

Ψηφιακές Τηλεπικοινωνίες

Θεωρία Πληροφορίας:

Κωδικοποίηση Πηγής

Ψηφιακή Μετάδοση

- Υπάρχουν ιδιαίτερα εξελιγμένες τεχνικές **αναλογικής** μετάδοσης (που ακόμη χρησιμοποιούνται σε ορισμένες εφαρμογές)
- Επίσης, υπάρχουν **Υβριδικές λύσεις** και μάλλον θα υπάρχουν για πολύ ακόμη **(γιατί ;)**
- Όμως, η **ψηφιακή μετάδοση** έχει σαφή **πλεονεκτήματα**, όπως:
 - μεγαλύτερη ανοσία σε θόρυβο, παρεμβολές, παραμορφώσεις
 - ευελιξία στην ανταλλαγή εύρους ζώνης και ισχύος
 - προσφέρει νέες δυνατότητες πολυπλεξίας
 - τεχνικές κρυπτογράφησης και προστασίας
 - ευελιξία στην υλοποίηση σε διάφορες πλατφόρμες υλικού
- Η **Ψηφιακή Μετάδοση** απαιτεί **Ψηφιακά Δεδομένα**
- Αν τα δεδομένα είναι **Αναλογικά**, θα πρέπει να μετατραπούν σε **Ψηφιακά**
- **Ερώτηση:** Χάνεται πληροφορία κατά τη μετατροπή A/D;

Θεωρία Πληροφορίας

- Βασικοί Στόχοι στις Ψηφιακές Τηλεπικοινωνίες:
 1. Η **αποδοτική αναπαράσταση** των δεδομένων που εξάγει μια πηγή πληροφορίας
 2. Η **αποδοτική μετάδοση** της πληροφορίας πάνω από ένα κανάλι
- Με το πρώτο ζήτημα ασχολείται η **κωδικοποίηση πηγής (source coding)**
 - θα μας απασχολήσει στα αμέσως επόμενα μαθήματα
- Με το δεύτερο ζήτημα ασχολείται η **κωδικοποίηση καναλιού (channel coding)** και έχουν άμεση σχέση και άλλα υποσυστήματα
 - θα μας απασχολήσει σε μεθεπόμενα μαθήματα
- Τα δύο αυτά αντικείμενα ανήκουν στον ευρύτερο χώρο της **Θεωρίας Πληροφορίας (Information Theory)**

Claude Shannon "(The→A) Mathematical Theory of Communication"

Κωδικοποίηση Πηγής

- Στόχος: η αποδοτική αναπαράσταση/κωδικοποίηση/συμπύεση της πληροφορίας/σήματος/εξόδου μιας πηγής
- Ερωτήματα που προκύπτουν:
 - πώς ορίζεται η πληροφορία μιας πηγής;
 - μπορώ να τη μετρήσω μαθηματικά;
 - πότε μια πηγή παράγει περισσότερη πληροφορία;
 - τι παθαίνει η πληροφορία μιας πηγής όταν εφαρμόζω κάποια επεξεργασία (π.χ. μετατροπή A/D, περαιτέρω συμπύεση);
 - πόσο πολύ μπορώ να συμπιέσω τα δεδομένα μιας πηγής;
 - Πληροφορία vs ψηφιακά δεδομένα
- Απαντήσεις
 - δίνονται μέσα από τη Θεωρία Πληροφορίας και ιδιαίτερα τη θεωρία και τις τεχνικές κωδικοποίησης πηγής

Πηγές Πληροφορίας

- Η έξοδος της πηγής είναι
 - κάτι **τυχαίο και άγνωστο**
 - μια **τυχαία διαδικασία**
- **Παραδείγματα** ειδών πληροφορίας:
 - Ήχος, ομιλία, εικόνα, video
 - Bits, χαρακτήρες ASCII
 - Βιο-ιατρικά σήματα, Γεωφ. Σήματα, Δεδομένα πλοήγησης,
 - Οικονομικές χρονοσειρές, Παραγωγικές διαδικασίες,
 - ... και πολλά άλλα.
- **Διάκριση ως προς το χρόνο (ή και χώρο):**
 - συνεχούς χρόνου (π.χ. σήμα μουσικής)
 - διακριτού χρόνου (π.χ. δείγματα μετρήσεων)
- **Διάκριση ως προς τις δυνατές τιμές (αλφάβητο):**
 - συνεχείς τιμές (π.χ. αναλογικό σήμα)
 - διακριτές τιμές (π.χ. κείμενο)

Πηγές Πληροφορίας (2)

- Μετατροπή πηγής από συνεχούς σε διακριτού χρόνου
 - δειγματοληψία
 - το σήμα πρέπει να έχει πεπερασμένο εύρος ζώνης
 - αν είναι κατωπερατό με μέγιστη συχνότητα f_{max} , τότε η συνθήκη Nyquist μας λέει ότι αρκεί να το δειγματοληπτήσω με

$$f_s \geq 2f_{max}$$

- και τότε μπορώ να ανακατασκευάσω το αναλογικό σήμα από τα δείγματα χωρίς απώλειες
- Οι πηγές που μας ενδιαφέρουν,
 - έχουν περιορισμένο εύρος ζώνης
 - ή μπορούμε να το περιορίσουμε εμείς με φιλτράρισμα
- **Συμπέρασμα:** αρκεί να μελετήσω τις πηγές διακριτού χρόνου
- **Ερώτημα:** Πώς γίνεται η δειγματοληψία στοχαστικού σήματος;

Πληροφορία

- Εστιάζουμε στις πηγές πληροφορίας με **διακριτό αλφάβητο** (λόγω ευκολίας αλλά όχι μόνο)
- Θα δούμε και λίγα πράγματα για πηγές με συνεχές αλφάβητο
- **Αλφάβητο Διακριτής Πηγής:** $\Phi = \{s_1, s_2, \dots, s_N\}$
- **Παράδειγμα:** Το αλφάβητό μας είναι το αποτέλεσμα δίκαιου ποδοσφαιρικού αγώνα ανάμεσα στις ομάδες

Real Madrid vs CEID team

- s_1 : 1
- s_2 : X
- s_3 : 2

Ποιο γεγονός φέρει **περισσότερη πληροφορία**;

- όταν τυχαίνει το σύμβολο s_1 , το s_2 ή το s_3 ;
- με τι σχετίζεται η πληροφορία που φέρει κάθε σύμβολο;

Μέτρο Πληροφορίας

1. Η πληροφορία ενός συμβόλου θα πρέπει να είναι μια **φθίνουσα συνάρτηση** της **πιθανότητας εμφάνισης**
2. Μικρή αλλαγή στην πιθανότητα \rightarrow μικρή αλλαγή στην πληροφορία (**συνεχής συνάρτηση**)
3. Έστω ότι **συνδυάζω δύο πηγές** και φτιάχνω μια τρίτη:
 - Φ_1 : καιρός στη Νέα Ζηλανδία την άνοιξη
 - Φ_2 : η παραγωγή ελαιολάδου στην Ελλάδα
 - Αν είναι ανεξάρτητες, τότε η πληροφορία της σύνθετης πηγής θα πρέπει να είναι το άθροισμα των πληροφοριών των δύο πηγών
 - πιθανότητα σύνθετου συμβόλου

Μέτρο Πληροφορίας

Σύνοψη ιδιοτήτων του μέτρου της πληροφορίας:

1. $I(s_k) = 0 \text{ for } p(s_k) = 1$

2. $I(s_k) \geq 0 \text{ for } 0 \leq p(s_k) \leq 1$

3. $I(s_k) > I(s_l) \text{ for } p(s_k) < p(s_l)$

4. $I(s_k, s_l) = I(s_k) + I(s_l) \text{ εαν } s_k, s_l \text{ στατιστικά ανεξάρτητα}$

5. Μικρή αλλαγή στην πιθανότητα \rightarrow μικρή αλλαγή στην πληροφορία (συνεχής συνάρτηση)

Ποια συνάρτηση ικανοποιεί τα παραπάνω: $\log \frac{1}{p(s_i)}$

Μέτρο Πληροφορίας (2)

- Πληροφορία (Information) ενός συμβόλου s_i με πιθανότητα εμφάνισης $p(s_i)$

$$I(s_i) = \log \frac{1}{p(s_i)} = -\log p(s_i)$$

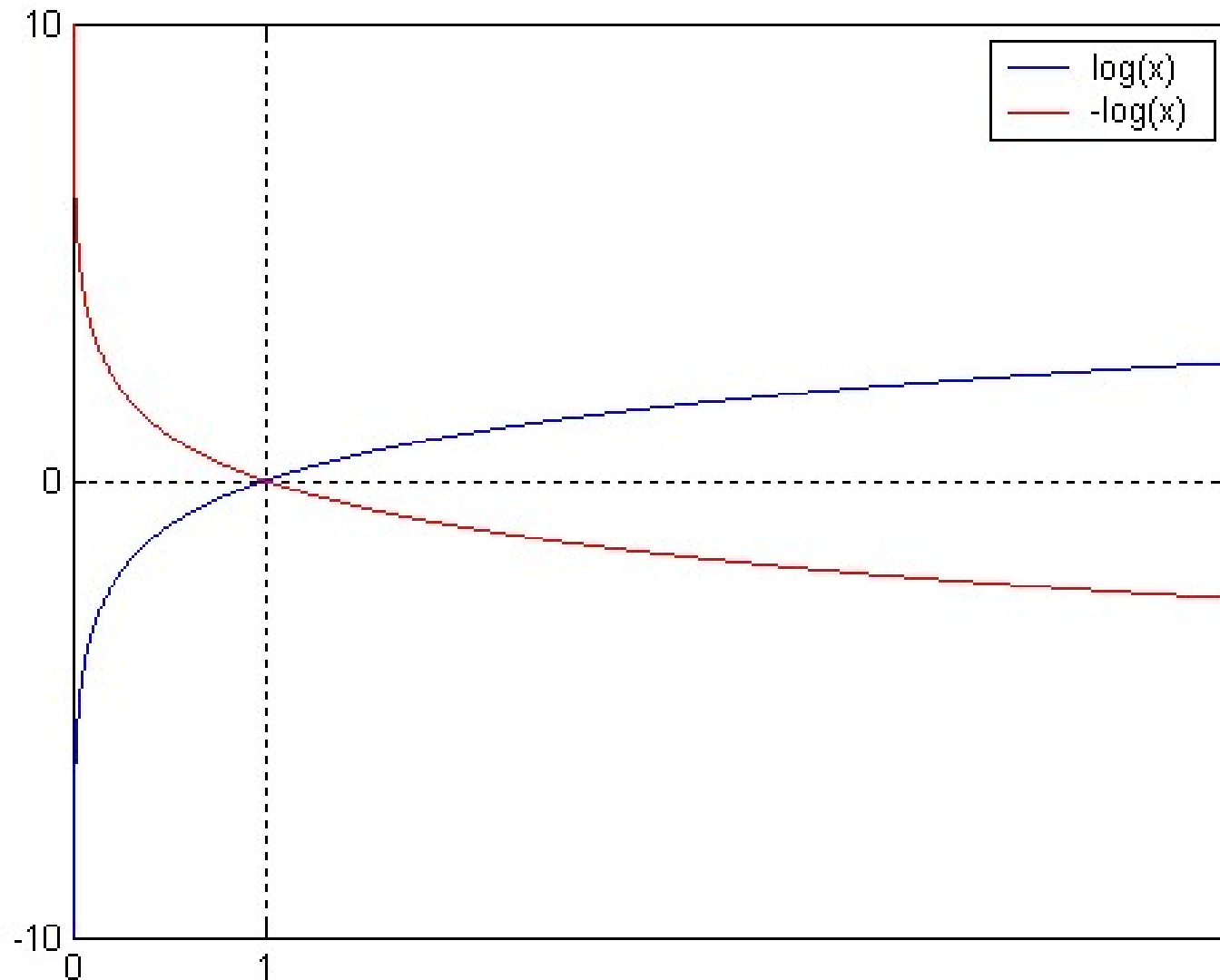
- Βάση του λογαρίθμου

- συνήθως χρησιμοποιείται το 2 με μονάδα μέτρησης **bit** (1 bit είναι η λαμβανόμενη ποσότητα πληροφορίας όταν προκύπτει ένα από δύο ισοπίθανα σύμβολα μιας δυαδικής πηγής)
- γενικά δεν ταυτίζεται με το bit που γνωρίζουμε ως δυαδικό ψηφίο (δεδομένα vs πληροφορία)

- Σύνθετη πηγή (αν οι αρχικές είναι ανεξάρτητες):

$$I(s_i, a_j) = I(s_i) + I(a_j)$$

Μέτρο Πληροφορίας (3)



Παρατηρήσεις:

1. Φθίνουσα
2. Πεδίο ορισμού (που ορίζεται;)
3. Όρια (τι συμβαίνει στα άκρα;)
4. Είναι συνεχής;

Διακριτή Πηγή Χωρίς Μνήμη

- **Discrete Memoryless Source (DMS):**
 - διακριτού χρόνου
 - διακριτού αλφαβήτου
 - τα σύμβολα στην έξοδο της είναι ανεξάρτητα
 - ακολουθούν συγκεκριμένη κατανομή πιθανότητας
- Περιγράφεται πλήρως από:
 - το αλφάβητο $\Phi = \{s_1, \dots, s_N\}$
 - και τις πιθανότητες εμφάνισης $\{p_1, \dots, p_N\}$
- Ειδικές Περιπτώσεις:
 - **Δυαδική Πηγή Χωρίς Μνήμη:** $\Phi = \{0, 1\}$ $\{p, 1 - p\}$
 - Για $p=0.5$, **Δυαδική Συμμετρική Πηγή Χωρίς Μνήμη**

Εντροπία

- Η εντροπία μιας DMS ορίζεται ως

$$H(\Phi) = \sum_{i=1}^N p_i I(s_i) = -\sum_{i=1}^N p_i \log_2 p_i$$

- Φυσική Σημασία:

- εκφράζει τη μέση αβεβαιότητα που έχω για την πηγή
- είναι ο μέσος όρος της πληροφορίας των συμβόλων

- Όσο **μεγαλύτερη εντροπία** έχει μια πηγή,
 - τόσο περισσότερη πληροφορία φέρει, και
 - τόσο περισσότερα bits χρειάζονται για την κωδικοποίησή της

Ορισμός της εντροπίας ενός φυσικού συστήματος στην Στατιστική Μηχανική (εκφράζει την μέση ενεργειακή κατάσταση)

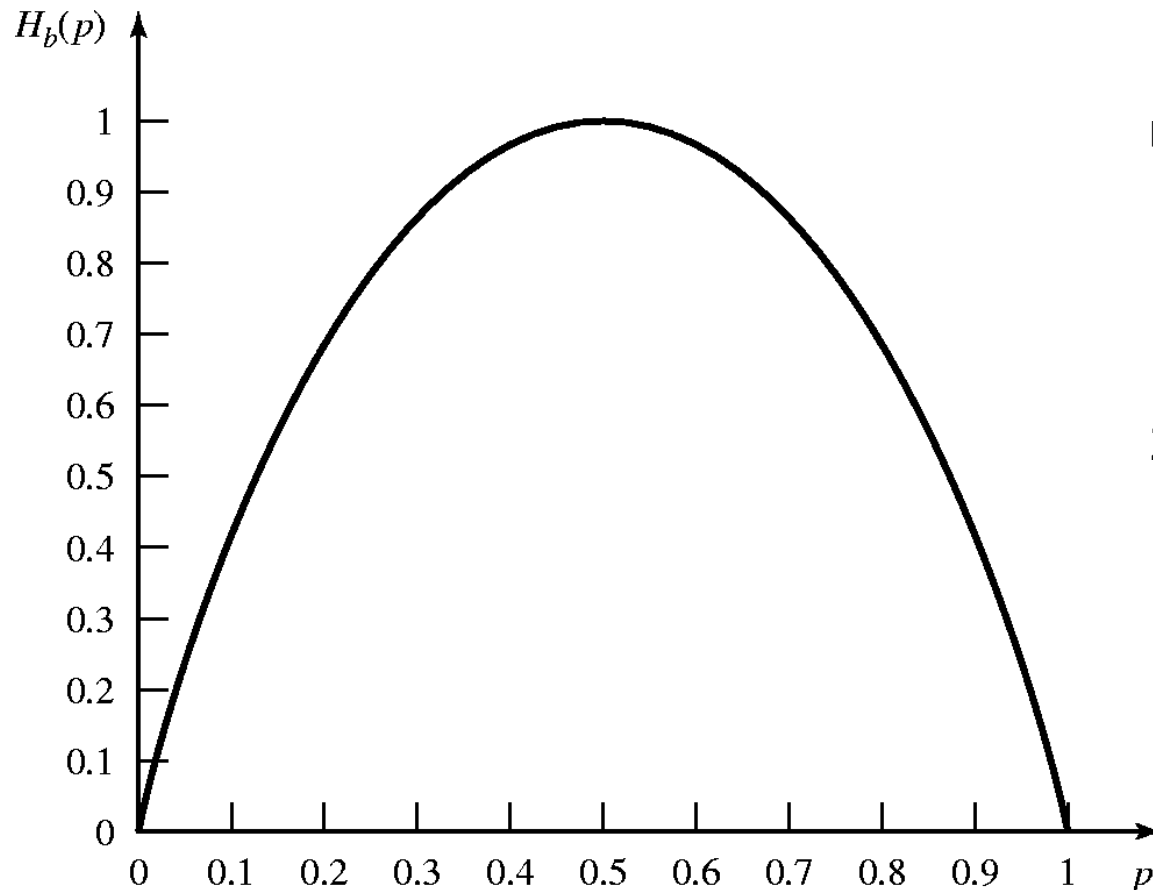
$$J = k \ln \Omega$$

2^{ος} Νόμος Θερμοδυναμικής: Η εντροπία ενός κλειστού συστήματος που δεν είναι σε ισορροπία τείνει να αυξάνεται.

Συνάρτηση Δυαδικής Εντροπίας

- Αν έχω δυαδική DMS $\Phi = \{0, 1\}$, με πιθανότητες εμφάνισης $\{p, 1-p\}$, τότε ορίζεται η **συνάρτηση δυαδικής εντροπίας**

$$H_b(p) = -p \log_2 p - (1-p) \log_2 (1-p)$$



- **Παρατηρήσεις:**
 1. ελαχιστοποιείται όταν $p=0$ ή 1 , οπότε $H(0)=H(1)=0$
 2. μεγιστοποιείται όταν τα σύμβολα είναι ισοπίθανα, $H(0.5)=1$

Εντροπία Ομοιόμορφης Πηγής

- Είδαμε ότι η εντροπία της δυαδικής DMS μεγιστοποιείται για ισοπίθανα σύμβολα

Γενίκευση: Η εντροπία μιας N -αδικής DMS μεγιστοποιείται όταν τα σύμβολά της ακολουθούν ομοιόμορφη κατανομή, δηλαδή $p_i = 1/N$ για $i = 1, \dots, N$.

- Συμπέρασμα: Η εντροπία φράσσεται ως

$$0 \leq H(\Phi) \leq \log_2 N$$

- όπου N το πλήθος του αλφαβήτου
- και το άνω όριο επιτυγχάνεται για ομοιόμορφη πηγή

Διαφορική Εντροπία

- Έστω πηγή διακριτού χρόνου αλλά **συνεχούς αλφάβητου**
- Έξοδος πηγής: πραγματικός αριθμός που απαιτεί **???? #bits**
- **Απαιτούνται άπειρα bits για αναπαράσταση.** Συνεπώς, δεν μπορεί να οριστεί η εντροπία
- Ορίζω τη **διαφορική εντροπία**

$$h(X) = - \int_{-\infty}^{\infty} f_X(x) \log_2 f_X(x) dx$$

- $f_X(x)$: η συνάρτηση πυκνότητας πιθανότητας της X
- Η $h(x)$ δεν έχει το δαισθητικό νόημα της εντροπίας
- μπορεί να πάρει και αρνητικές τιμές

Διαφορική Εντροπία Ομοιόμορφης

- X ομοιόμορφα κατανομημένο στο συνεχές διάστημα $[0, a]$

$$f_X(x) = \frac{1}{a}, \quad 0 \leq x \leq a$$

- Διαφορική Εντροπία:

$$h(X) = -\int_0^a \frac{1}{a} \log_2 \frac{1}{a} dx = \log_2 a$$

- Για $a < 1$, παίρνει αρνητικές τιμές

Διαφορική Εντροπία Gaussian

- X Gaussian κατανομημένη $N(0, \sigma^2)$

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

- Διαφορική Εντροπία:

$$h(X) = \frac{1}{2} \ln(2\pi e\sigma^2) \text{ nats} = \frac{1}{2} \frac{\log_2(2\pi e\sigma^2)}{\log_2 e} \text{ bits}$$

- Παρατήρηση:

- Όπως η ομοιόμορφη κατανομή μεγιστοποιεί την εντροπία για τις πηγές διακριτού αλφαβήτου,
- έτσι η **Gaussian κατανομή μεγιστοποιεί τη διαφορική εντροπία** για τις πηγές συνεχούς αλφαβήτου.

Ρυθμός Εντροπίας

- Τι γίνεται στην περίπτωση των **πηγών με μνήμη**;
- Αν X_n η έξοδος της πηγής τη χρονική στιγμή n
- $H(X_2|X_1)$: **αβεβαιότητα (καινούργια πληροφορία)** που φέρει το X_2 , αν γνωρίζω το X_1
- Η ποσότητα $H(X_2|X_1)$ λέγεται **υπό συνθήκη εντροπία** και θα οριστεί πλήρως σε επόμενα μαθήματα
- **Ρυθμός Εντροπίας** μιας στάσιμης τυχαίας διαδικασίας

$$H(X) = \lim_{n \rightarrow \infty} H(X_n | X_1, X_2, \dots, X_{n-1})$$

- **Φυσική Σημασία:**
 - παίζει το ρόλο της εντροπίας για τις πηγές με μνήμη
 - μέτρο πληροφορίας ανά σύμβολο εξόδου της πηγής
 - συγκλίνει σχετικά γρήγορα (δηλ. για μικρό n)

Κωδικοποίηση Πηγής

- Στόχος: Η αποδοτική αναπαράσταση μιας Μιαδικής πηγής
- Στη γενική περίπτωση αποδοτικές αναπαραστάσεις επιτυγχάνονται με **Κώδικες Μεταβλητού Μήκους (ΚΜΜ)**: Ένας ΚΜΜ αξιοποιεί τη γνώση των στατιστικών ιδιοτήτων της πηγής
- Λειτουργικές απαιτήσεις:
 - Οι κωδικές λέξεις είναι δυαδικές
 - Ο κώδικας είναι μοναδικά αποκωδικοποιήσιμος

- Μέσο μήκος κώδικα

$$\bar{L} = \sum_{i=1}^N p(s_i) l(s_i)$$

Θεώρημα Κωδικοποίησης Πηγής

- ή «Το Πρώτο Θεώρημα του Shannon» (1948)
- **Χρησιμότητα:** πόσο μπορούμε να συμπίεσουμε μια πηγή χωρίς να εισάγουμε σφάλματα;

Θεώρημα: Έστω πηγή με εντροπία H που κωδικοποιείται ώστε να παρέχει ρυθμό \bar{L} (*bits/έξοδο πηγής*).

-Αν $\bar{L} \geq H$, η πηγή μπορεί να κωδικοποιηθεί με οσοδήποτε μικρή πιθανότητα σφάλματος

-Αν $\bar{L} < H$, όσο πολύπλοκος κι αν είναι ο κωδικοποιητής πηγής, η πιθανότητα σφάλματος θα είναι μακριά από το 0

- **Σχόλια:**
 - ο Shannon δίνει την ικανή και αναγκαία συνθήκη
 - όμως δεν προτείνει κάποιο αλγόριθμο/μεθοδολογία για να φτιάξουμε έναν κωδικοποιητή όταν $\bar{L} \geq H$
 - $\bar{L} < H$: *Data compression, Rate-Distortion Theory*

Απόδειξη Θεωρήματος (1)

- Έστω **DMS** με αλφάβητο $X = \{a_1, \dots, a_N\}$ και πιθαν. $\{p_1, p_2, \dots, p_N\}$
- Παρατηρούμε ταυτόχρονα n **εξόδους** της πηγής (ένα μπλοκ)
- Αν το n τείνει στο άπειρο, τότε λογικά αν δω το σύνολο των εξόδων, κάθε σύμβολο εμφανίζεται περίπου τις εξής **φορές**
 - $a_1: np_1$
 - $a_2: np_2$
 - ...
 - $a_N: np_N$
- Αν επαναλάβω το πείραμα,
 - τα σύμβολα προφανώς θα είναι αλλιώς **ανακατεμένα**
 - όμως προκύπτουν περίπου **ίδιες φορές εμφάνισης**
- **Ορισμός:** όλες αυτές οι ακολουθίες
 - ονομάζονται **τυπικές ακολουθίες** (sample entropy \approx entropy)
 - κάθε μία εμφανίζεται με την **ίδια πιθανότητα εμφάνισης** (ασυμπτωτικά για μεγάλο n)

Απόδειξη Θεωρήματος (2)

- **Ερώτηση:** πόσες είναι οι τυπικές ακολουθίες;
- **Λύση:** Κάθε μία από αυτές εμφανίζεται με πιθανότητα

$$p_{\text{typical}} \approx \prod_{i=1}^N p_i^{np_i} = \prod_{i=1}^N 2^{np_i \log_2 p_i} = 2^{n \sum_{i=1}^N p_i \log_2 p_i} = 2^{-nH(X)}$$

- Κάθε μη τυπική ακολουθία έχει σχεδόν μηδενική πιθανότητα εμφάνισης (για μεγάλο n)
- Επομένως, όλες οι δυνατές ακολουθίες εξόδου είναι τυπικές (και μάλιστα εμφανίζονται ισοπίθانا)
- Αν η πιθανότητα εμφάνισης μίας τυπικής ακολουθίας είναι p_{typical} τότε το πλήθος των τυπικών είναι :

$$K = 1/p_{\text{typical}}$$

- Άρα, το πλήθος των τυπικών ακολουθιών είναι $K = 2^{nH(X)}$

Απόδειξη Θεωρήματος (3)

- Κωδικοποίηση όλων των δυνατών ακολουθιών

- το μπλοκ έχει n σύμβολα από αλφάβητο των N

- ⇒ το μπλοκ έχει πλήθος δυνατών ακολουθιών = ;

N^n δυνατές ακολουθίες

(ή σύμβολα εκτεταμένης πηγής)

- Απαιτούνται (πόσα bits/εξοδο);

$\log_2 N^n = n \log_2 N$ bits/μπλοκ ή $\log_2 N$ bits/έξοδο

Απόδειξη Θεωρήματος (4)

- Αν όμως το n είναι πολύ μεγάλο, μπορώ να αγνοήσω τις μη τυπικές ακολουθίες και να κωδικοποιήσω μόνο τις τυπικές
- Κωδικοποίηση μόνο των **τυπικών ακολουθιών** (θεωρώντας την κάθε μία από αυτές ως σύμβολο μιας K -αδικής πηγής). Έτσι ο αριθμός των bit μειώνεται σε:
 - $\log_2 K = \log_2(2^{nH(X)}) = nH(X)$ bits/μπλοκ
 - $H(X)$ bits/έξοδο
- Πότε υπάρχει σφάλμα:
 - αν εμφανιστεί **μη τυπική ακολουθία** (αν όμως το n είναι πολύ μεγάλο, η πιθανότητα μη τυπικής - και το σφάλμα - μπορούν να γίνουν οσοδήποτε μικρά)

Ειδικές Περιπτώσεις

- Ομοιόμορφη Πηγή:

- $H(X) = \log_2 N$
- δε μπορεί να συμπιεστεί
- κάθε ακολουθία εξόδου είναι δυνατή (τυπική) και ισοπίθανη

- Πηγές με μνήμη:

- ο **ρυθμός εντροπίας** παίζει τον ίδιο ρόλο με την εντροπία για στάσιμες πηγές
- ο ρυθμός εντροπίας συγκλίνει γρήγορα στην τελική τιμή

- Παράδειγμα πηγής με μνήμη: αγγλικό κείμενο

- για $n=1$ (αγνοώντας τη μνήμη), $H(X) = 4.03$ bits/letter
- για μπλοκ γραμμάτων (π.χ. $n=10$) συγκλίνει στην τιμή $H(X) = 1.3$ bits/letter