβαιότητα** του συμβουλευόμενος τον χρηματιστή.
 - Ο χρηματιστής γνωρίζει τα χρηματιστηριακά θέματα με **βεβαιότητα**.

- Στις αρχές με μέσα του 20^{ου} αιώνα, η **πληροφορία** ήταν:
 - Έννοια αφηρημένη και ποιοτική (τι αξίζει να πληροφορηθώ?)
 - Άρα, δεν μπορώ να βγάλω νόμους που να περιγράφουν με αυστηρότητα την πληροφορία και επικοινωνία (δύσκολος σχεδιασμός υπολογιστικών και επικοινωνιακών συστημάτων).
- Ενδιαφέρον για ποσοτικοποίηση της πληροφορίας
 - Πόση πληροφορία περιέχεται σε ένα γεγονός.
- **1948**
 - Shannon, “A Mathematical Theory of Communication”
 - Θεμελίωσε έννοιες/θεωρήματα για την μαθηματική περιγραφή της επικοινωνίας.
 - Ακριβής ανάλυση με μαθηματική αυστηρότητα της μετάδοσης πληροφοριών.
 - Μπορώ να σχεδιάσω καλύτερα επικοινωνιακά συστήματα (ξέρω πόση πληροφορία χρειάζεται να μεταδωθεί για ένα γεγονός!).

- Η **ΘτΠ** βασίζεται στη
 - πιθανοθεωρία
 - στατιστική
 - άλγεβρα
- Απαντά σε ερωτήματα που αφορούν:
 - περιγραφή διαύλου επικοινωνίας
 - επικοινωνία σε περιβάλλοντα θορύβου
 - συμπίεση δεδομένων
 - κρυπτογράφηση
- Αρχικά:
 - η **ΘτΠ** αποτέλεσε τμήμα της επιστήμης επικοινωνιών
- Σήμερα:
 - χωριστός κλάδος των μαθηματικών.

- Στη ΘτΠ η έννοια της **πληροφορίας** έχει ποσοτικό χαρακτήρα (\neq εννοιολογικού περιεχομένου).
- Η πληροφορία ενός γεγονότος **A** σχετίζεται με την πιθανότητα πραγματοποίησης του γεγονότος **P_A** και μόνον αυτή. Δηλαδή:

$$I(A) = f(p_A)$$

- Στην πράξη
 - μικρότερη p_A , περισσότερη $I(A)$. Δηλαδή:

$$I(A) \propto \frac{1}{p_A}$$

- Συμφωνεί με κοινή αντίληψη?
 - Μερικές φορές ναι, μερικές όχι!

• Παράδειγμα

- σε συμφωνία με την κοινή αντίληψη:
 - Γεγονός A: «Σήμερα έγινε ολική έκλειψη ηλίου».
 - Γεγονός B: «Σήμερα ο ήλιος ανέτειλε».
- σε ασυμφωνία με την κοινή αντίληψη:
 - Γεγονός A: «Στην εκλογική αναμέτρηση μεταξύ των κομμάτων X και Y, κέρδισε το X».
 - Γεγονός B: «Εριζα τα ζάρια και έτυχα 6-5».

$$I(A) > I(B)$$

$$I(B) > I(A)$$

- Αν A είναι ένα τυχαίο γεγονός, και p_A είναι η πιθανότητα να συμβεί το γεγονός αυτό τότε, το μέτρο της πληροφορίας του A , $I(A)$ θα πρέπει να έχει τις παρακάτω ιδιότητες:

1. Το $I(A)$ θα πρέπει να είναι συνάρτηση της p_A .

$$I(A) = f(p_A)$$

2. Το $I(A)$ θα πρέπει να είναι πραγματική θετική συνάρτηση.
3. Η συνάρτηση $I(A)$ θα πρέπει να είναι γνησίως φθίνουσα:

$$\forall p_A, p_B : p_A > p_B \Rightarrow I(A) < I(B)$$

4. Αν A και B είναι δύο ανεξάρτητα γεγονότα (δηλαδή $p(A \cap B) = p_A \cdot p_B$) τότε το μέτρο της πληροφορίας εμφάνισης και των δύο γεγονότων θα πρέπει να είναι το άθροισμα των δύο επιμέρους μέτρων πληροφορίας:

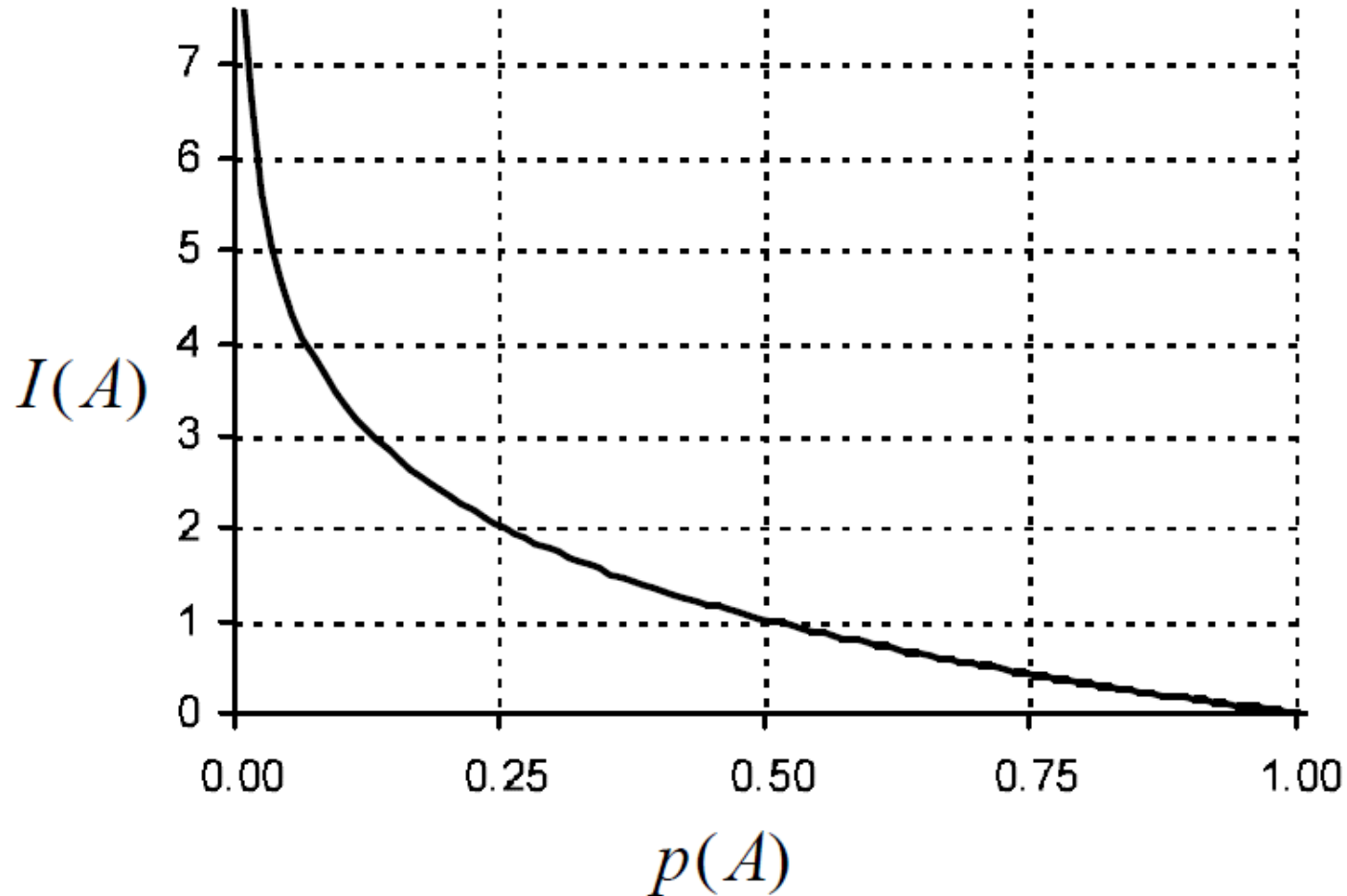
$$I(A \cap B) = I(A) + I(B)$$

- Αποδεικνύεται ότι η **Πληροφορία** (μέτρο της πληροφορίας) δίνεται από τη σχέση:

$$I(A) = -\log_K p_A$$

- Από εδώ και πέρα $K=2$, και μονάδα μέτρησης της πληροφορίας είναι το **bit**.

- Γραφική παράσταση της συνάρτησης της πληροφορίας



- **Εφαρμογή:** Έστω ότι έχουμε τα παρακάτω σύνολα γεγονότων:

$$\text{I. } E = [A_1, A_2] \quad P = \left[\frac{1}{256}, \frac{255}{256} \right] \quad \text{Απ.: } I(A_1) = 8 \text{ bit}, I(A_2) = 0.0056 \text{ bit}$$

$$\text{II. } E = [B_1, B_2] \quad P = \left[\frac{1}{2}, \frac{1}{2} \right] \quad \text{Απ.: } I(B_1) = 1 \text{ bit}, I(B_2) = 1 \text{ bit}$$

$$\text{III. } E = [\Gamma_1, \Gamma_2] \quad P = \left[\frac{7}{16}, \frac{9}{16} \right] \quad \text{Απ.: } I(\Gamma_1) = 1.19 \text{ bit}, I(\Gamma_2) = 0.830 \text{ bit}$$

Να βρεθούν τα μέτρα της πληροφορίας όλων των γεγονότων.

- Παρατηρήσεις:

- Στην I περίπτωση είναι εύκολο να μαντέψουμε ποιό γεγονός θα συμβεί.
- Στην III περίπτωση αυτή η πρόβλεψη είναι δυσκολότερη.
- Στην II περίπτωση είναι πολύ δύσκολο να προβλέψουμε το γεγονός που θα συμβεί.

- **Σχόλιο:** Μήπως υπάρχει ένα μέτρο για να περιγράψει αυτή την **αβεβαιότητα** μας για το σύνολο των γεγονότων και όχι για το καθένα ξεχωριστά;

- Η μέση **αβεβαιότητα** μας για το ποιό γεγονός θα συμβεί μέσα από ένα σύνολο γεγονότων ονομάζεται **εντροπία** και είναι ο σταθμισμένος μέσος όρος των μέτρων της πληροφορίας όλων των γεγονότων:

$$H = - \sum_{i=1}^N p_i \log p_i$$

- Ονομάζεται και μέση πληροφορία.
- Εδώ η μονάδες μέτρησης της εντροπίας είναι το bit/γεγονός.
- **Εφαρμογή:** Έστω ότι έχουμε τα παρακάτω σύνολα γεγονότων:

$$\text{I. } E = [A_1, A_2] \quad P = \left[\frac{1}{256}, \frac{255}{256} \right] \quad \text{Απ.: } H(E) = 0.0368 \text{ bit}$$

$$\text{II. } E = [B_1, B_2] \quad P = \left[\frac{1}{2}, \frac{1}{2} \right] \quad \text{Απ.: } H(E) = 1 \text{ bit}$$

$$\text{III. } E = [\Gamma_1, \Gamma_2] \quad P = \left[\frac{7}{16}, \frac{9}{16} \right] \quad \text{Απ.: } H(E) = 0.987 \text{ bit}$$

Να βρεθεί η μέση πληροφορία που περιλαμβάνεται σε κάθε σύνολο γεγονότων.

• Εφαρμογή I

- Ποιά είναι η πληροφορία που περιέχει το γεγονόςτος: «έριξα τα ζάρια και έτυχα έξι-πέντε»?
Απ.: $I=4.17$ bits

• Εφαρμογή II

- Πόση πληροφορία περιέχεται στον αριθμό κυκλοφορίας αυτοκινήτου μορφής $ΓΤΓaaaa$, όπου $Γ$ είναι κεφαλαίο γράμμα και a αριθμός.
(Βοήθεια: για ελληνικές πινακίδες χρησιμοποιούνται 14 διεθνή γράμματα και ο τετραψήφιος αριθμός μπορεί να πάρει 9000 διαφορετικές τιμές)
Απ.: $I=24.56$ bits

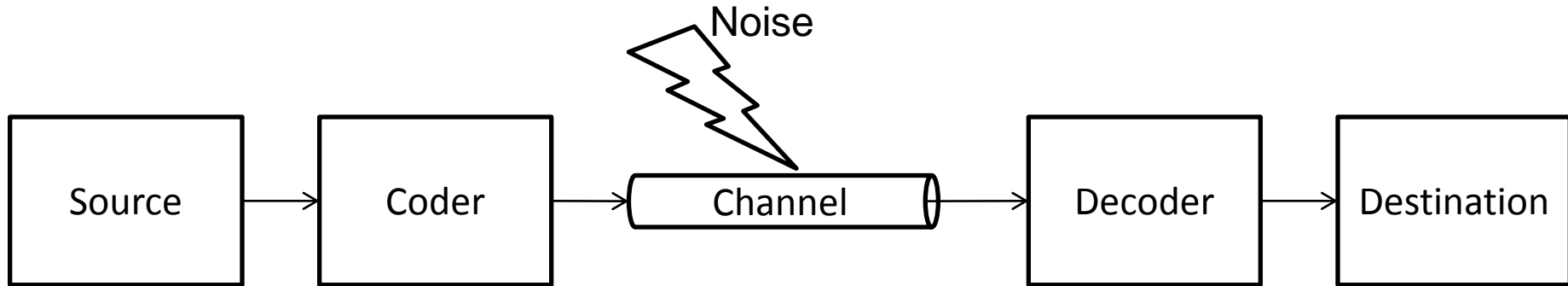
• Εφαρμογή III

- Να βρεθεί η εντροπία ενός ζαριού.
Απ.: $H=2.58$ bits

• Εφαρμογή IV

- Γνωρίζουμε από την ιστορία ότι ο τελευταίος αρχηγός της φυλής των Λιλιπούα είχε δύο παιδιά. Νεότερες έρευνες κατέληξαν σε δύο συμπεράσματα:
Α. Ο αρχηγός είχε μια κόρη και ένα γιο.
Β. Ο αρχηγός είχε μια κόρη και ένα μεγαλύτερο γιο.
Πόση πληροφορία θα λάβουμε με την ανακοίνωση μόνο του πρώτου συμπεράσματος και πόση μόνο με την ανακοίνωση του δεύτερου; Πόση θα είναι η πληροφορία εάν ανακοινωθούν και τα δύο μαζί;

- Σύμφωνα με την **ΘτΠ (Shannon)**
 - γενικό σύστημα επικοινωνίας



- **Πηγή:** οποιοδήποτε άτομο ή μηχανή που παράγει πληροφορία.
- **Κωδικοποιητής:** μετατρέπει κάθε πληροφορία της πηγής σε μορφή κατάλληλη για μετάδοση.
- **Κανάλι επικοινωνίας:** το μέσο μέσω του οποίου μεταδίδεται η πληροφορία.
- **Αποκωδικοποιητής:** προσπαθεί να εξάγει την αρχική πληροφορία από την κωδικοποιημένη μορφή της.
- **Προορισμός:** οποιοδήποτε άτομο ή μηχανή που είναι ο αποδέκτης της πληροφορίας.

- **1^{ος} Ορισμός**

- *Πληροφορία είναι μία συλλογή δεδομένων, τα οποία καταγράφονται με τη χρήση συμβόλων.*

- **2^{ος} Ορισμός**

- *Πηγή πληροφορίας είναι κάθε σύστημα που παράγει στην έξοδο του πληροφορία.*

- **3^{ος} Ορισμός**

- *Επικοινωνία είναι κάθε διαδικασία μεταφοράς της πληροφορίας μεταξύ δύο σημείων του χωροχρόνου.*

- **4^{ος} Ορισμός**

- *Αλφάβητο της Πηγής είναι το σύνολο των διακεκριμένων (διαφορετικών) συμβόλων, x_1, x_2, \dots, x_N που χρησιμοποιούνται για την αναπαράσταση της πληροφορίας που παράγεται από μία πηγή. Το αλφάβητο της πηγής συμβολίζεται ως: $X = \{x_1, x_2, \dots, x_N\}$. Το πλήθος N των συμβόλων δύναται να είναι πεπερασμένο ή άπειρο.*

- **5^{ος} Ορισμός**

- *Ως λέξη ορίζουμε μια διατεταγμένη ακολουθία συμβόλων.*

- **6^{ος} Ορισμός**

- *Ως μήνυμα ορίζουμε μια διατεταγμένη ακολουθία λέξεων.*

- Η πηγή παράγει στην έξοδο της πληροφορία η οποία έχει την μορφή συμβόλων.
- Τα σύμβολα προέρχονται από ένα σύνολο συμβόλων $X = \{x_1, x_2, \dots, x_N\}$ (αλφάβητο).
- Το κάθε σύμβολο έχει μια πιθανότητα εμφάνισης στην έξοδο της πηγής. Συνολικά η πηγή έχει μια κατανομή πιθανοτήτων του συνόλου των συμβόλων που διαθέτει $P_X = \{p_{x1}, p_{x2}, \dots, p_{xN}\}$.
- Η πηγή συμβολίζεται από την δυάδα που σχηματίζουν το αλφάβητο της και η κατανομή πιθανοτήτων των συμβόλων: (X, P_X)
- Τα διαδοχικά σύμβολα που εκπέμπονται από την πηγή είναι στατιστικά ανεξάρτητα μεταξύ τους:
 - το σύμβολο που εκπέμπεται οποιαδήποτε χρονική στιγμή είναι ανεξάρτητο από προηγούμενες επιλογές. (Διακριτή πηγή χωρίς μνήμη)

- Ισχύουν:

$$\sum_{i=1}^N p_i = 1$$

$$I(x_i) = -\log p_{x_i} \quad \text{Πληροφορία συμβόλου}$$

- Η **εντροπία πηγής** είναι ένα μέγεθος που σχετίζεται με την πηγή συνολικά.
- Εκφράζει την μέση αβεβαιότητα που έχουμε για το ποιό σύμβολο θα εμφανιστεί στην έξοδο της πηγής.

$$H(X) = -\sum_{i=1}^N p_{x_i} \log p_{x_i}$$

Εντροπία πηγής

- Μετράται σε **bits/symbol**.
- Όταν αναφερόμαστε σε πηγή πληροφορίας οι μονάδες εντροπίας θα είναι **bits/symbol**.
- Ιδιότητες της εντροπίας:

- Είναι μη αρνητική:

$$H(X) \geq 0$$

- Είναι συνεχής συνάρτηση των πιθανοτήτων p_1, p_2, \dots, p_N .

- Δηλαδή, μια μικρή μεταβολή στις πιθανότητες προκαλεί μικρή μόνο μεταβολή στην τιμή της εντροπίας.

- **Μέγιστη εντροπία**

- Η εντροπία μιας πηγής (X, P_X) διακριτών συμβόλων είναι μέγιστη όταν τα σύμβολα της πηγής είναι ισοπίθανα:

$$p_1 = p_2 = \dots = p_N = \frac{1}{N}$$

Η αβεβαιότητα μας (εντροπία) για την έξοδο της πηγής είναι μέγιστη όταν όλα τα σύμβολα της πηγής έχουν την ίδια πιθανότητα εμφάνισης. Άρα τα όρια της εντροπίας πηγής είναι:

$$0 \leq H(X) \leq \log N$$

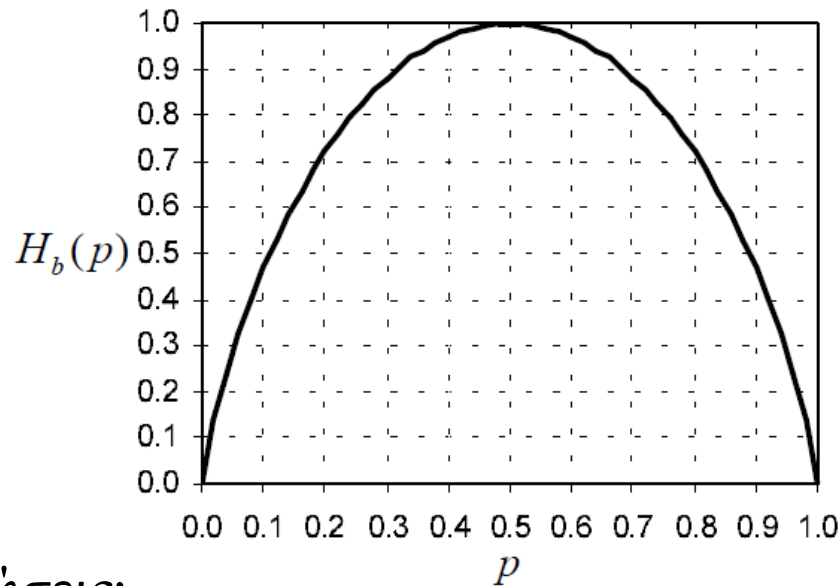
- **Ρυθμός μετάδοσης πληροφορίας**

- Αν ο ρυθμός εκπομπής συμβόλων στο επικοινωνιακό κανάλι είναι r σύμβολα/sec τότε ο μέσος ρυθμός πληροφορίας, R , στην είσοδο του καναλιού είναι:

$$R = H \cdot r \quad \text{bits / sec}$$

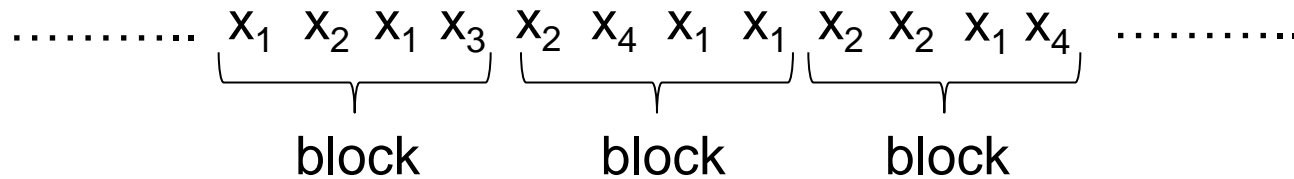
- Δυαδική πηγή πληροφορίας
 - το αλφάβητο της διαθέτει δύο σύμβολα, π.χ. $X=\{0,1\}$, $X=\{A,B\}$.
- Εντροπία Δυαδικής Πηγής δίνεται από την **Συνάρτηση Shannon**:

$$H_b(p) = -p \log p - (1-p) \log(1-p)$$



- Παρατηρήσεις:
 - Όταν $p=0$ ή $p=1$, η $H_b(p)=0$ γιατί $0\log 0=0$ και $1\log 1=0$.
 - Όταν $p=1/2$, η $H_b(p)=1$ (μέγιστη τιμή)

- Πολλές φορές είναι χρήσιμο να θεωρούμε τμήματα (**blocks**) συμβόλων αντί για μεμονωμένα σύμβολα:



- Το κάθε τμήμα αποτελείται από n σύμβολα πηγής (λέξεις σταθερού μήκους).
- Μπορούμε να θεωρήσουμε ότι το κάθε υπερ-σύμβολο (**block**) παράγεται από μια εκτεταμένη πηγή X^n με αλφάβητο το οποίο αποτελείται από N^n διακριτά υπερ-σύμβολα, όπου N ο αριθμός των διακριτών συμβόλων της αρχικής πηγής X .
- **Παράδειγμα:** έστω η δυαδική πηγή $X=\{0,1\}$ με κατανομή $P_x=\{p_0,p_1\}$. Η δεύτερη επέκταση της θα παράξει την εκτεταμένη πηγή $X^2=\{00,01,10,11\}$ η οποία θα έχει κατανομή $P_{X^2}=\{p_0p_0, p_0p_1, p_1p_0, p_1p_1\}$ (διότι τα σύμβολα είναι ανεξάρτητα μεταξύ τους).
- Εντροπία n -ιοστής επέκτασης πηγής:

$$H(X^n) = -\sum_{i=1}^{N^n} p_{s_i} \log p_{s_i}$$

$$H(X^n) = n \cdot H(X)$$

όπου p_{s_i} πιθανότητα υπερ-συμβόλου

- **Εφαρμογή I:** Να υπολογιστεί η εντροπία ενός νομίσματος, όταν:
 - α) αυτό είναι τίμιο. Απ.: $H=1$ bit
 - β) η ένδειξη «κεφαλή» έχει δύο φορές μεγαλύτερη πιθανότητα να εμφανιστεί από την ένδειξη «γράμματα». Απ.: $H=0.918$ bits
- **Εφαρμογή II:** Θεωρούμε πηγή με αλφάβητο $X=\{0,1\}$. Και $p_1=0.7$. Να βρεθεί η πληροφορία του κάθε συμβόλου της πηγής. Επίσης, να βρεθεί η εντροπία της πηγής.
Απ.: $I(1)=0.515$ bits, $I(0)=1.737$ bits, $H(X)=0.8816$ bits/symbol
- **Εφαρμογή III :** Μία πηγή έχει αλφάβητο $X=\{O,E,B,\Delta\}$ και κατανομή πιθανοτήτων $P_X=\{1/2, 1/4, 1/8, 1/8\}$. Εάν το κάθε σύμβολο του αλφαβήτου είναι ανεξάρτητο, ποιά η πληροφορία της λέξης ΟΕΟ. Ποιά η εντροπία της πηγής; Απ.: $I(OEO)=4$ bits, $H(X)=1.75$ bits/sym
- **Εφαρμογή IV:** Θεωρούμε μια πηγή X με N σύμβολα και κατανομή πιθανοτήτων $P_X=\{p_1, p_2, \dots, p_N\}$. Να αποδειχθεί ότι για την εντροπία ισχύει:

$$H(p_1, p_2, p_3, \dots, p_N) = H(p_1 + p_2, p_3, \dots, p_N) + (p_1 + p_2) \cdot H\left(\frac{p_1}{p_1 + p_2}, \frac{p_2}{p_1 + p_2}\right)$$
- **Εφαρμογή V:** Θεωρούμε διακριτή πηγή χωρίς μνήμη με αλφάβητο πηγής $X=\{s_\emptyset, s_p, s_2\}$ και κατανομή $P_X=\{1/4, 1/4, 1/2\}$. Να γραφεί το αλφάβητο, η κατανομή πιθανοτήτων και να βρεθεί η εντροπία της δεύτερης επέκτασης της πηγής X .

• Σχετική εντροπία

• Αν $P_X = \{p_1, p_2, \dots, p_N\}$ και $Q_X = \{q_1, q_2, \dots, q_N\}$ είναι δύο εναλλακτικές κατανομές πιθανοτήτων των συμβόλων $X = \{x_1, x_2, \dots, x_N\}$ μιας πηγής τότε:

$$H(X, P_X / Q_X) = \sum_{i=1}^N p_i \log \frac{p_i}{q_i}$$

Είναι η **απόκλιση Kullback-Leibler** των κατανομών P_X και Q_X για το αλφάβητο X .

Πρόκειται για μια μέθοδο «σύγκρισης» δύο διαφορετικών κατανομών για την ίδια τυχαία μεταβλητή.

- **Παράδειγμα:** Έστω μια πηγή πληροφορίας με αλφάβητο $\mathbf{X}=\{\mathbf{K},\mathbf{\Gamma}\}$. Τα σύμβολα εμφανίζονται στην έξοδο της πηγής μετά την ρίψη ενός νομίσματος. Το σύμβολο K εάν το αποτέλεσμα της ρίψης είναι «Κεφαλή» και το σύμβολο Γ εάν είναι «Γράμματα». Εάν θέλαμε να σχεδιάσουμε ένα επικοινωνιακό σύστημα τότε θα θεωρούσαμε ως κατανομή πιθανοτήτων της πηγής X την θεωρητική κατανομή πιθανοτήτων $\mathbf{Q}_X=\{\mathbf{0.5},\mathbf{0.5}\}$. Ωστόσο, στην πραγματικότητα η κατανομή πιθανοτήτων μπορεί να είναι $\mathbf{P}_X=\{\mathbf{0.4},\mathbf{0.6}\}$ λόγω των αλλοιώσεων στην μορφολογία του νομίσματος.
- Επομένως θα είχαμε λάβει ως κατανομή πιθανοτήτων της πηγής \mathbf{X} την \mathbf{Q}_X (μοντέλο) ενώ η πραγματική κατανομή θά είναι η \mathbf{P}_X .
- Αυτή η αναποδοτικότητα φαίνεται από την απόκλιση Kullback-Leibler:

$$H(X, P_X / Q_X) = \sum_{i=1}^N p_i \log \frac{p_i}{q_i} = 0.4 \log \frac{0.4}{0.5} + 0.6 \log \frac{0.6}{0.5} = 0.029049406 \text{ bits / symbol}$$

- Θα θεωρήσουμε ότι επιπλέον 0.029 bits/symbol ότι θα παραχθούν από την πηγή
- Προφανώς θα ισχύει:

$$H(X, P_X / P_X) = 0$$

- Σημασία της σχετικής εντροπίας:
 - Εκφράζει την απόκλιση της κατανομής P_X από την Q_X . Πόση δηλαδή επιπλέον πληροφορία ανά σύμβολο θα παραχθεί από την πηγή εάν θεωρήσουμε ως κατανομή πιθανοτήτων των συμβόλων της πηγής την Q_X , ενώ στην πραγματικότητα είναι η P_X .
 - Η απόκλιση Kullback-Leibler «αποκαλύπτει» και ποσοτικοποιεί την αναποδοτικότητα που θα υπάρξει εάν ο σχεδιασμός ενός επικοινωνιακού συστήματος βασιστεί στην λανθασμένη κατανομή.
- Η σχετική εντροπία είναι πάντα μεγαλύτερη ή ίση του μηδενός:

$$H(X, P_X / Q_X) = 0 \quad \text{για } P_X = Q_X$$

$$H(X, P_X / Q_X) > 0 \quad \text{για } P_X \neq Q_X$$

- Η σχετική εντροπία δεν είναι συμμετρική ως προς τις δύο κατανομές:

$$H(X, P_X / Q_X) \neq H(X, Q_X / P_X)$$

Γι' αυτό και λέγεται **απόκλιση (divergence)** και όχι **απόσταση (distance)**.

- **Εφαρμογή I:** Θεωρούμε την πηγή $X = \{0, 1\}$ με δύο εναλλακτικές κατανομές πιθανοτήτων, $P_X = \{0.3, 0.7\}$ και $Q_X = \{0.6, 0.4\}$. Να υπολογιστούν οι αποκλίσεις Kullback-Leibler, $H(X, P_X/Q_X)$ και $H(X, Q_X/P_X)$.

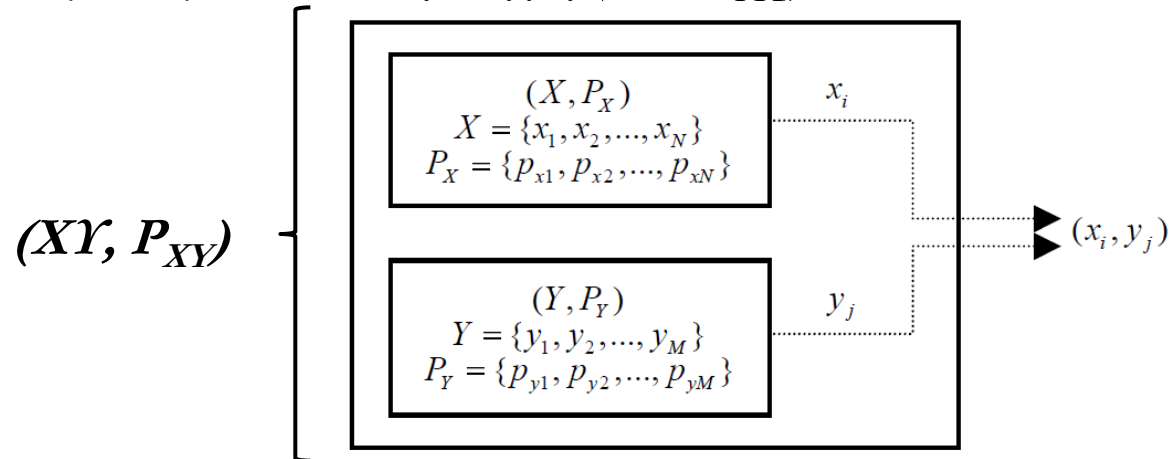
Απ.: $H(X, P_X/Q_X) = 0.2651$ bits/symbol, $H(X, Q_X/P_X) = 0.277$ bits/symbol

- **Εφαρμογή II:** Να υπολογιστούν οι αποκλίσεις Kullback-Leibler μεταξύ των εναλλακτικών κατανομών πιθανοτήτων $P = \{0.2, 0.3, 0.5\}$ και $Q = \{0.4, 0.5, 0.1\}$. Ισχύει η αντιμεταθετική ιδιότητα; **Απ.:** $H(X, P_X/Q_X) = 0.741$ bits/symbol, $H(X, Q_X/P_X) = 0.536$ bits/symbol, Όχι δεν ισχύει

- **Εφαρμογή III:** Να δειχθεί ότι:

$$H(X, P_X / Q_X) + H(X, Q_X / P_X) = \sum_{i=1}^N (p_i - q_i) \log \frac{p_i}{q_i}$$

- Θεωρούμε την σύνθετη πηγή (XY, P_{XY}) :



- Αλφάβητο της νέας πηγής:

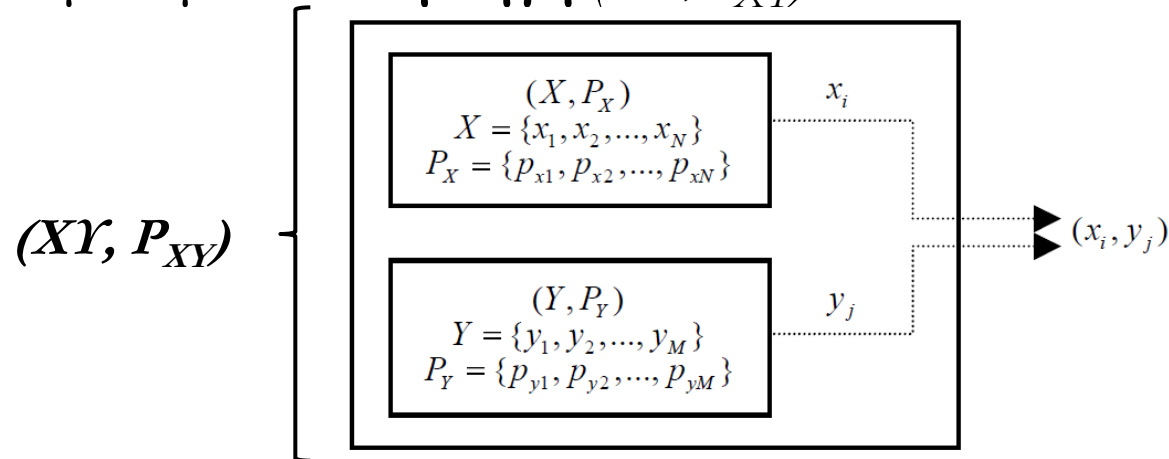
$$XY = \{(x_1, y_1), (x_2, y_1), \dots, (x_N, y_1), (x_1, y_2), (x_2, y_2), \dots, (x_N, y_2), \dots, (x_1, y_M), (x_2, y_M), \dots, (x_N, y_M)\}$$

- Εντροπία της σύνθετης πηγής:

$$H(XY) = - \sum_{i=1}^N \sum_{j=1}^M p(x_i, y_j) \log p(x_i, y_j)$$

- Ισχύει: $H(XY) = H(X) + H(Y)$ εάν οι πηγές είναι ανεξάρτητες
 $H(XY) < H(X) + H(Y)$ αλλιώς

- Θεωρούμε την σύνθετη πηγή (XY, P_{XY}) :



- Θεωρούμε ότι γνωρίζουμε ει των προτέρων την έξοδο της πηγής (Y, P_Y) . Δηλαδή ισχύει:

$$p(x_i | y_j) = \frac{p(x_i, y_j)}{p(y_j)}$$

- Η υπό συνθήκη εντροπία της σύνθετης πηγής (XY, P_{XY}) γνωρίζοντας την έξοδο της απλής πηγής (Y, P_Y) δίνεται:

$$H(X | Y) = -\sum_{i=1}^N \sum_{j=1}^M p(x_i, y_j) \log p(x_i | y_j)$$

Αντίστοιχα θα ισχύει:

$$H(Y | X) = -\sum_{i=1}^N \sum_{j=1}^M p(x_i, y_j) \log p(y_j | x_i)$$

- Σχέση υπο συνθήκη εντροπίας με την συνδυαστική εντροπία και τις εντροπίες πηγών:

$$H(X | Y) = H(XY) - H(Y)$$

- Η παραπάνω σχέση ερμηνεύεται και διαισθητικά:
 - Η υπό συνθήκη εντροπία $H(X | Y)$ γνωρίζοντας την έξοδο μιας απλής πηγής $H(Y)$ θα προκύπτει εάν από την συνδυαστική εντροπία της πηγής $H(XY)$ αφαιρέσουμε την εντροπία της γνωστής πηγής $H(Y)$.
- Προφανώς θα ισχύει:

$$H(Y | X) = H(XY) - H(X)$$

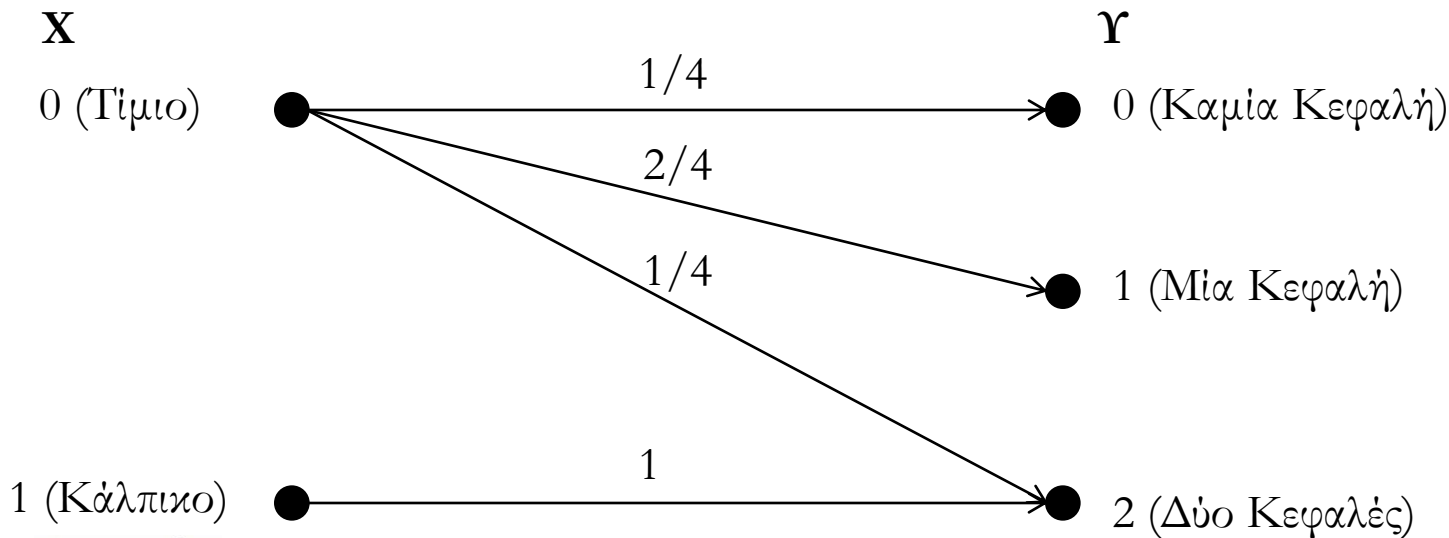
- Εκτελούμε το ακόλουθο πείραμα:
 1. Διαθέτουμε 2 νομίσματα. Το ένα «τίμιο» και το άλλο «κάλπικο». Το «κάλπικο» διαθέτει δύο Κεφαλές.
 2. Επιλέγουμε ένα από τα δύο νομίσματα **τυχαία** και το ρίχνουμε δύο φορές.
 3. Καταγράφουμε τον αριθμό των κεφαλών που προκύπτουν.
- Κατόπιν κάνουμε την ερώτηση:

«Πόση πληροφορία πήραμε για την ταυτότητα του νομίσματος (τίμιο ή κάλπικο) μετρώντας πόσες Κεφαλές είδαμε στο τέλος του πειράματος;»
- **Παρατηρήσεις**
 - **Σίγουρα** ο αριθμός των κεφαλών μπορεί να μας δώσει μια ιδέα για το ποιο νόμισμα επιλέχθηκε:
 - Αριθμός Κεφαλών < 2 , **σίγουρα** το νόμισμα που επιλέχθηκε ήταν το τίμιο νόμισμα.
 - Αριθμός Κεφαλών $= 2$, τότε ενδεχομένως να επιλέχθηκε το κάλπικο νόμισμα.

• Έστω:

- Τυχαία μεταβλητή X =«επιλογή του νομίσματος» (0 για το τίμιο και 1 για το κάλπικο).
- Τυχαία μεταβλητή Y =«ο αριθμός των κεφαλών» (0 για καμία 1 για μία και 2 για δύο).

• Γραφική αναπαράσταση του πειράματος:



Δειγματοχώρος
«Τίμιου» Ζαριού

1. ΚΓ
2. ΓΚ
3. ΚΚ
4. ΓΓ

Δειγματοχώρος
«Κάλπικου» Ζαριού

1. ΚΚ

- Θεωρούμε τον διάυλο πληροφορίας που στην είσοδο και στην έξοδο του λειτουργούν δυο πηγές πληροφορίας (X, P_X) και (Y, P_Y) .
- Θεωρούμε παρατηρητή στην έξοδο (δηλαδή στην πηγή (Y, P_Y)).
- Κάποια στιγμή ο παρατηρητής βλέπει στην πηγή (Y, P_Y) το σύμβολο y_j .
- **Ερώτημα:**
 - «Βλέποντας το σύμβολο y_j , πόση πληροφορία αποκόμισε ο παρατηρητής για το ποιό σύμβολο x_i ειπέμθηκε αρχικά από την πηγή στην είσοδο του διαύλου;»
- Αρχικά (πριν την εμφάνιση του συμβόλου y_j στην έξοδο του διαύλου)
 - η αβεβαιότητα του παρατηρητή για το ποιό σύμβολο θα εμφανιστεί στην είσοδο του διαύλου είναι $H(X)$.
- Με την εμφάνιση του συμβόλου y_j
 - η αβεβαιότητα του μειώθηκε κατά $H(X | Y)$.

- Άρα:
 - Η πληροφορία που αποκόμισα για την πηγή X γνωρίζοντας το αποτέλεσμα της πηγής Y θα είναι:
- $$I(X \rightarrow Y) = H(X) - H(X | Y)$$
- Η $I(X \rightarrow Y)$ ονομάζεται διαπληροφορία και προσδιορίζει: «πόσο μειώθηκε η αβεβαιότητα του παρατηρητή για την έξοδο της πηγής X γνωρίζοντας την έξοδο της πηγής Y ».
 - Πρακτικά εκφράζει το ποσό της πληροφορίας που μεταφέρθηκε από την είσοδο του διαύλου στην έξοδο του (σε **bits/symbol**).
 - Ιδιότητες
 - Η $I(X \rightarrow Y)$ είναι συμμετρική συνάρτηση. Δηλαδή ισχύει:

$$I(X \rightarrow Y) = I(Y \rightarrow X) = H(Y) - H(Y | X)$$

- Η $I(X \rightarrow Y)$ είναι μη αρνητική:

$$I(X \rightarrow Y) \geq 0$$

- Πότε η διαπληροφορία είναι ίση με μηδέν;

- **Εφαρμογή I:** Να δείξετε ότι για τις πηγές X (στην είσοδο ενός διαύλου) και Y (στην έξοδο του διαύλου) ισχύει:

$$H(Y) = H(X) - H(X | Y) + H(Y | X)$$

- **Εφαρμογή II:** Να δείξετε ότι για τις πηγές X (στην είσοδο ενός διαύλου) και Y (στην έξοδο του διαύλου) ισχύει:

$$I(X \rightarrow Y) = H(X) - H(XY) + H(Y)$$

- **Εφαρμογή III:** Να δείξετε ότι ισχύει η παρακάτω σχέση:

$$I(X \rightarrow Y) = H(XY, P_{XY} / (P_X \cdot P_Y))$$

- **Εφαρμογή IV:** Θεωρούμε δυο δυαδικές πηγές πληροφορίας με αλφάβητα $X = \{x_1, x_2\}$ και $Y = \{y_1, y_2\}$, αντίστοιχα. Γνωρίζουμε ότι ισχύουν οι εξής πιθανότητες: $p(x_1) = 0.2$, $p(y_1) = 0.3$ και $p(x_1, y_2) = 0.15$. Να βρεθούν:

1. Οι εντροπίες των πηγών. **Απ.:** $H(X) = 0.722$ bits/symbol, $H(Y) = 0.881$ bits/symbol
2. Η συνδυαστική εντροπία της σύνθετης πηγής. **Απ.:** $H(XY) = 1.601$ bits/symbol
3. Οι υπό συνθήκη εντροπίες. **Απ.:** $H(X | Y) = 0.720$ bits/symbol, $H(Y | X) = 0.879$ bits/symbol
4. Η διαπληροφορία μεταξύ των πηγών X και Y . **Απ.:** $I(X \rightarrow Y) = 0.002$ bits/symbol

• **Εφαρμογή I** (Εξεταστική 2009):

• Έστω δύο δυαδικές πηγές A και B. Υποθέτουμε $0 < p_A(0) < p_B(0) < 0.5$. Ποιά δυαδική πηγή έχει την μεγαλύτερη εντροπία; **Απ.: B**

• **Εφαρμογή II** (Εξεταστική 2009):

• Έστω μια τριαδική πηγή $A = \{0,1,2\}$. Υπολογίστε τις πιθανότητες $p(0)$, $p(1)$ και $p(2)$, έτσι ώστε να μεγιστοποιείται η εντροπία της πηγής A. **Απ.: $p(0)=p(1)=p(2)=1/3$**

• **Εφαρμογή III** (Εξεταστική 2007):

• Θεωρούμε δυο δυαδικές πηγές πληροφορίας $X = \{x_1, x_2\}$ και $Y = \{y_1, y_2\}$ για τις οποίες ισχύουν $p(x_2) = 0.2$, $p(y_1) = 0.3$ και $p(y_2 | x_2) = 0.3$. Να βρεθούν:

1. Οι εντροπίες $H(X)$ και $H(Y)$. **Απ.: $H(X) = 0.721$ bits/symbol, $H(Y) = 0.881$ bits/symbol**
2. Η συνδεδειγμένη εντροπία $H(XY)$. **Απ.: $H(XY) = 1.475$ bits/symbol**
3. Η διαπληροφορία $I(X;Y)$ των πηγών. **Απ.: $I(X \rightarrow Y) = 0.127$ bits/symbol**

• **Εφαρμογή IV**

• Ρίχνουμε ένα «τίμιο» ζάρι μια φορά. Εάν το αποτέλεσμα είναι 1, 2, 3, ή 4, τότε ρίχνουμε ένα «τίμιο» νόμισμα μια φορά. Εάν η ένδειξη του ζαριού είναι 5 ή 6, τότε ρίχνουμε το νόμισμα δύο φορές. Να βρεθεί η πληροφορία που αποκομίσαμε για την ένδειξη του ζαριού από την καταμέτρηση των «Κεφαλών» μετά την ρίψη/εις του νομίσματος.

Απ.: $H(X) \sim 0.918$ bits, $H(Y) \sim 1.324$ bits, $H(XY) \sim 2.083$ bits $\longrightarrow I(X \rightarrow Y) \sim 0.16$ bits

Τέλος Ενότητας

