1 Βασικές Έννοιες Θεωρίας Πληροφορίας

Εντροπία τυχαίων μεταβλητών X, Y:

$$H(X) = -E\left[\log \Pr(x)\right] \tag{1}$$

$$H(X,Y) = -E\left[\log \Pr(x,y)\right] \tag{2}$$

$$H(X|Y) = -E\left[\log \Pr(x|y)\right] \tag{3}$$

$$H(Y|X) = -E\left[\log \Pr(y|x)\right] \tag{4}$$

Ιδιότητες Εντροπίας:

- Νόμος Bayes: $\Pr(y|x) = \frac{\Pr(x,y)}{\Pr(x)}$
- Κανόνας Αλυσίδας (chain rule):

$$H(X,Y) = H(X) + H(Y|X) \tag{5}$$

$$H(X,Y) = H(Y) + H(X|Y) \tag{6}$$

- Μείωση εντροπίας υπό συνθήκες:

$$H(X|Y) \leq H(X) \tag{7}$$

$$H(X|Y,Z) \leq H(X|Y) \leq H(X) \tag{8}$$

Αμοιβαία Πληροφορία

$$I(X;Y) = E\left[\log \frac{\Pr(X,Y)}{\Pr(X)\Pr(Y)}\right] \tag{9}$$

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y) \tag{10}$$

Ιδιότητες Αμοιβαίας Πληροφορίας

- Θετικότητα: $I(X;Y) \geq 0$
  ισότητα όταν $Y = g(X)$ όπου g ντετερμινιστική 1-1.
- Κανόνας Αλυσίδας

$$I(X;Y,Z) = I(X;Y) + I(X;Z|Y) \tag{11}$$

$$I(X;Y,Z) = I(X;Z) + I(X;Y|Z) \tag{12}$$

- Υπό συνθήκη αμοιβαία πληροφορία

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) = H(Y|Z) - H(Y|X,Z) \tag{13}$$

Απόσταση Kullback-Leibler μεταξύ κατανομών p, q τυχαίας μεταβλητής X

$$D(p||q) = \int p(x) \log \frac{p(x)}{q(x)} dx \geq 0 \tag{14}$$

Ιδιότητες

- δεν υπακούει στη συμμετρία $D(p||q) \neq D(q||p)$
- $I(X;Y) = D(\Pr(X,Y)||\Pr(X)\Pr(Y))$

Τυχαίες μεταβλητές X, Y, Z οι οποίες σχηματίζουν αλυσίδα Markov $X \to Y \to Z$

$$\Pr(Z, X|Y) = \Pr(Z|Y)\Pr(X|Y) \tag{15}$$

Data processing inequality:

$$I(X;Y) \geq I(X;Z) \tag{16}$$

2 Τυπικές Ακολουθίες

Ακολουθία x^n με σύμβολα στο αλφάβητο $\mathcal{X}$, (π.χ. δυαδικό αλφάβητο $X = \{0, 1\}$)
Εμπειρική κατανομή ακολουθίας

$$\pi(x|x^n) = \frac{|i : x_i = x|}{n}, x \in \mathcal{X} \tag{17}$$

Παράδειγμα: $\tilde{x}^n = (1, 0, 0, 1, 0, 0, 1)$, $n = 7$

$$\pi(0|\tilde{x}^n) = 4/7 \quad \pi(1|\tilde{x}^n) = 3/7 \tag{18}$$

Ακολουθία $X_n = (X_1, X_2, \ldots, X_n)$ ανεξάρτητων τυχαίων μεταβλητών X_i με την ίδια κατανομή $p_X(x)$

$$p_{X^n}(x^n) = \prod_{i=1}^{n} p_X(x_i) \tag{19}$$

Νόμος μεγάλων αριθμών: για αρκετό μεγάλο n

$$\pi(x|X^n) \to p_X(x) \tag{20}$$

Σύνολο τυπικών ακολουθιών:

$$T_\epsilon^{(n)}(X) = \{x^n : |\pi(x|X^n) - p_X(x)| < \epsilon p_X(x), \forall x \in \mathcal{X}\} \tag{21}$$

Νόμος μεγάλων αριθμών:

$$\lim_{n\to\infty} \Pr(X^N \in T_\epsilon^n(X)) \to 1 \tag{22}$$

Ποια η πιθανότητα εμφάνισης μιας τυπικής ακολουθίας x^n;

$$p_{X^n}(x^n) = \prod_{i=1}^{n} \pi(x_i|X^n)^{n\pi(x_i|X^n)} = \exp\left(n \sum_{i=1}^{n} \pi(x_i|X^n) \log \pi(x_i|X^n)\right) \tag{23}$$

$$(1-\epsilon)p_X(x_i) \leq \pi(x_i|X^N) \leq (1+\epsilon)p_X(x_i) \tag{24}$$

$$\exp\left(-n(H(X)+\delta(\epsilon)\right) \leq p_{X^n}(x^n) \leq \exp\left(-n(H(X)-\delta(\epsilon)\right) \tag{25}$$

Για πολύ μεγάλα μήκη n η κατανομή μιας τυπικής ακολουθίας είναι σχεδόν ομοιόμορφη.
Πόσες τυπικές ακολουθίες υπάρχουν;

$$(1-\epsilon)\exp\left(n(H(X)-\delta(\epsilon))\right) \leq |T_\epsilon^n(X)| \leq \exp\left(n(H(X)+\delta(\epsilon))\right) \tag{26}$$

3 Από κοινού τυπικές ακολουθίες

Ακολουθίες x^n και y^n στα αλφάβητα $\mathcal{X}$ και $\mathcal{Y}$ αντίστοιχα.
Από κοινού εμπειρική κατανομή

$$\pi(x,y|x^n,y^n) = \frac{|i : (x_i,y_i) = (x,y)|}{n}, \quad \forall (x,y) \in \mathcal{X}\times\mathcal{Y} \tag{27}$$

Παράδειγμα:

$$\tilde{x}^n = (0\ 1\ 0\ 1\ 0\ 0\ 0)$$
$$\tilde{y}^n = (0\ 1\ 1\ 0\ 0\ 1\ 1)$$

$$\begin{aligned} \pi(0,0|\tilde{x}^n,\tilde{y}^n) &= 2/7, \quad \pi(1,0|\tilde{x}^n,\tilde{y}^n) = 1/7 \\ \pi(0,1|\tilde{x}^n,\tilde{y}^n) &= 3/7, \quad \pi(1,1|\tilde{x}^n,\tilde{y}^n) = 1/7 \end{aligned} \tag{28}$$

Ακολουθίες $X^n = (X_1, X_2, \ldots, X_n)$, $Y^n = (Y_1, Y_2, \ldots, Y_n)$ από κοινού ανεξάρτητων ζευγών τυχαίων μεταβλητών (X_i, Y_i) με την ίδια κατανομή $p_{X,Y}(x,y)$

$$p_{X^n,Y^n}(x^n,y^n) = \prod_{i=1}^{n} p_{X,Y}(x_i,y_i) \tag{29}$$

Από κοινού τυπικές ακολουθίες:

$$T_\epsilon^n(X,Y) = \{(x^n, y^n) : |\pi(x,y|X^n, Y^n) - p_{X,Y}(x,y)| \leq \epsilon p_{X,Y}(x,y), \quad \forall (x,y) \in \mathcal{X} \times \mathcal{Y}\} \tag{30}$$

Νόμος μεγάλων αριθμών:

$$\lim_{n\to\infty} \Pr((X^n, Y^n) \in T_\epsilon^n(X,Y)) \to 1 \tag{31}$$

Ιδιότητες από κοινού τυπικών ακολουθιών $(x^n, y^n) \in T_\epsilon^n(X,Y)$

- x^n ϵ-τυπική $x^n \in T_\epsilon^n(X)$ και y^n ϵ-τυπική $y^n \in T_\epsilon^n(Y)$
- από κοινού πιθανότητα:

$$\exp\left(-n(H(X,Y) + \delta(\epsilon))\right) \leq p_{X^n,Y^n}(x^n, y^n) \leq \exp\left(-n(H(X,Y) - \delta(\epsilon))\right) \tag{32}$$

- υπό συνθήκη πιθανότητα

$$\exp\left(-n(H(Y|X) + \delta(\epsilon))\right) \leq p_{Y^n|X^n}(y^n|x^n) \leq \exp\left(-n(H(Y|X) - \delta(\epsilon))\right) \tag{33}$$

- αριθμός από κοινού τυπικών ακολουθιών:

$$(1-\epsilon)\exp\left(n(H(X,Y) - \delta(\epsilon))\right) \leq |T_\epsilon^n(X,Y)| \leq \exp\left(n(H(X,Y) + \delta(\epsilon))\right) \tag{34}$$

Υπό συνθήκη τυπικές ακολουθίες: για δοθείσα ακολουθία x^n

$$T_\epsilon^n(Y|x^n) = \{y^n : (x^n, y^n) \in T_\epsilon^n(X,Y)\} \tag{35}$$

Νόμος μεγάλων αριθμών: για ϵ' τυπική ακολουθία $x^n \in T_{\epsilon'}^n(X)$ και $\epsilon > \epsilon'$

$$\lim_{n\to\infty} \Pr((x^n, Y^n) \in T_\epsilon^n(Y|x^n)) \to 1 \tag{36}$$

Ιδιότητες υπό συνθήκη τυπικών ακολουθιών

- για κάθε $x^n \in \mathcal{X}^n$

$$|T_\epsilon^n(Y|x^n)| \leq \exp\left(n(H(Y|X) + \delta(\epsilon))\right) \tag{37}$$

- αν $x^n \in T_{\epsilon'}^n(X)$ και $\epsilon > \epsilon'$

$$|T_\epsilon^n(Y|x^n)| \geq (1-\epsilon)\exp\left(n(H(Y|X) - \delta(\epsilon))\right) \tag{38}$$

4 Achievability Bounds

Στόχος: Για κάθε ρυθμό κώδικα R μικρότερο από τη χωρητικότητα του καναλιού C, υπάρχει ένας κώδικας με οσοδήποτε μικρή πιθανότητα σφάλματος.
Βασικό εργαλείο: αποκωδικοποίηση από κοινού τυπικών συνόλων.

Βήματα κωδικοποίησης

- Μετάδοση συνόλου μηνυμάτων $\mathcal{M}$ όπου $|\mathcal{M}| = e^{nR}$
- Παραγωγή ενός τυχαίου κώδικα $\mathcal{C}$
  - Τυχαία και ανεξάρτητα κατασκευάζουμε e^{nR} κωδικές λέξεις $x^n(m)$ με την ίδια κατανομή $p_{X^n}(x^n) = \prod_{i=1}^{n} p_X(x_i(m))$. Πιθανότητα ενός κώδικα $\mathcal{C}$;

$$\Pr(\mathcal{C}) = \prod_{m=1}^{e^{nR}} \prod_{i=1}^{n} p_X(x_i(m)) \tag{39}$$

- μετάδοση μηνύματος m μέσω της κωδικής λέξης $x^n(m)$

Αποκωδικοποίηση: για τη ληφθείσα ακολουθία y^n βρες το μοναδικό μήνυμα m για το οποίο $(x^n(m), y^n) \in T_\epsilon^n(X,Y)$. Αν υπάρχει παραπάνω από ένα μήνυμα, δήλωσε σφάλμα.
Μέση πιθανότητα σφάλματος ως προς όλους τους δυνατούς κώδικες που έχουν παραχθεί:

$$P_e = \sum_{\mathcal{C}} \Pr(\mathcal{C}) P_e(\mathcal{C}) \tag{40}$$

Πιθανότητα σφάλματος $P_e(\mathcal{C})$ ενός κώδικα $\mathcal{C}$

$$P_e(\mathcal{C}) = \frac{1}{2^{nR}} \sum_{m=1}^{e^{nR}} P_{e,m}(\mathcal{C}) \tag{41}$$

$$P_e = \frac{1}{2^{nR}} \sum_{m=1}^{e^{nR}} \sum_{\mathcal{C}} \Pr(\mathcal{C}) P_{e,m}(\mathcal{C}) \tag{42}$$

Υποθέτουμε ότι μεταδίδεται το μήνυμα $m = 1$.
Σφάλματα αποκωδικοποίησης $P_{e,1}(\mathcal{C})$:

1. το ζεύγος $(x^n(1), y^n)$ δεν είναι ϵ-τυπικό

$$E_1 = \{x^n(1) \in \mathcal{X}^n, y^n \in \mathcal{Y}^n : (x^n(1), y^n) \notin T_\epsilon^n(X,Y)\} \tag{43}$$

2. υπάρχει ένα μήνυμα $m' \neq 1$ για το οποίο το ζεύγος $(x^n(m'), y^n)$ είναι ϵ-τυπικό.

$$E_2 = \left\{\exists m' \neq 1, x^n(m) \in \mathcal{X}^n, y^n \in \mathcal{Y}^n : (x^n(m'), y^n) \in T_\epsilon^n(X,Y)\right\} \tag{44}$$

Φράγμα για την πιθανότητα σφάλματος $P_{e,1}(\mathcal{C})$:

$$P_{e,1}(\mathcal{C}) = \Pr(E_1 \cup E_2) \leq \Pr(E_1) + \Pr(E_2) \tag{45}$$

Λόγω τυπικότητας (σχέση (31))

$$\Pr(E_1) \leq \epsilon_1 \tag{46}$$

Φράγμα συνόλου:

$$\Pr(E_2) \leq \sum_{m'=2}^{e^{nR}} \Pr((x^n(m'), y^n) \in T_\epsilon(X,Y)) \tag{47}$$

Προσοχή: οι ακολουθίες $x^n(m')$ και y^n είναι στατιστικά ανεξάρτητες.

Για στατιστικά ανεξάρτητες ακολουθίες $x^n(m)$ ϵ-τυπική και y^n ϵ-τυπική

$$\Pr\left((x^n(m), y^n) \in T_\epsilon^n(X,Y)\right) \leq \exp\left(-n(I(X;Y) - \delta(\epsilon))\right) \tag{48}$$

Από (38)–(45) καταλήγουμε

$$P_e \leq \epsilon_1 + \exp\left(-n(I(X;Y) - R - \delta(\epsilon)\right) \tag{49}$$

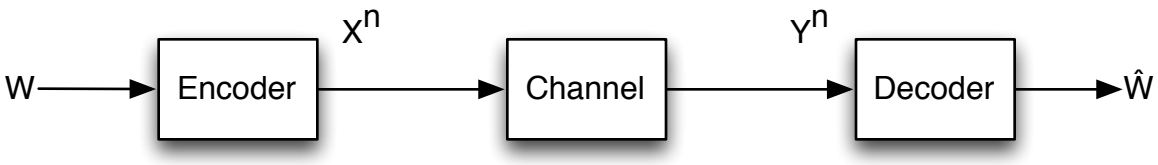
5 Converse Bounds

Κάθε κώδικας $\mathcal{C}$ με οσοδήποτε μικρή πιθανότητα σφάλματος έχει ρυθμό R μικρότερο της χωρητικότητας του καναλιού.
Βασικό εργαλείο: Ανισότητα Fano

Ανισότητα Fano:

- W τυχαία μεταβλητή μηνυμάτων στην είσοδο του καναλιού, $W \in [1, M]$
- $\hat{W}$ τυχαία μεταβλητή μηνυμάτων στην έξοδο του καναλιού
- Πιθανότητα σφάλματος $P_e = \Pr(\hat{W} \neq W)$

$$H(W|\hat{W}) \leq 1 + P_e \log M \tag{50}$$



Υπόθεση: ομοιόμορφή κατανομή της τυχαίας μεταβλητής των μηνυμάτων $nR = H(W)$

$$nR = H(W) = H(W|\hat{W}) + I(W;\hat{W}) \tag{51}$$

Ανισότητα Fano + Data Processing inequality

$$nR \leq 1 + P_e \log M + I(X^n;Y^n) \leq 1 + nRP_e + nC$$
$$\text{ή} \quad P_e \geq 1 - \frac{C}{R} - \frac{1}{nR} \tag{52}$$