(25) ΟΙ ΚΩΔΙΚΕΣ HUFFMAN ΕΙΝΑΙ ΒΕΛΤΙΣΤΟΙ

ΘΕΩΡΗΜΑ: Η ΚΩΔΙΚΟΠΟΙΗΣΗ HUFFMAN ΕΙΝΑΙ ΒΕΛΤΙΣΤΗ, ΔΗΛΑΔΗ ΑΝ C^* ΕΙΝΑΙ ΕΝΑΣ ΚΩΔΙΚΑΣ HUFFMAN ΚΑΙ C' ΕΝΑΣ ΟΠΟΙΟΣΔΗΠΟΤΕ ΑΛΛΟΣ ΚΩΔΙΚΑΣ, ΤΟΤΕ $L(C^*) \leq L(C') \Leftrightarrow$

$$\sum_i p_i l_i^* \leq \sum_i p_i l_i'$$

(ΠΡΩΤΑ, ΘΑ ΑΠΟΔΕΙΞΟΥΜΕ ΕΝΑ ΛΗΜΜΑ:)

ΛΗΜΜΑ: ΓΙΑ ΚΑΘΕ ΚΑΤΑΝΟΜΗ $\{p_i\}$, ΥΠΑΡΧΕΙ ΕΝΑΣ ΠΡΟΘΕΜΑΤΙΚΟΣ ΚΩΔΙΚΑΣ ΠΟΥ ΕΙΝΑΙ ΒΕΛΤΙΣΤΟΣ ΚΑΙ ΕΧΕΙ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΙΔΙΟΤΗΤΕΣ:

1. $p_j > p_k \Rightarrow l_j \leq l_k$
2. ΟΙ ΔΥΟ ΜΑΚΡΥΤΕΡΕΣ ΚΩΔΙΚΟΛΕΞΕΙΣ ΕΧΟΥΝ ΤΟ ΙΔΙΟ ΜΗΚΟΣ (ΑΛΛΙΩΣ: ΔΕΝ ΥΠΑΡΧΕΙ ΚΩΔΙΚΟΛΕΞΗ ΠΟΥ ΝΑ ΕΙΝΑΙ ΠΙΟ ΜΑΚΡΥΑ ΑΠΟ ΟΛΕΣ ΤΙΣ ΑΛΛΕΣ)
3. ΔΥΟ ΑΠΟ ΤΙΣ ΜΑΚΡΥΤΕΡΕΣ ΚΩΔΙΚΟΛΕΞΕΙΣ ΔΙΑΦΕΡΟΥΝ ΜΟΝΟ ΣΤΟ ΤΕΛΕΥΤΑΙΟ BIT, ΚΑΙ ΑΝΤΙΣΤΟΙΧΟΥΝ ΣΤΑ ΔΥΟ ΠΙΟ ΣΠΑΝΙΑ (LEAST LIKELY) ΣΥΜΒΟΛΑ.

ΠΑΡΑΤΗΡΗΣΗ: ΥΠΑΡΧΟΥΝ ΠΟΛΛΟΙ ΒΕΛΤΙΣΤΟΙ ΚΩΔΙΚΕΣ. ΜΠΟΡΕΙ ΜΑΛΙΣΤΑ ΝΑ ΜΗΝ ΕΧΟΥΝ ΟΛΟΙ ΤΑ ΙΔΙΑ ΜΗΚΗ ΚΩΔΙΚΟΛΕΞΕΩΝ!

ΑΠΟΔΕΙΞΗ: (1) ΕΣΤΩ C_m Ο ΒΕΛΤΙΣΤΟΣ ΚΩΔΙΚΑΣ, ΓΙΑ ΤΟΝ ΟΠΟΙΟ $L(C_m) = \sum_i p_i l_i$ (ΕΣΤΩ $p_1 \geq p_2 \geq \ldots \geq p_m$) ΕΣΤΩ ΕΝΑΣ ΚΩΔΙΚΑΣ C_m' ΓΙΑ ΤΟΝ ΟΠΟΙΟ ΑΛΛΑΖΟΥΝ ΟΙ ΚΩΔΙΚΟΛΕΞΕΙΣ j ΚΑΙ k ΜΕ $j<k$. ΤΟΤΕ:

$$L(C_m') = p_1 l_1 + \ldots + p_j l_k + p_k l_j + \ldots + p_m l_m$$

$$\Rightarrow L(C_m') - L(C_m) = p_j l_k - p_j l_j + p_k l_j - p_k l_k =$$

$$p_k(l_j - l_k) + p_j(l_k - l_j)$$

$$= \underbrace{(p_j - p_k)}_{\geq 0,\ \text{ΓΙΑΤΙ } j<k}(l_k - l_j) \geq 0 \quad \text{(ΓΙΑΤΙ } C_m \text{ ΒΕΛΤΙΣΤΟΣ)}$$

$\Rightarrow l_k \geq l_j$ ΑΝΑΓΚΑΣΤΙΚΑ

(ΠΑΡΑΤΗΡΗΣΗ: Η ΙΔΕΑ ΕΙΝΑΙ ΠΟΛΥ ΑΠΛΗ· ΕΙΝΑΙ ΠΑΡΑΛΟΓΟ ΚΑΤΙ ΣΠΑΝΙΟ ΝΑ ΕΧΕΙ ΜΙΑ ΠΙΟ ΜΙΚΡΗ ΠΕΡΙΓΡΑΦΗ ΑΠΟ ΚΑΤΙ ΠΙΟ ΣΥΧΝΟ) ΑΡΑ ΟΛΟΙ ΟΙ ΒΕΛΤΙΣΤΟΙ ~~ΚΩ~~ΚΩΔΙΚΕΣ ΕΧΟΥΝ ΑΥΤΗ ΤΗΝ ΙΔΙΟΤΗΤΑ, ΑΛΛΙΩΣ ΕΧΩ ΑΝΤΙΦΑΣΗ

(2) ΕΣΤΩ ΟΤΙ ΥΠΑΡΧΕΙ ΜΙΑ ΚΩΔΙΚΟΛΕΞΗ ΜΕ ΜΗΚΟΣ ℓ, ΚΑΙ ΟΛΕΣ ΟΙ ΑΛΛΕΣ ΕΧΟΥΝ ΜΗΚΟΣ ΤΟ ΠΟΛΥ $\ell-k$. ΜΠΟΡΩ ΝΑ ΠΕΤΑΞΩ ΤΑ k ΤΕΛΕΥΤΑΙΑ BITS ΚΑΙ ΝΑ ΦΤΙΑΞΩ ΜΙΑ ΜΕ ΜΗΚΟΣ $\ell-k$, ΠΟΥ ΔΕΝ ΥΠΗΡΧΕ ΣΤΟΝ ΚΩΔΙΚΑ (Ο ΟΠΟΙΟΣ ΕΙΝΑΙ ΠΡΟΘΕΜΑΤΙΚΟΣ) ΚΑΙ Ο ΟΠΟΙΟΣ ΔΕΝ ΜΠΟΡΕΙ ΝΑ ΕΙΝΑΙ ΠΡΟΘΕΜΑ ΑΛΛΗΣ ΛΕΞΗΣ (ΑΦΟΥ ΔΕΝ ΥΠΑΡΧΟΥΝ ΠΙΟ ΜΑΚΡΙΕΣ)

ΑΡΑ ΟΛΟΙ ΟΙ ΒΕΛΤΙΣΤΟΙ ΚΩΔΙΚΕΣ ΕΧΟΥΝ ΑΥΤΗ ΤΗΝ ΙΔΙΟΤΗΤΑ, ΑΛΛΙΩΣ ΕΧΩ ΑΝΤΙΦΑΣΗ

(3) ΕΣΤΩ ΕΝΑΣ ΒΕΛΤΙΣΤΟΣ ΚΩΔΙΚΑΣ C. ΚΡΑΤΩΝΤΑΣ ΤΑ ΜΗΚΗ $\ell_1 \leq \ell_2 \leq \ldots \leq \ell_m$ ΔΗΜΙΟΥΡΓΩ ΕΝΑΝ ΑΛΛΟ ΚΩΔΙΚΑ ΓΕΜΙΖΟΝΤΑΣ ΕΝΑ ΠΛΗΡΩΣ ΙΣΟΣΤΑΘΜΙΣΜΕΝΟ ΔΥΑΔΙΚΟ ΔΕΝΤΡΟ ΞΕΚΙΝΩΝΤΑΣ ΑΠΟ ΤΙΣ ΛΕΞΕΙΣ ΜΕ ΜΙΚΡΟΤΕΡΑ ΜΗΚΗ

ΑΡΑ, ΔΕΝ ΕΧΟΥΝ ΟΛΟΙ ΟΙ ΒΕΛΤΙΣΤΟΙ ΚΩΔΙΚΕΣ ΑΥΤΗ ΤΗΝ ΙΔΙΟΤΗΤΑ, ΑΛΛΑ ΚΑΠΟΙΟΙ ΑΠΟ ΑΥΤΟΥΣ

ΟΡΙΣΜΟΙ: (1) ΟΙ ΚΩΔΙΚΕΣ ΠΟΥ ΙΚΑΝΟΠΟΙΟΥΝ ΤΙΣ ΣΥΝΘΗΚΕΣ (1)-(3) ΚΑΛΟΥΝΤΑΙ ΚΑΝΟΝΙΚΟΙ (CANONICAL)

(2) ΑΝ $(p_1, p_2, \ldots, p_m)$ ΕΙΝΑΙ ΜΙΑ ΜΑΖΑ ΠΙΘΑΝΟΤΗΤΑΣ ΜΕ $p_1 \geq p_2 \geq \ldots \geq p_m$, ΤΟΤΕ ΟΡΙΖΟΥΜΕ ΤΗΝ ΜΕΙΩΣΗ HUFFMAN (HUFFMAN REDUCTION) ΩΣ ΤΗΝ ΜΑΖΑ $(p_1, p_2, \ldots, p_{m-1} + p_m)$

ΑΠΟΔΕΙΞΗ ΤΟΥ ΘΕΩΡΗΜΑΤΟΣ

ΒΗΜΑ 1: ΕΣΤΩ ΠΩΣ ΕΧΟΥΜΕ ΕΝΑ ΒΕΛΤΙΣΤΟ ΚΩΔΙΚΑ $C^*_{m-1}(p')$ ΓΙΑ ΤΗΝ ΜΕΙΩΣΗ HUFFMAN p'. ΘΑ ΦΤΙΑΞΩ ΕΝΑ ΚΩΔΙΚΑ ΓΙΑ ΤΗΝ p ΩΣ ΕΞΗΣ:

$$\begin{array}{ccc}
 & C^*_{m-1}(p') & \\
p_1 & w'_1 & \ell'_1 \\
p_2 & w'_2 & \ell'_2 \\
\vdots & & \\
p_{m-2} & w'_{m-2} & \ell'_{m-2} \\
p_{m-1}+p_m & w'_{m-1} & \ell'_{m-1} \\
\uparrow & \uparrow & \uparrow \\
\text{ΠΙΘΑΝΟΤΗΤΕΣ} & \text{CODEWORDS} & \text{ΜΗΚΗ}
\end{array}
\Rightarrow
\begin{array}{cc}
 C_m(p) & \\
w_1 = w'_1 & \ell_1 = \ell'_1 \\
w_2 = w'_2 & \ell_2 = \ell'_2 \\
\vdots & \\
w_{m-2} = w'_{m-2} & \ell_{m-2} = \ell'_{m-2} \\
w_{m-1} = w'_{m-1}0 & \ell_{m-1} = \ell'_{m-1}+1 \\
w_m = w'_{m-1}1 & \ell_m = \ell'_{m-1}+1
\end{array}$$

ΑΡΑ· $\boxed{L(p) = L^*(p') + p_{m-1} + p_m}$ (A)

(ΠΡΑΓΜΑΤΙ: $L(p) = p_1\ell_1 + p_2\ell_2 + \dots + p_{m-1}w_{m-1} + p_m w_m$

$= p_1\ell_1 + \dots + p_{m-1}(w'_{m-1}+1) + p_m(w'_{m-1}+1)$

$= p_1\ell_1 + \dots + (p_{m-1}+p_m)w'_{m-1} + p_{m-1} + p_m$

$= L^*(p') + p_{m-1} + p_m$)

<u>ΒΗΜΑ 2ο</u>: ΑΠΟ ΕΝΑΝ <u>ΒΕΛΤΙΣΤΟ ΚΑΝΟΝΙΚΟ</u> ΚΩΔΙΚΑ ΓΙΑ ΤΗΝ p, ΦΤΙΑΧΝΟΥΜΕ ΕΝΑ ΚΩΔΙΚΑ ΓΙΑ ΤΗΝ p' ΩΣ ΕΞΗΣ:

$$\begin{array}{ccc}
 & C^*_m(p) & \\
p_1 & w_1 & \ell_1 \\
p_2 & w_2 & \ell_2 \\
\vdots & & \\
p_{m-1} & w_{m-1} = A0 & \ell_{m-1} \\
p_{m-1} & w_m = A1 & \ell_m
\end{array}
\Rightarrow
\begin{array}{cc}
 C_{m-1}(p') & \\
w'_1 = w_1 & \ell'_1 = \ell_1 \\
w'_2 = w_2 & \ell'_2 = \ell_1 \\
\vdots & \\
w'_{m-1} = A & \ell'_{m-1} = \ell_{m-1} - 1
\end{array}$$

ΑΡΑ $\boxed{L(p') = L^*(p) - p_{m-1} - p_m}$ (B)

(**ΠΡΑΓΜΑΤΙ:** $L(p') = p'_1 l'_1 + p'_2 l'_2 + \dots + p'_{m-1} l'_{m-1}$

$= p_1 l_1 + p_2 l_2 + \dots + p_{m-1}(l_{m-1}-1) + p_m(l_m - 1)$

$= L^*(p) - p_{m-1} - p_m$)

(A), (B) $\Rightarrow$ $$\left.\underbrace{\left[L(p') - L^*(p')\right]}_{\geq 0} + \underbrace{\left[L(p) - L^*(p)\right]}_{\geq 0} = 0 \right\} \Rightarrow$$

$L(p') = L^*(p')$, $L(p) = L^*(p) \Rightarrow$

1) Η ΕΠΕΚΤΑΣΗ ΤΟΥ ΒΕΛΤΙΣΤΟΥ ΚΩΔΙΚΑ ΤΗΣ p' ΕΙΝΑΙ ΒΕΛΤΙΣΤΗ ΓΙΑ ΤΗΝ p

2) Η ΜΕΙΩΣΗ ΤΟΥ ΒΕΛΤΙΣΤΟΥ ΚΩΔΙΚΑ ΤΗΣ p ΕΙΝΑΙ ΒΕΛΤΙΣΤΗ ΓΙΑ ΤΗΝ p'

(ΕΜΑΣ ΜΑΣ ΕΝΔΙΑΦΕΡΕΙ ΤΟ 1))

ΠΑΡΑΤΗΡΗΣΤΕ ΟΤΙ ΓΙΑ $m=2$, Ο ΒΕΛΤΙΣΤΟΣ ΚΩΔΙΚΑΣ ΕΙΝΑΙ Ο ΠΡΟΦΑΝΗΣ (0 ΚΑΙ 1). Ο ΚΩΔΙΚΑΣ HUFFMAN ΠΡΟΚΥΠΤΕΙ ΑΠΟ ΔΙΑΔΟΧΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ ΟΠΩΣ Η ΑΝΩ, ΑΡΑ ΣΕ ΚΑΘΕ ΒΗΜΑ ΔΙΑΤΗΡΕΙΤΑΙ Η ΒΕΛΤΙΣΤΟΤΗΤΑ, ΑΡΑ Ο ΚΩΔΙΚΑΣ HUFFMAN ΕΙΝΑΙ ΒΕΛΤΙΣΤΟΣ.

ΠΑΡΑΤΗΡΗΣΗ: Ο ΚΩΔΙΚΑΣ HUFFMAN ΕΙΝΑΙ GREEDY.

ΠΑΡ' ΟΛΑ ΑΥΤΑ, ΕΙΝΑΙ ΒΕΛΤΙΣΤΟΣ

(26) SHANNON–FANO–ELIAS CODING

ΟΡΙΖΟΥΜΕ ΤΗΝ ΣΥΝΑΡΤΗΣΗ ΚΑΤΑΝΟΜΗΣ (CUMULATIVE DISTRIBUTION FUNCTION)

$$F(x) = \sum_{a \le x} p(a)$$

(ΣΥΝΕΧΗΣ)

ΟΡΙΖΟΥΜΕ ΤΗΝ ΤΡΟΠΟΠΟΙΗΜΕΝΗ ΣΥΝΑΡΤΗΣΗ ΚΑΤΑΝΟΜΗΣ

$$\overline{F}(x) = \sum_{a < x} + \frac{1}{2} p(x)$$ (ΔΙΑΚΡΙΤΗ, ΓΙΑ ΤΙΣ ΤΙΜΕΣ ΤΟΥ x)

<u>ΙΔΕΑ</u>: ΟΛΑ ΤΑ $x_1, x_2, \dots, x_m$ ΕΙΝΑΙ ΔΙΑΦΟΡΕΤΙΚΑ, ΑΡΑ ΜΠΟΡΩ ΝΑ ΣΤΕΙΛΩ ΩΣ CODEWORDS ΤΗΝ ΔΥΑΔΙΚΗ ΕΠΕΚΤΑΣΗ ΤΩΝ $\overline{F}(x_1), \dots \overline{F}(x_m)$.

ΟΜΩΣ, ΤΟΤΕ ΙΣΩΣ ΧΡΕΙΑΖΟΜΟΥΝ ΑΠΕΙΡΑ BITS. ΑΡΚΕΙ ΝΑ ΣΤΕΙΛΩ ΤΟΣΑ ΩΣΤΕ ~~ΟΙ~~ ΚΩΔΙΚΟΛΕΞΕΙΣ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΝΑ ΕΙΝΑΙ ΔΙΑΚΡΙΤΕΣ. ΑΡΑ, ΑΝΤΙ ΝΑ ΣΤΕΙΛΩ ΤΑ $\overline{F}(x_1), \dots, \overline{F}(x_m)$, ΣΤΕΛΝΩ ΤΑ

$$\lfloor \overline{F}(x_1) \rfloor_{\ell(x_1)}, \dots, \lfloor \overline{F}(x_m) \rfloor_{\ell(x_m)}$$

<u>ΕΡΩΤΗΜΑ</u>: ΠΟΣΟ ΠΡΕΠΕΙ ΝΑ ΕΙΝΑΙ ΤΟ $\ell(x_i)$;

ΠΑΡΑΤΗΡΗΣΤΕ ΟΤΙ

$$\overline{F}(x) - \lfloor \overline{F}(x) \rfloor_{\ell(x)} < \frac{1}{2^{\ell(x)}}$$

(Π.Χ.: ΑΝ $\overline{F}(x) = 0.1111111111$ $(= 1)$

ΤΟΤΕ $\lfloor \overline{F}(x) \rfloor_1 = 0.1 \Rightarrow F(x) - \lfloor \overline{F}(x) \rfloor = 1 - \frac{1}{2} = \frac{1}{2}$)

ΑΣ ΕΠΙΛΕΞΩ

$$l(x) = \left\lceil \log \frac{1}{p(x)} \right\rceil + 1$$

ΑΡΑ

$$\frac{1}{2^{l(x)}} = \frac{1}{2^{\lceil \log \frac{1}{p(x)} \rceil + 1}} < \frac{1}{2 \cdot 2^{\log(\frac{1}{p(x)})}} = \frac{p(x)}{2} = \overline{F}(x) - F(x-1)$$

$$\Rightarrow \overline{F}(x) - \lfloor \overline{F}(x) \rfloor_{l(x)} < \overline{F}(x) - F(x-1) \Rightarrow$$

$$\lfloor \overline{F}(x) \rfloor_{l(x)} > F(x-1) \Rightarrow \text{ ΤΑ } \lfloor \overline{F}(x) \rfloor_{l(x)}$$

ΑΝΗΚΟΥΝ ΣΤΟ ΔΙΑΣΤΗΜΑ $(F(x-1), F(x))$, ΑΡΑ ΟΙ $\lfloor \overline{F}(x) \rfloor_{l(x)}$ ΕΙΝΑΙ ΔΙΑΚΡΙΤΕΣ ΜΕΤΑΞΥ ΤΟΥΣ, ΓΙΑΤΙ ΑΝΗΚΟΥΝ ΣΕ ΔΙΑΦΟΡΕΤΙΚΑ ΔΙΑΣΤΗΜΑΤΑ

ΜΕΣΟ ΜΗΚΟΣ:

$$L = \sum_x p(x) l(x) = \sum_x p(x) \left(\left\lceil \log \frac{1}{p(x)} \right\rceil + 1 \right)$$

$$< \sum p(x) \left(\log \frac{1}{p(x)} + 2 \right)$$

$$= H(x) + 2 \Rightarrow L \leq H(x) + 2$$

ΠΑΡΑΔΕΙΓΜΑ: (5.3.1)

x	$p(x)$	$F(x)$	$\overline{F}(x)$	$\overline{F}(x)$ (ΒΙΝΑΡΥ)	$\lceil \log \frac{1}{p(x)} \rceil + 1$	CODEWORD
1	0.25	0.25	0.125	0.001000	3	001
2	0.5	0.75	0.5	010000	2	10
3	0.125	0.875	0.8125	0.1101000	4	1101
4	0.125	1.0	0.9375	0.1111	4	1111

27 ΧΩΡΗΤΙΚΟΤΗΤΑ ΚΑΝΑΛΙΟΥ

(ΘΑ ΓΙΝΕΙ ΠΙΟ ΑΝΑΛΥΤΙΚΩΣ ΑΡΓΟΤΕΡΑ)

ΟΡΙΣΜΟΣ:

$$X \longrightarrow \boxed{p(y|x)} \longrightarrow Y$$

ΟΡΙΖΩ ΕΝΑ ΔΙΑΚΡΙΤΟ ΚΑΝΑΛΙ ΩΣ ΜΙΑ ΔΟΜΗ ΠΟΥ ΑΠΟΤΕΛΕΙΤΑΙ ΑΠΟ ΜΙΑ Τ.Μ. X ΜΕ ΑΛΦΑΒΗΤΟ $\mathcal{X}$, ΜΙΑ ΤΥΧΑΙΑ ΜΕΤΑΒΛΗΤΗ Y ΜΕ ΑΛΦΑΒΗΤΟ $\mathcal{Y}$, ΚΑΙ ΜΙΑ ΥΠΟ ΣΥΝΘΗΚΗ ΜΑΖΑ ΠΙΘΑΝΟΤΗΤΑΣ $p(y|x)$ $\left(p_{Y|X}(y|x)\right)$ ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΓΡΑΦΕΙ ΩΣ ΠΙΝΑΚΑΣ ΜΕΤΑΒΑΣΗΣ

$$[p_{Y|X}] = \begin{bmatrix} p_{1|1} & p_{2|2} & \cdots & p_{|\mathcal{Y}|/1} \\ p_{2|1} & p_{2/2} & \cdots & p_{|\mathcal{Y}|/2} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1/|\mathcal{X}|} & p_{2/|\mathcal{X}|} & \cdots & p_{|\mathcal{Y}|/|\mathcal{X}|} \end{bmatrix}$$

ΟΡΙΣΜΟΣ: ΟΡΙΖΩ ΤΗΝ "ΠΛΗΡΟΦΟΡΙΑΚΗ ΧΩΡΗΤΙΚΟΤΗΤΑ ΚΑΝΑΛΙΟΥ" ΩΣ

$$\boxed{C = \max_{p(x)} I(X;Y)}$$

ΑΡΑ ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ ΩΣ ΠΡΟΣ ΤΟ ΔΙΑΝΥΣΜΑ $p(x)$

ΠΑΡΑΤΗΡΗΣΕΙΣ:

1) ΘΑ ΔΕΙΞΟΥΜΕ ΟΤΙ Η C ΕΙΝΑΙ Ο ΜΕΓΙΣΤΟΣ ΡΥΘΜΟΣ ΜΕ ΑΥΘΑΙΡΕΤΑ ΜΙΚΡΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ ΜΕΤΑΔΟΣΗΣ, ΟΠΟΥ Ο ΡΥΘΜΟΣ ΜΕΤΑΔΟΣΗΣ ΕΙΝΑΙ BITS/ΧΡΗΣΗ, ΚΑΙ ΥΠΟΘΕΤΟΥΜΕ ΚΑΝΑΛΙ ΧΩΡΙΣ ΜΝΗΜΗ

2) $C \geq 0$, ΓΙΑΤΙ $I(X;Y) \geq 0$

3) $C \leq \log|\mathcal{X}|$, ΓΙΑΤΙ

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \left(H(X) - H(X|Y)\right)$$

$$\leq \max_{p(x)} H(X) = |\mathcal{X}| \quad (p(x) \text{ uniform})$$

4) $C \leq \log|\mathcal{Y}|$ ΟΜΟΙΩΣ.

5) $I(X;Y)$ ΕΙΝΑΙ ΣΥΝΕΧΗΣ ΣΥΝΑΡΤΗΣΗ ΤΗΣ $p(x)$

(ΑΡΑ ΑΝ ΑΛΛΑΞΩ ΛΙΓΟ ΤΟ $p(x)$ ΔΕΝ ΘΑ ΑΛΛΑΞΕΙ ΤΟ $I(X;Y)$)

6) $I(X;Y)$ ΕΙΝΑΙ <u>ΚΟΙΛΗ</u> (CONCAVE) ΣΥΝΑΡΤΗΣΗ ΤΟΥ $p(x)$,

ΔΗΛΑΔΗ

$$I(X;Y)\Big|_{p(x)=\alpha p_1(x)+(1-\alpha)p_2(x)} \geq \alpha I(X;Y)\Big|_{p(x)=p_1(x)} + (1-\alpha) I(X;Y)\Big|_{p(x)=p_2(x)}$$

(ΑΠΟΔΕΙΞΗ ΜΕΣΩ LOG-SUM-INEQUALITY, THEOREM 2.7.4. COVER)

ΜΟΝΟΔΙΑΣΤΑΤΗ ΠΕΡΙΠΤΩΣΗ ΚΟΙΛΗΣ ΣΥΝΑΡΤΗΣΗΣ:

ΠΑΡΑΤΗΡΗΣΤΕ ΟΤΙ ΕΙΝΑΙ ΕΥΚΟΛΟ ΝΑ <u>ΒΡΟΥΜΕ ΤΟ ΜΕΓΙΣΤΟ.</u>

7) <u>ΘΕΩΡΗΜΑ ΤΟΥ WEIERSTRASS</u>: ΜΙΑ ΣΥΝΕΧΗΣ ΣΥΝΑΡΤΗΣΗ f ΣΕ ΕΝΑ ΣΥΜΠΑΓΕΣ (= ΦΡΑΓΜΕΝΟ ΚΑΙ ΚΛΕΙΣΤΟ) ΣΥΝΟΛΟ $C \subset \mathbb{R}^n$ ΕΧΕΙ ΜΕΓΙΣΤΗ ΚΑΙ ΕΛΑΧΙΣΤΗ ΤΙΜΗ, ΔΗΛΑΔΗ $\exists\, x_0, x_1 \in C : f(x_1) \geq f(x)\ \forall x \in C$

$f(x_0) \leq f(x)\ \forall x \in C$

<u>ΠΑΡΑΔΕΙΓΜΑΤΑ</u>

1) 

2) $(0,+\infty)$

(ΟΧΙ ΕΛΑΧΙΣΤΟ, ΓΙΑΤΙ ΔΙΑΣΤΗΜΑ ΟΧΙ ΦΡΑΓΜΕΝΟ)

3) $[0,1)$

(ΟΧΙ ΜΕΓΙΣΤΟ, ΓΙΑΤΙ ΣΥΝΟΛΟ ΟΧΙ ΚΛΕΙΣΤΟ)

4) $[1,2]$

ΟΧΙ ΜΕΓΙΣΤΟ, ΓΙΑΤΙ ΣΥΝΑΡΤΗΣΗ ΟΧΙ ΣΥΝΕΧΗΣ

(ΤΑ ΑΝΩ ΠΑΡΑΔΕΙΓΜΑΤΑ ΓΕΝΙΚΕΥΟΝΤΑΙ ΣΤΟ $\mathbb{R}^n$)

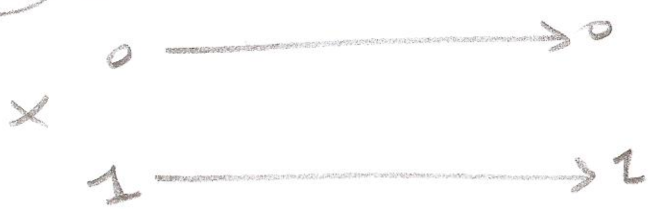
Η $I(X;Y)$ ΕΙΝΑΙ ΜΙΑ ΣΥΝΕΧΗΣ ΣΥΝΑΡΤΗΣΗ ΤΗΣ $p(x) \in \mathbb{R}^{|X|}$ ΣΤΟ ΚΛΕΙΣΤΟ ΚΑΙ ΦΡΑΓΜΕΝΟ ΣΥΝΟΛΟ ΤΩΝ ΔΙΑΝΥΣΜΑΤΩΝ ΚΑΤΑΝΟΜΩΝ

$$\left\{ (x_1, x_2, \ldots, x_{|X|}) : \sum_{i=1}^{|X|} x_i = 1 \right\}$$

ΑΡΑ ΕΧΕΙ ΜΕΓΙΣΤΟ

28 Η ΧΩΡΗΤΙΚΟΤΗΤΑ ΜΕΡΙΚΩΝ ΑΠΛΩΝ ΚΑΝΑΛΙΩΝ

7.1.1 ΑΘΟΡΥΒΟ ΔΥΑΔΙΚΟ ΚΑΝΑΛΙ (NOISELESS BINARY CHANNEL)



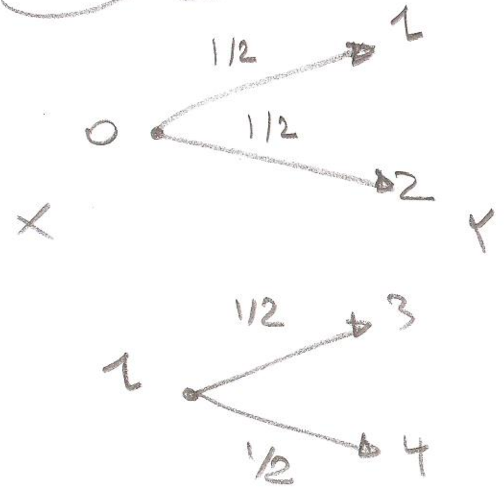
$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array}$$ ⟵ ΠΙΝΑΚΑΣ ΜΕΤΑΒΑΣΗΣ

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \left(H(Y) - H(Y|X) \right)$$

$$= \max_{p(x)} H(Y) = 1, \text{ ΓΙΑ } p(x) = \begin{cases} 1/2, & x=0 \\ 1/2, & x=1 \end{cases} \Rightarrow$$

$$p(y) = \begin{cases} 1/2, & x=0 \\ 1/2, & x=1 \end{cases}$$

7.1.2 ΘΟΡΥΒΩΔΕΣ ΚΑΝΑΛΙ ΜΕ ΜΗ ΕΠΙΚΑΛΥΠΤΟΜΕΝΑ ΣΥΜΒΟΛΑ ΕΞΟΔΟΥ



ΠΙΝΑΚΑΣ ΜΕΤΑΒΑΣΗΣ:

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 0 & 1/2 & 1/2 & 0 & 0 \\ 1 & 0 & 0 & 1/2 & 1/2 \end{array}$$

$$C = \max I(X;Y)$$

$$= \max \left[H(Y) - H(Y|X) \right]$$

ΟΜΩΣ: $H(Y|X) = p_X(0)\, H(Y|X=0) + p_X(1)\, H(Y|X=1) = p_X(0)\cdot 1 + p_X(1)\cdot 1 = 1$

$\Rightarrow$ $C = \max\left[H(Y) - 1\right] \leq 2-1$

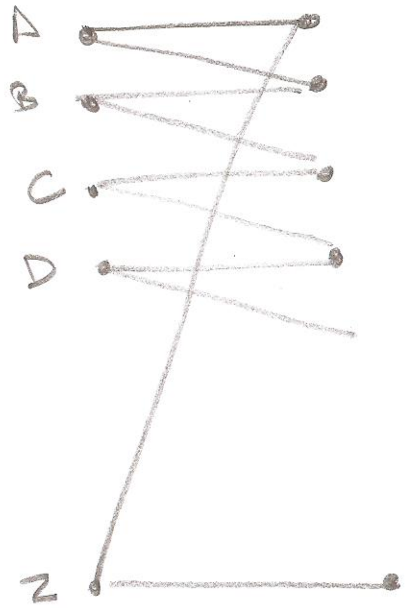
ΤΟ ΑΝΩ ΦΡΑΓΜΑ ΕΠΙΤΥΓΧΑΝΕΤΑΙ ΑΝ $p_X(0) = p_X(1) = \frac{1}{2}$.

ΕΝΑΛΛΑΚΤΙΚΑ:

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \left(H(X) - H(X|Y)\right)$$

$$= \max_{p(x)} H(X) = 1, \text{ ΓΙΑ } p_X(0) = p_X(1) = \tfrac{1}{2}$$

7.1.3 ΘΟΡΥΒΩΔΗΣ ΓΡΑΦΟΜΗΧΑΝΗ



$$C = \max\left(H(Y) - H(Y|X)\right)$$

$$= \max\left(H(Y) - 1\right)$$

$$\leq \log(26) - 1 = \log 13,$$

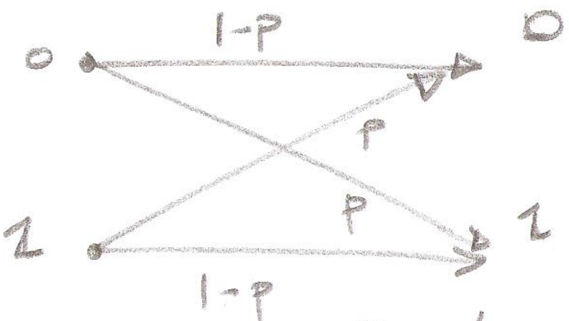
ΠΟΥ ΕΠΙΤΥΓΧΑΝΕΤΑΙ ΓΙΑ ΔΙΑΦΟΡΑ $p(x)$, ΓΙΑ ΠΑΡΑΔΕΙΓΜΑ

$$p(x) = \left(\tfrac{1}{26}, \tfrac{1}{26}, \dots, \tfrac{1}{26}\right)$$

ΚΑΙ

$$p(x) = \left(1/13, 0, 1/13, 0, 1/13, 0, \dots\right)$$

7.1.4 BINARY SYMMETRIC CHANNEL (ΔΥΑΔΙΚΟ ΣΥΜΜΕΤΡΙΚΟ ΚΑΝΑΛΙ)



$$I(X;Y) = H(Y) - H(Y|X)$$

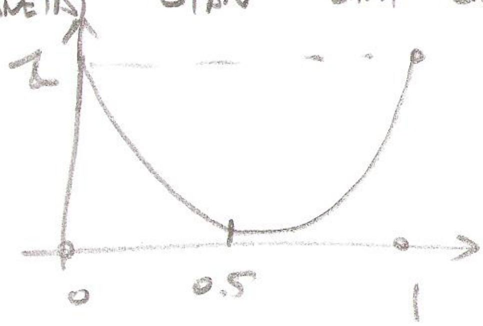
$$= H(Y) - \sum p(x) H(Y|X=x)$$

$$= H(Y) - \underbrace{H(p)}_{-p\log p - (1-p)\log(1-p)}$$

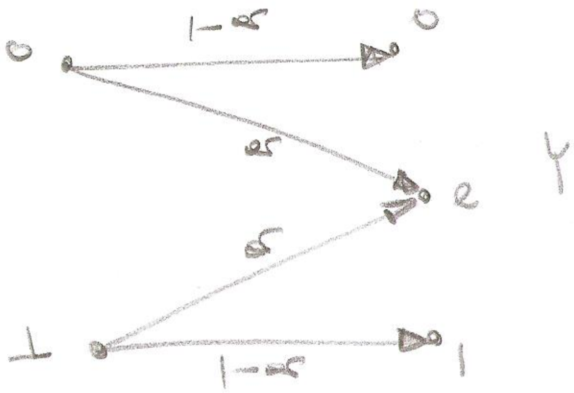
ΠΙΝΑΚΑΣ ΜΕΤΑΒΑΣΑΣ:

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1-p & p \\ 1 & p & 1-p \end{array}$$

$\leq 1 - H(p)$, που επιτυγχάνεται όταν είναι ομοιόμορφη η $P(x) \Rightarrow \boxed{C = 1 - H(p)}$



7.1.5 BINARY ERASURE CHANNEL (ΔΥΑΔΙΚΟ ΚΑΝΑΛΙ ΔΙΑΓΡΑΦΗΣ)



ΠΙΝΑΚΑΣ ΜΕΤΑΒΑΣΗΣ:

$$T = \begin{array}{c|ccc} & 0 & e & 1 \\ \hline 0 & 1-\alpha & \alpha & 0 \\ 1 & 0 & \alpha & 1-\alpha \end{array}$$

$$C = \max_{P(x)} I(X;Y) = \max_{P(x)} \big(H(Y) - H(Y|X)\big)$$

$$= \max_{P(x)} \big(H(Y) - H(\alpha)\big)$$

$$= \max_{\pi} \underbrace{H\big((1-\pi)(1-\alpha),\ \underbrace{(1-\pi)\alpha + \pi\alpha}_{=\alpha},\ \pi(1-\alpha)\big)}_{=H(Y)} - H(\alpha)$$

$(\Pr(X=1) = \pi)$

ΕΣΤΩ $E = \begin{cases} 1, & Y = e \\ 0, & Y \neq e \end{cases}$

$$H(Y) = H(Y,E) = H(E) + H(Y|E)$$

$$= H(\alpha) + \alpha \cdot H(Y|E=1) + (1-\alpha) H(Y|E=0)$$

$$= H(\alpha) + (1-\alpha) H(\pi)$$

$$\Rightarrow \quad C = \max \left\{ H(\alpha) + (1-\alpha) H(\pi) \right\} - H(\alpha)$$

$$= \max (1-\alpha) H(\pi) = 1-\alpha, \quad \text{ΓΙΑ } \pi = \frac{1}{2}$$

ΤΟ ΑΠΟΤΕΛΕΣΜΑ ΕΙΝΑΙ ΕΝΤΥΠΩΣΙΑΚΟ: ΑΝ ΚΑΙ ΧΑΝΟΝΤΑΙ 100α % ΤΩΝ BITS, Η ΧΩΡΗΤΙΚΟΤΗΤΑ ΠΑΡΑΜΕΝΕΙ $1-\alpha$, ΔΗΛΑΔΗ ΥΠΑΡΧΕΙ ΤΡΟΠΟΣ ΝΑ ΔΙΟΡΘΩΘΕΙ Ο,ΤΙ ΧΑΘΗΚΕ, ΧΩΡΙΣ FEEDBACK.

(29) ΣΥΜΜΕΤΡΙΚΑ ΚΑΝΑΛΙΑ

ΟΡΙΣΜΟΣ: ΕΝΑ ΚΑΝΑΛΙ ΚΑΛΕΙΤΑΙ ΣΥΜΜΕΤΡΙΚΟ ΑΝ ΟΙ ΓΡΑΜΜΕΣ ΤΟΥ ΠΙΝΑΚΑ ΜΕΤΑΒΑΣΗΣ ΕΙΝΑΙ ΜΕΤΑΘΕΣΕΙΣ Η ΜΙΑ ΤΗΣ ΑΛΛΗΣ, ΚΑΙ ΑΝ ΟΙ ΣΤΗΛΕΣ ΤΟΥ ΠΙΝΑΚΑ ΜΕΤΑΒΑΣΗΣ ΕΙΝΑΙ ΜΕΤΑΘΕΣΕΙΣ Η ΜΙΑ ΤΗΣ ΑΛΛΗΣ

ΠΑΡΑΔΕΙΓΜΑ: ΕΝΘΟΡΥΒΗ ΓΡΑΦΟΜΗΧΑΝΗ:

$$P_{X|Y} = \begin{bmatrix} 1/2 & 1/2 & 0 & \cdots & 0 & 0 \\ 0 & 1/2 & 1/2 & \cdots & 0 & 0 \\ & & & \ddots & & \\ & & & & 1/2 & 1/2 \\ 0 & 0 & 0 & \cdots & 0 & 1/2 \\ 1/2 & 0 & 0 & \cdots & 0 & \end{bmatrix}$$

ΟΡΙΣΜΟΣ: ΕΝΑ ΚΑΝΑΛΙ ΛΕΓΕΤΑΙ ΑΣΘΕΝΩΣ ΣΥΜΜΕΤΡΙΚΟ ΑΝ ΟΙ ΓΡΑΜΜΕΣ ΤΟΥ ΠΙΝΑΚΑ ΜΕΤΑΒΑΣΗΣ ΕΙΝΑΙ ΜΕΤΑΘΕΣΕΙΣ Η ΜΙΑ ΤΗΣ ΑΛΛΗΣ ΚΑΙ ΟΛΑ ΤΑ ΑΘΡΟΙΣΜΑΤΑ ΤΩΝ ΣΤΗΛΩΝ

$\sum_{x} p(y|x)$ ΕΙΝΑΙ ΙΣΑ

ΠΑΡΑΔΕΙΓΜΑ:

$$p(y|x) = \begin{pmatrix} 1/3 & 1/6 & 1/2 \\ 1/3 & 1/2 & 1/6 \end{pmatrix} \quad \text{ΜΕΤΑΘΕΣΗ}$$

$$\Sigma: \quad \frac{2}{3} \qquad \frac{2}{3} \qquad \frac{2}{3}$$

ΠΡΟΦΑΝΩΣ ΟΛΑ ΤΑ ΣΥΜΜΕΤΡΙΚΑ ΚΑΝΑΛΙΑ ΕΙΝΑΙ ΑΣΘΕΝΩΣ ΣΥΜΜΕΤΡΙΚΑ

ΘΕΩΡΗΜΑ: ΓΙΑ ΚΑΘΕ ΑΣΘΕΝΩΣ ΣΥΜΜΕΤΡΙΚΟ ΚΑΝΑΛΙ,

$$C = \log|\mathcal{Y}| - H(\underbrace{\text{ΜΙΑ ΓΡΑΜΜΗ ΤΟΥ ΠΙΝΑΚΑ ΜΕΤΑΒΑΣΗΣ}}_{= r})$$

ΚΑΙ ΕΠΙΤΥΓΧΑΝΕΤΑΙ ΓΙΑ ΤΗΝ ΟΜΟΙΟΜΟΡΦΗ ΚΑΤΑΝΟΜΗ $P(x) = \frac{1}{|\mathcal{X}|}$ ΣΤΟ ΑΛΦΑΒΗΤΟ ΤΗΣ ΕΙΣΟΔΟΥ.

ΑΠΟΔΕΙΞΗ:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(Y) - H(r) \\ &\le \log|\mathcal{Y}| - H(r). \end{aligned}$$

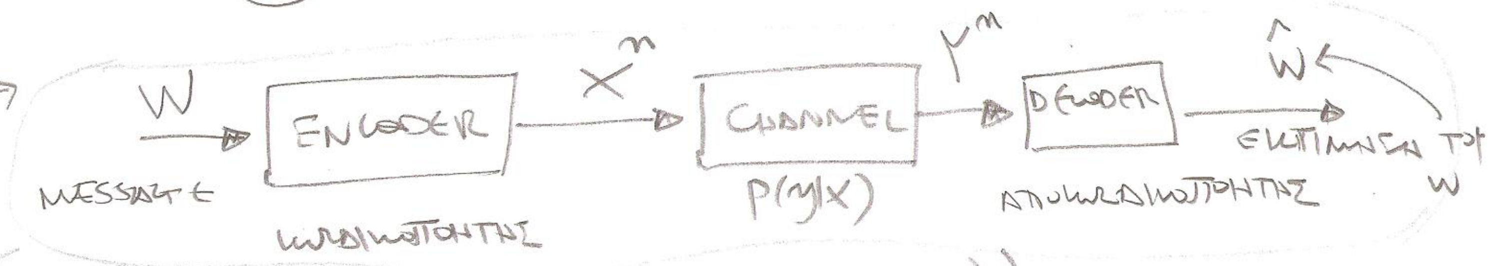
ΟΜΩΣ, ΕΣΤΩ Η ΚΑΤΑΝΟΜΗ ΕΙΣΟΔΟΥ $p(x) = \frac{1}{|\mathcal{X}|}$, ΓΙΑ ΤΗΝ ΟΠΟΙΑ ΕΧΟΥΜΕ:

$$p(y) = \sum_{x \in \mathcal{X}} p(y|x)\, p(x) = \frac{1}{|\mathcal{X}|} \underbrace{\sum_{x \in \mathcal{X}} p(y|x)}_{= c \text{ ΕΞ ΥΠΟΘΕΣΕΩΣ}} = \frac{c}{|\mathcal{X}|} = \frac{1}{|\mathcal{Y}|}$$

$\Rightarrow$ ΓΙΑ ΑΥΤΗΝ ΤΗΝ $P_X(x)$,

$$I(X;Y) = \log|\mathcal{Y}| - H(r) \Rightarrow \boxed{C = \log|\mathcal{Y}| - H(r)}$$

(30) CHANNEL CODING THEOREM - ΟΡΙΣΜΟΙ



(ΥΠΕΝΘΥΜΙΣΗ: ΚΑΝΑΛΙ $= (\mathcal{X}, p(y|x), \mathcal{Y})$)

ΟΡΙΣΜΟΣ: Η n-ΟΣΤΗ ΕΠΕΚΤΑΣΗ ΤΟΥ ΔΙΑΚΡΙΤΟΥ ΚΑΝΑΛΙΟΥ ΧΩΡΙΣ ΜΝΗΜΗ ΚΑΙ ΧΩΡΙΣ ΑΝΑΔΡΑΣΗ (FEEDBACK) ΕΙΝΑΙ ΤΟ ΚΑΝΑΛΙ $(\mathcal{X}^n, p(y^n|x^n), \mathcal{Y}^n)$ ΟΠΟΥ

$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i)$$

ΟΡΙΣΜΟΣ: ΕΝΑΣ ΚΩΔΙΚΑΣ (M,n) ΓΙΑ ΤΟ ΚΑΝΑΛΙ $(\mathcal{X}, p(y|x), \mathcal{Y})$ ΑΠΟΤΕΛΕΙΤΑΙ ΑΠΟ ΤΑ ΑΚΟΛΟΥΘΑ:

1. ΕΝΑ ΣΥΝΟΛΟ ΜΗΝΥΜΑΤΩΝ $\{1,2,\dots,M\}$
2. ΜΙΑ ΣΥΝΑΡΤΗΣΗ ΚΩΔΙΚΟΠΟΙΗΣΗΣ $X^n: \{1,2,\dots,M\} \to \mathcal{X}^n$ ΠΟΥ ΑΠΟΤΕΛΕΙΤΑΙ ΑΠΟ $x^n(1), x^n(2), \dots, x^n(M)$ ΠΟΥ ΑΠΟ ΚΟΙΝΟΥ ΚΩΔΙΚΕΣ ΛΕΞΕΙΣ ΚΑΛΟΥΝΤΑΙ CODEBOOK (ΚΩΔΙΚΟΒΙΒΛΙΟ)
3. ΜΙΑ ΣΥΝΑΡΤΗΣΗ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ

$$g: \mathcal{Y}^n \to \{1,2,\dots,M\}$$

ΠΟΥ ΕΙΝΑΙ ΕΝΑΣ ΚΑΝΟΝΑΣ ΠΟΥ ΑΠΕΙΚΟΝΙΖΕΙ ΚΑΘΕ ΔΥΝΑΤΗ ΕΞΟΔΟ ΤΟΥ ΚΑΝΑΛΙΟΥ ΣΕ ΚΑΠΟΙΟ ΜΗΝΥΜΑ

ΟΡΙΣΜΟΣ: ΕΣΤΩ

$$\lambda_i = \Pr\left[g(Y^n) \neq i \mid X^n = x^n(i)\right] = \sum_{y^n} p(y^n|x^n(i))\, I(g(y^n) \neq i)$$

Η ΥΠΟ ΣΥΝΘΗΚΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ ΜΕ ΔΕΔΟΜΕΝΟ ΟΤΙ ΣΤΑΛΘΗΚΕ ΤΟ ΜΗΝΥΜΑ i, ΚΑΙ

$$I(\text{TRUE})=1, \quad I(\text{FALSE})=0.$$

ΟΡΙΣΜΟΣ: Η ΜΕΓΙΣΤΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ $\lambda^{(n)}$ ΕΝΟΣ ΚΩΔΙΚΑ (M,n) ΕΙΝΑΙ Η $\lambda^{(n)} = \max_{i \in \{1,2,\ldots,M\}} \lambda_i$

ΟΡΙΣΜΟΣ: Η ΑΡΙΘΜΗΤΙΚΗ ΜΕΣΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ $P_e^{(n)}$ ΙΣΟΥΤΑΙ ΜΕ $P_e^{(n)} = \frac{1}{M}\sum_{i=1}^{M} \lambda_i$

ΠΑΡΑΤΗΡΗΣΗ: ΕΧΕΙ ΝΟΗΜΑ ΟΤΑΝ ΤΑ ΜΗΝΥΜΑΤΑ ΕΙΣΟΔΟΥ ΕΙΝΑΙ ΙΣΟΠΙΘΑΝΑ.

ΟΡΙΣΜΟΣ: Ο ΡΥΘΜΟΣ (RATE) R ΕΝΟΣ (M,n) ΚΩΔΙΚΑ ΕΙΝΑΙ Ο $R = \frac{\log M}{n}$ BITS ΑΝΑ ΜΕΤΑΔΟΣΗ

ΟΡΙΣΜΟΣ: Ο ΡΥΘΜΟΣ R ΚΑΛΕΙΤΑΙ ΕΠΙΤΕΥΞΙΜΟΣ ΑΝ ΥΠΑΡΧΕΙ ΑΚΟΛΟΥΘΙΑ ΚΩΔΙΚΩΝ $(\lceil 2^{nR} \rceil, n)$ ΕΤΣΙ ΩΣΤΕ

$$\lambda^{(n)} \to 0 \quad \text{ΓΙΑ } n \to \infty$$

ΟΡΙΣΜΟΣ: Η ΧΩΡΗΤΙΚΟΤΗΤΑ ΕΝΟΣ ΚΑΝΑΛΙΟΥ ΕΙΝΑΙ ΤΟ SUPREMUM ΟΛΩΝ ΤΩΝ ΕΠΙΤΕΥΞΙΜΩΝ ΡΥΘΜΩΝ.

(31) ΑΠΟ ΚΟΙΝΟΥ ΤΥΠΙΚΕΣ ΑΚΟΛΟΥΘΙΕΣ

ΟΡΙΣΜΟΣ: ΤΟ ΣΥΝΟΛΟ $A_\epsilon^{(n)}$ ΤΩΝ ΑΠΟ ΚΟΙΝΟΥ ΤΥΠΙΚΩΝ ΑΚΟΛΟΥΘΙΩΝ ΣΕ ΣΧΕΣΗ ΜΕ ΤΗΝ ΚΑΤΑΝΟΜΗ $p(x,y)$ ΕΙΝΑΙ ΤΟ ΣΥΝΟΛΟ $\{(x^n, y^n)\}$ ΤΩΝ ΑΚΟΛΟΥΘΙΩΝ ΜΕ ΕΜΠΕΙΡΙΚΕΣ ΕΝΤΡΟΠΙΕΣ ΚΟΝΤΑ ΣΤΙΣ ΕΝΤΡΟΠΙΕΣ:

$$A_\epsilon^{(n)} = \Big\{ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n :$$

$$\Big| -\frac{1}{n} \log \overset{\prod p(x_i)}{p(x^n)} - H(X) \Big| < \epsilon ,$$

$$\Big| -\frac{1}{n} \log \overset{\prod p(y_i)}{p(y^n)} - H(Y) \Big| < \epsilon$$

$$\Big| -\frac{1}{n} \log p(x^n, y^n) - H(X,Y) \Big| < \epsilon \Big\}$$

$$p(x^n, y^n) = \prod_{i=1}^{n} p(x_i, y_i)$$

(ΠΑΡΑΔΕΙΓΜΑ ΜΕ ΥΨΗ ΚΑΙ ΒΑΡΗ ΦΟΙΤΗΤΩΝ)

ΘΕΩΡΗΜΑ (JOINT AEP)

① $P\big((X^n, Y^n) \in A_\epsilon^{(n)}\big) \to 1$, ΓΙΑ $n \to \infty$

② $|A_\epsilon^{(n)}| \le 2^{n(H(X,Y)+\epsilon)}$

③ ΕΣΤΩ $(\tilde{X}^n, \tilde{Y}^n) \sim p(x^n)\,p(y^n)$, ΔΗΛΑΔΗ ΟΙ $\tilde{X}^n, \tilde{Y}^n$ ΑΝΕΞΑΡΤΗΤΕΣ ΑΛΛΑ ΜΕ ΚΑΤΑΝΟΜΕΣ $p(x), p(y)$,

ΤΟΤΕ $$P\big((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\big) \le 2^{-n(I(X;Y) - 3\epsilon)}$$

ΚΑΙ ΓΙΑ $n > n_0$,

$$P\big((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\big) \ge (1-\epsilon)\, 2^{-n(I(X;Y) + 3\epsilon)}$$

ΑΠΟΔΕΙΞΗ:

① $P\left[\left|-\frac{1}{n}\log p(X^n)-H(X)\right|\geq\epsilon\right]$

$= P\left[\underbrace{\left|-\frac{1}{n}\sum_i \log p(X_i)-H(X)\right|\geq\epsilon}_{A}\right] < \frac{\epsilon}{3} \quad \forall n>n_1$

ΟΜΟΙΩΣ: $P\left[\underbrace{\left|-\frac{1}{n}\log p(Y^n)-H(Y)\right|\geq\epsilon}_{B}\right] < \frac{\epsilon}{3} \quad \forall n>n_2$

$P\left[\underbrace{\left|-\frac{1}{n}\log p(X,Y)-H(X,Y)\right|\geq\epsilon}_{C}\right] < \frac{\epsilon}{3} \quad \forall n>n_3.$

ΑΡΑ ΓΙΑ $n>\max(n_1,n_2,n_3)=n_0$,

$P(A\cup B\cup C)\leq P(A)+P(B)+P(C) = \frac{\epsilon}{3}+\frac{\epsilon}{3}+\frac{\epsilon}{3}=\epsilon$

② $1=\sum p(x^n,y^n)\geq\sum_{A_\epsilon^{(n)}} p(x^n,y^n)$

$\geq |A_\epsilon^{(n)}|\, 2^{-n[H(X,Y)+\epsilon]} \Rightarrow$

$|A_\epsilon^{(n)}|\leq 2^{n(H(X,Y)+\epsilon)}$

③ $P\left((\tilde{X}^n,\tilde{Y}^n)\in A_\epsilon^{(n)}\right)=\sum_{(x^n,y^n)\in A_\epsilon^{(n)}} p(x^n)\,p(y^n)$

$\leq 2^{n(H(X,Y)+\epsilon)}\cdot 2^{-n(H(X)-\epsilon)}\cdot 2^{-n(H(Y)-\epsilon)}$

$= 2^{-n(I(X;Y)-3)}$

ΕΠΙΣΗΣ:

$$1-\epsilon \leq P(A_\epsilon^{(n)}) = \sum_{(x^n,y^n)\in A_\epsilon^{(n)}} p(x^n,y^n)$$

Ήπιστα,

$$\leq |A_\epsilon^{(n)}|\, 2^{-n(H(X,Y)-\epsilon)}$$

$$\Rightarrow |A_\epsilon^{(n)}| \geq (1-\epsilon)\, 2^{n(H(X,Y)-\epsilon)}.$$

ΑΡΑ: $$P((\tilde{X}^n,\tilde{Y}^n)\in A_\epsilon^{(n)}) = \sum_{A_\epsilon^{(n)}} p(x^n)\,p(y^n)$$

$$\geq (1-\epsilon)\, 2^{n(H(X,Y)-\epsilon)} \cdot 2^{-n(H(X)+\epsilon)} \cdot 2^{-n(H(Y)+\epsilon)}$$

$$= (1-\epsilon)\, 2^{-n(I(X;Y)+3\epsilon)}$$ QED.

32 CHANNEL CODING THEOREM - ΑΠΟΔΕΙΞΗ ΕΥΘΕΩΣ

($\Rightarrow$)

ΘΕΩΡΗΜΑ: ΣΕ ΕΝΑ ΔΙΑΚΡΙΤΟ ΚΑΝΑΛΙ ΧΩΡΙΣ ΜΝΗΜΗ ΚΑΙ ΑΝΑΔΡΑΣΗ, ΟΛΟΙ ΟΙ ΡΥΘΜΟΙ ΚΑΤΩ ΑΠΟ ΤΗ ΧΩΡΗΤΙΚΟΤΗΤΑ ΕΙΝΑΙ ΕΠΙΤΕΥΞΙΜΟΙ. ΣΥΓΚΕΚΡΙΜΕΝΑ, ΓΙΑ ΚΑΘΕ $R<C$, ΥΠΑΡΧΕΙ ΑΚΟΛΟΥΘΙΑ ΚΩΔΙΚΩΝ $(2^{nR}, n)$ ΜΕ ΜΕΓΙΣΤΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ $\lambda^{(n)} \to 0$.

($\Leftarrow$) ΟΠΟΙΑΔΗΠΟΤΕ ΑΚΟΛΟΥΘΙΑ ΚΩΔΙΚΩΝ $(2^{nR}, n)$ ΜΕ $\lambda^{(n)} \to 0$ ΠΡΕΠΕΙ ΝΑ ΕΧΕΙ $R \leq C$.

ΑΠΟΔΕΙΞΗ ΤΟΥ ($\Rightarrow$): ΒΗΜΑ 1º (ΑΡΧΙΚΟΠΟΙΗΣΗΣ) ΕΠΙΛΕΓΩ ΜΙΑ $p(x)$. ΦΤΙΑΧΝΩ ΕΝΑ ΚΩΔΙΚΑ $(2^{nR}, n)$ ΣΤΗΝ ΤΥΧΗ, ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΚΑΤΑΝΟΜΗ $p(x)$ ΩΣ ΕΞΗΣ:

$$\mathcal{C} = \begin{bmatrix} x_1(1) & x_2(1) & \cdots & x_n(1) \\ \vdots & \vdots & & \vdots \\ x_1(2^{nR}) & x_2(2^{nR}) & \cdots & x_n(2^{nR}) \end{bmatrix}$$

ΟΛΑ ΤΑ ΣΥΜΒΟΛΑ ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΚΑΤΑΝΟΜΗ $p(x)$

ΑΡΑ $$P(\mathcal{C}) = \prod_{w=1}^{2^{nR}} \prod_{i=1}^{n} p(x_i(w))$$

ΒΗΜΑ 2ο: Ο ΚΩΔΙΚΑΣ $\mathcal{C}$ (ΑΡΧΙΚΟΠΟΙΗΣΗΣ) ΥΙΟΘΕΤΕΙΤΑΙ ΑΠΟ ΠΟΜΠΟ ΚΑΙ ΔΕΚΤΗ, ΟΙ ΟΠΟΙΟΙ ΕΠΙΠΛΕΟΝ ΓΝΩΡΙΖΟΥ ΤΟ $p(y|x)$

ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΩΝ

ΒΗΜΑ 3ο: ΕΠΙΛΕΓΟΥΜΕ ΕΝΑ ΣΥΜΒΟΛΟ W ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΟΜΟΙΟΜΟΡΦΗ ΚΑΤΑΝΟΜΗ

$$P(W=w) = 2^{-nR}, \quad w=1,2,\dots,2^{nR}$$

ΒΗΜΑ 4ο: ΣΤΕΛΝΟΥΜΕ, ΜΕΣΩ ΤΟΥ ΚΑΝΑΛΙΟΥ, ΤΗΝ w ΚΩΔΙΚΟΛΕΞΗ $X^n(w) = [x_w(1) \quad x_w(2) \dots x_w(2^{nR})]$

ΒΗΜΑ 5ο: Ο ΔΕΚΤΗΣ ΛΑΜΒΑΝΕΙ ΤΗΝ ΑΚΟΛΟΥΘΙΑ Y^n ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΚΑΤΑΝΟΜΗ

$$p(y^n | x^n(w)) = \prod_{i=1} p(y_i | x_i(w))$$

ΒΗΜΑ 6ο: Ο ΑΠΟΚΩΔΙΚΟΠΟΙΗΤΗΣ ΑΠΟΦΑΣΙΖΕΙ ΓΙΑ ΤΟ ΜΗΝΥΜΑ ΠΟΥ ΣΤΑΛΘΗΚΕ, ΩΣ ΕΞΗΣ:

ΠΡΩΤΗ ΠΕΡΙΠΤΩΣΗ: ΥΠΑΡΧΕΙ ΑΚΡΙΒΩΣ ΕΝΑ ΜΗΝΥΜΑ $\hat{W}$ ΕΤΣΙ ΩΣΤΕ ΤΟ ΖΕΥΓΟΣ $(X^n(\hat{W}), Y^n)$ ΕΙΝΑΙ ΑΠΟ ΚΟΙΝΟΥ ΤΥΠΙΚΟ ΣΥΜΦΩΝΑ ΜΕ ΤΗΝ ΚΑΤΑΝΟΜΗ $p(x)p(y|x)$

$\Rightarrow$ ΕΠΙΛΕΓΩ ΤΟ ΜΗΝΥΜΑ $\hat{W}$ ΩΣ ΑΥΤΟ ΠΟΥ ΕΧΕΙ ΣΤΑΛΕΙ

ΔΕΥΤΕΡΗ ΠΕΡΙΠΤΩΣΗ: ΟΛΑ ΤΑ ~~ΑΛΛΑ~~ ΕΝΔΕΧΟΜΕΝΑ $\Rightarrow$ ΔΗΛΩΝΩ ΣΦΑΛΜΑ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ

ΥΠΟΛΟΓΙΣΜΟΣ ΛΑΘΟΥΣ ΣΤΑ ΒΗΜΑΤΑ 1-6

ΕΣΤΩ $\mathcal{E} = \{\hat{W}(Y^n) \neq W\}$ ΤΟ ΕΝΔΕΧΟΜΕΝΟ ΣΦΑΛΜΑΤΟΣ.

ΘΑ ΥΠΟΛΟΓΙΣΟΥΜΕ ΤΗΝ ΠΙΘΑΝΟΤΗΤΑ ΤΟΥ ΑΝ ΓΙΝΟΥΝ ΤΑ ΒΗΜΑΤΑ 1-6

$$P(\mathcal{E}) = \sum_{\mathcal{C}} P(\mathcal{C})\, P_e^{(n)}(\mathcal{C})$$

$$= \sum_{\mathcal{C}} P(\mathcal{C}) \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \lambda_w(\mathcal{C})$$

$$= \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \sum_{\mathcal{C}} P_r(\mathcal{C})\, \lambda_w(\mathcal{C})$$

DOES NOT DEPEND ON w

$$= \sum_{\mathcal{C}} P(\mathcal{C})\, \lambda_1(\mathcal{C})$$

(ΛΟΓΩ ΣΥΜΜΕΤΡΙΑΣ)

$$= P_r(\mathcal{E} \mid W=1)$$

$$= P(E_1^c \cup E_2 \cup E_3 \cup \dots \cup E_{2^{nR}} \mid W=1)$$

ΟΠΟΥ $E_i = \{ (X^n(i), Y^n) \in A_\epsilon^{(n)}, \dots\ i \in \{1,2,\dots,2^{nR}\} \}$

$$\leq P(E_1^c / W_1) + \sum_{i=2}^{2^{nR}} P(E_i \mid W=1)$$

($\forall n>n_1$ ΑΠΟ JOINT AEP)

$$\leq \epsilon + \sum_{i=2}^{2^{nR}} P(E_i \mid W=1)$$

$$\leq \epsilon + \sum_{i=2}^{2^{nR}} 2^{-n(I(X;Y)-3\epsilon)}$$

(ΑΠΟ ③ ΤΟΥ ΘΕΩΡ. ΓΙΑ JOINT AEP)

$$\leq \epsilon + 2^{nR} \cdot 2^{-nI(X;Y)+3\epsilon n}$$

$$= \epsilon + 2^{3\epsilon n + n(R - I(X;Y))}$$

$$\leq 2\epsilon \quad \text{ΑΝ} \quad R < I(X;Y) - 3\epsilon$$

$\forall n > n_1$

ΚΑΙ ΤΟ ϵ ΟΣΟ ΜΙΚΡΟ ΘΕΛΟΥΜΕ

ΕΣΤΩ $R = C - \epsilon_1 = \max I(X;Y) - \epsilon_1$.

ΘΕΤΩ $\epsilon_1 = 3\epsilon \Leftrightarrow \epsilon = \frac{\epsilon_1}{3}$ ΚΑΙ ΓΙΑ ΑΥΤΟ ΤΟ

$\epsilon, \exists n_1 : \forall n > n_1 \quad P(\mathcal{E}) \le 2\epsilon$

ΠΑΡΑΤΗΡΗΣΗ: ΜΕΧΡΙ ΤΩΡΑ, ΒΡΗΚΑΜΕ ΟΤΙ Η ΑΡΙΘΜΗΤΙΚΗ ΜΕΣΗ ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ ΕΙΝΑΙ $P(\mathcal{E}) \le 2\epsilon$ ΑΝ Ο ΚΩΔΙΚΑΣ ΕΠΙΛΕΓΕΙ ΣΤΗΝ ΤΥΧΗ. ΑΡΑ ΠΡΕΠΕΙ ΝΑ ΥΠΑΡΧΕΙ ΤΟΥΛΑΧΙΣΤΟΝ 1 ΚΩΔΙΚΑΣ C^* ΤΕΤΟΙΟΣ ΩΣΤΕ

$$P(\mathcal{E}|C^*) \le 2\epsilon \Leftrightarrow \frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} \lambda_i(C^*) \le 2\epsilon$$

ΑΠΟ ΤΙΣ 2^{nR} ΛΕΞΕΙΣ ΤΟΥ C^*, ΚΡΑΤΑΜΕ ΤΙΣ ΜΙΣΕΣ (2^{nR-1}) ΓΙΑ ΤΙΣ ΟΠΟΙΕΣ $\lambda_i(C^*) \le 4\epsilon$ (ΣΙΓΟΥΡΑ ΥΠΑΡΧΟΥΝ, ΑΛΛΙΩΣ ΑΤΟΠΟ) $\rightarrow$ ΥΠΑΡΧΕΙ ΚΩΔΙΚΑΣ ΜΕ ΡΥΘΜΟ $R - \frac{1}{n}$ ΚΑΙ MAXIMAL ΠΙΘΑΝΟΤΗΤΑ ΣΦΑΛΜΑΤΟΣ $\lambda^{(n)} = \max_i \lambda_i(C^*) \le 4\epsilon$ (ΟΧΙ ΜΕΣΗ)