Θεωρία Πληροφορίας και Στοιχεία Κωδίκων

Κωδικοποίηση Πηγής και Χωρητικότητα Διακριτών Καναλιών

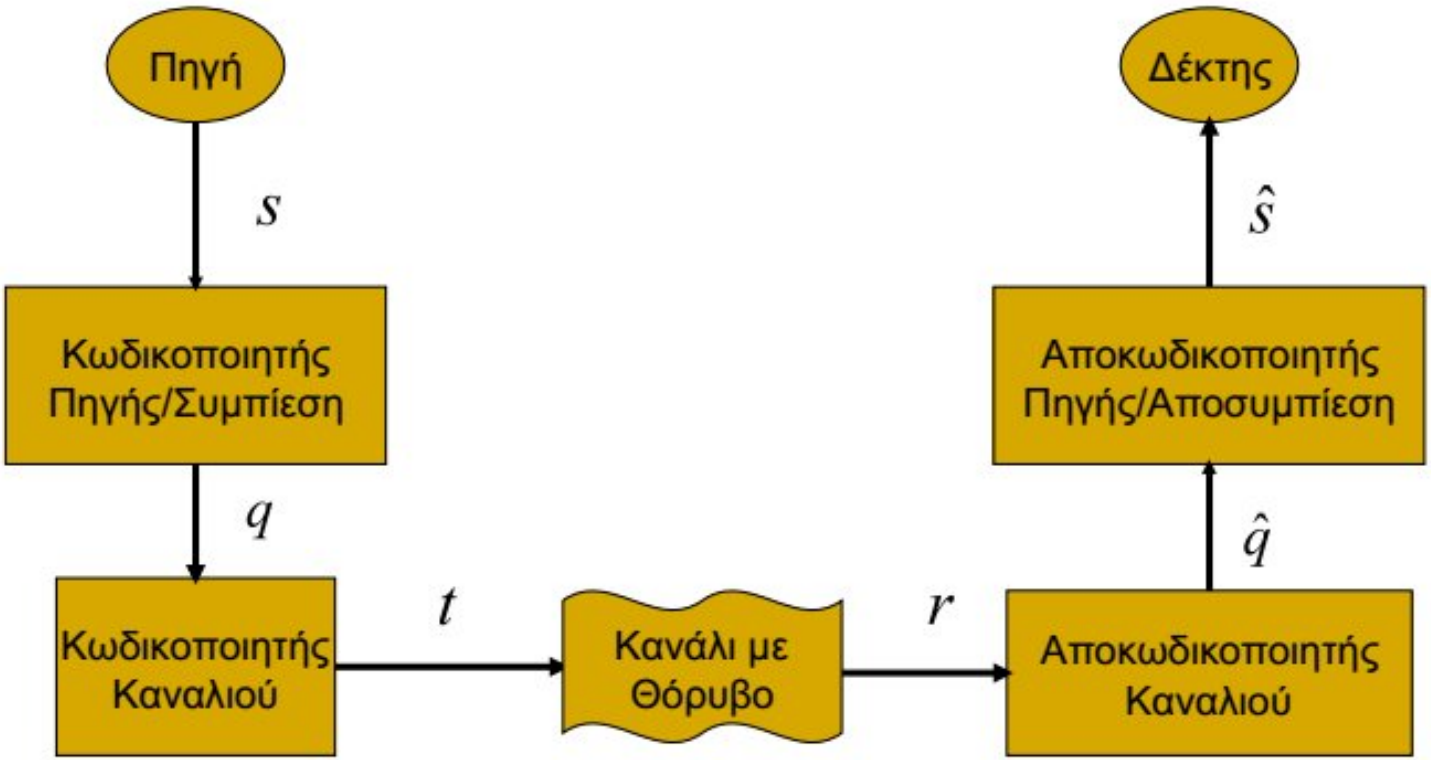
Διδάσκων: Καλουπτσίδης Νικόλαος
Επιμέλεια: Κατσάνος Κωνσταντίνος

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Εαρινό Εξάμηνο 2017-2018

Περιεχόμενα

Συμπίεση Πληροφορίας (Κωδικοποίηση Πηγής)



Βασικοί Ορισμοί Κωδίκων Πηγής

- **Μη ιδιάζων (nonsingular) κώδικας**: Όταν όλες οι κωδικές λέξεις είναι διαφορετικές.
- **Μοναδικώς αποκωδικοποιήσιμος (uniquely decodable) κώδικας**: Όταν τόσο οι κωδικές λέξεις όσο και όλες οι πιθανές ακολουθίες των κωδικών λέξεων είναι διαφορετικές.
- **Άμεσος ή Προθεματικός κώδικας (instantaneous/ prefix code)**: Ο κώδικας του οποίου καμία κωδική λέξη δεν αποτελεί πρόθεμα κάποιας άλλης. Κάθε προθεματικός κώδικας επιτρέπει την άμεση αποκωδικοποίηση της κωδικής λέξης χωρίς να χρειάζεται να ληφθούν υπόψη οι επόμενες κωδικές λέξεις.

Προκύπτει το συμπέρασμα ότι: Άμεσος $\Longrightarrow$ Μοναδικώς Αποκωδικοποιήσιμος $\Longrightarrow$ Μη ιδιάζων

Παραδείγματα Κωδίκων

- Μη ιδιάζοντες: I, II, III, IV
- Μοναδικώς αποκωδικοποιήσιμοι: II,III,IV
- Άμεσοι: II και III: Ο IV δεν είναι άμεσος, αφού για την αποκωδικοποίηση χρειάζεται να περιμένουμε την εμφάνιση ψηφίων που ανήκουν στην επόμενη κωδική λέξη, π.χ.011**0111**00

Κώδικας

	I	II	III	IV
Φ	0	00	0	0
Χ	11	01	10	01
Ψ	00	10	110	011
Ω	01	11	1110	0111

Ανισότητα Kraft

($\Rightarrow$) Για κάθε **άμεσο** κώδικα με μέγεθος κωδικού αλφαβήτου q και μήκη των n κωδικών του λέξεων ℓ_i, όπου i=1,2,. . . ,n, ισχύει

$$\sum_{i=1}^{n} q^{-\ell_i} \leq 1.$$

($\Leftarrow$) Αντιστρόφως, εάν για ένα σύνολο μηκών ℓ_i ικανοποιείται η ανισότητα Kraft, υπάρχει άμεσος κώδικας του οποίου οι κωδικές λέξεις έχουν αυτά τα μήκη.

Μη Άμεσοι Κώδικες

- Για να είναι ένας κώδικας άμεσος πρέπει να ισχύει η ανισότητα Kraft, η οποία επιβάλλει περιορισμούς στα μήκη κωδίκων που μπορούμε να επιλέξουμε.
- Τι συμβαίνει εάν ένας κώδικας είναι μοναδικώς αποκωδικοποιήσιμος αλλά όχι, κατ' ανάγκη, άμεσος;
  - Δεδομένου ότι οι άμεσοι κώδικες αποτελούν υποσύνολο των μοναδικώς αποκωδικοποιήσιμων, υπάρχει περίπτωση οι μοναδικώς αποκωδικοποιήσιμοι να είναι πιο αποδοτικοί;
- Παρόλο που δε θα το δείξουμε λεπτομερώς, για την απόδειξη του Θεωρήματος Κωδικοποίησης Πηγής (Θεώρημα 5.1 στη συνέχεια των διαφανειών), βασική προϋπόθεση είναι να ισχύει η ανισότητα Kraft.
- Αποδεικνύεται (McMillan – βλ. π.χ. Cover & Thomas Theorem 5.5.1) ότι και οι μοναδικώς αποκωδικοποιήσιμοι κώδικες υπακούουν στην ανισότητα Kraft.
- Επομένως, δε χάνουμε τίποτα (ως προς την αποδοτικότητα της συμπίεσης) με το να χρησιμοποιούμε άμεσους κώδικες αντί για απλώς μοναδικώς αποκωδικοποιήσιμους!

Βέλτιστος Κώδικας Μεταβλητού Μήκους

- **Κωδικοποίηση μεταβλητού μήκους**:
  - Προκειμένου η συμπίεση να είναι αναπωλειακή, ο κώδικας πρέπει να είναι μοναδικώς αποκωδικοποιήσιμος
  - $\longrightarrow$ Αναγκαία συνθήκη: πρέπει να ισχύει η ανισότητα Kraft.
  - Επιπλέον, θέλουμε η συμπίεση να είναι αποδοτική, δηλαδή το μέσο μήκος κώδικα ($\bar{L} = \sum_{i=1}^{n} p(s_i)\ell_i$) να είναι το μικρότερο δυνατό.
- **Ερωτήματα**:
  - Υπάρχει συστηματικός τρόπος για να βρίσκουμε το βέλτιστο άμεσο κώδικα δεδομένης μιας κατανομής, p; $\rightarrow$ ΝΑΙ! (κώδικας Huffman).
  - Πόσο καλή συμπίεση πετυχαίνουμε, τελικά, όταν χρησιμοποιήσουμε κώδικες μεταβλητού μήκους; $\rightarrow$ Το πολύ 1 bit μακριά από την εντροπία.

Βέλτιστος Άμεσος Κώδικας

- Η ανισότητα Kraft εγγυάται ότι ένας κώδικας είναι άμεσος. Ωστόσο, ο κώδικας δεν είναι, απαραίτητα και βέλτιστος.
- **Ορισμός**: *Βέλτιστος* είναι ο κώδικας του οποίου οι κωδικές λέξεις έχουν το ελάχιστο μέσο μήκος, δηλαδή πρέπει να ισχύει ότι

$$\mathbb{E}[\ell^\star] = \min_{\{\ell_i\}} \sum_i p_i \ell_i,$$

$$\mathbf{l}^\star = [\ell_1^\star, \ldots, \ell_n^\star] = \arg\min_{\{\ell_i\}} \sum_i p_i \ell_i$$

Κωδικοποίηση Huffman

- Δοθείσης μιας πηγής χωρίς μνήμη με πιθανότητες εμφάνισης συμβόλων p_i, ποιος είναι ο βέλτιστος άμεσος κώδικας;
- Η διαδικασία Huffman βασίζεται σε τρεις παρατηρήσεις/ιδιότητες που έχουν σχέση με βέλτιστους κώδικες:
  - Σε ένα βέλτιστο κώδικα τα σύμβολα με μεγαλύτερη πιθανότητα εμφάνισης θα πρέπει να αντιστοιχούν σε πιο σύντομες κωδικές λέξεις από τα σύμβολα με μικρότερη πιθανότητα εμφάνισης, δηλαδή $p_i > p_j \Rightarrow \ell_i \leq \ell_j$ (Cover & Thomas Lemma 5.8.1)
  - Σε ένα (δυαδικό) βέλτιστο κώδικα οι δύο μακρύτερες κωδικές λέξεις (οι οποίες αντιστοιχούν στα 2 λιγότερο πιθανά σύμβολα) έχουν το ίδιο μήκος (Cover & Thomas Lemma 5.8.1).
  - Για το (δυαδικό) κώδικα Huffman ισχύει, επίσης, ότι οι κωδικές λέξεις που ανήκουν στα 2 λιγότερο πιθανά σύμβολα διαφέρουν μόνο κατά 1 bit. ! Προσοχή: Αυτό είναι χαρακτηριστικό του κώδικα Huffman και **δεν** είναι απαραίτητο να ισχύει για να είναι ένας κώδικας βέλτιστος!

Αλγόριθμος Κωδικοποίησης Huffman

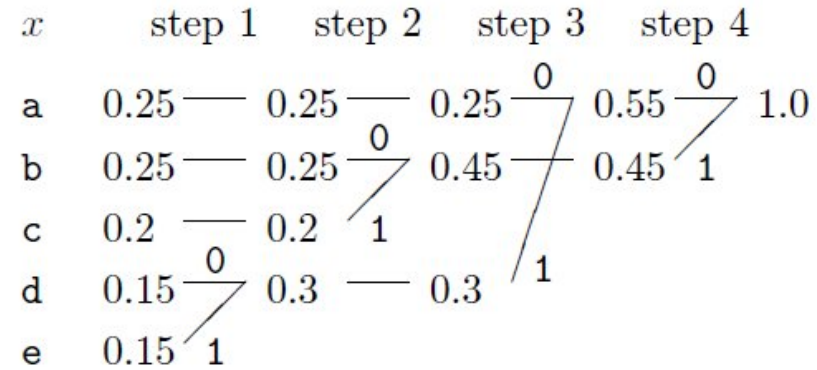
Ο (δυαδικός) αλγόριθμος Huffman κατασκευάζει το (δυαδικό) δέντρο αρχίζοντας από τα φύλλα του και προχωρώντας προς τη ρίζα του.

Αλγόριθμος:

- **Βήμα 1**: Τα σύμβολα (ή τα μηνύματα) ταξινομούνται έτσι ώστε οι πιθανότητές τους να είναι σε φθίνουσα ακολουθία.
- **Βήμα 2**: Στη συνέχεια, επιλέγουμε τα δύο (ή δύο από τα) σύμβολα με τις μικρότερες πιθανότητες.
- **Βήμα 3**: Συνδυάζουμε τα δύο σύμβολα που επιλέξαμε στο Βήμα 2 σε ένα και αναθέτουμε στο συνδυασμένο σύμβολο το άθροισμα των πιθανοτήτων των επιμέρους συμβόλων. Επαναλαμβάνουμε τη διαδικασία από το Βήμα 1 μεταξύ των συμβόλων που απομένουν και του συμβόλου που δημιουργήσαμε μέχρις ότου καταλήξουμε σε ένα σύμβολο με πιθανότητα 1.
- **Βήμα 4**: Οι κωδικές λέξεις που αντιστοιχούν στο κάθε σύμβολο αποτελούνται από τις ακολουθίες 0 και 1 που δημιουργούνται εάν διατρέξουμε το δέντρο που δημιουργήθηκε από τον κόμβο με το μοναδικό σύμβολο προς τα σύμβολα από τα οποία ξεκινήσαμε.

Παράδειγμα Κωδικοποίησης Huffman

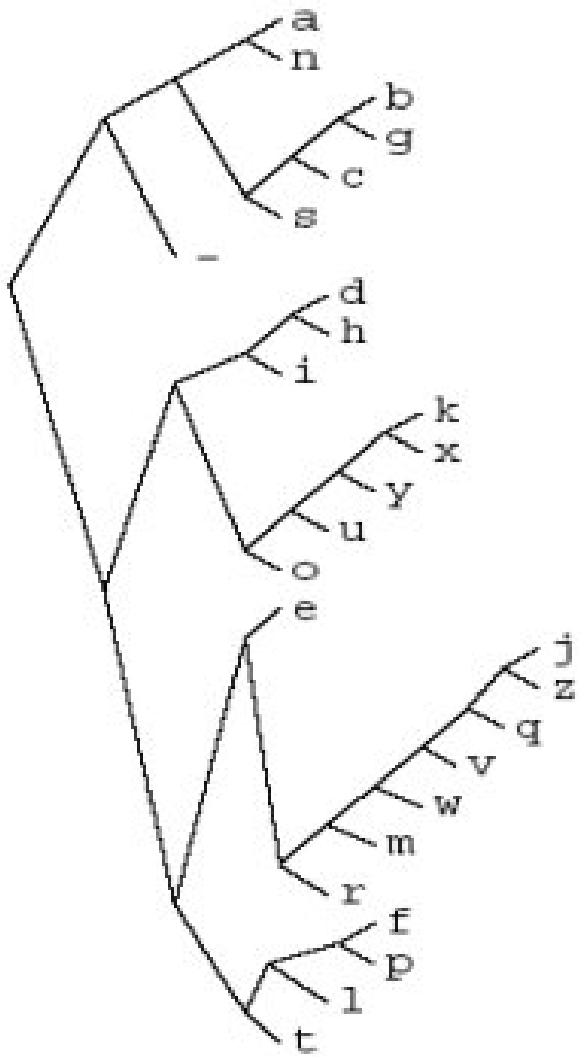
a_i	p_i	$h(p_i)$	l_i	$c(a_i)$
a	0.25	2.0	2	00
b	0.25	2.0	2	10
c	0.2	2.3	2	11
d	0.15	2.7	3	010
e	0.15	2.7	3	011



Μέσο μήκος 2.30 bits, εντροπία 2.28 bits

Κωδικοποίηση Huffman Αγγλικού Αλφαβήτου

a_i	p_i	$\log_2 \frac{1}{p_i}$	l_i	$c(a_i)$
a	0.0575	4.1	4	0000
b	0.0128	6.3	6	001000
c	0.0263	5.2	5	00101
d	0.0285	5.1	5	10000
e	0.0913	3.5	4	1100
f	0.0173	5.9	6	111000
g	0.0133	6.2	6	001001
h	0.0313	5.0	5	10001
i	0.0599	4.1	4	1001
j	0.0006	10.7	10	1101000000
k	0.0084	6.9	7	1010000
l	0.0335	4.9	5	11101
m	0.0235	5.4	6	110101
n	0.0596	4.1	4	0001
o	0.0689	3.9	4	1011
p	0.0192	5.7	6	111001
q	0.0008	10.3	9	110100001
r	0.0508	4.3	5	11011
s	0.0567	4.1	4	0011
t	0.0706	3.8	4	1111
u	0.0334	4.9	5	10101
v	0.0069	7.2	8	11010001
w	0.0119	6.4	7	1101001
x	0.0073	7.1	7	1010001
y	0.0164	5.9	6	101001
z	0.0007	10.4	10	1101000001
–	0.1928	2.4	2	01



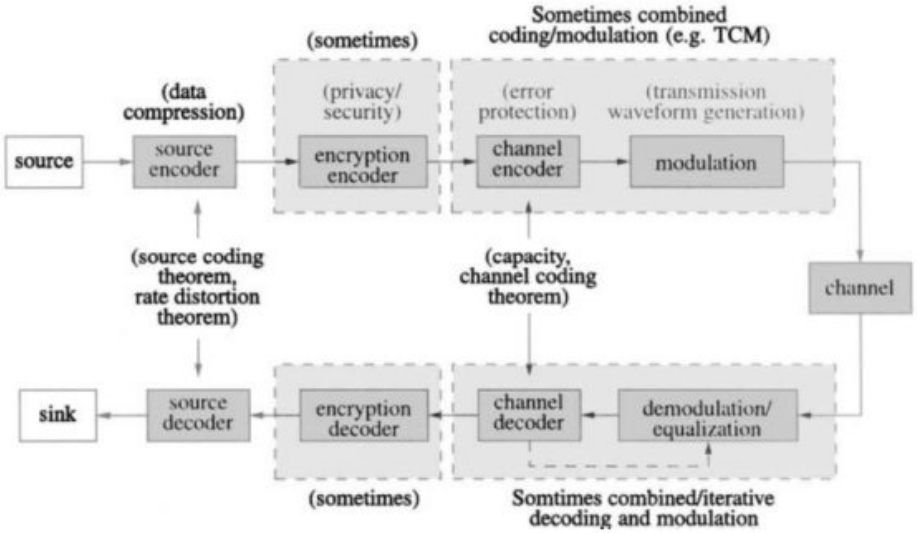
Κωδικοποίηση Huffman MATLAB

```
% Διάνυσμα γραμμάτων
s=[1 2 3 4 5];
% Διάνυσμα πιθανοτήτων γραμμάτων
p=[0.25, 0.25, 0.20, 0.15, 0.15];
% Δημιουργεί το κωδικό βιβλίο dict ως cell array με γραμμές όσες τα
γράμματα. Πχ Dict{4,:}=[0 0 1] Dict{5,:}=[0 0 0]
[dict, avglength]=huffmandict(s,p)
% Δημιουργία σήματος πηγής δεδομένων
sig = randsrc(100,1,[symbols; p]);
% Δημιουργία κωδικοποιημένης ακολουθίας
comp = huffmanenco(sig,dict);
% Αποκωδικοποίηση της ακολουθίας εισόδου comp με βάση το λεξικό dict
dsig = huffmandeco(comp,dict);
% Σύγκριση του αρχικού μηνύματος με το αποκωδικοποιημένο
isequal(sig,dsig)
ans = logical 1
```

Βασικό Μοντέλο Καναλιού

- Κανάλι: Ένα στοχαστικό σύστημα.
- Γενικά, πολλών εισόδων, πολλών εξόδων (MIMO).
- Στη γενική περίπτωση, κάθε έξοδος κάθε χρονική στιγμή i εξαρτάται στατιστικά από όλες τις εισόδους του συστήματος μέχρι και τη χρονική στιγμή i (θεωρώντας αιτιατό σύστημα).
- Στο μάθημα θα ασχοληθούμε με κανάλια μιας εισόδου και μίας εξόδου (SISO).
- Είδη Καναλιών:
  - Κανάλια διακριτών/συνεχών τιμών.
  - Κανάλια χωρίς μνήμη/με μνήμη.
  - Κανάλια συνεχούς χρόνου/διακριτού χρόνου.

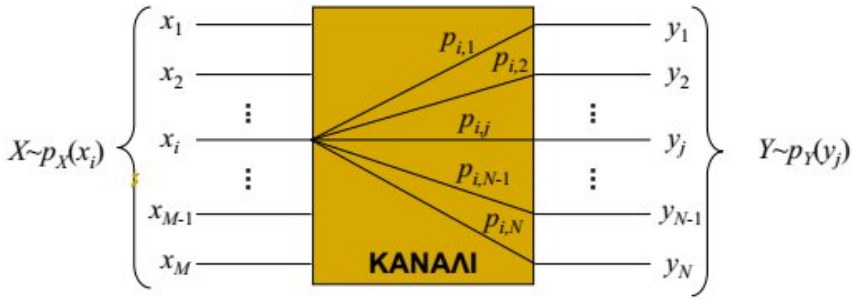
Θεώρημα κωδικοποίησης καναλιού



Ερώτημα: Πόση ποσότητα πληροφορίας μπορεί να μεταφερθεί μέσα από ένα διακριτό κανάλι χωρίς μνήμη κάθε φορά που χρησιμοποιούμε το κανάλι (κατά μέσο όρο);

2ο Θεμελιώδες θεώρημα του Shannon : Υπάρχει τρόπος να μεταδώσουμε με ρυθμό C και αυθαίρετα μικρή πιθανότητα σφάλματος αποκωδικοποίησης (ευθύ – achievability). Αντιστρόφως, είναι αδύνατο να μεταδώσουμε με ρυθμό μεγαλύτερο του C εάν επιθυμούμε αυθαίρετα μικρή πιθανότητα σφάλματος (αντίστροφο – converse).

Διακριτά κανάλια χωρίς μνήμη



Πίνακας Μετάβασης Καναλιού:

$$[P_{Y|X}] = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,N} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ p_{M,1} & p_{M,2} & \cdots & p_{M,N} \end{bmatrix},$$

όπου $[p_{i,j}] = [p(y_j|x_i)]$ και $P_Y = P_X P_{Y|X}$. Στην ουσία, το κανάλι χωρίς μνήμη είναι μια ομάδα δεσμευμένων κατανομών.
Ένα κανάλι δεν έχει μνήμη όταν η έξοδός του σε οποιαδήποτε χρονική στιγμή i εξαρτάται (στατιστικά) μόνο από την είσοδό του τη χρονική στιγμή i.

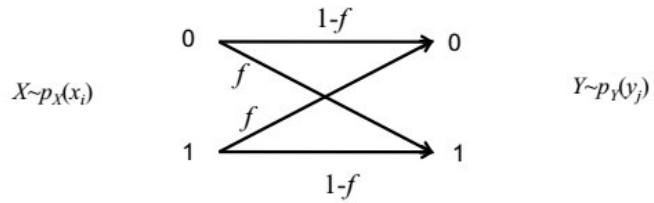
Μετάδοση πληροφορίας

- Η ποσότητα της πληροφορίας που μπορούμε να «περάσουμε» μέσα από ένα κανάλι χωρίς μνήμη κάθε φορά που το χρησιμοποιούμε (κατά μέσο όρο) ισούται με την αμοιβαία πληροφορία $I(X;Y)$, όπου X η είσοδος και Y η έξοδος του καναλιού.
- Θυμίζουμε ότι $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$.
- Διαισθητικά (και όχι αυστηρώς μαθηματικά) αυτό εξηγείται ως εξής: Αρχικά, η αβεβαιότητα που έχουμε στο δέκτη για τη μεταδοθείσα τ.μ. X είναι H(X). Μετά τη λήψη της Y, η αβεβαιότητά μας για τη X ισούται με $H(X|Y)$. Επομένως, η αβεβαιότητά μας μειώθηκε κατά $I(X;Y)$. Αυτή είναι η πληροφορία που καταφέραμε να «περάσουμε» από τον πομπό στο δέκτη.

Πληροφοριακή και Λειτουργική Χωρητικότητα

- Η *πληροφοριακή χωρητικότητα* (information capacity) ενός διακριτού καναλιού χωρίς μνήμη (DMC) με είσοδο X και έξοδο Y ισούται με $C = \max_{p_X(x)} I(X;Y)$.
- Έστω ότι κάθε φορά που χρησιμοποιούμε το κανάλι μεταδίδουμε ένα από M πιθανά μηνύματα. Ο ρυθμός μετάδοσης R ισούται με $\log M$
- Η *λειτουργική χωρητικότητα* (operational capacity) ενός καναλιού ισούται με το μέγιστο ρυθμό R για τον οποίο μπορούμε να επιτύχουμε πιθανότητα σφάλματος μετάδοσης οποιουδήποτε μηνύματος αυθαίρετα κοντά στο 0.
- **Θεώρημα (Shannon)**: Η λειτουργική χωρητικότητα ενός διακριτού καναλιού χωρίς μνήμη ισούται με την πληροφοριακή του χωρητικότητα.

Χωρητικότητα Δυαδικού Συμμετρικού Καναλιού (BSC)



$$[p_Y(0) \quad p_Y(1)] = [p_X(0) \quad p_X(1)] \begin{bmatrix} 1-f & f \\ f & 1-f \end{bmatrix} \Rightarrow$$

$$\begin{cases} p_Y(0) = & (1-f)p_X(0) + f p_X(1) \\ p_Y(1) = & f p_X(0) + (1-f)p_X(1) \end{cases}$$

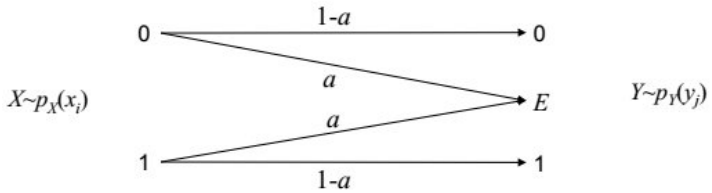
Χωρητικότητα:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) = H(Y) - \sum_{x=0,1} p(x) H(Y|X=x) \\ &= H(Y) - \sum_{x=0,1} p(x) H(f) \\ &= H(Y) - H(f) \end{aligned}$$

Άρα, $C_{BSC} = 1 - H(f)$ και είναι επιτεύξιμη με ομοιόμορφη κατανομή για τη X.

Χωρητικότητα Δυαδικού Καναλιού Διαγραφής (BEC)

Μοντελοποιεί καλά περιπτώσεις όπου χρησιμοποιούμε κώδικα ανίχνευσης σφαλμάτων στο δέκτη.



$$[p_Y(0) \quad p_Y(E) \quad p_Y(1)] = [p_X(0) \quad p_X(1)] \begin{bmatrix} 1-a & a & 0 \\ 0 & a & 1-a \end{bmatrix}$$

Χωρητικότητα:
$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \{H(Y) - H(Y|X)\} = \max_{p(x)} H(Y) - H(a)$.
Έτσι, μία πρωτη ιδέα είναι να πούμε ότι $\max_{p(x)} H(Y) = \log 3$. Ωστόσο, κάτι τέτοιο δεν επιτυγχάνεται για καμία κατανομή $p(x)$. Η λύση προκύπτει θέτοντας $p(X=1) = \pi$. Τότε προκύπτει ότι
$p(Y=0) = (1-\pi)(1-a)$, $p(Y=E) = a$ και $p(Y=1) = \pi(1-a)$.