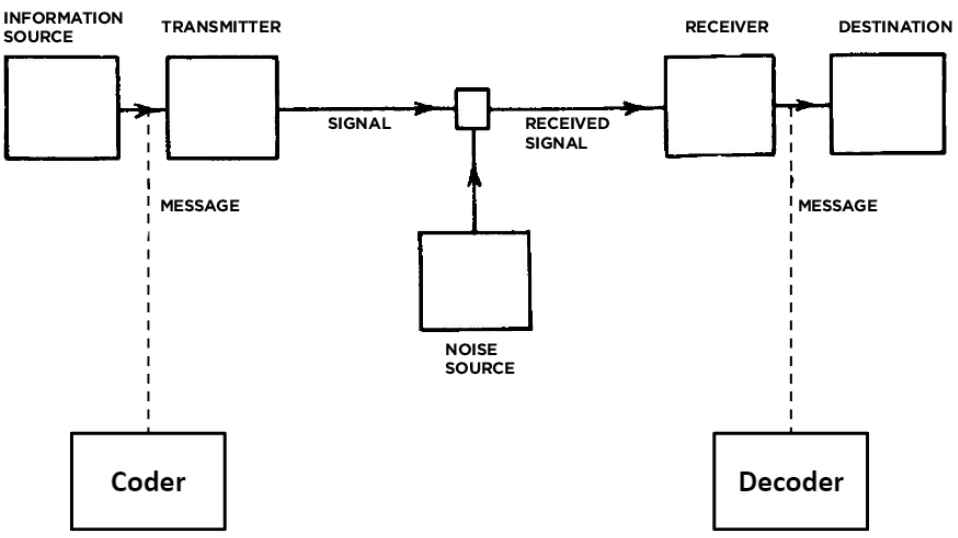
Τμήμα Ηλεκτρολόγων Μηχανικών
& Μηχανικών Υπολογιστών
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΛΟΠΟΝΝΗΣΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΑΛΓΟΡΙΘΜΩΝ ΚΩΔΙΚΟΠΟΙΗΣΗΣ ΚΑΝΑΛΙΟΥ ΜΕ ΚΩΔΙΚΕΣ BLOCK ΣΕ ΠΡΟΓΡΑΜΜΑΤΙΣΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

ΣΠΗΛΙΩΤΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ 2917
ΣΚΡΕΚΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ 2914

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΜΙΧΑΗΛ ΠΑΡΑΣΚΕΥΑΣ



Πίνακας περιεχομένων

Περίληψη

Εδώ και χρονια οι τηλεπικοινωνίες εχουν ένα πολύ σημαντικο ρολο στην καθημερινότητα των ανθρώπων. Όμως κατά την μετάδοση σε κανάλια επικοινωνιας η πληροφορία είναι ευάλωτη σε σφάλματα, με αποτέλεσμα να μεταφέρονται κατεστραμμένα δεδομένα. Η πρόκληση του εντοπισμού και της επιδιόρθωσης προβλημάτων μετάδοσης που προκαλούνται από το θόρυβο στα κανάλια επικοινωνίας αντιμετωπίζεται από τη θεωρία κωδικοποίησης. Αυτή η θεωρία εστιάζει σε συστήματα που μπορούν να αναγνωρίσουν και να διορθώσουν σφάλματα στις πληροφορίες που αποστέλλονται σε ένα κανάλι που είναι επιρρεπές σε θόρυβο και σφάλματα.

Στόχος αυτης της εργασίας είναι να μελετήσουμε και να υλοποιήσουμε την κωδικοποίηση ενός καναλιού επικοινωνίας με κώδικες Block και να δώσουμε παραδείγματα σε περιβάλλον Matlab. Ακόμη θα μελετήσουμε καποιες μαθηματικές θεωρίες οπου είναι αναγκαίες για την κατανόηση του αντικειμενου και θα αναφέρουμε ποσο μεγαλο ρολο εχει η τεχνολογια αυτή στην καθημερινότητα.

Abstract

For years, telecommunications have played a very important role in people's daily lives. However, when we transmit over communication channels, the information is vulnerable to errors, resulting in corrupted data being transferred. The challenge of detecting and correcting transmission problems caused by noise in communication channels is addressed by coding theory. This theory focuses on systems that can recognize and fix faults in information that is sent across a channel that is susceptible to noise and errors.

The aim of this work is to study and implement the coding of a communication channel with Block codes and to give examples in a Matlab environment. We will also study some mathematical theories where they are necessary for the understanding of the subject and we will mention how big of a role this technology has in everyday life.

Ευχαριστίες

Θέλουμε να ευχαριστήσουμε τον καθηγητή μας κ. Μιχάλη Παρασκευά οπου μας βοήθησε κατά την εκπόνηση αυτής της εργασίας και που μας στήριξε καθ’ όλη την διάρκεια της φοίτησης μας στο τμήμα. Τέλος θέλουμε να ευχαριστήσουμε τις οικογένειες μας .

Κεφάλαιο 1ο
ΘΕΩΡΙΑ ΠΛΗΡΟΦΟΡΙΑΣ

1.1 Θεωρία πιθανοτήτων
1.1.1 Εισαγωγη

Η θεωρία της πληροφορίας είναι ένας κλάδος των εφαρμοσμένων μαθηματικών που ασχολείται με την ποσοτικοποίηση δεδομένων. Η εντροπία πληροφοριών, η οποία συνήθως αναπαρίσταται ως ο μέσος αριθμός bits που απαιτούνται για την αποθήκευση ή τη μεταφορά ενός συμβόλου σε ένα μήνυμα, είναι η πιο βασική μέτρηση της πληροφορίας. Η αβεβαιότητα που εμπλέκεται στην πρόβλεψη της τιμής μιας τυχαίας μεταβλητής ποσοτικοποιείται με την εντροπία πληροφοριών. Η γνώση του αποτελέσματος μιας δίκαιης "ρίψης νομίσματος" (- Κορώνα ή γράμματα - δύο ισοδύναμα πιθανά αποτελέσματα) για παράδειγμα προσφέρει λιγότερες πληροφορίες (χαμηλή εντροπία) από τον προσδιορισμό του αποτελέσματος μιας ρίψης ζαριών (6 ισοδύναμα πιθανά αποτελέσματα). Τα μαθηματικά, η στατιστική, η επιστήμη των υπολογιστών, η φυσική, η νευρολογία και η ηλεκτρική μηχανική διασταυρώνονται σε αυτόν τον κλάδο. Ο πηγαίος κώδικας, η χωρητικότητα καναλιού, η αλγοριθμική θεωρία πολυπλοκότητας, η αλγοριθμική θεωρία πληροφοριών, τα δεδομένα θεωρίας ασφάλειας και οι μετρήσεις πληροφοριών είναι όλα σημαντικά «υποπεδία» της θεωρίας πληροφοριών.

1.1.2 Τι είναι η θεωρία πιθανοτήτων

Είναι μια μαθηματική θεωρία μέτρησης που ασχολείται με τη μελέτη τυχαίων φαινομένων. Η θεωρία πιθανοτήτων περιστρέφεται γύρω από την έννοια όπως πιθανότητας, καθώς και τυχαίες μεταβλητές, συναρτήσεις κατανομής, στοχαστικές διαδικασίες και γεγονότα, όπως μαθηματικές αφαιρέσεις μη ντετερμινιστικών περιστατικών που συμβαίνουν μία φορά ή εξελίσσονται με την πάροδο του χρόνου. Η πιθανότητα είναι ένας θετικός αριθμός μικρότερος ή ίσος με έναν που αντιπροσωπεύει την αβεβαιότητα του ανθρώπου σχετικά με την εξέλιξη των φαινομένων. Η θεωρία πιθανοτήτων, ως μαθηματική βάση των στατιστικών, απαιτείται σε όπως εργασίες που περιλαμβάνουν την ανάλυση τεράστιων συνόλων δεδομένων. Οι μέθοδοι όπως θεωρίας πιθανοτήτων χρησιμοποιούνται όπως για την περιγραφή περίπλοκων συστημάτων, όπως η στατιστική μηχανική. Σύμφωνα με μελέτες κβαντομηχανικής, η πιθανολογική φύση των φυσικών νόμων σε υποατομικό επίπεδο ήταν μια σημαντική ανακάλυψη του εικοστού αιώνα για την μελέτη και ανάλυση τυχαίων φαινομένων.

1.1.3 Πείραμα τύχης

Ένα πείραμα τύχης είναι μια διαδικασία κατά την οποία, ακόμη και αν εκτελεστεί με τον ίδιο τρόπο υπό ίδιες συνθήκες, το αποτέλεσμα δεν μπορεί να προβλεφθεί με βεβαιότητα. Ωστόσο, μπορούμε να παρακολουθούμε όλα τα πιθανά αποτελέσματα του πειράματος.

1.1.4 Δειγματικός χώρος Ω

Δειγματικός χώρος Ω ενός πειράματος τύχης λέμε το σύνολο των δυνατών αποτελεσμάτων τα οποία μπορούν να εμφανιστούν σε μία εκτέλεσή του.

- Κάθε δυνατό αποτέλεσμα της εκτέλεσης του πειράματος λέγεται απλό γεγονός, γνωστό κι ως δειγματικό σημείο ω: $\omega \in \Omega$.
- Κάθε υποσύνολο του δειγματικού χώρου ονομάζεται γεγονός. Δηλαδή, ένα σύνολο από τα απλά γεγονότα του πειράματος δημιουργεί ένα γεγονός.
- Στα ενδεχόμενα συμπεριλαμβάνεται ολόκληρος ο δειγματικός χώρος Ω (βέβαιο ενδεχόμενο) και το κενό σύνολο Ø (αδύνατο ενδεχόμενο).
- Τα στοιχεία του δειγματοχώρου είναι αμοιβαία αποκλειόμενα και συλλεκτικά εξαντλημένα.

Ο αριθμός των δειγματικών σημείων μπορεί να είναι:

1) Διακριτός (πεπερασμένος ή άπειρος αριθμήσιμος)

2) Συνεχής (άπειρος μη αριθμήσιμος)

Παράδειγμα:

Ρίχνουμε δύο νομίσματα και θέλουμε να βρούμε το δειγματοχώρο. Συμβολίζουμε με Κ την περίπτωση να εμφανιστεί κορώνα και με Γ στην περίπτωση να εμφανιστεί γράμματα. Ρίχνοντας δύο νομίσματα θα έχουμε τέσσσερις περιπτώσεις ανάλογα με το τι εμφανίστηκε σε καθένα από αυτά. Γράφοντας πρώτα την ένδειξη που φέρνει το ένα και μετά την ένδειξη που φέρνει το άλλο, οι τέσσερις περιπτώσεις συμβολίζονται ΚΚ,ΚΓ,ΓΚ,ΓΓ. Άρα, ο δειγματοχώρος είναι: Ω = { ΚΚ,ΚΓ,ΓΚ,ΓΓ }.

Έτσι έχουμε και τον αριθμήσιμα άπειρο δειγματοχώρο , δηλαδή ένα δείγμα με άπειρο πλήθος στοιχείων, για τον οποίο υπάρχει ένα προς ένα αντιστοιχία των στοιχείων του με τους φυσικούς αριθμούς 1, 2, 3.

Αλλά αντίστοιχα και τον Μη-αριθμήσιμα άπειρο ή συνεχή δειγματοχώρο , ο οποίος είναι ένας δειγματοχώρος με άπειρο πλήθος στοιχείων, για τον οποίο υπάρχει μια ένα προς ένα αντιστοιχία των στοιχείων του στα σημεία ενός διαστήματος των πραγματικών αριθμών (a, b).

1.1.5 Σημαντικά θεωρήματα πιθανότητας

- P(Ø) = 0 : Η πιθανότητα του αδύνατου γεγονότος είναι μηδέν
- P(Ω) = 1 : Η πιθανότητα του βέβαιου γεγονότος είναι ένα
- 0 ≤ P(α) ≤ 1 : Κάθε πιθανότητα είναι μεταξύ 0 και 1
- Αν α1 ⊂ α2 τότε:
  - P(α1) ≤ P(α2)
  - P(α2 − α1) = P(α2) − P(α1)
- P α) = 1 − P(α) α΄συμπληρωματικό ενδεχόμενο του α
- P(α ∪ β) = P(α) + P(β) − P(α ∩ β) Θεώρημα ολικών πιθανοτήτων
- P Un=1N αn ≤ σn=1 N P(α)

1.1.6 Δεσμευμένη / Υπό Συνθήκη Πιθανότητα

Ας υποθέσουμε ότι ένας χώρος δείγματος έχει δύο πιθανότητες Α και Β και P (B)> 0. Δεδομένου ότι το σενάριο Β έχει ή θα συμβεί, η πιθανότητα να συμβεί το ενδεχόμενο Α ορίζεται ως: P (α/β)= P(α ∩ β) / P(β)

Παράδειγμα:

Έστω ένα πείραμα τύχης με το ρίξιμο ζαριού και με τα ενδεχόμενα:
α = {1,2,3} και β = {1,2}.

Η πιθανότητα πραγματοποίησης του α είναι: P(α) = ½

Η πιθανότητα πραγματοποίησης του α, δοθέντος ότι έχει πραγματοποιηθεί το β, είναι:

P (α/β) =P(α ∩ β) P(β) = P({1,2}) / P ({1,2}) = 1

1.1.7 Στατιστική Ανεξαρτησία Γεγονότων

Δυο γεγονότα α και β ονομάζονται στατιστικά ανεξάρτητα αν ισχύει P(α ∩ β) = P(α) P(β).

Δηλαδή η πραγματοποίηση του γεγονότος β δεν μας δίνει καμία επιπλέον πληροφορία για την πραγματοποίηση ή μη του γεγονότος α.

Επομένως ισχύει : P(α/β) = P(α) και P(β/α) = P(β)

Παράδειγμα:

Έστω ένα πείραμα τύχης στο οποίο ρίχνουμε δύο ζάρια. Ας ορίσουμε τα ενδεχόμενα α = «το πρώτο ζάρι φέρνει 1» και β = «το δεύτερο ζάρι φέρνει 1». Αν (x,y) είναι το αποτέλεσμα του πειράματος για τα αποτελέσματα κάθε ζαριού, τότε:

α = {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6)}

β = {(1,1),(2,1),(3,1),(4,1),(5,1),(6,1)}

(α) = 1/6 και $P(\beta)$ = 1/6, επομένως :

P α β = P(α ∩ β) $P(\beta)$ = P({1,1})/ 1/6 =(1/36) / (1/6) = 1/6

1.1.8 Κανόνας Bayes

Το θεώρημα του Bayes είναι μια έννοια στη θεωρία πιθανοτήτων και τη στατιστική. Ο νόμος του Bayes είναι η σχέση μεταξύ της τρέχουσας πιθανότητας και της αρχικής πιθανότητας. Οι πιθανότητες που χρησιμοποιούνται στο θεώρημα του Bayes μπορεί να έχουν πολλαπλές ερμηνείες ανάλογα με τον τρόπο εφαρμογής τους. Το θεώρημα χρησιμοποιείται απευθείας ως μέρος μιας συγκεκριμένης μεθόδου για τη στατιστική εξαγωγή συμπερασμάτων σε μία από αυτές τις ερμηνείες. Το θεώρημα περιγράφει πώς μια υποκειμενική άποψη πρέπει να μεταβάλλεται αναλογικά καθώς πλησιάζει η απόδειξη. Το συμπέρασμα του Bayes καθορίζει τη στατιστική σημασία κατα Bayes. Το θεώρημα Bayes, από την άλλη πλευρά, μπορεί να χρησιμοποιηθεί σε ένα ευρύ φάσμα υπολογισμών πιθανοτήτων, όχι απλώς σε συμπέρασμα Bayes.

1.1.9 Μαθηματικός ορισμός Bayes

Το θεώρημα Bayes ορίστηκε μαθηματικά ως η ακόλουθη εξίσωση:

$$P(A/B) = P(B/A)PA/P(B)$$

όπου Α και Β είναι γεγονότα:

- P(A) και P(B) είναι οι πιθανότητες των Α και Β που είναι ανεξάρτητα μεταξύ τους.
- P(A|B), η υπό συνθήκη πιθανότητα, είναι η πιθανότητα του Α δεδομένου του Β να είναι αληθής.
- P(B|A), είναι η πιθανότητα του Β δεδομένου του Α να είναι αληθής.

Η δεσμευμένη πιθανότητα πραγματοποίησης του γεγονότος β, με δεδομένη την πραγματοποίηση του γεγονότος α, δίνεται από τη σχέση:

($\beta|\alpha$) = P (β ∩ α)/ P α = (P α ∩ β)/ P α = P (α/ β) P β /P α =P (β)/ P (α) ($\alpha|\beta$)

Επομένως:

$P(\beta|\alpha) = P(\beta)/ P(\alpha) P(\alpha|\beta)$

Στο τέλος σημειώνεται ότι ο κανόνας του Bayes είναι σημαντικός σε προβλήματα εκτίμησης σημάτων.

1.2 Τυχαίες μεταβλητές και στοχαστικά σήματα

1.2.1 Ορισμός τυχαίων μεταβλητών

Μια τυχαία μεταβλητή είναι μια μεταβλητή της οποίας η τιμή υπόκειται σε τυχαίες διακυμάνσεις στη θεωρία πιθανοτήτων. Κάθε μία από τις δυνητικές τιμές για μια τυχαία μεταβλητή συσχετίζεται με μια πιθανότητα ή μια πυκνότητα πιθανότητας. Οι διάφορες τιμές μιας τυχαίας μεταβλητής μπορεί να αντιπροσωπεύουν τα διαφορετικά αποτελέσματα ενός πειράματος που διεξάγεται ή θα διεξαχθεί, αλλά το αποτέλεσμα είναι άγνωστο (για παράδειγμα λόγω έλλειψης πληροφοριών ή ανακριβούς μέτρησης). Μια τυχαία μεταβλητή είναι μια πραγματική συνάρτηση που ορίζεται σε ένα χώρο δείγματος, όπως η συνάρτηση:

X : Ω -> R ή X : Ω -> A (A σύνολο πραγματικών αριθμών).

1.2.2 Διακριτή & συνεχής μεταβλητή

Μια τυχαία μεταβλητή μπορεί να είναι διακριτή, με την έννοια ότι έχει ένα πεπερασμένο ή μετρήσιμο σύνολο πιθανών τιμών, ή συνεχής, με την έννοια ότι μπορεί να πάρει οποιαδήποτε τιμή σε ένα εύρος ακεραίων. Η συνάρτηση μάζας πιθανότητας υπολογίζει την πιθανότητα κάθε πιθανής τιμής για διακριτές τυχαίες μεταβλητές.

Η συνάρτηση πυκνότητας πιθανότητας ή η συνάρτηση αθροιστικής κατανομής μπορεί να χρησιμοποιηθεί για τον υπολογισμό της πιθανότητας μια τιμή να βρίσκεται σε κάποιο χώρο για συνεχείς μεταβλητές όπου δεν έχει νόημα να μιλάμε για την πιθανότητα μιας μεμονωμένης τιμής. Μια τυχαία μεταβλητή μπορεί να αποτελείται από διακριτές και συνεχείς μεταβλητές. Βασικές διακριτές κατανομές

1.2.3 Κατανομή Bernoulli και Διωνυμική κατανομή.

Η δοκιμή Bernoulli πρόκειται για ένα πείραμα τύχης με μόνο δύο, αμοιβαίως αποκλειόμενα, δυνατά αποτελέσματα. Το ένα αποτέλεσμα έχει επικρατήσει να ονομάζεται επιτυχία (success) και το άλλο αποτυχία (failure). Ένα παράδειγμα είναι η ρίψη ενός νομίσματος μία φορά. Τα δυνατά αποτελέσματα είναι προφανώς μόνο δύο, κεφαλή και γράμματα, ένα ακόμη θα μπορούσε να είναι η επιλογή ενός ζώου και η εξέτασή του για να διαπιστωθεί αν έχει προσβληθεί από μια συγκεκριμένη ασθένεια, τα δυνατά αποτελέσματα είναι μόνο δύο, το ζώο είτε έχει προσβληθεί (επιτυχία) είτε δεν έχει προσβληθεί (αποτυχία).

Ας δώσουμε τώρα τον ορισμό της διωνυμικής κατανομής.

Ορισμός: Αν **X** ο αριθμός των επιτυχιών σε μια ακολουθία **v** ανεξάρτητων δοκιμών Bernoulli με σταθερή πιθανότητα επιτυχίας **p**, σε όλες τις δοκιμές, τότε η κατανομή

της τυχαίας μεταβλητής **X** ονομάζεται διωνυμική κατανομή, με παραμέτρους **v** και **p** και συμβολίζεται με

B(v , p) . Επίσης, γράφουμε X ~ B(v , p).

1.2.4 Πολυωνυμική κατανομή

Αποτελεί μια ευθεία και εύλογη γενίκευση της δοκιμής Bernoulli

Είναι ένα πείραμα με **k ≥ 2** αμοιβαίως αποκλειόμενα δυνατά αποτελέσματα. Αντίστοιχα, η πολυωνυμική κατανομή αποτελεί γενίκευση της διωνυμικής κατανομής.

Ορισμός: Έστω ένα πείραμα τύχης που αποτελείται από ν ανεξάρτητες πολυωνυμικές δοκιμές, όπου σε κάθε δοκιμή τα δυνατά αποτελέσματα είναι k έστω έστω r1,r2,…,rk, και η πιθανότητα να εμφανισθεί το r :

Αν Xi (i = 1,2,… k) τυχαία μεταβλητή που εκφράζει πόσες φορές εμφανίσθηκε το αποτέλεσμα ri στις ν ανεξάρτητες επαναλήψεις της πολυωνυμικής δοκιμής, τότε η τυχαία μεταβλητή (X1, X2,…Xk) λέμε ότι ακολουθεί την πολυωνυμική κατανομή.

1.2.5 Κατανομή Poisson

Είναι μία διακριτή συνάρτηση κατανομής που εκφράζει την πιθανότητα ενός δεδομένου αριθμού γεγονότων που συμβαίνουν σε ένα σταθερό διάστημα χρόνου ή χώρου αν αυτά τα γεγονότα συμβαίνουν με ένα γνωστό μέσο ρυθμό και είναι ανεξάρτητα από το χρονικό διάστημα. Η κατανομή Poisson μπορεί επίσης να χρησιμοποιηθεί για τον αριθμό γεγονότων σε άλλα καθορισμένα διαστήματα όπως η απόσταση, η επιφάνεια ή ο όγκος, ο τύπος της κατανομής Poisson είναι ο εξής :

F(x) = P(X = x) = e-λ λχ/χ!, όπου χ = 0,1,2… όπου λ > 0 .

1.2.6 Αθροιστική συνάρτηση κατανομής

Έστω ένας χώρος πιθανότητας {Ω,F,P}, και μια πραγματική τυχαία μεταβλητή

X :Ω R πάνω σε αυτόν, τότε η συνάρτηση Fx : R [0,1]

Με Fx(x) = P(X<=x)=P ({ω ε Ω / X(ω)<=X}), Ονομάζεται συνάρτηση κατανομής, ή αθροιστική συνάρτηση κατανομής της τυχαίας μεταβλητής. Αν το X παίρνει πεπερασμένο πλήθος τιμών X1,X2,X3,…Xn τότε η συνάρτηση κανατομής είναι:

$$F(x) \begin{cases} 0 , & -\infty < X < X1 \\ F(x1) , & X1 <= X <= X2 \\ F(x1) + F(x2) , & X2 <= X <= X3 \\ F(x1) + \ldots + F(xn) , & Xn <= X < \infty \end{cases}$$

Μέσω της συνάρτησης κατανομής $F(x)$ μπορούμε να υπολογίσουμε την πιθανότητα η διακριτή τυχαία μεταβλητή να λαμβάνει τιμή εντός ενός διαστήματος $(a,b]$, όπου $b > a$.

Επομένως είναι:

$F\ (b) - F\ (a) =$

$= P\ (X \leq b) - P\ (X \leq a)$

$= \{P\ (X \leq a) + P(\ a < X \leq b) - P\ (x < a)$

$= P(a < X \leq b)$

Έτσι προκύπτει η τελική πιθανότητα η οποία είναι:

$P\ (a < X \leq b) = F\ (b) - F\ (a)$

1.2.7 Συνάρτηση Πυκνότητας πιθανότητας

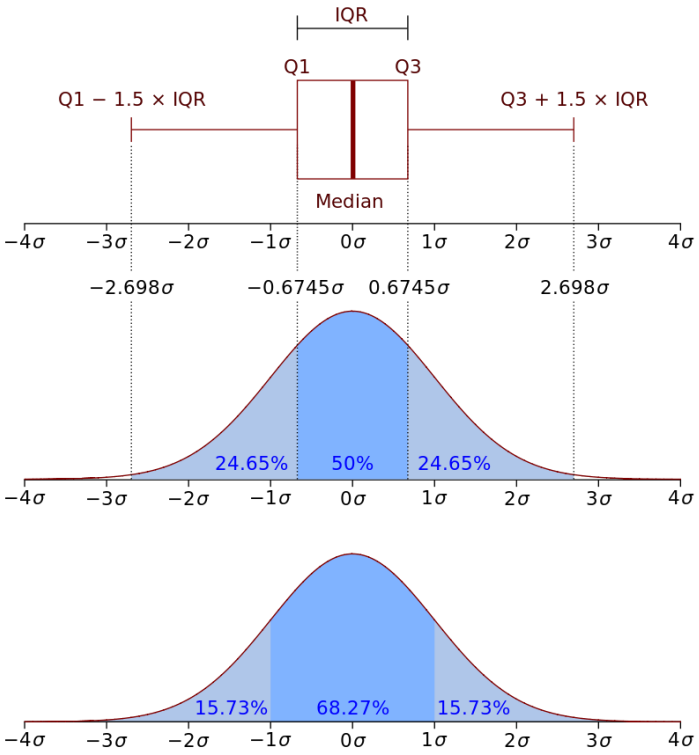
Η παράγωγος της συνάρτησης κατανομής $F(x)$ συμβολίζεται με $f(x)$ και ονομάζεται συνάρτηση πυκνότητας πιθανότητας (Probability Density Function, PDF) της τυχαίας μεταβλητής X.

$F\ (x) = \int_{-\infty}^{\infty} f(\ x)\ dx$

Η πιθανότητα μια συνεχής τυχαία μεταβλητή X να λάβει τιμή εντός ενός διαστήματος $(a,b]$ μπορεί να εκφραστεί μέσω της συνάρτησης πυκνότητας πιθανότητας από τη σχέση:

$P(\ a < X \leq b) = \int_{a}^{b} f\ (x)\ dx$

Παραδειγμα:
Ας υποθέσουμε οτι ενα είδος βακτηρίων ζεί για περίπου 4 με 6 ώρες. Η πιθανότητα ενα βακτήριο να ζήσει 5 ωρες, είναι 0. Πολλά βακτήρια ζουν για περίπου 5 ώρες αλλα δεν υπάρχει πιθανότητα να πεθάνει στις 5.0 ώρες ακριβώς. Ωστόσο, η πιθανότητα να πεθάνει ανάμεσα σε 5.0 και 5.01 ώρες είναι υπολογίσιμη . Εαν υποθέσουμε οτι η πιθανότητα αυτή ειναι 0.02 (2%) , τοτε η πιθανότητα για να πεθάνει ανάμεσα σε 5.0 και 5.001 ώρες είναι 0.002 εφόσον η διαφορά χρόνου ειναι 1/10 απο πριν. Η πιθανότητα να πεθάνει αναμεσά σε 5.0 και 5.0001 ειναι 0,0002, κτλ. Σε αυτα τα 3 παραδείγματα , η αναλογία (πιθανότητα να πεθάνει σε ενα διάστημα χρόνου)/ (διάρκεια χρόνου) ειναι περίπου σταθερή και είναι ίση με 2/1 δηλαδή 2 ανα ωρα (0.02 πιθανότητα/0.01 ωρες)= 2/1 hour. Αυτη η πιθανότητα λεγεται πιθανότητα πυκνότητας για να πεθάνει το βακτήριο σε χρόνο περίπου ισο με 5 ωρες. Αρα το να πεθάνει σε χρονο 5 ωρων μπορεί να γραφτει (2 hour−1) dt . Αυτη ειναι η πιθανοτητα οπου το βακτήριο πεθάνει σε ενα άπειρο ελάχιστο "παράθυρο" χρόνου των περίπου 5 ωρών οπου dt ειναι η διάρκεια αυτου του παραθύρου . Για παράδειγμα η πιθανότητα να ζησει παραπάνω απο 5 ωρες αλλα λιγότερο απο (5 ωρες + 1 ns) ειναι (2 hour−1) x (1ns) ≈ 6×10−13 (με μετατροπή μοναδων). Ετσι η probability density function ή Συνάρτηση Πυκνότητας πιθανότητας ή PDF f(5hours) = 2 hour-1 . Το ακέραιο του f σε οποιοδήποτε "παράθυρο" χρόνου ειναι η πιθανότητα να πεθάνει σε αυτό το βακτήριο (οχι μόνο σε απειρο ελάχιστο "παράθυρο" αλλα και σε μεγαλύτερο)



Εικονα 1: Probability Density Function (PDF)

1.3 Εντροπια

Η εντροπία στη θεωρία πληροφορίας είναι ένα μέτρο αβεβαιότητας που διακατέχει ένα σύστημα. Παρατηρείτε ότι η εντροπία λαμβάνει υπόψη της τις διαφορετικές πιθανότητες εμφάνισης κάθε ενδεχόμενου yi, δηλαδή κάθε συμβόλου που απαρτίζει ένα μήνυμα . Ο όρος εντροπία χρησιμοποιήθηκε αρχικά στη θερμοδυναμική. Η εντροπία της θερμοδυναμικής μπορεί να αντιστοιχιστεί με την εντροπία στη θεωρία πληροφορίας. Η εντροπία ορίζεται ως :

$$H(X) = \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i}\right) = -\sum_{i=1}^{n} p_i \log_2 p_i,$$

1.3.1 Ιδιότητες της Εντροπίας

- Η μέση ποσότητα πληροφορίας είναι συνεχής στο p.
- Η μέση πληροφορία H(Y) είναι συμμετρική, δηλαδή διάταξη των πιθανοτήτων δεν την επηρεάζει.
- Η εντροπία H(Y) παίρνει την μέγιστη τιμή όταν όλα τα ενδεχόμενα είναι ισοπίθανα.
- Η εντροπία είναι προσθετική. Η ιδιότητα αυτή αναφέρεται στην περίπτωση κατά την οποία δύο ανεξάρτητες τυχαίες μεταβλητές X και Y συνδυάζονται.

1.3.2 Δοκιμή Bernoulli

Έστω μία δοκιμή Bernoulli με πιθανότητα επιτυχίας p. Συγκεκριμένα μπορούμε να θεωρήσουμε ένα δοχείο με N μπάλες, Np από τις οποίες είναι άσπρες και N(1-p) μαύρες από το οποίο επιλέγουμε τυχαία μία μπάλα. Αν όλες οι μπάλες είναι λευκές ή όλες είναι μαύρες (p = 1 ή p = 0 αντίστοιχα), τότε ξέρουμε με βεβαιότητα το αποτέλεσμα του πειράματος και η εντροπία είναι 0.Τότε η μέγιστη αβεβαιότητα για τα αποτελέσματα προκύπτει όταν οι μισές μπάλες είναι λευκές και οι μισές μαύρες, p = 0,5.

1.3.3 Ισοπίθανα γεγονότα

Έστω η τυχαία μεταβλητή X μπορεί να πάρει n τιμές που είναι ισοπίθανες μεταξύ τους, p=1/n.

Η εντροπία τότε είναι: $$H(X) = -\sum_{i=1}^{n} \frac{1}{n} \log_2 \frac{1}{n} = \log_2 n$$

Παρατηρούμε ότι η εντροπία αυξάνει με τον αριθμό των καταστάσεων.

1.3.4 Μέτρο πληροφορίας κατά Shannon.

Μέση Ποσότητα Πληροφορίας ή Μέσο Πληροφοριακό Περιεχόμενο ή Εντροπία. Αν Y είναι μια διακριτή τυχαία μεταβλητή με δειγματοχώρο Y={y1,y2,…yn}, και συνάρτηση πιθανότητα μάζας $p\ yi$, τότε η μέση ποσότητα πληροφορίας $H(Y)$ ισούται με:

$$H(Y) = -\sum_{i=1}^{n} p(y_i)\ log\ p(y_i)$$

Παρατηρούμε ότι η εντροπία υπολογίζει τις διαφορετικές πιθανότητες εμφάνισης για κάθε yi , δηλαδή κάθε συμβόλου οπου περιέχει ένα μήνυμα.

1.3.5 Κοινή & υπο συνθήκη Εντροπία

Η εντροπία του ζεύγους (X, Y) είναι η κοινή εντροπία δύο χωριστών μεταβλητών X και Y. Εάν τα X και Y είναι ανεξάρτητα, τότε η κοινή εντροπία ισούται με το άθροισμα των ατομικών εντροπιών. Εάν το (X, Y) αντιπροσωπεύει τη θέση ενός πιονιού σκακιού, με το X να αντιπροσωπεύει τη γραμμή και το Y να αντιπροσωπεύει τη στήλη, τότε η

εντροπία της γραμμής και η στήλη του πιόνι θα ισούται με την εντροπία της θέσης του.

Με δεδομένη μια τυχαία μεταβλητή Y, η υπό όρους εντροπία ή η υπό όρους αβεβαιότητα του X είναι η μέση υπό όρους εντροπία έναντι του Y.

1.4 Συνδυασμένη, αμοιβαία και υπό συνθήκη ποσότητα πληροφορίας

1.4.1 Συνδιασμένη ποσότητα πληροφορίας

Αρκετές φορές, μάς ενδιαφέρει να εξετάσουμε την ποσότητα πληροφορίας ενός συνδυασμού δύο τυχαίων μμεταβλητών, δηλαδή ενός πειράματος που αποτελείται από δύο υποπειράματα. Αν (X,Y) είναι ένα τυχαίο πείραμα με δισδιάστατο δειγματοχώρο και κατανομή πιθανοτήτων όπως ανωτέρω, τότε η συνδυασμένη πληροφορία H(X,Y) ορίζεται ως η μέση τιμή. Ένα τυχαίο πείραμα (X,Y) , έχει ως δυνατά αποτελέσματα όλους τους δυνατούς συνδυασμούς των αποτελεσμάτων X= {χ1,χ2,…,χn} και Y = {Y1,Y2,…,Yn}

Η κατανομή πιθανοτήτων δίνεται από την παρακάτω σχέση

P = {$p(x1,y1)$,$p(x1,y2)$,…,$p(x1,ym)$,…$p(xn,y1)$,p $(xn,y2)$,…p(xn,ym }

1.4.2 Αμοιβαία ποσότητα πληροφορίας

Είναι ορισμός ενός μέτρου αμοιβαίας πληροφορίας δύο τυχαίων μεταβλητών X, Y.

Η αμοιβαία πληροφορία είναι ένα μέτρο της ποσότητας πληροφορίας που μια τυχαία μεταβλητή περιέχει για μια άλλη τυχαία μεταβλητή ή ένα μέτρο της εξάρτησης μεταξύ δύο τυχαίων μεταβλητών.

Από τον ορισμό της αμοιβαίας πληροφορίας έχουμε:

I(X ;Y)= H(X) + H(Y)- H(X,Y)= H(X)-H(X/Y)=H(Y) - H(X/Y)

Παρατηρούμε πως η αμοιβαία ποσότητα πληροφορίας δύο ανεξάρτητων τυχαίων μεταβλητών είναι I(X ;Y)= 0, Τότε I(X ;Y)= H(X)=H(Y).

1.4.3 Υπό συνθήκη ποσότητα πληροφορίας

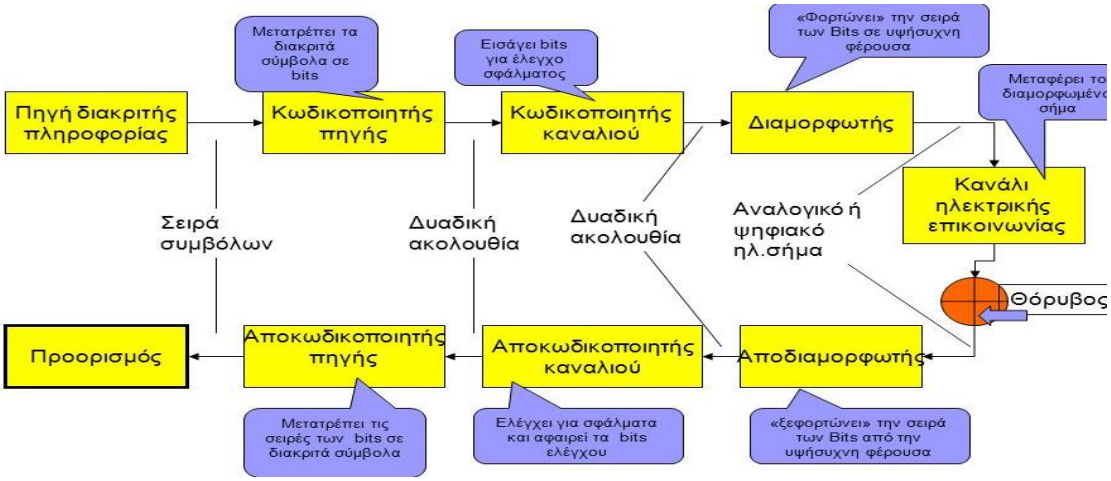
Επίσης, μας ενδιαφέρει, αρκετές φορές, να υπολογίσουμε την ποσότητα πληροφορίας μιας τυχαίας μεταβλητής X, όταν δίνεται το αποτέλεσμα μιας άλλης τυχαίας μεταβλητής Y. Αυτή καλείται υπό συνθήκη ποσότητα πληροφορίας της X ως προς την Y. Η υπό συνθήκη ποσότητα πληροφορίας του αποτελέσματος xi αν είναι γνωστό ότι έχει λάβει χώρα το αποτέλεσμα yj δίνεται από: H (xi /yj) = - log p(xi /yj).

Κεφάλαιο 2ο
ΚΑΝΑΛΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

2.1 Διακριτά κανάλια επικοινωνίας

2.1.1 Κανάλια επικοινωνίας

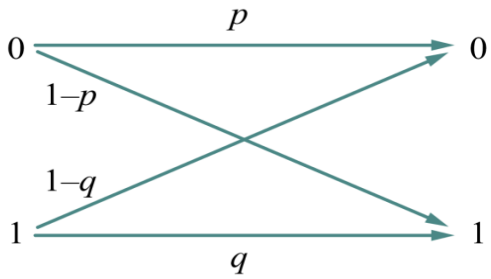
Τα δεδομένα δημιουργούνται από την πηγή σε μορφή που δεν είναι συμβατή με την απευθείας μετάδοση μέσω του καναλιού. Ως αποτέλεσμα, τα δεδομένα υποβάλλονται σε ειδική επεξεργασία γνωστή ως "κωδικοποίηση καναλιού", καθώς και μετατροπή σε σήμα προσαρμοσμένο στις φυσικές ιδιότητες του καναλιού. Ωστόσο, η παραμόρφωση του σήματος μπορεί να προκληθεί από θόρυβο μετάδοσης. Από την άλλη πλευρά, τα δεδομένα που δημιουργούνται από την πηγή υποβάλλονται σε επεξεργασία για να αφαιρεθεί το ασήμαντο κομμάτι της μείωσης των δεδομένων και να συμπυκνωθεί ο πηγαίος κώδικας. Το παρακάτω γράφημα απεικονίζει μια λεπτομερή απεικόνιση του διακριτού καναλιού επικοινωνίας.



Εικόνα 2: Πίνακας καναλιού επικοινωνίας i

Ένα σύμβολο (ή μια ακολουθία συμβόλων) είναι ένα αντικείμενο κωδικοποίησης όταν παράγεται από μια πηγή, η οποία οδηγεί στην αναπαράστασή του με μια κωδική λέξη. Η είσοδος του καναλιού επικοινωνίας είναι η κωδική λέξη, η οποία είναι μια σειρά από κωδικούς συμβόλων. Ως αποτέλεσμα, η έξοδος του καναλιού είναι επίσης μια σειρά από κωδικούς συμβόλων. Ωστόσο, λόγω ελαττωμάτων καναλιού, κυρίως θορύβου, η ακολουθία κωδικών συμβόλων εξόδου μπορεί να διαφέρει από την ακολουθία εισόδου.

Το διακριτό κανάλι περιγράφεται πλήρως με ένα σύνολο πιθανοτήτων pi και pij, όπου pi είναι η πιθανότητα να έχουμε στην είσοδο του καναλιού το i – οστό σύμβολο του κωδικού αλφαβήτου και pij η πιθανότητα το i – οστό σύμβολο στην είσοδο να ληφθεί στην έξοδο σαν j – οστό. Στην περίπτωση του δυαδικού κωδικού αλφαβήτου, το μαθηματικό υπόδειγμα του διακριτού καναλιού φαίνεται στο Σχήμα:



Εικόνα 3: Είσοδος καναλιού i

Η είσοδος του καναλιού αντιπροσωπεύεται στο μαθηματικό μοντέλο από μια δυαδική τυχαία μεταβλητή X, της οποίας οι δύο τιμές αντιπροσωπεύονται από τους δύο κύβους στην αριστερή πλευρά του γραφήματος. Η έξοδος του καναλιού αντιπροσωπεύεται επίσης από τη δυαδική τυχαία μεταβλητή Y, της οποίας οι δύο τιμές αντιπροσωπεύονται από τους δύο κόμβους στη δεξιά πλευρά του γραφήματος. Οι θέσεις εισόδου και εξόδου του καναλιού μπορούν να συνδεθούν με έναν από τους τέσσερις τρόπους. Ο κωδικός συμβόλου εισόδου διαφεύγει από το κανάλι επικοινωνίας ανέπαφο στις οριζόντιες συνδέσεις, αλλά ο κωδικός συμβόλου εισόδου παραμορφώνεται στο κανάλι και εξέρχεται σε διαφορετική τιμή στις διαγώνιες συνδέσεις. Έστω xi το κωδικό σύμβολο εισόδου και yj το κωδικό σύμβολο εξόδου του καναλιού, με i, j = 1, 2 και x1= y1= 0 και x2= y2= 1, τότε p(xi) καιp(yj) είναι οι πιθανότητες να έχουμε στην είσοδο την τιμή xi και στην έξοδο την τιμή yj, αντίστοιχα. Ακόμα, pij = p(yj/xi) = p(xi/yj) συμβολίζει, όπως είπαμε πιο πάνω, την πιθανότητα το i – οστό σύμβολο στην είσοδο του καναλιού να εξέρχεται από αυτό ως το j – οστό κωδικό σύμβολο. Επομένως, από το μοντέλο του δυαδικού καναλιού έχουμε p11 = p, p12= (1 – p), p21= (1 – q) και p22= q (Σχήμα 3.2). Εάν ισχύει p = q για το δυαδικό συμμετρικό κανάλι, μπορούμε να υποστηρίξουμε ότι η πιθανότητα το "0" να μεταφερθεί ως "0" είναι ίση με την πιθανότητα το "1" να μεταφερθεί ως "1". Επειδή η πιθανότητα ακριβούς μετάδοσης είναι p στο δυαδικό συμμετρικό κανάλι, η πιθανότητα σφάλματος είναι 1 - p. Η πιθανότητα σφάλματος μετάδοσης, το οποίο αναφερόμαστε ως perror, στη γενική περίπτωση του δυαδικού καναλιού μπορεί να υπολογιστεί ως εξής:

P_{error} = p(X = x1 = 0, Y = y2 = 1) + p(X = x2 = 1, Y = y1 = 0) = p(x1) p12 + p(x2) p21.

Μπορούμε να προσδιορίσουμε τη μέση ποσότητα πληροφοριών, την είσοδο και την έξοδο καναλιού, καθώς και την υπό όρους ποσότητα πληροφοριών εξόδου, χρησιμοποιώντας σχέσεις εντροπίας ή την σχεση του μέσου πληροφορικού περιεχομένου, δεδομένης της εισόδου καναλιού και των συνδυασμένων και αμοιβαίων πληροφοριών μεταξύ εισόδου και εξόδου:

$$H(Y) = -\sum_{j=1}^{2} p(y_j) \log p(y_j).$$

$$H(X) = -\sum_{i=1}^{2} p(x_i) \log p(x_i).$$

$$H(X,Y) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(x_i, y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(y_j)p(x_i / y_j)\log p(y_j)p(x_i / y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i)p(y_j / x_i)\log p(x_i)p(y_j / x_i)$$
$$= H(X / Y) + H(Y) = H(Y / X) + H(X).$$

$$H(X / Y) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(x_i / y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(y_j)p(x_i / y_j)\log p(x_i / y_j).$$

$$H(Y / X) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(y_j / x_i)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i)p(y_j / x_i)\log p(y_j / x_i).$$

$$I(X;Y) = H(Y) - H(Y / X) = H(X) - H(X / Y).$$

Επειδή εκφράζει ακριβώς πόσο αβέβαιοι είμαστε για το σύμβολο εισόδου x αν το y λαμβάνεται στην έξοδο, η υπό όρους ποσότητα πληροφοριών H(PC) είναι επίσης γνωστή ως αβεβαιότητα. Όταν το Y είναι γνωστό, η υπό όρους εντροπία είναι ένα μετρο μέσης αβεβαιότητας σε σχέση με το X, η οποία σχετίζεται με την επίδραση του θορύβου. Η μέση ποσότητα bit ανά σύμβολο αντιπροσωπεύεται από τις δεκαδικές τιμές πληροφοριών H (X) και H (Y) (απαιτούνται για την κωδικοποίηση της εισόδου και της εξόδου του καναλιού, αντίστοιχα).

Η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού, από την άλλη πλευρά, μπορεί να θεωρηθεί ως η αβεβαιότητα σχετικά με το σύμβολο x πριν από τη λήψη και δεδομένου του y, μειωμένη κατά την αβεβαιότητα για το x μετά τη λήψη και δεδομένου του y. Ως αποτέλεσμα, η αμοιβαία πληροφόρηση είναι ανάλογη με την ποσότητα των δεδομένων που μεταφέρονται μέσω του καναλιού. Αντί του συμβολισμού I(X;Y) χρησιμοποιείται και ο συμβολισμός R, και τότε μιλάμε για το ρυθμό μετάδοσης. Σ’ ένα κανάλι χωρίς θόρυβο οι υπό συνθήκη ποσότητες πληροφορίας H(X/Y) και H(Y/X). είναι ίσες με μηδέν και επομένως η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού λαμβάνει τη μέγιστη τιμή της, η οποία είναι H(X). Οι πιθανότητες pij ή p(yj/xi)ήp(xi/yj) αντιπροσωπεύουν την επίδραση του θορύβου στο κανάλι επικοινωνίας και είναι αυτές ακριβώς που το χαρακτηρίζουν. Οι πιθανότητες αυτές σχηματίζουν τον πίνακα πιθανοτήτων μετάβασης του καναλιού, που ονομάζουμε και πίνακα μετάβασης του καναλιού.

Ωστόσο, η αμοιβαία ποσότητα πληροφορίας I(X;Y) εξαρτάται επίσης από τις πιθανότητες εμφάνισης των συμβόλων εισόδου p(xi), και επομένως είναι

διαφορετική για διαφορετικές πιθανότητες εμφάνισης των συμβόλων εισόδου σ' ένα δεδομένο κανάλι.

Παράδειγμα:
Ζητείται να υπολογιστεί η αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου ενός δυαδικού συμμετρικού καναλιού με δεδομένες τις πιθανότητες p(x1 = 0) = a, p(y1= 0) = b και p(0/0) = p(1/1) = p.

Λύση:
Από τις δεδομένες πιθανότητες υπολογίζουμε πολύ εύκολα και τι πιθανότητες να έχουμε στην είσοδο και στην έξοδο το σύμβολο «1», p(x2= 1) = 1 – a,

p(y2= 1) = 1 – b και τις πιθανότητες εμφάνισης σφάλματος p(1/0) = p(0/1) = 1 – p. Με την εφαρμογή των ανωτέρω σχέσεων μπορούμε τώρα να υπολογίσουμε την αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου του καναλιού:

I(X;Y) = H(Y)- H (Y/ X) = -β logβ –(1-β)log(1-β)

= αplog p – α(1-p)log(1-p)-(1-α)(1-p)log(1-p)-1(1-α)plogp

=-βlogβ-(1-β)log(1-β)-(1-p)log(1-p)-plogp

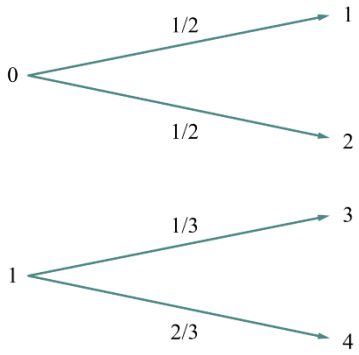
Παρατηρούμε ότι στο αποτέλεσμα δεν περιλαμβάνεται η παράμετρος α (ή θα μπορούσε να εκφραστεί ως συνάρτηση μόνον του α και p), αφού το συμμετρικό δυαδικό κανάλι χαρακτηρίζεται πλήρως από τις παραμέτρους β και p (ή α και p).

2.1.2 Διακριτά κανάλια χωρίς μνήμη

Η αβεβαιότητα (μέσο πληροφορικό περιεχόμενο) συμβόλου ή μηνύματος που έχει εισέλθει στο κανάλι αλλά δεν έχει ληφθεί ακόμα στην έξοδο είναι ίση με H(X). Η αβεβαιότητα ενός συμβόλου ή μηνύματος που μεταδόθηκε είναι ίση H(X/Y). Επομένως, το πληροφορικό περιεχόμενο που μεταδόθηκε μέσω του καναλιού είναι ίσο με τη διαφορά των πληροφορικών περιεχομένων που αναφέραμε, H(X) – H(X/Y) Η χωρητικότητα του ενθόρυβου καναλιού ορίζεται ως το μέγιστο πληροφορικό περιεχόμενο που μπορεί να μεταδοθεί από το κανάλι και δινεται από την ακολουθη σχεση:

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \{H(X) - H(X/Y)\}$$
$$= \max_{p(x)} \{H(Y) - H(Y/X)\} \text{ bits / symbol.}$$

Η μέγιστη τιμή προσδιορίζεται από την σύγκριση ολων των δυνατών κατανομών .



Εικόνα 4: Κατανομές i

Η χωρητικότητα ενός καναλιού χωρίς θόρυβο ισούται με τη μέγιστη τιμή του H(X), που συνεπάγεται ίσες πιθανότητες για όλα τα κωδικά σύμβολα. Στην περίπτωση του δυαδικού καναλιού: C = log2 = 1 bit/code_symbol, και στην περίπτωση καναλιού με q κωδικά σύμβολα: C = logq bits/code_symbol. (Εδώ αναφερόμαστε πλέον στα κωδικά σύμβολα τα οποία αποτελούν την είσοδο και την έξοδο του επικοινωνιακού καναλιού.)

Παράδειγμα:

Θεωρούμε ένα κανάλι επικοινωνίας του οποίου καθεμία από τις δύο δυνατές εισόδους μπορεί να ληφθεί στην έξοδο ως μία από δύο διαφορετικές τιμές . Να υπολογιστεί η χωρητικότητα του καναλιού.

Αν και το κανάλι αυτό εμφανίζεται να είναι ενθόρυβο, στην πραγματικότητα δεν είναι, αφού από το σύμβολο της εξόδου μπορούμε να συμπεράνουμε με βεβαιότητα το σύμβολο της εισόδου. Επομένως, η χωρητικότητα αυτού του καναλιού είναι επίσης ίση με 1 bit/μετάδοση. Η χωρητικότητα είναι ίση με τη μέγιστη τιμή του H(X), αφού η ποσότητα πληροφορίας H(X/Y) ισούται με το 0. Η μέγιστη τιμή H(X) λαμβάνεται για ισοπίθανα σύμβολα εισόδου, δηλαδή για p(x1= 0) = 1/2 και p(x2= 1) = 1/2.

Η χωρητικότητα του καναλιού μπορεί να εκφραστεί σε bits/sec αν πολλαπλασιάσουμε το ρυθμό των μεταδιδόμενων συμβόλων r με την:

$$C = \max_{p(x)} I(X;Y)r$$
$$= \max_{p(x)} \{H(X) - H(X/Y)\}r \text{ bits/sec}$$

Επομένως τώρα μπορούμε να ορίσουμε τη χωρητικότητα διακριτού καναλιού χωρίς θόρυβο και δινεται από την ακολουθη σχέση:

$$C = \lim_{T \to \infty} \frac{\log N(T)}{T} \text{ bits / sec}$$

Οπου N(T) είναι το πληθος των επιτρεπτων μηνυμάτων χρονικής διάρκειας Τ.

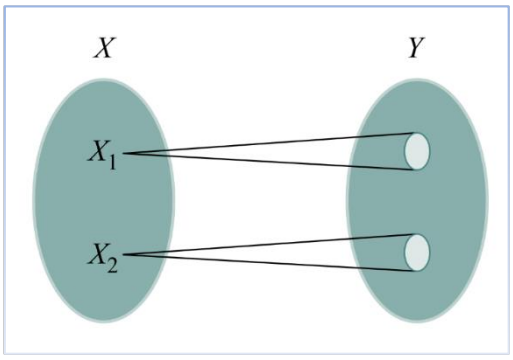
Η χωρητικότητα του διακριτού καναλιού χωρίς θόρυβο με q κωδικά σύμβολα είναι C = logq bits/code_symbol. Αν υποθέσουμε ότι η μετάδοση κάθε κωδικού συμβόλου έχει μια διάρκεια d, τότε η χωρητικότητα του καναλιού σε bits/sec δίνεται από την ακόλουθη σχέση:

$$C = \frac{\log q}{d} \text{ bits / sec.}$$

Αντίστοιχα η χωρητικότητα καναλιού με θόρυβο είναι μικρότερη από αυτή ενός καναλιού χωρίς θόρυβο. Καθώς στα ενθόρυβα κανάλια κατά την μετάδοση υπεισέρχονται σφάλματα. Σε κάποιες περιπτώσεις να μειώσουμε την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση. Τη μείωση της πιθανότητας σφάλματος την επιτυγχάνουμε με την αύξηση του πλεονασμού κατά την κωδικοποίηση. Το ζήτημα αυτό αποτελεί αντικείμενο του ακόλουθου θεωρήματος κωδικοποίησης του Shannon.

2.1.3 Θεώρημα κωδικοποίησης

Κατά τη μετάδοση μηνυμάτων μέσω ενός διακριτού καναλιού χωρις θόρυβο, δεν παρουσιάζονται σφάλματα. Όταν οι πληροφορίες μεταφέρονται σε μορφή που έχει πλεονασμό, ελαχιστοποιούνται οι πιθανότητες σφαλμάτων. Αναμένετε ότι η ενσωμάτωση πλεονασμού θα είναι απαραίτητη για τη μείωση της πιθανότητας σφάλματος πρακτικά στο μηδέν, κάτι που θα είχε επίσης ως αποτέλεσμα τη μείωση του ρυθμού μετάδοσης στο μηδέν. Σύμφωνα με τη θεωρία του Shannon, ωστόσο, οι πληροφορίες C-rate μπορούν να μεταδοθούν μέσω του καναλιού με όση μικρή πιθανότητα σφάλματος απαιτείται. Όμως, ας προσπαθήσουμε πρώτα να αποκτήσουμε μια διαισθητική ιδέα του γιατί μπορούν να μεταδοθούν C bits μέσω του καναλιού.



Εικόνα 5: Μετάδοση i

Η βασική ιδέα είναι ότι κάθε κανάλι είναι ένα υποσύνολο εισόδων που παράγουν στην έξοδο διαφορετικές ακολουθίες. Για κάθε τυπική (πιθανή) ακολουθία εισόδου

X μήκους l συμβόλων υπάρχουν περίπου 2lH(Y/X) δυνατές ακολουθίες εξόδου Y, όλες με την ίδια πιθανότητα.

Η ανωτέρω διαισθητική περιγραφή αναφέρεται σε ένα άνω φράγμα της χωρητικότητας. Στη συνέχεια θα εξετάσουμε το ιδιαίτερα σημαντικό αποτέλεσμα της Θεωρίας Πληροφορίας, το δεύτερο θεώρημα κωδικοποίησης του Shannon. Για την απόδειξη του θεωρήματος θα χρησιμοποιήσουμε τα επιχειρήματα της προηγούμενης παραγράφου σε μια πιο αυστηρή εκδοχή.

2.1.4 Δεύτερο θεώρημα Shannon

Απόδειξη:

Σε ένα κανάλι χωρίς μνήμη χωρητικότητας C, είναι δυνατή η μετάδοση ποσότητας πληροφορίας H(X) διακριτής πηγής με οσοδήποτε μικρή πιθανότητα σφάλματος θέλουμε, αν ισχύει H(X)<= C.

Επομένως είναι αδύνατο να μεταδοθεί πληροφορία με ρυθμό μεγαλύτερο της χωρητικότητας, H(X)>C, ανεξαρτήτως της κωδικοποίησης που χρησιμοποιείται, χωρίς να αυξάνεται ανεξέλεγκτα ο αριθμός των σφαλμάτων.

Εξετάζουμε πρώτα την περίπτωση μιας διακριτής πηγής με εντροπία H(X) και με τέτοια κατανομή πιθανοτήτων των συμβόλων εισόδου ώστε να ισχύει C = H(X) – H(X/Y). (Η χωρητικότητα εκφράζεται σε bits/symbol. Αν είχαμε λάβει υπόψη και το ρυθμό μετάδοσης r, τότε η χωρητικότητα θα εκφραζόταν σε bits/sec.) Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην είσοδο του καναλιού είναι ίσο με Mx = 2lH(X), όπου όλα τα μηνύματα είναι ισοπίθανα Ανάλογα, το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην έξοδο του καναλιού είναι ίσο με My = 2lH(Y). Ένα μήνυμα m(y) που λαμβάνεται στην έξοδο του ενθόρυβου καναλιού μπορεί να προέρχεται από ένα πλήθος μηνυμάτων εισόδου m(x) εξαιτίας του θορύβου. Το πλήθος των πιο πιθανών μηνυμάτων εισόδου που οδηγούν στη λήψη του ίδιου μηνύματος εξόδου είναι ίσο με Mx/y = 2lH(X/Y).

Αν rI(X;Y) = C, δηλαδή η πηγή προσαρμόζεται ιδανικά στο κανάλι, τότε το πλήθος των πιο πιθανών μηνυμάτων που μεταδίδονται είναι ίσο με MC = 2lC. Στην περίπτωση μη ιδανικής προσαρμογής, ισχύει MR = 2lR, όπου rI(X;Y) = R. Με την τελευταία αυτή περίπτωση, της μη ιδανικής προσαρμογής, δηλαδή R < C, θα ασχοληθούμε στη συνέχεια.

Η πιθανότητα μεταφοράς ενός μηνύματος m(xi), το οποίο ανήκει στο σύνολο των πιο πιθανών μηνυμάτων Mx, από το κανάλι ισούται με την πιθανότητα να ανήκει το μήνυμα m(xi) στο σύνολο των μηνυμάτων που μεταφέρονται από το κανάλι M_R. Η πιθανότητα αυτή υπολογίζεται ως εξής:

$$p(m(x_i) \in M_R) = \frac{2^{lR}}{2^{lH(X)}} = 2^{l\left(R-H(X)\right)}$$

Από την άλλη πλευρά, το πλήθος των μηνυμάτων εισόδου που οδηγούν, κατά μέσο όρο, στη λήψη του ίδιου μηνύματος στην έξοδο m(y) δίνεται από Mx/y. Τώρα επιλέγουμε τυχαία ένα μήνυμα εισόδου m(xi). Αν υπάρχει τουλάχιστον ένα άλλο μήνυμα m(xj), εκτός του m(xi), το οποίο να ανήκει τόσο στο Mx/y όσο και στο MR = 2lR που μπορεί να οδηγήσει στη λήψη του ίδιου μηνύματος m(yi), τότε μπορεί να συμβεί σφάλμα. Η πιθανότητα της εμφάνισης ενός σφάλματος είναι:

$$\begin{aligned}
p_{error} &= p\left\{m(x_j) \in (M_{x/y} \cap M_R), j \neq i\right\} \\
&\leq \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p\left[(m(x_j) \in M_{x/y}) \cap (m(x_j) \in M_R)\right] \\
&= \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p(m(x_j) \in M_{x/y}) p(m(x_j) \in M_R) \\
&\leq \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p(m(x_j) \in M_R) = \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} \frac{2^{lR}}{2^{lH(X)}} = \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} 2^{l\left(R-H(X)\right)} = \left\{M_{x/y} - 1\right\} 2^{l\left(R-H(X)\right)}
\end{aligned}$$

Αφού R < C, έχουμε R = C– ε = H(X) – H(X/Y) – ε, όπου είναι ένας θετικός σταθερός αριθμός. Επομένως, η πιθανότητα σφάλματος ικανοποιεί την ακόλουθη ανισότητα:

$$p_{error} \leq \left\{2^{lH\left(X|Y\right)} - 1\right\} 2^{l\left(-H\left(X|Y\right)-\varepsilon\right)} \leq 2^{-l\varepsilon}.$$

Από την τελευταία σχέση προκύπτει ότι η πιθανότητα εμφάνισης λάθους μπορεί να γίνει οσοδήποτε μικρή επιθυμούμε, αρκεί να επιλέξουμε κατάλληλα μεγάλο μήκος l. Το δεύτερο μέρος του θεωρήματος μπορεί να δειχθεί ως ακολούθως: Αν είναι H(X) > C, τότε η αβεβαιότητα H(X/Y) είναι μεγαλύτερη του μηδενός και τουλάχιστον ίση με H(X) – C. Για να το αποδείξουμε, ας υποθέσουμε καταρχήν το αντίθετο, δηλαδή ότι η αβεβαιότητα H(X/Y) είναι μικρότερη της ποσότητας H(X) – C. Αλλά τότε θα έπρεπε να ισχύει H(X/Y) = H(X) – C – ε, για κάποιο θετικό αριθμό ε. Επομένως, H(X/Y) = H(X) – C – ε και H(X) – H(X/Y) = C + ε. Όμως, αφού η χωρητικότητα είναι η μέγιστη τιμή της

ποσότητας H(X) – H(X/Y), η τελευταία σχέση δεν μπορεί να ισχύει. Άρα, η αβεβαιότητα H(X/Y) είναι μεγαλύτερη του μηδενός και τουλάχιστον ίση της διαφοράς H(X) – C, δηλαδή H(X/Y) = H(X) – C + ε. Επομένως, δεν είναι δυνατή η μετάδοση με ρυθμό H(X) > C.

2.1.5 Διακριτά κανάλια με μνήμη

Στην προηγούμενη υποενότητα εξετάσαμε την περίπτωση των διακριτών καναλιών επικοινωνίας χωρίς μνήμη. Δηλαδή κανάλια στα οποία η εμφάνιση ενός σφάλματος κατά τη μετάδοση ενός συμβόλου δεν επηρεάζει τη μετάδοση των επόμενων συμβόλων. Οι περισσότεροι από τους κώδικες ελέγχου σφάλματος που εφαρμόζονται βασίζονται στην παραδοχή ότι τα σφάλματα εμφανίζονται ως ανεξάρτητα τυχαία γεγονότα. Ωστόσο, σε πολλά κανάλια τα σφάλματα εκδηλώνονται μάλλον συσχετισμένα. Αυτό οφείλεται και στο ότι χρησιμοποιούνται πολύ υψηλοί ρυθμοί μετάδοσης, οι οποίοι έχουν σαν αποτέλεσμα να προκαλούν ατέλειες των επικοινωνιακών συστημάτων και να προκαλούν διαδοχικά σφάλματα.

Για παράδειγμα σε μαγνητικά και οπτικά μέσα αποθήκευσης, που χαρακτηρίζονται από υψηλές πυκνότητες αποθήκευσης, αυτές έχουν ως αποτέλεσμα την εμφάνιση ακολουθιών διαδοχικών σφαλμάτων όταν παρουσιάζονται βλάβες. Επίσης, τα τηλεφωνικά κανάλια επηρεαζόμενα από τις διατάξεις μεταγωγής συμπεριφέρονται ως κανάλια με μνήμη.

Στα κανάλια με μνήμη εκδηλώνονται, ορισμένες φορές, ξαφνικοί θόρυβοι, που επικρατούν του θορύβου Gauss και προκαλούν καταιγισμούς σφαλμάτων. Τα φαινόμενα των θορύβων είναι πολύπλοκα και γι’ αυτό κάνουν δύσκολο το λεπτομερή χαρακτηρισμό των καναλιών με μνήμη.

2.1.6 ορισμός χωρητικότητας διακριτού καναλιού με μνήμη

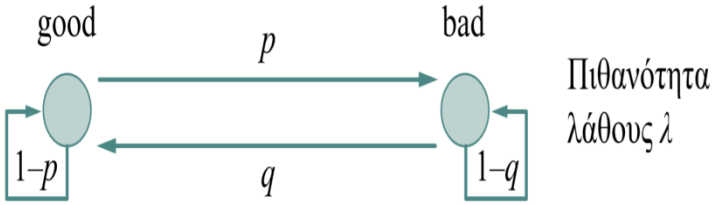
Ορίζετε ως η χωρητικότητα διακριτού καναλιού με μνήμη με υποθετικές ακολουθίες κωδικών συμβόλων στην είσοδο και στην έξοδο μήκους L, δηλαδή:

$$C = \lim_{L\to\infty} \frac{1}{L} \max_{p(x_1 \ldots x_L)} I(X_1 \ldots X_L; Y_1 \ldots Y_L)$$

Η μέγιστη τιμή της αμοιβαίας πληροφορίας προκύπτει από τη σύγκριση των κατανομών πιθανοτήτων όλων των κωδικών ακολουθιών εισόδου μήκους L.

Ο υπολογισμός και η αξιολόγηση της χωρητικότητας καναλιών με μνήμη είναι αρκετά σύνθετη υπόθεση. Για το λόγο αυτό θα περιοριστούμε στη συνέχεια στην εξέταση δυαδικών καναλιών. Η εμφάνιση μιας ακολουθίας σφαλμάτων ονομάζεται «καταιγισμός». Ως μήκος του καταιγισμού εννοούμε το μήκος από το πρώτο μέχρι και το τελευταίο σφάλμα. Για να μελετήσουμε τα κανάλια με μνήμη μπορούμε να χρησιμοποιήσουμε στατιστικές μεθόδους ή υποδείγματα (μοντέλα) που δημιουργούν ακολουθίες σφαλμάτων παρόμοιες με αυτές των καναλιών.

Τέτοια υποδείγματα αποτελούνται από μία Μαρκοβιανή αλυσίδα με συγκεκριμένο αριθμό καταστάσεων και τις αντίστοιχες πιθανότητες μετάβασης. Αυτά ονομάζονται υποδείγματα Gilbert, και ακολουθεί το πιο μοντέλο στο παρακάτω σχήμα.



Εικόνα 6: Μοντέλο Gilbert i

Το μοντέλο έχει δύο καταστάσεις. Η μία είναι η good η άλλη η bad. Υποθέτουμε ότι ο ρυθμός μετάδοσης των δυαδικών ψηφίων είναι ίσος με 1 symbol/sec. Αν είμαστε στην κατάσταση «good» στην αρχή του χρονικού διαστήματος συμβόλου t = n, τότε το δυαδικό ψηφίο που μεταδίδεται λαμβάνεται χωρίς λάθος στην έξοδο. Αμέσως μετά, στην αρχή του επόμενου χρονικού διαστήματος συμβόλου t = n + 1, αποφασίζεται αν θα παραμείνει στην κατάσταση «good» με πιθανότητα 1 – p ή θα μεταπέσει στην κατάσταση «bad» με πιθανότητα p. Αν παραμείνει στην κατάσταση «good», έχουμε και πάλι ορθή μετάδοση ενός δυαδικού ψηφίου. Αντίθετα, αν μεταπέσει στην κατάσταση «bad», τότε η μετάδοση του δυαδικού ψηφίου είναι ορθή με πιθανότητα 1 – λ και εσφαλμένη με πιθανότητα λ. Μετά τη μετάδοση, στην αρχή του χρονικού διαστήματος συμβόλου t = n + 2 αποφασίζεται αν θα παραμείνει στην κατάσταση «bad» με πιθανότητα 1 – q ή θα μεταπέσει στην κατάσταση «good» με πιθανότητα q. Παρατηρούμε ότι το μοντέλο προβλέπει πάντα ορθή μετάδοση στην κατάσταση «good» και ορθή ή εσφαλμένη μετάδοση στην κατάσταση «bad».

2.1.7 Μοντέλο Gilbert

Με την ανάλυση του μοντέλου Gilbert , μπορούμε να υπολογίσουμε τις πιθανότητες να βρίσκετε το κανάλι σε καταστάσεις good και bad που είδαμε στο παραπάνω σχήμα, καθώς και την πιθανότητα εμφάνισης σφαλμάτων κατά την μετάδοση.

Επομένως μεταξύ των πιθανοτήτων κατάστασης και των πιθανοτήτων μετάπτωσης ισχύουν οι ακόλουθες σχέσεις:

$$p(good) + p(bad) = 1,$$

$$p(good)p + p(good)(1-p) = p(good)(1-p) + p(bad)q,$$

$$p(bad)q + p(bad)(1-q) = p(bad)(1-q) + p(good)p.$$

Από το παραπάνω σύστημα εξισώσεων μπορούν να υπολογιστούν οι πιθανότητες των καταστάσεων και από την πιθανότητα της κατάστασης «bad», p(bad), λαμβανομένης υπόψη της πιθανότητας εσφαλμένης μετάδοσης στην κατάσταση «bad», υπολογίζεται η πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση, perror. Σημειώνεται επίσης ότι ενώ η πιθανότητα λ αναφέρεται στην εσφαλμένη μετάδοση όταν το κανάλι είναι στην κατάσταση «bad», η perror αναφέρεται στην πιθανότητα εσφαλμένης μετάδοσης ανεξαρτήτως της κατάστασης στην οποία βρίσκεται.

$$p(good) = \frac{q}{p+q}.$$

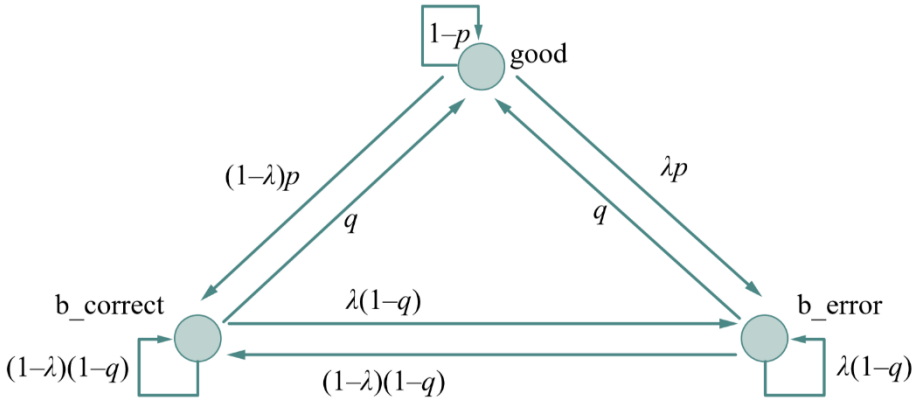
$$p(bad) = \frac{p}{p+q}.$$

$$p_{error} = \lambda p(bad) = \lambda \frac{p}{p+q}.$$

Μπορούμε να επεκτείνουμε το πλήθος των καταστάσεων του μοντέλου του σχήματος μπορούμε να διακρίνουμε τρεις καταστάσεις την κατάσταση bad, και δύο υποκαταστάσεις. Την (b_correct), και την εσφαλμένης (b_error)

Το άθροισμα των παραπάνω είναι η P_{error} . Επομένως αυτό το επεκταμένο μοντέλο που θα δείξουμε στην παρακάτω εικόνα με τις τρεις καταστάσεις επιτρέπει επίσης τον υπολογισμό των πιθανοτήτων καλής, κακής και εσφαλμένης μετάδοσης, δηλαδή των p(good), p(bad) και P_{error}.

Το ανωτέρω μοντέλο γίνεται πιο συνθετο όταν προβλεπονται περισσοτερες των τριων καταστασεων, οι οποιες είναι απαραιτητες για την αναλυση της συμπεριφορας των ακουλουθιων σφαλματων.



Εικόνα 7: Μοντέλο Gilbert ii

Παράδειγμα:

Για το μοντέλο του παραπάνω σχήματος δίνονται οι παρακάτω τιμές
p = 0,02, q = 0,1 και λ = 0,2. Ζητούνται οι πιθανότητες p(good), p(bad) και P_{error}

Λύση:

Με εφαρμογή των σχετικών τύπων μπορούμε εύκολα να υπολογίσουμε τις ζητούμενες πιθανότητες: p(good) = (q/(p + q)) = (0,1/0,12) = 0,83, p(bad) =

(p/(p + q)) = 0,17 και P_{error} = λ p(bad) = 0,034.

2.2 Συνεχής κανάλια επικοινωνίας

Στα συνεχή επικοινωνιακά κανάλια η κωδικοποίηση και η αποκωδικοποίηση ερμηνεύονται διαφορετικά απ' ό,τι στα διακριτά κανάλια.

Με την κωδικοποίηση εννοούμε διαμόρφωση πλάτους και συχνότητας ή τη φραγή εύρους με τη χρήση φίλτρων. Με τη διαμόρφωση το σήμα που παράγεται από την πηγή μετατρέπεται σε μορφή κατάλληλη για το συνεχές κανάλι.

Όπως στην περίπτωση του διακριτού καναλιού, κατά τη μετάδοση του σήματος στο συνεχές κανάλι επενεργεί προσθετικός ή και πολλαπλασιαστικός θόρυβος. Για το λόγο αυτό το μεταδιδόμενο σήμα θα πρέπει να επανακατασκευαστεί στην έξοδο από το διαστρεβλωμένο σήμα που λαμβάνεται. Ο προσθετικός θόρυβος εμφανίζεται πιο συχνά από τον πολλαπλασιαστικό. Μπορεί δε να είναι γκαουσιανός ή κρουστικός. Ο γκαουσιανός θόρυβος είναι θερμικός ή βολής από τις διατάξεις και από ακτινοβολία που λαμβάνεται από την κεραία λήψης. Ο κρουστικός θόρυβος, από την άλλη

πλευρά, οφείλεται σε μεταβατικά φαινόμενα στη λειτουργία των διακοπτών και χαρακτηρίζεται από μεγάλα διαστήματα χωρίς θόρυβο που διακόπτονται από καταιγισμούς παλμών θορύβου μεγάλου πλάτους.

2.2.1 Χωρητικότητα συνεχών καναλιών χωρίς μνήμη

Στην είσοδο του καναλιού έχουμε ένα συνεχές σήμα x(t) και στην έξοδο επίσης ένα σήμα y(t).

Για τη συνάρτηση πυκνότητας πιθανότητας το σήμα λαμβάνει την έξοδο του καναλιού y(t) με δεδομένο το σήμα εισόδου x(t). Τότε ισχύει:

$$f(y/x) = f(y_1,\ldots,y_N / x_1,\ldots,x_N).$$

Αν ένα δείγμα του σήματος εξόδου εξαρτάται μόνο από το αντίστοιχο δείγμα του σήματος εισόδου, τότε μιλάμε για συνεχή κανάλια χωρίς μνήμη. Σε αυτή την περίπτωση τα μέτρα ποσότητας πληροφορίας που μας ενδιαφέρουν μπορούν να οριστούν στη βάση ενός ζεύγους δειγμάτων X και Y. Τα X και Y είναι τυχαίες μεταβλητές που αναπαριστούν τα δείγματα των σημάτων εισόδου και εξόδου x(t) και y(t).

Έτσι ακολουθεί ο παρακάτω τύπος:

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log\frac{f(x,y)}{f(x)f(y)}dxdy.$$

Στην παραπάνω σχέση, με f(x,y) συμβολίζεται η συνδυασμένη συνάρτηση πυκνότητας πιθανότητας των τυχαίων μεταβλητών X και Y.

Η αμοιβαία ποσότητα πληροφορίας καλείται και «ρυθμός μετάδοσης πληροφορίας», αφού πρόκειται για την ποσότητα πληροφορίας που μεταφέρεται μέσω του καναλιού.

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y).$$

2.2.2 Ορισμός Χωρητικότητα συνεχών καναλιών χωρίς μνήμη

Ορίζουμε τη χωρητικότητα του συνεχούς καναλιού ως τη μέγιστη τιμή της αμοιβαίας πληροφορίας μεταξύ της εισόδου και της εξόδου ή του ρυθμού μετάδοσης, που μπορεί να επιτευχθεί συνδέοντας όλες τις πηγές πληροφορίας στο κανάλι και λαμβάνοντας υπόψη τους υφιστάμενους περιορισμούς.

$$C = \max_{f(x)} I(X;Y) = \max_{f(x)} \left\{ H(Y) - H(Y/X) \right\}.$$

Η μέγιστη τιμή της αμοιβαίας πληροφορίας προκύπτει από τη σύγκριση των συναρτήσεων πυκνότητας πιθανότητας των δειγμάτων του σήματος εισόδου. Ωστόσο, ο υπολογισμός της χωρητικότητας ενός συνεχούς καναλιού είναι δύσκολος.

Στην περίπτωση των αθροιστικών καναλιών ο θόρυβος n(t) προστίθεται στο μεταδιδόμενο σήμα x(t), οπότε με βάση την συνάρτηση πυκνότητας πιθανότητας του σήματος εισόδου , εξόδου αλλά και θορύβου ακολουθεί η σχέση (X + N = Y):

$$f(y/x) = f(x+n/x) = f(n/x).$$

Αφού ο θόρυβος είναι στατιστικά ανεξάρτητος του σήματος εισόδου, η υπό συνθήκη συνάρτηση πιθανότητας του δείγματος του θορύβου με δεδομένο το δείγμα του σήματος εισόδου μπορεί να εκφραστεί μόνο ως προς τα σήματα εισόδου και εξόδου.

$$f(y/x) = f(n/x) = f(n) = f(y-x).$$

Στην περίπτωση του αθροιστικού καναλιού, η επενέργεια του θορύβου στη χωρητικότητα του καναλιού αντανακλάται στην υπό συνθήκη ποσότητα πληροφορίας H(Y/X).

Έτσι μπορεί να υπολογιστεί ως εξής:

$$H(Y/X) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log f(y/x)dxdy$$
$$= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(y/x)\log f(y/x)dxdy$$
$$= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(n)\log f(n)dxdn$$
$$= -\int_{-\infty}^{\infty} f(n)\log f(n)dn = H(N).$$

Επομένως η χωρητικότητα του αθροιστικού καναλιού μπορεί να εκφραστεί ως συνάρτηση της μέγιστης μέσης ποσότητας πληροφορίας της εξόδου και της μέσης ποσότητας πληροφορίας του θορύβου.

$$C = \max_{f(x)} I(X;Y) = \max_{f(x)}\{H(Y) - H(N)\} = \max_{f(x)} H(Y) - H(N).$$

2.2.3 Ορισμός χωρητικότητας συνεχων καναλιών με μνήμη

Ορίζουμε τη χωρητικότητα του συνεχούς καναλιού με μνήμη ως τη μέγιστη τιμή της αμοιβαίας ποσότητας πληροφορίας μεταξύ διανύσματος δειγμάτων της εισόδου και διανύσματος δειγμάτων της εξόδου ή του ρυθμού μετάδοσης ως προς τη συνάρτηση πυκνότητας πιθανότητας του διανύσματος των δειγμάτων.

$$C = \lim_{N\to\infty} \max_{f(x_1,\ldots,x_N)} I(X_1,\ldots,X_N/Y_1,\ldots,Y_N).$$

Όπως στην περίπτωση των διακριτών καναλιών, έτσι και στην περίπτωση των συνεχών καναλιών είναι δυνατή η μετάδοση πληροφορίας με οσοδήποτε μικρή πιθανότητα εμφάνισης σφάλματος. Αυτό διατυπώνεται στο ακόλουθο θεώρημα κωδικοποίησης του Shannon για τα συνεχή κανάλια, το οποίο είναι ανάλογο του θεωρήματος του Shannon για τα διακριτά κανάλια. Είναι δυνατή η μεταφορά ποσότητας πληροφορίας H(X) (bits/sec) μέσω συνεχούς καναλιού χωρητικότητας C, στο οποίο επενεργεί λευκός γκαουσιανός θόρυβος, με οσοδήποτε μικρή πιθανότητα ζμφάνισης σφάλματος επιθυμούμε, αν ισχύει H(X) < C.

2.2.4 Συνεχής κανάλια με μνήμη

Για τον προσδιορισμό της χωρητικότητας συνεχούς καναλιού με μνήμη θα πρέπει να λάβουμε υπόψη τις φασματικές πυκνότητες ισχύος του στοχαστικού σήματος εισόδου και του θορύβου. Υποθέτουμε ότι το στοχαστικό σήμα εισόδου και ο θόρυβος ακολουθούν γκαουσιανή κατανομή και ότι είναι φραγμένα ως προς την ισχύ και το εύρος ζώνης. Μεταξύ της ισχύος και της φασματικής πυκνότητας ισχύος ισχύει η ακόλουθη σχέση, όπου W είναι το εύρος ζώνης του σήματος εισόδου και του θορύβου:

$$\sigma_x^2 = \frac{1}{2\pi}\int_{-2\pi W}^{2\pi W} \Phi_x(\omega)d\omega,$$

$$\sigma_n^2 = \frac{1}{2\pi}\int_{-2\pi W}^{2\pi W} \Phi_n(\omega)d\omega.$$

Αν χωρίσουμε το φάσμα σε τόσο μικρά τμήματα Δω ώστε να μπορεί να ληφθεί σ' αυτά ως σταθερό, τότε μπορούμε να θεωρήσουμε τα αντίστοιχα σήματα εξόδου ως ασυσχέτιστα μεταξύ τους. Η μέση ισχύς ανά τμήμα Δω είναι:

$$\sigma_{x_i}^2 = \frac{1}{2\pi}\Phi_{x_i}(\omega_i)\Delta\omega,$$

$$\sigma_{n_i}^2 = \frac{1}{2\pi}\Phi_{n_i}(\omega_i)\Delta\omega.$$

- ✓ Αν υποθέσουμε ότι το πλήθος των τμημάτων Δω είναι ίσο με Μ, όπου Μ = 4πW/Δω και επομένως W = Μωi και ωi = Δω/4π. Για τον υπολογισμό της χωρητικότητας κάθε τμήματος Δω λαμβάνουμε υπόψη και την υφιστάμενη στατιστική ανεξαρτησία μεταξύ των διαφόρων δειγμάτων:

$$C_i = \omega_i \log\left\{1+\frac{\sigma_{x_i}^2}{\sigma_{n_i}^2}\right\} = \frac{\Delta\omega}{4\pi}\log\left\{1+\frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}.$$

$$C = \sum_{i=1}^{\cdots} C_i = \frac{\Delta\omega}{4\pi}\sum_{i=1}^{\cdots}\log\left\{1+\frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}.$$

- ✓ Η χωρητικότητα όλου του φάσματος μεταξύ – 2πW και 2πW δίνεται από την σχέση:

- ✓ Αν πάρουμε το όριο για Δω $\rightarrow$ 0 τότε έχουμε:

$$C = \frac{1}{4\pi} \int_{-2\pi W}^{2\pi W} \log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\} d\omega \text{ bits / sec.}$$

- ✓ Αν ισχύει Φx(ω) = Φx(– ω), τότε:

$$C = \frac{1}{2\pi} \int_{0}^{2\pi W} \log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\} d\omega \text{ bits / sec.}$$

Έτσι καταλαβαίνουμε ότι η χωρητικότητα εξαρτάται πό το φάσμα του σήματος εισόδου, καθώς και από το φάσμα του θορύβου.

2.2.5 Λευκός θόρυβος

Ο λευκός θόρυβος χαρακτηρίζεται από μια γκαουσιανή συνάρτηση πυκνότητας πιθανότητας N(0, σ), δηλαδή μηδενικής μέσης τιμής, και από σταθερή ισχύ πυκνότητας φάσματος στο εύρος ζώνης W. Επίσης χαρακτηρίζεται από εσωτερική ανεξαρτησία, δηλαδή τα δείγματα του θορύβου είναι στατιστικά ανεξάρτητα και, επομένως, κάθε δείγμα του θορύβου μπορεί να εξεταστεί ξεχωριστά από τα υπόλοιπα δείγματα. Η συνάρτηση πυκνότητας πιθανότητας του λευκού θορύβου είναι κανονικής κατανομής με μηδενική μέση τιμή, τότε η ποσότητα πληροφορίας είναι ίση με τη μέγιστη ποσότητα πληροφορίας σήματος συνεχούς πηγής πληροφορίας με σταθερή ισχύ. Η μέγιστη ποσότητα πληροφορίας μιας συνεχούς πηγής πληροφορίας με σταθερή ισχύ, σ^2, είναι ίση με H(X) = log(σ÷2πe) και ισχύει για κανονική συνάρτηση πυκνότητας πιθανότητας, f(x). Το αποτέλεσμα μπορούμε να το εκφράσουμε σε bits/sec, λαμβάνοντας υπόψην υποτιθέμενο πλήθος M, που είναι ίσο με το διπλάσιο εύρος ζώνης σήματος 2W.

Έτσι προκύπτει η παρακάτω λύση:

$$\begin{aligned} H(N) &= \log\left(\sigma\sqrt{2\pi e}\right) \text{ bits / δείγμα} \\ &= M\frac{1}{2}\log\left(2\pi e\sigma^2\right) \text{ bits / sec} \\ &= 2\text{W}\frac{1}{2}\log\left(2\pi e\sigma^2\right) = \text{ W}\log\left(2\pi e\sigma^2\right) \text{ bits / sec} \end{aligned}$$

Από την άλλη πλευρά η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος της εξόδου λαμβάνεται όταν είναι κανονικά κατανεμημένο, με ισχύ σ^2_y. Αλλά τότε, αφού και ο λευκός θόρυβος ακολουθεί την κανονική κατανομή, το σήμα εισόδου πρέπει να είναι και αυτό γκαουσιανό. Επομένως, αφού Y = X + N και $\sigma^2_y = \sigma^2_x + \sigma^2_n$, η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εισόδου ως προς τη συνάρτηση πυκνότητας πιθανότητας του σήματος εισόδου δίνεται από την ακόλουθη σχέση:

$$\begin{aligned}\max_{f(x)} H(Y) &= \log\sqrt{\sigma_x^2+\sigma_n^2}\left(\sqrt{2\pi e}\right) \text{ bits / δείγμα} \\ &= \frac{1}{2}\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / δείγμα} \\ &= \text{W}\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / sec.}\end{aligned}$$

Έτσι λοιπόν αφού έχουμε υπολογίσει την ποσότητα πληροφορίας του λευκού θορύβου και τη μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εξόδου για την περίπτωση περιορισμένης μέσης ισχύος, μπορούμε πλέον να υπολογίσουμε τη χωρητικότητα του συνεχούς καναλιού με αθροιστικό λευκό θόρυβο.

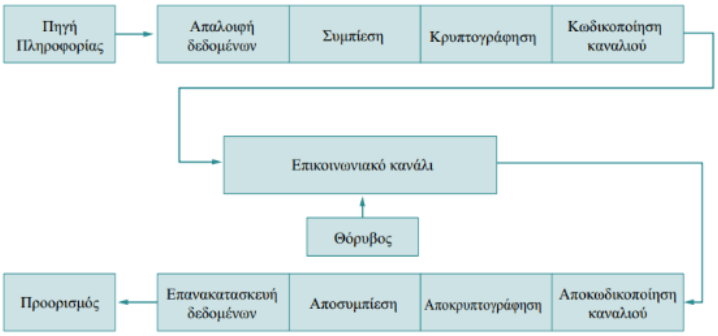
$$\begin{aligned}C &= \max_{f(x)}\left\{H(Y)\right\} - H(N) \text{ bits / sec} \\ &= W\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} - W\log\left\{2\pi e\,\sigma_n^2\right\} \\ &= W\log\frac{\sigma_x^2+\sigma_n^2}{\sigma_n^2} = W\log\left\{1+\frac{\sigma_x^2}{\sigma_n^2}\right\} \text{ bits / sec.}\end{aligned}$$

Παρατηρούμε ότι, μειώνοντας το εύρος ζώνης W και ταυτόχρονα αυξάνοντας το λόγο της ισχύος του σήματος εισόδου προς την ισχύ του λευκού θορύβου ή αντίστροφα, η χωρητικότητα μπορεί να διατηρηθεί η ίδια.

Κεφάλαιο 3ο
ΚΩΔΙΚΟΠΟΙΗΣΗ ΚΑΝΑΛΙΟΥ

Εισαγωγη:

Η μελέτη μεθόδων για αποτελεσματική και σωστή μεταφορά πληροφοριών από την πηγή στον προορισμό είναι γνωστή ως θεωρία κωδικοποίησης. Η θεωρία ανάπτυξής της βασίζεται σε σχετικές απαιτήσεις εφαρμογών, όπως οικονομικές πληροφορίες μέσω τηλεφωνικών γραμμών, μεταφορά δεδομένων από έναν υπολογιστή σε άλλο ή μεταφορά δεδομένων από την μνήμη στην κεντρική μονάδα επεξεργασίας και μετάδοση δεδομένων από δορυφόρους ή διαστημόπλοια στη Γη. Το κανάλι επικοινωνίας είναι το φυσικό μέσο , μέσω του οποίου παραδίδονται οι πληροφορίες, όπως είδαμε στο Κεφάλαιο 2. Οι τηλεφωνικές γραμμές και η ατμόσφαιρα είναι παραδείγματα καναλιών. Δυστυχώς, υπάρχει θόρυβος στα κανάλια επικοινωνίας, με αποτέλεσμα να μεταφέρονται κατεστραμμένα δεδομένα. Η πρόκληση του εντοπισμού και της επιδιόρθωσης προβλημάτων μετάδοσης που προκαλούνται από το θόρυβο στα κανάλια επικοινωνίας αντιμετωπίζεται από τη θεωρία κωδικοποίησης. Ένα πλήρες μοντέλο επικοινωνίας απεικονίζεται στο παρακάτω διάγραμμα. Η κωδικοποίηση και η αποκωδικοποίηση του καναλιού είναι τα στοιχεία αυτού του διαγράμματος που θα συζητηθούν σε αυτό και στα επόμενα κεφάλαια.



Εικόνα 8: Μοντέλο καναλιού επι/νιας i

Όπως είδαμε και στο Κεφάλαιο 2, ένας δυαδικός κώδικας, C, είναι ένα σύνολο κωδικών λέξεων. Οι κωδικές λέξεις είναι ακολουθίες δυαδικών ψηφίων. Για παράδειγμα, ο κώδικας που απαρτίζεται από όλες τις λέξεις μήκους δύο ψηφίων είναι C = {00, 10, 01, 11}. Ένας κώδικας ονομάζεται ισομήκης κώδικας (ή κώδικας μπλοκ) αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος. Στην περιπτωση μας θα μας απασχολήσουν μόνο κώδικες μπλοκ. Το πλήθος των κωδικών λέξεων ενός κώδικα C συμβολίζεται με |C|. Σχετικά με το κανάλι κάνουμε δύο παραδοχές, καθοριστικές για την ανάπτυξη της θεωρίας κωδικοποίησης. Σύμφωνα με την πρώτη παραδοχή, μια κωδική λέξη μήκους n δυαδικών ψηφίων, που εισέρχεται στο κανάλι, λαμβάνεται στην έξοδό του ως λέξη μήκους και πάλι n δυαδικών ψηφίων, αν και η ακολουθία εισόδου του καναλιού μπορεί να διαφέρει από αυτή της εξόδου του καναλιού. Επίσης, χωρίς δυσκολία διαπιστώνεται, από το δέκτη, η αρχή της πρώτης λέξης μιας ακολουθίας κωδικών λέξεων που μεταδίδεται μέσω του καναλιού. Για παράδειγμα,

αν στο κανάλι μεταδίδεται η δυαδική ακολουθία 010011, τότε στην έξοδό του λαμβάνεται η ακολουθία 010011 ή κάποια άλλη του ιδίου μήκους, όχι όμως η ακολουθία 10011 ή κάποια άλλη μικρότερου μήκους, επειδή χάθηκε το 1ο ψηφίο (το «0») της 1ης λέξης της ακολουθίας. Επομένως, η πρώτη παραδοχή αναφέρεται στη δυνατότητα του δέκτη να λάβει όλες τις λέξεις που μεταδόθηκαν, με ή χωρίς σφάλματα.

Η δεύτερη παραδοχή αναφέρεται στο ότι τα σφάλματα, δηλαδή ο θόρυβος, εμφανίζονται διασκορπισμένα κατά τυχαίο τρόπο και όχι σε συστάδες (ή καταιγισμούς, bursts). Με άλλα λόγια, η πιθανότητα να αλλοιωθεί ένα bit κατά τη μετάδοση εξ αιτίας του θορύβου είναι η ίδια με αυτή οποιουδήποτε άλλου bit και δεν επηρεάζεται από σφάλματα σε γειτονικά δυαδικά ψηφία. Αυτή η παραδοχή δεν είναι ιδιαίτερα ρεαλιστική, αν λάβουμε υπόψη φυσικά φαινόμενα όπως αστραπές ή ακόμα και «γρατσουνιές» δίσκων, που οδηγούν σε καταιγισμούς σφαλμάτων.

Όπως προαναφεραμε κατά την μετάδοση κάποιου σήματος σε κανάλι επικοινωνίας , η πληροφορία είναι ευάλωτη σε παρεμβολές ή αλλιώς θόρυβο. Ο θόρυβος μπορεί να προέρχεται από φυσικά αίτια όπως κακές καιρικές συνθήκες ή και ακόμη από άλλα κανάλια επικοινωνίας. Αυτό έχει ως αποτέλεσμα να αλλοιώνεται η πληροφορία μας και έτσι ο δέκτης να την λαμβάνει λανθασμένα.

3.1 Βασικές έννοιες κωδίκων

Στην ενότητα αυτή εισάγουμε την έννοια του κώδικα και αναφέρουμε ορισμένες βασικές ιδιότητες, οι οποίες είναι απαραίτητες για την συνέχεια.

3.1.1 Τι είναι κώδικας

Κώδικες, κρυπτογραφημένα μηνύματα, κρυπτογράφηση μηνυμάτων και αποκρυπτογράφηση είναι όλοι όροι που έχουμε ακούσει στο παρελθόν. Ωστόσο, λίγοι άνθρωποι συνειδητοποιούν ότι όλοι χρησιμοποιούν κωδικούς συνεχώς. Η γλώσσα επικοινωνίας μας δεν είναι παρά ένας κωδικός. Όλα όσα θέλουμε να πούμε προφορικά ή γραπτά κωδικοποιούνται σε μια σειρά λέξεων που αποτελούνται από γράμματα ενός αλφαβήτου. Ένα μήνυμα είναι μια συλλογή λέξεων που επικοινωνούμε φωνητικά, γραπτά ή με κάποιον άλλο τρόπο. Μπορούμε να σχηματίσουμε πάρα πολλές «λέξεις» σε μια γλώσσα με αλφάβητο (θεωρητικά άπειρο). Ωστόσο, μόνο μερικά από αυτά έχουν νόημα, δηλ. αποτελούν μέρος του κώδικα γλώσσας επικοινωνίας. Για την ανάπτυξη λέξεων με νόημα και γενικά την κατασκευή της γλωσσικής δομής εφαρμόζονται κανόνες όπως η ορθογραφία, η γραμματική, η σύνταξη κ.λπ. Κατά την αποστολή ενός μηνύματος, είναι πιθανό να τροποποιηθεί (μερικώς) με κάποιο τρόπο. Για παράδειγμα, εάν το μήνυμα μεταδίδεται προφορικά και ο ομιλητής (αποστολέας) δεν έχει καλή άρθρωση ή ο παραλήπτης δεν έχει καλή ακοή ή, πιθανότατα, υπάρχουν ήχοι που παρεμβαίνουν και παρεμποδίζουν την ακριβή λήψη του μηνύματος. Ο ακροατής (ο παραλήπτης του μηνύματος) αναγκάζεται να μαντέψει ποιο μήνυμα στάλθηκε με βάση το μήνυμα που έλαβε (για να αποκωδικοποιήσει το μήνυμα). Διαθέτει έναν κωδικό γλωσσικής

επικοινωνίας για βοήθεια. Συχνά αναγκάζεται να κάνει μορφωμένες εικασίες σχετικά με το μήνυμα με βάση τα «πλαίσια» ή ακόμα και να δίνει μέρη του μηνύματος τυχαία, διακινδυνεύοντας να παραποιηθεί. Ο πλούτος του λεξιλογίου μιας γλώσσας είναι ένα από τα ιδιαίτερα χαρακτηριστικά της, που μας επιτρέπει να μεταδώσουμε ένα ευρύ φάσμα νοημάτων. Δηλαδή, είμαστε σε θέση να μεταδώσουμε τεράστιες ποσότητες δεδομένων. Το μέγεθος των πληροφοριών που μεταφέρονται, καθώς και η αποτελεσματικότητα με την οποία μεταδίδονται, συνδέονται στενά με την ποιότητα των πληροφοριών που μεταδίδονται. Η δομή του γλωσσικού κώδικα, φυσικά, καθορίζει αυτές τις δυνατότητες. Αυτές οι ανάγκες, με τη σειρά τους, επηρεάζουν τον τρόπο κατασκευής ενός αποτελεσματικού γλωσσικού κώδικα σε κάποιο βαθμό. Ωστόσο, δεν πρέπει να παραβλέπουμε τον τρόπο που επικοινωνούμε, δηλαδή τα εργαλεία που έχουμε στη διάθεσή μας για να στείλουμε ένα μήνυμα. Η δομή ενός γλωσσικού κώδικα επικοινωνίας επιβάλλεται περιστασιακά από τα μέσα ενημέρωσης. Είναι σημαντικό να θυμάστε ότι μια γλώσσα πρέπει να είναι ικανή να μεταφέρει τόσο προφορικό όσο και γραπτό λόγο. Οι «ανάγκες» μας ωθούν συχνά να σχεδιάσουμε νέες μεθόδους επικοινωνίας (κώδικες). Ο καθένας μπορεί να φανταστεί αυτό που θέλει όταν λέμε ανάγκες. Από το γεγονός ότι δεν θέλουμε να κοινοποιηθεί ένα μήνυμα με άλλους μέχρι τις μεθόδους μετάδοσης που έχουμε στη διάθεσή μας. Τα σήματα καπνού, για παράδειγμα, χρησιμοποιήθηκαν από τους Ινδιανούς. Τα σύγχρονα ηλεκτρομαγνητικά μέσα είναι πλέον διαθέσιμα για εγγραφή, αποθήκευση και αποστολή μηνυμάτων. Ακόμη, ενώ έχουμε τη βασική χρήση της ηλεκτρικής ενέργειας στη διάθεσή μας, θα πρέπει να σημειώσουμε την εφεύρεση και τη χρήση του κώδικα Μορς. Το παραπάνω είναι ένας θολός ορισμός του κώδικα επικοινωνίας. Θα προσπαθήσουμε να γίνουμε πιο συγκεκριμένοι στην επόμενη παράγραφο.

3.1.2 Ορισμοί και στοιχειώδεις ιδιότητες

Έστω $\mathbb{A}$ = { $a1$, $a2$, … , ar } ένα τυχαίο μη κενό πεπερασμένο σύνολο. Το

σύνολο $\mathbb{A}$ θα το ονομάζουμε αλφάβητο, τα δε στοιχεία του γράμματα ή χαρακτήρες.

Μια πεπερασμένη ακολουθία χαρακτήρων από το αλφάβητο $\mathbb{A}$ θα ονομάζεται στοιχειοσειρά ή λέξη. Μια λέξη συνήθως θα τη συμβολίζουμε με ένα έντονο γράμμα του λατινικού αλφάβητου. Παράδειγμα 1.2.1. Έστω $\mathbb{A}$ = { 2, a, d, $\diamond$ }, τότε τα $\mathbf{a}$ = $a2d2aa$, $\mathbf{b}$ = $d \diamond 2$, $\mathbf{c}$ = a είναι μερικές λέξεις που σχηματίζονται με χαρακτήρες από το αλφάβητο $\mathbb{A}$.

Το σύνολο όλων των λέξεων που μπορούμε να σχηματίσουμε με τους χαρακτήρες από ένα αλφάβητο $\mathbb{A}$ είναι άπειρο (γιατί;) και συμβολίζεται με $\mathbb{A}*$. Το πλήθος των χαρακτήρων σε μια λέξη $\mathbf{u} \in \mathbb{A}*$ ονομάζεται μήκος και συμβολίζεται με $\ell(\mathbf{u})$. Στο προηγούμενο παράδειγμα, οι λέξεις κατά σειρά έχουν μήκη $\ell(\mathbf{a}) = 6$, $\ell(\mathbf{b}) = 3$ και $\ell(\mathbf{u}) = 1$, αντίστοιχα. Κάνουμε την παραδοχή ότι στο σύνολο $\mathbb{A}*$ ανήκει και η κενή λέξη, δηλαδή η λέξη που δεν περιέχει κανέναν χαρακτήρα, η οποία συνήθως συμβολίζεται με $\boldsymbol{\vartheta}$. Το μήκος της κενής λέξης προφανώς ισούται με μηδέν ($\ell(\boldsymbol{\vartheta}) = 0$). Έστω $\mathbf{u}, \mathbf{v} \in \mathbb{A}*$ δύο λέξεις. Τότε, με την παράθεση των δύο λέξεων τη μια δίπλα στην άλλη σχηματίζεται μια άλλη λέξη $\mathbf{z} = \mathbf{uv} \in \mathbb{A}*$. Προφανώς $\ell(\mathbf{z}) = \ell(\mathbf{u}) + \ell(\mathbf{v})$.

3.2 Τεχνικές διόρθωσης λαθών

3.2.1 Αναφορά στις τεχνικές διόρθωσης λαθών

Για την διόρθωση αυτών των λαθών υπάρχουν κάποιες τεχνικές οι οποίες ειναι:

Forward error - control (FEC) :

- Χρησιμοποιώντας έξτρα bit (bit ισοτιμίας) στα μεταδιδόμενα δεδομένα, μπορούμε να εντοπίσουμε και να διορθώσουμε λάθη κατά την διάρκεια της λήψης.
- Μονόδρομη επικοινωνία

Automatic - repeat request (ARQ) :

- Χρησιμοποιούμε έξτρα bit κυρίως για τον εντοπισμό λαθών.
- Ο δέκτης ενημερώνει τον αποστολέα για την ορθότητα ή μη των λαμβανόμενων δεδομένων (ACK (Acknowledgement) ή NACK (NotAcknowledgement) αντίστοιχα).
- Ο αποστολέας επαναμεταδίδει δεδομένα για τα οποία έλαβε NACK.
- Αμφίδρομη επικοινωνία

Υβριδική ARQ (ARQ + FEC) :

- Αμφίδρομη επικοινωνία
- Εντοπισμός λαθών και διόρθωση

Η πιο γνωστή μέθοδος είναι η Automatic repeat request (ARQ) η οποία δουλεύει αποτελεσματικά κυρίως κατά την unicast μετάδοση. Όταν η μέθοδος ARQ εφαρμόζεται σε μία multicast, οι αποδέκτες στέλνουν αιτήσεις για αναμετάδοση χαμένων πακέτων μέσω καναλιών επικοινωνίας προς τον αποστολέα. Η μέθοδος ARQ γενικά είναι σχετικά αποτελεσματική κατά τη multicast μετάδοση και αποτελεί ένα αξιόπιστο εργαλείο. Παρόλα αυτά, όταν ο αριθμός των αποδεκτών αυξάνει, οι περιορισμοί στις δυνατότητες της μεθόδου αυτής αποκαλύπτονται. Ένας σημαντικός περιορισμός είναι το πρόβλημα του καταιγισμού ανατροφοδοτήσεων. Αυτό το φαινόμενο συμβαίνει όταν πολλοί αποδέκτες στέλνουν ταυτόχρονα αιτήσεις για αναμετάδοση στον αποστολέα. Ένα δεύτερο πρόβλημα είναι ότι, για ένα δεδομένο ρυθμό απώλειας πακέτων, όσο ο αριθμός των αποδεκτών αυξάνει, τόσο η πιθανότητα να αναμεταδοθεί ένα πακέτο τείνει προς τη μονάδα. Με άλλα λόγια, ένας μεγάλος μέσος αριθμός από μεταδόσεις χρειάζονται για κάθε πακέτο. Σε ένα ασύρματο περιβάλλον, η μέθοδος ARQ έχει ένα ακόμα μεγάλο μειονέκτημα το οποίο οφείλεται στην προϋπόθεση ύπαρξης αμφίδρομου συνδέσμου επικοινωνίας. Στην περίπτωση μας θα ασχοληθούμε την FEC τεχνική οπου είναι μία μέθοδος ελέγχου λαθών η οποία μπορεί να χρησιμοποιηθεί για να συμπληρώσει ή να αντικαταστήσει άλλες μεθόδους για αξιόπιστη μετάδοση δεδομένων.

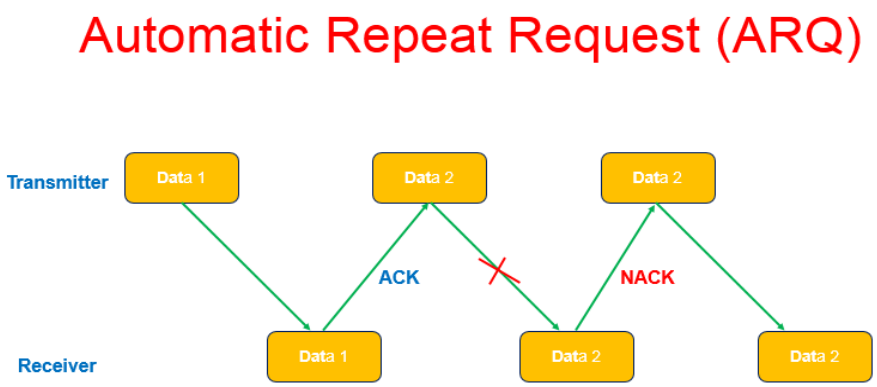
3.2.2 Automatic-repeat request (ARQ)

Ο αυτόματο αίτημα επανάληψης (ARQ), επίσης γνωστό ως αυτόματο επανάληψη ερωτήματος, είναι μια μέθοδος ελέγχου σφαλμάτων για μετάδοση δεδομένων που χρησιμοποιεί επιβεβαιώσεις (μηνύματα που αποστέλλονται από τον παραλήπτη που

υποδεικνύουν ότι έχει λάβει σωστά ένα πακέτο) και χρονικά όρια (καθορισμένες χρονικές περιόδους παρέλθει πριν από τη λήψη επιβεβαίωσης) για την επίτευξη αξιόπιστης μετάδοσης δεδομένων μέσω ενός αναξιόπιστου καναλιού επικοινωνίας. Εάν ο αποστολέας δεν λάβει μια επιβεβαίωση πριν από το χρονικό όριο, συνήθως εκπέμπει ξανά το πακέτο έως ότου ο αποστολέας λάβει μια επιβεβαίωση ή υπερβεί έναν προκαθορισμένο αριθμό αναμεταδόσεων. Οι τύποι πρωτοκόλλων ARQ περιλαμβάνουν ARQ Stop-and-waiting, Go-Back-N ARQ και Selective Repeat ARQ / Selective Reject ARQ. Και τα τρία πρωτόκολλα χρησιμοποιούν συνήθως κάποια μορφή πρωτοκόλλου συρόμενου παραθύρου για να βοηθήσουν τον πομπό να προσδιορίσει ποια (εάν υπάρχουν) πακέτα πρέπει να μεταδοθούν εκ νέου. Αυτά τα πρωτόκολλα βρίσκονται στον σύνδεσμο δεδομένων ή στα επίπεδα μεταφοράς επίπεδα 2 και 4 του μοντέλου OSI.

Το πρωτόκολλο ελέγχου μετάδοσης χρησιμοποιεί μια παραλλαγή του Go-Back-N ARQ για να εξασφαλίσει αξιόπιστη μετάδοση δεδομένων μέσω του πρωτοκόλλου Διαδικτύου, το οποίο δεν παρέχει εγγυημένη παράδοση πακέτων. με Επιλεκτική Επιβεβαίωση (SACK), χρησιμοποιεί Selective Repeat ARQ. Η ασύρματη δικτύωση IEEE 802.11 χρησιμοποιεί αναμετάδοση ARQ στο επίπεδο σύνδεσης δεδομένων.

Το πρότυπο ITU-T G.hn, το οποίο παρέχει έναν τρόπο δημιουργίας ενός τοπικού δικτύου υψηλής ταχύτητας (έως 1 Gbit / s) χρησιμοποιώντας υπάρχουσες καλωδιώσεις κατοικιών (γραμμές τροφοδοσίας, τηλεφωνικές γραμμές (ADSL) και ομοαξονικά καλώδια), χρησιμοποιεί Επιλεκτική επανάληψη ARQ για διασφάλιση αξιόπιστης μετάδοσης σε θορυβώδη μέσα. Τα συστήματα ARQ χρησιμοποιήθηκαν ευρέως στο ραδιόφωνο μικρών κυμάτων για να διασφαλιστεί η αξιόπιστη παράδοση δεδομένων, όπως για τηλεγραφήματα. Αυτά τα συστήματα ήρθαν σε μορφές που ονομάζονταν ARQ-E και ARQ-M, οι οποίες περιελάμβαναν επίσης τη δυνατότητα πολλαπλών δύο ή τεσσάρων καναλιών. Υπάρχουν διάφορα διπλώματα ευρεσιτεχνίας για τη χρήση του ARQ σε περιβάλλοντα ζωντανής συνεισφοράς βίντεο. Σε αυτά τα περιβάλλοντα υψηλής απόδοσης χρησιμοποιούνται αρνητικές αναγνωρίσεις για τη μείωση των γενικών εξόδων.

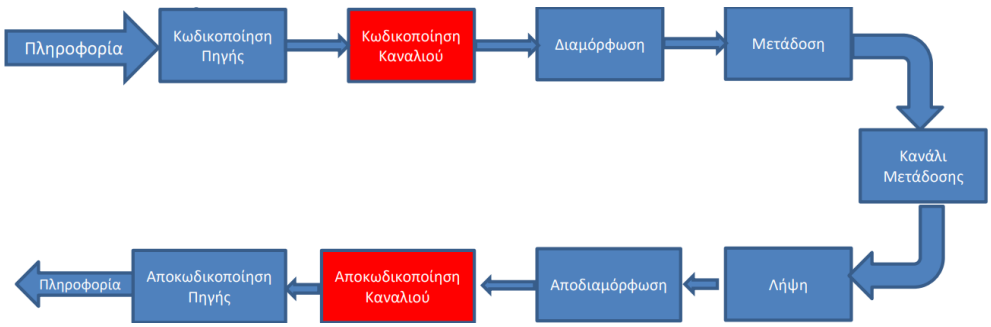


Εικόνα 9: Automatic repeat request i

3.2.3 Forward error - control (FEC)

Το βασικό χαρακτηριστικό των μηχανισμών FEC είναι ότι ο αποστολέας προσθέτει επιπλέον πληροφορία στα μηνύματα προς τον αποδέκτη. Αυτά τα επιπλέον δεδομένα δίνουν τη δυνατότητα στον αποδέκτη να ανακατασκευάσει την αρχική πληροφορία. Αναπόφευκτα, αυτού του είδους οι μηχανισμοί προκαλούν μία σταθερή επιβάρυνση στον όγκο των μεταδιδόμενων δεδομένων και είναι υπολογιστικά ακριβοί. Όμως η χρήση των τεχνικών FEC έχει πολύ δυνατά πλεονεκτήματα. Η κωδικοποίηση περιορίζει το φαινόμενο των ανεξάρτητων απωλειών πακέτων σε διαφορετικούς αποδέκτες. Αυτό κάνει τους μηχανισμούς αυτούς να μπορούν να κλιμακωθούν σε πολλούς αποδέκτες ανεξάρτητα από το ρυθμό απώλειας πακέτων. Επιπλέον, η δραματική μείωση στο ρυθμό απώλειας πακέτων περιορίζει σημαντικά την ανάγκη για την αποστολή ανατροφοδότησης στον αποδέκτη.

Επομένως, ένα κανάλι ανατροφοδότησης μπορεί να μην είναι απαραίτητο ή αν χρησιμοποιείται τέτοιου είδους κανάλι, η πιθανότητα εμφάνισης καταιγισμού από ανατροφοδοτήσεις εκμηδενίζεται. Είναι προφανές ότι οι μηχανισμοί FEC είναι τόσο απλοί ώστε να εξυπηρετούν ένα από τους βασικούς στόχους των multicast κινητών υπηρεσιών και ο οποίος είναι η επεκτασιμότητα σε εφαρμογές με χιλιάδες χρηστών. Αυτός είναι και ο λόγος που το 3GPP συστήνει τη χρήση του FEC επιπέδου εφαρμογής για την υπηρεσία MBMS και πιο συγκεκριμένα υιοθετεί τη χρήση του κώδικα Raptor FEC .



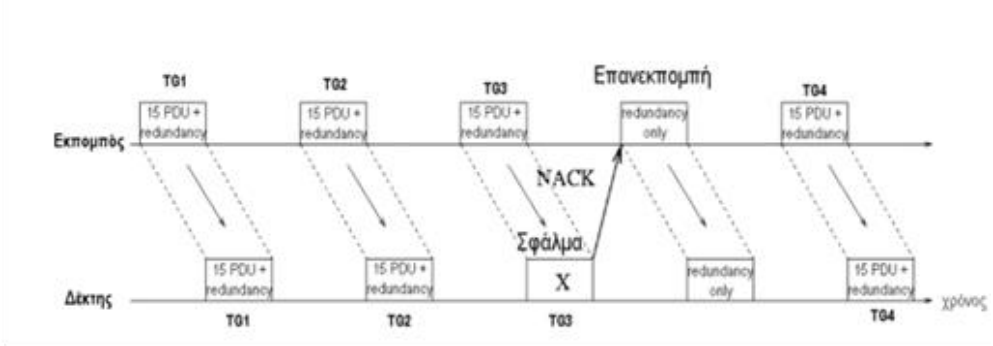
Εικόνα 10: Μοντέλο εφαρμογής διόρθωσης i

Μεγάλο κομματι στις FEC τεχνικές διόρθωσης λαθών ειναι οι κώδικες block οπου κωδικοποιεί δεδομένα σε block. Πρακτικά η κωδικοποίηση με κώδικες block ειναι σαν «χάρτης» ή αλλιως κωδικολέξη μηκους n bit όπου εισάγεται στον κωδικοποιητή για κάθε k bit μιας λεξης δεδομένων. Οι γραμμικοί μπλοκ κώδικες είναι γενικά οι πιο ευρέως χρησιμοποιούμενοι κώδικες.

3.2.4 Υβριδική ARQ (ARQ+FEC)

Η τεχνική υβριδικού HARQ αποτελεί συνδυασμό των τεχνικών FEC και ARQ. Σε ένα σύστημα αμφίδρομης επικοινωνίας ο έλεγχος σφαλμάτων μπορεί να επιτευχθεί με αναγνώριση σφαλμάτων στο δέκτη (error detection) και αίτηση για επανεκπομπή της απολεσθείσας πληροφορίας (ARQ). Το κυριότερο πλεονέκτημα του ARQ με

παράλληλη χρήση της τεχνικής FEC είναι ότι ο εντοπισμός σφαλμάτων που γίνεται στο δέκτη απαιτεί πολύ πιο απλό εξοπλισμό σε σχέση με αυτόν που θα χρειαζόταν για διόρθωση σφαλμάτων (error correction). Επιπλέον, το HARQ είναι αποδοτικότερο με την έννοια ότι ζητείται να επανεκπεμθεί η πληροφορία, με την αποστολή ενός NACK μόνο όταν προκύψει σφάλμα. Οι μηχανισμοί του HARQ ανήκουν στο RLC υποεπίπεδο. Το RLC είναι υποεπίπεδο ελέγχου ραδιοφάσματος και βρίσκεται στο 2ο επίπεδο του OSI δηλαδή το επίπεδο ζεύξης ενός δικτύου UMTS Το RLC υπάρχει τόσο στο Δικτυακό Ελεγκτή
Ραδιοφάσματος RNC (Radio Network Controller) όσο και στον εξοπλισμό του χρήστη. Σκοπός του είναι η εξασφάλιση αξιόπιστης μετάδοσης και ανταλλαγής πακέτων μεταξύτου RNC και του χρήστη.



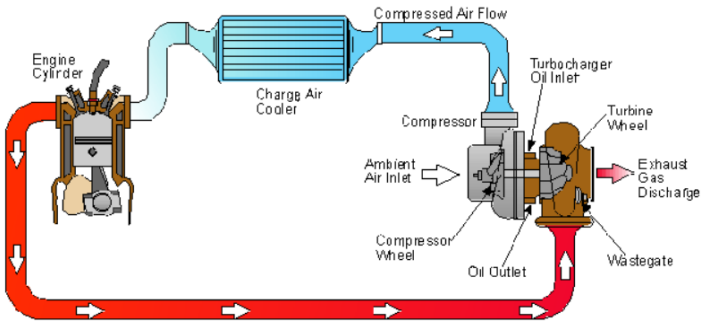
Εικόνα 11: Υβριδική ARQ i

3.3 Εναλλακτικές επιλογες

Πριν αναφερθούμε στους κώδικες μπλοκ, στο επόμενο κεφάλαιο, θα αναφέρουμε τις επιλογές που έχουμε στην κωδικοποίηση καναλιών.

3.3.1 Κώδικες Turbo

Οι κώδικες Turbo έχουν πάρει το όνομά τους από το γεγονός πως ο αποκωδικοποιητής χρησιμοποιεί ανάδραση, όπως ένας turbo κινητήρα. Οι κώδικες turbo θεωρούνται περισσότερο αποδοτικοί από τους FEC. Ενώ αντίστοιχα είναι σχήματα που χρησιμοποιούν και συνδυάζουν γνωστούς κώδικες όπως συνελικτικούς ή κώδικες block. Οι Turbo κώδικες συνήθως χρησιμοποιούνται σε εφαρμογές χαμηλής ισχύος όπως δορυφορικές επικοινωνίες.



Εικόνα 12: Μοντέλο αναπαράστασης Turbo i

Χαρακτηριστικά κωδικών Turbo:

- Παράλληλη διαδοχική κωδικοποίηση
- Αναδρομικοί συνελικτικοί κωδικοποιητές
- Ψευδο-τυχαία διεμπλοκή
- Επαναληπτική αποκωδικοποίηση

Η απόδοση των κωδικών turbo και η σύγκριση τους γίνεται με ρυθμό ½, K=5 (κώδικας turbo), και K=14 (συνελικτικός κώδικας)

Πλεονεκτήματα και μειονεκτήματα κωδικών Turbo:

- **Πλεονεκτήματα:**

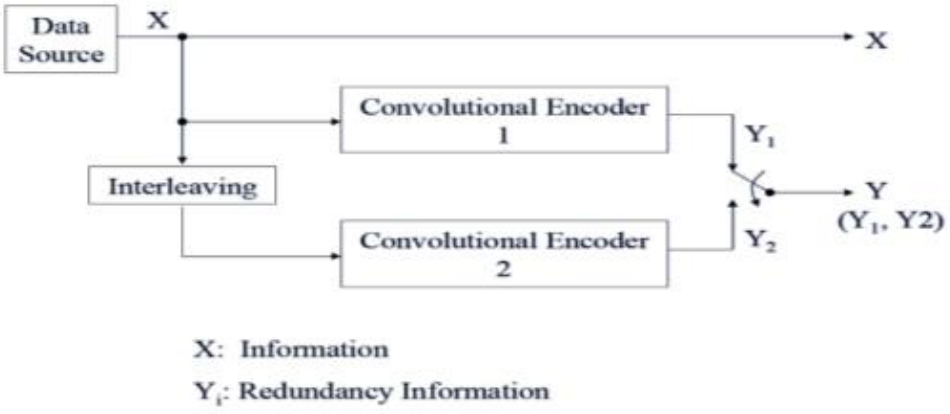
1.Αξιοσημείωτη απόδοση ισχύος σε AWGN και flat-fading κανάλια για μετρίως χαμηλό BER.
2. Κατάλληλοι για την παροχή υπηρεσιών πολυμέσων.

- **Μειονεκτήματα:**

1.Μεγάλη καθυστέρηση
2.Κακή απόδοση σε πολύ χαμηλό BER.
3. Επειδή οι κώδικες turbo λειτουργούν σε πολύ χαμηλό SNR, η εκτίμηση καναλιού και η παρακολούθησης είναι ένα κρίσιμο ζήτημα.

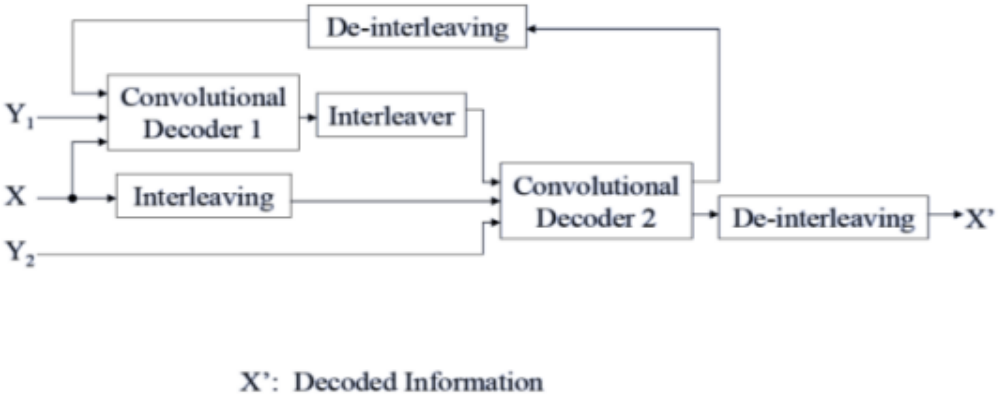
Η λειτουργία κωδικών turbo μπορεί να εφαρμοστεί και για λύσεις άλλων προβλημάτων, όπως για παράδειγμα στην βελτίωση και απόδοση κωδικοποιημένων συτημάτων πολλαπλής πρόσβασης.

Κωδικοποιητής Turbo



Εικόνα 13: Κωδικοποιητής Turbo i

Αποκωδικοποιητής Turbo



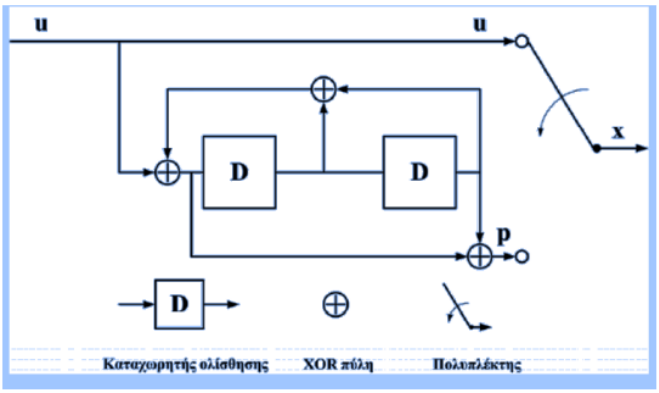
Εικόνα 14: Αποκωδικοποιητής Turbo i

3.3.2 Συνελικτικοί κώδικες

Οι συνελικτικοί κώδικες διαθέτουν στοιχεία μνήμης, με αποτέλεσμα να διαφέρουν από τους κώδικες block. Αυτό σημαίνει αυτόματα ότι η έξοδος τους δεν εξαρτάται μόνο από την τρέχουσα είσοδο, αλλά και από τις προηγούμενες καταστάσεις.
Οι συνελικτικοί κώδικες χαρακτηρίζονται από 3 παραμέτρους n, k, m, όπου:

- n είναι το πλήθος των bits εξόδου
- k είναι το πλήθος των bits εισόδου
- m είναι το πλήθος των στοιχείων μνήμης

Με ρυθμό κώδικα R=k/n και μήκος περιορισμού $L = k(m - 1)$. Μήκος περιορισμού είναι το πλήθος των bits της μνήμης που επηρεάζουν την παραγωγή των n bits εξόδου.
Οι συνελικτικοί κώδικες ανήκουν στην κατηγορία των κωδίκων trellis, με αποτέλεσμα να κωδικοποιούν δεδομένα συνεχώς.



Εικόνα 15: Μοντέλο συνελιξης i

Κωδικοποιητής για έναν συνελικτικό κώδικα είναι ο δυαδικός συνελικτικός κωδικοποιητής, με ρυθμό R=1/2 και μνήμη της τάξης m=2
Στην από πάνω εικόνα βλέπουμε το ακολουθιακό λογικό κύκλωμα μνήμης m, από την μηχανή πεπερασμένων καταστάσεων.

Κωδικοποίηση

Βάζοντας ως είσοδο το bit 1 στον κωδικοποιητή, παράγεται η «έξοδος παρόρμησης»
Η έξοδος του κωδικοποιητή μπορεί να υπολογιστεί συνελίσοντας την είσοδο u με την έξοδο παρόρμησης g είναι v=u*g .

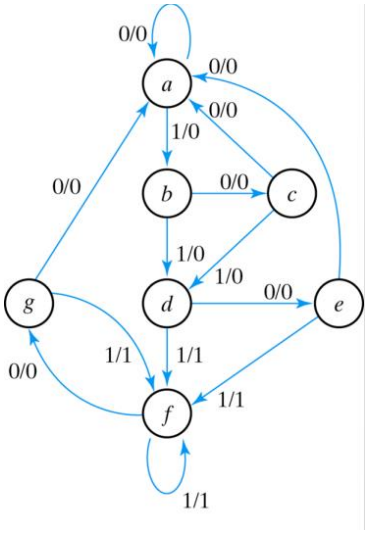
Τρόποι Αναπαράστασης

Υπάρχουν τρεις γραφικοί τρόποι αναπαράστασης ενός συνελεκτικού κωδικοποιητή:

1. Διάγραμμα καταστάσεων
2.– Δέντρο
3.– Διάγραμμα Trellis

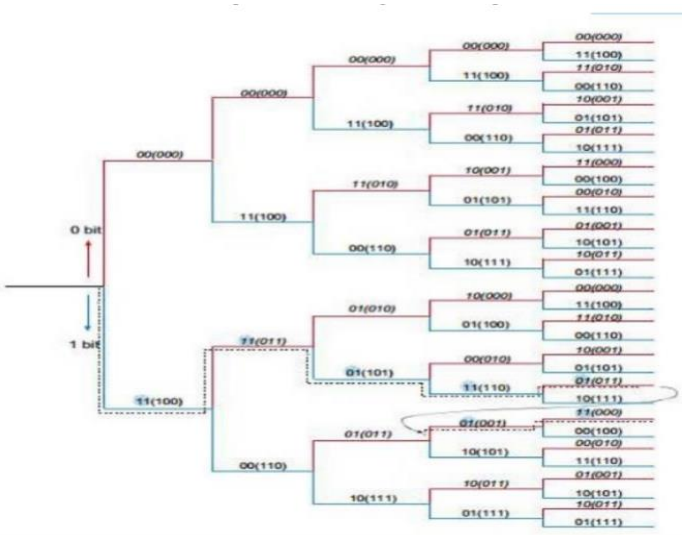
Ακολουθούν γραφικές απεικονίσεις για το καθένα από τα παραπάνω:

1. Διάγραμμα καταστάσεων



Εικόνα 16: Διάγραμμα καταστάσεων

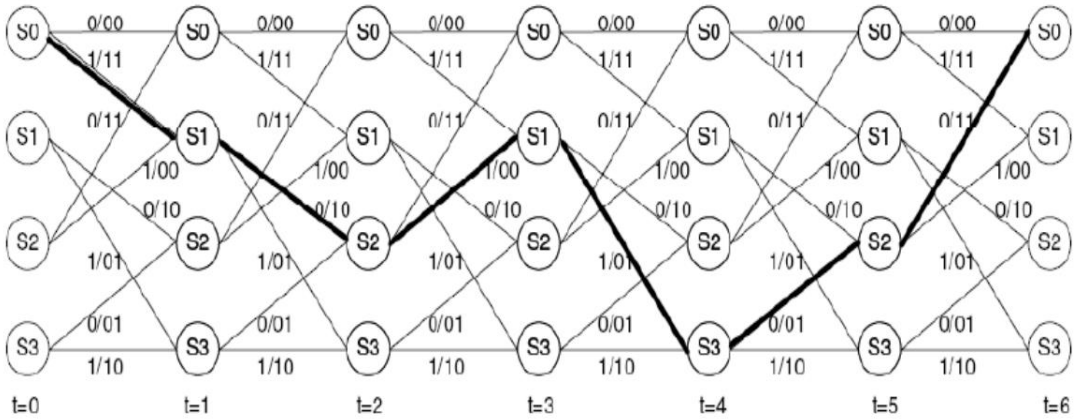
2. Δέντρο



Εικόνα 17: Δέντρο αναπαράστασης i

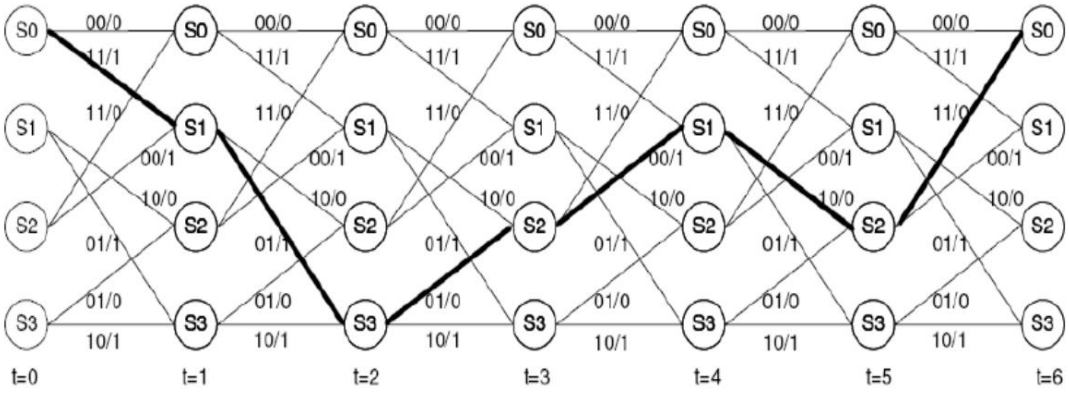
3.Διάγραμμα Trellis

Παράδειγμα: Για είσοδο 101100, η αλληλουχία καταστάσεων και η έξοδος είναι η εξής:



Εικόνα 18: Διάγραμμα Trellis i

Αποκωδικοποιηση: για λαμβανόμενη έξοδο 11 01 01 00 10 11, έχουμε



Εικόνα 18: Διάγραμμα Trellis ii

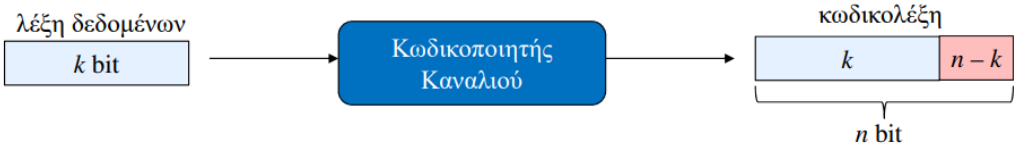
Οι συνελικτικοί κώδικες είναι ένα μεγάλο κομμάτι της κωδικοποίησης καναλιού και για λόγους συντομίας δεν θα αναφερθούμε πιο αναλυτικά.

Κεφάλαιο 4ο
ΚΩΔΙΚΕΣ BLOCK

4.1 Κωδικες block

4.1.1 Τι είναι οι κώδικες block

Οι κώδικες μπλοκ ειναι γραμμικοί κώδικες μονοσήμανσης απεικόνισης στοιχείων απο ενα σύνολο A σε ενα άλλο σύνολο B. Δηλαδή, σε κάθε στοιχείο του μη κενού συνόλου A αντιστοιχεί ένα και μοναδικό στοιχείο του μη κενού συνόλου B, αυτή η μορφή απεικόνισης λέγεται ένα προς ένας (1-1) ή αλλιως Injective function. Τα στοιχεία του συνόλου A ορίζονται ως λέξεις πληροφορίας (ορίζονται) και τα στοιχεία του συνόλου B ορίζονται ως κώδικες λέξεις (codeword) . Οι κώδικές λέξεις σε ένα (n,k) μπλοκ κώδικα c αποτελείται από ένα σύνολο q^k για n διανύσματα οπού, q είναι τα σύμβολα του αλφάβητου του κώδικα. Ο μπλοκ κωδικοποιητής , ουσιαστικά , αντιστοιχεί ένα μήνυμα από k σύμβολα στις αντίθετες κώδικές λέξεις. Από την μαθηματική δομή του κώδικα προκύπτει ότι τα n,k είναι επιπλέον σύμβολα για τα οποία ισχύει ότι n > k . Για να είναι δυνατή η διόρθωση λαθών είναι αναγκαίο η απεικόνιση να είναι μονοσήμαντη . Βέβαια η αντιστοίχιση μπορεί να γίνει με πολλούς διαφορετικούς τρόπους. Επίσης, η αναπαράσταση ενός μπλοκ κώδικα μπορεί να γίνει με μια πλήρης λίστα για μεγάλο k , αυτό όμως, δεν συμφέρει ούτε ως προς το υλικό , αλλά ούτε για την αποκωδικοποίηση. Ένα βασικό χαρακτηριστικό ενός μπλοκ κώδικα είναι ότι αποτελεί μια διάταξη χωρίς μνήμη. Αφού, η έξοδος, δηλαδή η κωδική λέξη , δεν εξαρτάται από προηγούμενες εισόδους αλλά μόνο από την είσοδο στην δεδομένη χρονική στιγμή. Ένας μπλοκ κώδικας μπορεί να θεωρηθεί γραμμικός αν και μόνο αν ισχύει ότι στο πεδίο F_q οπού q είναι τα σύμβολα για μήκος n οι κώδικές λέξεις q^k σχηματίζουν ένα διάνυσμα k διαστάσεων . Ο ρυθμός του κώδικα είναι R = k/n, οπού k είναι το μήκος του κώδικα και n η διάσταση του πίνακα.



Εικόνα 19: Κωδικολέξη i

4.1.2 Συστηματικοί και γραμμικοί κωδικες Block

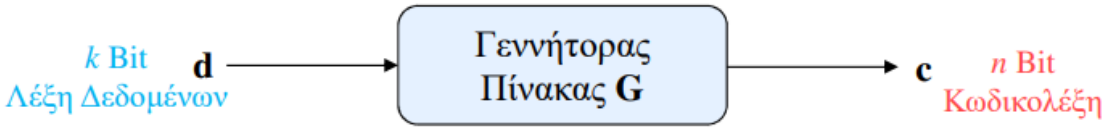
Οι κώδικες μπλοκ, των οποιων οι λεξεις δεδομένων τοποθετούνται στην αρχή (ή στο τέλος) των κωδικολέξεων αναλλοίωτες, ονομάζονται συστηματικοί (systematic). Για την κατηγορία των block κωδίκων, οι συστηματικοί είναι πιο αποδοτικοί. Τα k bits πληροφορίας συν τα r bits ισοτιμίας σχηματίζουν την κωδική λέξη ($k + r$ = n). Στους συστηματικούς γραμμικούς block αλγόριθμους, τα r bits ισοτιμίας τοποθετούνται στο τέλος του block.

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

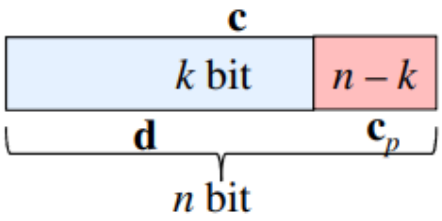
Όπως είδαμε και στο Κεφάλαιο 2, ένας δυαδικός κώδικας, C, είναι ένα σύνολο κωδικών λέξεων. Οι κωδικές λέξεις είναι ακολουθίες δυαδικών ψηφίων. Για παράδειγμα, ο κώδικας που απαρτίζεται από όλες τις λέξεις μήκους δύο ψηφίων είναι C ={00, 10, 01, 11}. Ένας κώδικας ονομάζεται ισομήκης κώδικας (ή κώδικας μπλοκ) αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος. Στο κεφάλαιο αυτό θα μας απασχολήσουν μόνο κώδικες μπλοκ. Το πλήθος των κωδικών λέξεων ενός κώδικα C συμβολίζεται με |C|.

Ενας κώδικας μπλοκ ονομάζεται **γραμμικός** (**linear**) οταν το αποτέλεσμα της πρόσθεσης, με αριθμητική modulo-2 , οποιονδήποτε δυο κωδικολέξεων ειναι μια αλλη κωδικολέξη του κώδικα. Ενας συστηματικος γραμμικός κώδικας μπλοκ γράφεται:

$$\mathbf{c} = \mathbf{d}\,\mathbf{G}$$



Εικόνα 20: Συστηματικός Μπλοκ κώδικας i



Εικόνα 21:Κωδικολέξη i

$$
\begin{aligned}
c_1 &= d_1 \\
c_2 &= d_2 \\
&\vdots \\
c_k &= d_k
\end{aligned}
$$

k Bit
Λέξη Δεδομένων

$$
\begin{aligned}
c_{k+1} &= p_{11}\, d_1 \oplus p_{12}\, d_2 \oplus \cdots \oplus p_{1k}\, d_k \\
c_{k+2} &= p_{21}\, d_1 \oplus p_{22}\, d_2 \oplus \cdots \oplus p_{2k}\, d_k \\
&\vdots \\
c_n &= p_{m1}\, d_1 \oplus p_{m2}\, d_2 \oplus \cdots \oplus p_{mk}\, d_k
\end{aligned}
$$

$m = n - k$
Bit Ελέγχου

Εικόνα 21:Κωδικολέξη ii

4.1.3 Παράδειγμα γραμμικού κώδικα

Η κωδικοποίηση για κάθε κωδικολέξη ενός συστηματικού γραμμικού κώδικα μπλοκ σχηματίζεται βάσει του γεννήτορα πίνακα (generator matrix) G διάστασης k x n :

$$
\mathbf{G} = \underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}}_{\mathbf{I}_k \ (k \times k)} \underbrace{\begin{bmatrix} p_{11} & p_{21} & \cdots & p_{m1} \\ p_{12} & p_{22} & \cdots & p_{m2} \\ \vdots & \vdots & \cdots & \vdots \\ p_{1k} & p_{2k} & \cdots & p_{mk} \end{bmatrix}}_{\mathbf{P} \ (k \times m)} = [\mathbf{I}_k \ \mathbf{P}]
$$

Εικόνα 22: Γεννήτορας πίνακας i

Παραδειγμα : Εστω γεννήτορας πίνακας κώδικα μπλοκ , διαστασης k x n = 3 x 6 δηλαδη ο κώδικας μπλοκ ειναι (n, k) = (6,3) :

Ο κώδικας ικανοποιει το όριο Hamming αφου

$$n \leq 2^m - 1 \Leftrightarrow 6 \leq 2^3 - 1 = 7$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

με πολ/σμο της κάθε λέξης **d** με τον πίνακα **G** προκύπτουν οι αντίστοιχες κωδικολέξεις **c**

Λέξη Δεδομένων	Κωδικολέξη
000	000000
001	001110
010	010011
011	011101
100	100101
101	101011
110	110110
111	111000

4.1.4 Κώδικες Hamming και μετρικά σύγκρισης

Οι κώδικες Hamming είναι γραμμικοί, block κώδικες με:

$$n = 2^m - 1, k = 2^m - m - 1, d_{min} = 3, \text{όταν } m \geq 3$$

Ο πίνακας ισοτιμίας περιγράφεται από όλους τους συνδυασμούς ψηφιών εκτός από αυτόν με όλα τα ψηφία ίσα με το μηδέν.

- **Βάρος Hamming:** Το πλήθος των μη-μηδενικών στοιχείων μιας κωδικής λέξης.

$$w_{min} = \min_{\mathbf{c}_i \neq 0} w(\mathbf{c}_i)$$

- **Ελάχιστη Απόσταση Κώδικα:** Η ελάχιστη απόσταση Hamming για όλα τα ζεύγη κωδικών λέξεων του κώδικα.

$$d_{min} = \min_{\mathbf{c}_i, \mathbf{c}_j} d(\mathbf{c}_i, \mathbf{c}_j), i \neq j$$

- **Ελάχιστο Βάρος Κώδικα:** Το ελάχιστο βάρος που μπορεί να έχει μία κωδική λέξη, αν αγνοήσουμε την κωδική λέξη που αποτελείται μόνο από μηδενικά.

$$d(\mathbf{c}_i, \mathbf{c}_j) = w(\mathbf{c}_i \oplus \mathbf{c}_j) = w(\mathbf{c}_l)$$

- **Θεώρημα:** Σε οποιονδήποτε γραμμικό κώδικα η ελάχιστη απόσταση Hamming ισούται με το ελάχιστο βάρος του κώδικα.

Απόδειξη: Είναι, δηλαδή, κάθε απόσταση Hamming γράφεται σαν βάρος κάποιας κωδικής λέξης και άρα η ελαχιστοποίηση γίνεται πάνω στα ίδια σύνολα.

- **Απόσταση Hamming :** Μια από τις ιδιότητες των γραμμικών κωδίκων είναι ότι αν αθροίσουμε δυο κώδικές λέξεις το αποτέλεσμα θα είναι επίσης μια κωδικη λέξη . Σε μια κωδική λέξη ο αριθμός της σε bits που ισούται με την μονάδα καλείται βάρος Hamming της κωδικός λέξης και συμβολίζεται με το γράμμα w . Η διαφορά των θέσεων στις οποίες ορίζονται δυο κώδικές λέξεις αποτελεί την απόσταση Hamming και συμβολιζεται με το γραμμα d. Σε ένα γραμμικο μπλοκ κωδικα πρεπει το βαρος Hamming να ισουται με την ελαχιστη αποσταση Hamming δηλαδη w_{min}= d_{min}. Επομένως σε κάθε γραμμικό μπλοκ κωδικα υπαρχει η δυνατοτητα διορθωσης οπου πρεπει να ισχυει ότι $t \leq (d_{min} - 1) / 2$.

  Πχ: Οι λεξεις 01110 και 01111 εχουν αποσταση Hamming ίση με 1 γιατι εχουν μονο 1 διαφορετικο ψηφιο / bit.

- **Ευκλείδεια απόσταση :**
  Εάν χ1 = [$a1\ a2 \dots an$] και χ2 = [$b1\ b2 \dots bn$] δύο κωδικές λέξεις μεγέθους n, τότε η Ευκλείδεια απόσταση ορίζεται από τη σχέση

$$E_{dis} = \sqrt{\sum_{i=1}^{n} (|a_i - b_i|^2)}$$

  Η επιλογή μετρικού γινεται ανάλογα με το κανάλι μετάδοσης, δηλαδή εαν εχουμε καναλι Gaussian με υψηλό SNR τοτε επιλέγουμε την Ευκλείδεια απόσταση ενώ εαν έχουμε Raleigh Fading επιλέγουμε την απόσταση Hamming.

Παράδειγμα για κατανόηση:

Έστω μια κωδική λεξη **c** με **n** bits και μήνυμα προς κωδικοποίηση **d** με **k** bits . Με γεννήτορα πίνακα **G** διάστασης k x n= 3x6

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Ένας γραμμικός κώδικας $\boldsymbol{n}, \boldsymbol{k}$ ορίζεται από τον πίνακα γεννήτορα $\boldsymbol{G}[\boldsymbol{k} \times \boldsymbol{n}]$.
Οπου ο G αναλύεται ως εξής:
–$\boldsymbol{G}$ = [$\mathbf{I}\boldsymbol{k}$| $\boldsymbol{P}$] , όπου ο $\mathbf{P}$ έχει μέγεθος $\boldsymbol{k} \times (\boldsymbol{n} - \boldsymbol{k})$ και ορίζεται από τον κώδικα (n, k) και $\boldsymbol{Ik}$ ο μοναδιαίος πίνακας τάξης k

Συνεπώς ο κώδικας μπλοκ είναι **(n,k)=(6,3)**

4.2 Αποκωδικοποίηση

4.2.1 Soft αποκωδικοποίηση

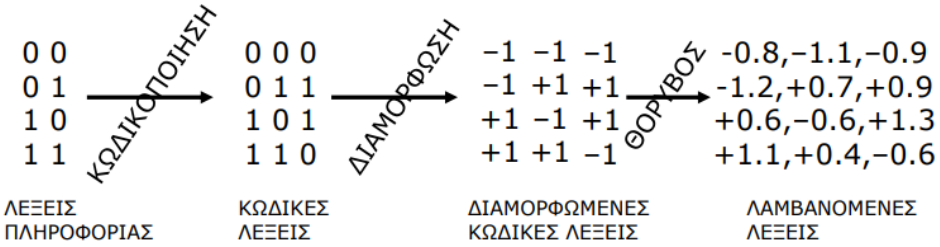
1. Υπολογίζουμε τις Ευκλείδειες αποστάσεις μεταξύ όλων των κωδικών λέξεων που έχουν διαμορφωθεί και των δειγμάτων που έχουν ληφθεί.
2. Επιλέγουμε την κωδική λέξη που έχει τη μικρότερη Ευκλείδεια απόσταση.
3. Για να βρουμε τη λέξη - πληροφορία, αντιστρέφουμε την αντιστοίχιση.

Στην Soft αποκωδικοποίηση η λήψη και η αποκωδικοποίηση γίνονται ταυτόχρονα .

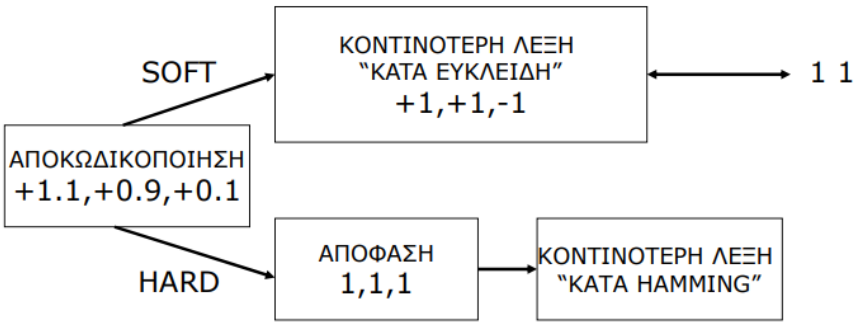
4.2.2 Hard αποκωδικοποίηση

1. Πραγματοποιούμε αποδιαμόρφωση των δειγμάτων που ελήφθησαν και καταλήγουμε με τα αντίστοιχα δυαδικά δεδομένα.
2. Υπολογίζουμε την πλησιέστερη κωδική λέξη με βάση την απόσταση Hamming. (Συνήθως χρησιμοποιώντας έναν πίνακα)
3. Για να βρουμε τη λέξη - πληροφορία, αντιστρέφουμε την αντιστοίχιση.

Στην Hard αποκωδικοποίηση γίνεται πρώτα η λήψη και μετα η αποκωδικοποίηση.



Εικόνα 23:Κωδικοποίηση i



Εικόνα 24: Αποκωδικοποίηση i

4.3 Κυκλικοί κώδικες block

Τώρα θα στρέψουμε την προσοχή μας σε μια ειδική κατηγορία γραμμικών κωδίκων, τους κυκλικούς κώδικες. Η κυκλική μετατόπιση κ(x) μιας λέξης x είναι η λέξη y που έχει ως πρώτο ψηφίο της το τελευταίο ψηφίο της x και τα υπόλοιπα ψηφία της προκύπτουν με απλή μετατόπιση κατά μία θέση προς τα δεξιά όλων των ψηφίων της x. Για παράδειγμα, κ(010011) = 101001 και κ(101001) = 110100. Με τη βοήθεια της συνάρτησης της κυκλικής μετατόπισης μπορούμε να ορίσουμε τους κυκλικούς κώδικες,

Ορισμός:

Ένας γραμμικός κώδικας C καλείται κυκλικός αν η κυκλική μετατόπιση κάθε κωδικής λέξης είναι και αυτή κωδική λέξη.

Ένα μήνυμα μήκους k bits: d = [d0, d1, … , dk−1] μπορεί να περιγραφεί

με ένα πολυώνυμο: $d(x) = d_0 + d_1x^1 + d_2x^2 + \cdots + d_{k-1}x^{k-1}$

Ο κώδικας ορίζεται από το πολυώνυμο γεννήτορα:

$$g(x) = g_0 + g_1x^1 + \cdots + g_rx^r \text{ με } g_0 = 1 \text{ και } g_r = 1$$

Μία κωδική λέξη **c** = [c0, c1, … , cn−1] για το d μπορεί να περιγραφεί με την βοήθεια πολυωνύμου.

$$c(x) = Rem\left(\frac{x^r d(x)}{g(x)}\right) + x^r d(x)$$

Το υπόλοιπο του Rem είναι ένα πολυώνυμο μέχρι τάξης x^{r-1} (r bits ισοτιμίας) ονομάζεται πολυώνυμο ελέγχου ισοτιμίας του d (x) . Στο τέλος σημειώνεται πως όλοι οι υπολογισμοί είναι με βάση του modulo -2.

Παράδειγμα:

Παράδειγμα κυκλικού κώδικα (7,4) με πολυώνυμο γεννήτορα:

$g(x)$ = 1 + x^2 + x^3

Έστω μήνυμα d=0101, τότε:

d (x) = x^1 + x^3

x^3d (x) = x^4 + x^6

Επομένως: $Rem\left(\frac{x^3 d(x)}{g(x)}\right) = 1$

$c(x) = 1 + x^4 + x^6$

Άρα c = 1 0 0 0 1 0 1, με τα 3 πρώτα bits να είναι τα bit ισοτιμίας

και τα υπόλοιπα τα bit πληροφορίας.

Παράδειγμα 2:

Στην αποκωδικοποίηση, το λαμβανόμενο $r\ (x) = c\ (x) + e\ (x)$ με τα μη-μηδενικά bits του $e\ (x)$ υποδεικνύουν τα λάθη και το πολυώνυμο σύνδρομο λάθους υπολογίζεται ως εξής:

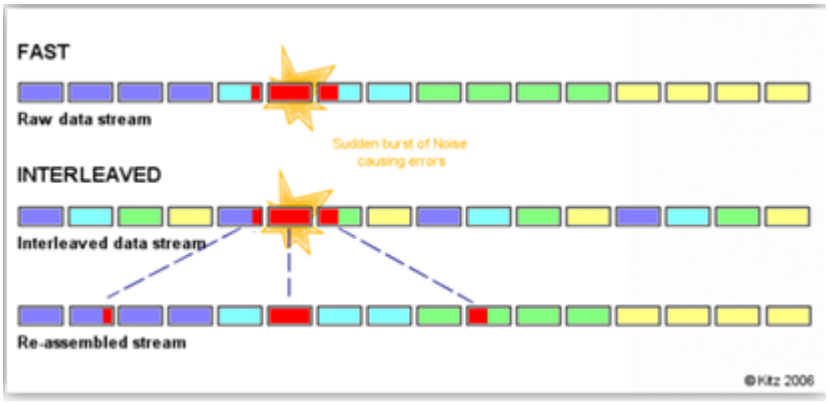
$$Rem\left(\frac{c(x)+e(x)}{g(x)}\right) = Rem\left(\frac{e(x)}{g(x)}\right) = s(x)$$

- ✓ Εάν το $s(x)$ είναι μηδενικό, τότε το λαμβανόμενο σήμα είτε δεν περιέχει λάθη είτε περιέχει λάθη που δεν μπορούν να ανιχνευθούν.
- ✓ Εάν το $s(x)$ είναι μη μηδενικό, τότε θα λάθη ανιχνεύονται και διορθώνονται.

4.4 Διεμπλοκή (Interleaving)

4.4.1 Διεμπλοκή

Το βασικό πρόβλημα είναι ότι σε περιπτώσεις όπου κατά την μετάδοση ψηφιακής πληροφορίας συμβαίνει κάποιο λάθος, αυτό αναμένεται να επηρεάσει συνεχόμενα bits (burst errors) Σε αυτή την περίπτωση οι αλγόριθμοι ανίχνευσης και διόρθωσης λαθών αποτυγχάνουν.



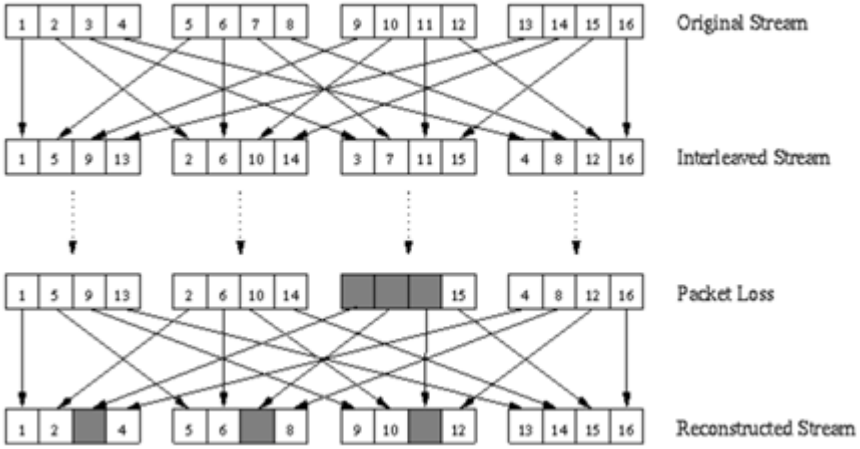
Εικόνα 25: Διεμπλοκή i

Η λύση είναι πριν την εφαρμογή κωδικοποιήσεων καναλιού, εφαρμόζουμε Διεμπλοκή (interleaving).

Ορισμός:

Έστω ότι έχουμε ένα μήνυμα προς μετάδοση, το οποίο αποστέλλεται σε blocks.

Διεμπλοκή είναι η διαδικασία «ανάμιξης» blocks από bit με σκοπό την αντιμετώπιση των burst λαθών.



Εικόνα 25: Διεμπλοκή ii

Η τεχνική interleaving χρησιμοποιείται για να προσθέσει τυχαιότητα στις θέσεις των σφαλμάτων, ιδίως στην περίπτωση που αυτά παρουσιάζουν πυκνώματα σε μία διάσταση τυπικά στον χρόνο.

οι ριπές σφαλμάτων ή η απώλεια μια συχνότητας στη μετάδοση με διαμόρφωση OFDM (Orthogonal Frequency Division Multiplexing), η οποία χρησιμοποιείται στην ψηφιακή τηλεόραση.Εάν τα σφάλματα αυτά καταφέρουμε να τα διασπείρουμε, να τα απομακρύνουμε, δηλαδή, αρκετά το ένα από το άλλο, υπάρχουν περισσότερες δυνατότητες να διορθωθούν (με τους τυπικούς αλγόριθμους προληπτικής διόρθωσης σφαλμάτων).

Έτσι στον πομπό, τα κωδικοποιημένα bits αναδιατάσσονται με συγκεκριμένο τρόπο. Στον δέκτη επανέρχονται στην αρχική τους θέση με την αντίστροφη διαδικασία πριν την αποκωδικοποίηση.

Συγκεκριμένα η διεμπλοκή (interleaving) είναι μια περιοδική και αναστρέψιμη αντιμετάθεση συμβόλων ή bits. Τα σύμβολα ή τα bits επανέρχονται στη σωστή σειρά στον δέκτη.

4.4.2 Αλγόριθμοι διεμπλοκής και βασικοί ορισμοί

Περίοδος: Η περίοδος του διεμπλοκέα, έστω **T**, είναι το πιο σύντομο χρονικό διάστημα εντός του οποίου ο αλγόριθμος αναδιάταξης των συμβόλων ή bits επαναλαμβάνεται. Συχνά η περίοδος **L** αντιστοιχεί στο μέγεθος μιας κωδικής λέξης (codeword).

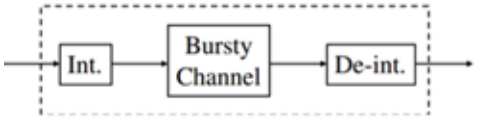
Βάθος: (depth): Ως βάθος του διεμπλοκέα, έστω **D**, ορίζουμε την ελάχιστη απόσταση μεταξύ δύο συμβόλων (ή bits) στην έξοδο του διεμπλοκέα, όταν τα σύμβολα (ή bits) αυτά ήταν συνεχόμενα στην είσοδο αυτού.

Η περίοδος καθορίζεται από τη δομή του διεμπλοκέα και μας δίνει το σύνολο τωνσυμβόλων (ή bits) στο οποίο εφαρμόζεται κάθε φορά ο αλγόριθμος της

αντιμετάθεσης. Το βάθος του διεμπλοκέα είναι σημαντικό στην αντιμετώπιση ριπών σφαλμάτων. Συγκεκριμένα, εάν μια ριπή σφαλμάτων έχει μήκος μικρότερο από το βάθος του διεμπλοκέα, τότε δεν θα υπάρχουν συνεχόμενα εσφαλμένα σύμβολα στην έξοδο του διεμπλοκέα (που να οφείλονται βέβαια σε αυτήν τη ριπή σφαλμάτων).

4.4.3 Κατηγορίες αλγορίθμων διεμπλοκής

- Block διεμπλοκή
- Διεμπλοκή με πίνακα μετάθεσης
- Συνελικτική διεμπλοκή



Εικόνα 25: Διεμπλοκή iii

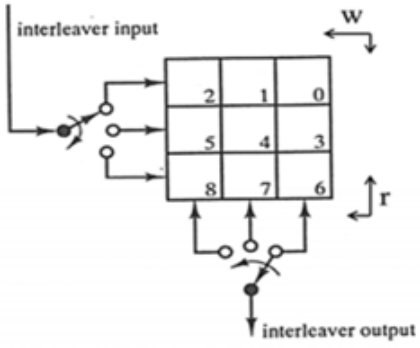
Block Διεμπλοκή:

Ιδιότητες:

- Οι απαιτήσεις μνήμης τόσο και στον πομπό όσο και στον δέκτη είναι n·m σύμβολα.
- Η καθυστέρηση που εισάγεται στο σύστημα είναι $D = 2\ m\ n - 1 + 1 \approx 2nm$ σύμβολα
    - Δύο διαδοχικά σύμβολα στην αρχική ροή χωρίζονται από (n - 1)σύμβολα μετά την διεμπλοκή
    - Συνήθως, κάθε γραμμή του πίνακα μνήμης αντιστοιχεί σε μία κωδική λέξη m συμβόλων
    - Χρησιμοποιώντας έναν κώδικα διόρθωσης λαθών, ικανότητας διόρθωσης t λαθών/γραμμή, το μήκος της μικρότερης μη-διορθώσιμης έξαρσης λαθών είναι $\boldsymbol{nt + 1}$ σύμβολα

Ένας $n \times m$ block διεμπλοκέας μεταθέτει ένα block από n·m σύμβολα χρησιμοποιώντας έναν πίνακα μνήμης n·m θέσεων και ακολουθώντας τα εξής βήματα:

1. Γράφει τα δεδομένα εισόδου από δεξιά προς τα αριστερά και από πάνω προς τα κάτω



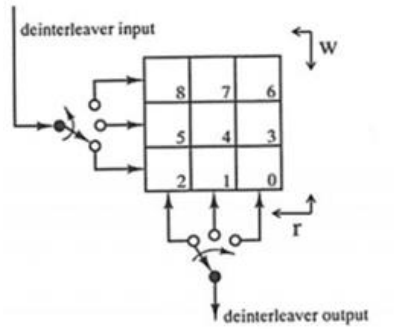
Εικόνα 25: Διεμπλοκή iv

2. Εξάγει τα δεδομένα προσπελαύνοντάς τα από κάτω προς τα πάνω και από δεξιά προς τα αριστερά.

Block Απεμπλοκή:

Ένας $n \times m$ block απεμπλοκέας μεταθέτει ένα block από n·m σύμβολα χρησιμοποιώντας έναν πίνακα μνήμης n·m θέσεων και ακολουθώντας τα εξής βήματα:

1. Γράφει τα δεδομένα εισόδου από πάνω προς τα κάτω και από δεξιά προς τα αριστερά



Εικόνα 26: Απεμπλοκή i

2. Εξάγει τα δεδομένα προσπελαύνοντάς τα από δεξιά προς τα αριστερά και από κάτω προς τα πάνω.

Διεμπλοκή με πίνακα μετάθεσης:

- Έστω x =[$x1$ $x2$ $x3$ …xL] ένα διάνυσμα εισόδου μήκους L συμβόλων
- Ο πίνακας μετάθεσης διεμπλοκής $\boldsymbol{P}$ είναι ένας τετραγωνικός πίνακας $L \times L$, ο οποίος έχει ένα 1 σε κάθε γραμμή και σε κάθε στήλη.
    - Για παράδειγμα, ο block διεμπλοκέας του προηγούμενου παραδείγματος είναι ισοδύναμος με τον πίνακα μετάθεσης:

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$ Αυτό συμβαίνει επειδή: $$P \times \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \\ 0 \\ 7 \\ 4 \\ 1 \\ 8 \\ 5 \\ 2 \end{bmatrix}$$

Ο απεμπλοκέας εκτελεί την αντίστροφη μετάθεση χρησιμοποιώντας ως πίνακα μετάθεσης τον ανάστροφο πίνακα (εξαιτίας της κατασκευής του P, ισχύει: $P^{-1} = P^T$)

Με βάση το προήγουμενο παράδειγμα:

$$P^{-1} = P^T = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

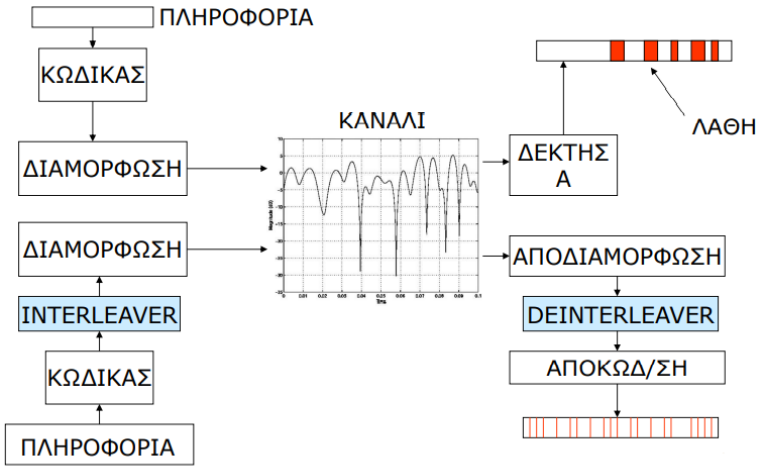
Συνελικτική διεμπλοκή:

- Οι προηγούμενες μέθοδοι είναι κατάλληλες για δεδομένα που μπορούν να οργανωθούν σε block
  - Στην περίπτωση που τα δεδομένα είναι μία συνεχή ροή συμβόλων, χρησιμοποιούμε τη συνελικτική διεμπλοκή, για να αποφύγουμε την «πακετοποίηση» των δεδομένων
  - Ο διεμπλοκέας/απεμπλοκέας αποτελείται από: – m γραμμές καθυστέρησης – η k-οστή γραμμή καθυστέρησης έχει $k - 1$ στοιχεία καθυστέρησης D συμβόλων.

Ιδιότητες συνελικτικής δεμπλοκής:

Τυπικά, μία λέξη m συμβόλων χρησιμοποιείται, κάθε σύμβολο της οποίας ανήκει σε διαφορετική γραμμή καθυστέρησης

- Κάθε 2 διαδοχικά σύμβολα στο αρχικό μήνυμα διαχωρίζονται από $\boldsymbol{mD}$ σύμβολα
- Χρησιμοποιώντας έναν αλγόριθμο διόρθωσης λαθών ικανότητας t λαθών, το μήκος της μικρότερης μη διορθώσιμης έξαρσης λαθών είναι $\boldsymbol{mD} + \mathbf{1}\ \boldsymbol{t} + \mathbf{1}$ σύμβολα • Οι απαιτήσεις μνήμης τόσο στον διεμπλοκέα όσο και στο απεμπλοκέα είναι $\boldsymbol{m}\ \boldsymbol{m} - \mathbf{1}\ \boldsymbol{D}/\mathbf{2}$
- Η καθυστέρηση συμβόλου από άκρο σε άκρο είναι $\boldsymbol{m}(\ \boldsymbol{m} - \mathbf{1})\ \boldsymbol{D}$ σύμβολα
- Χρησιμοποιώντας τον ίδιο αλγόριθμο διόρθωσης λαθών, η συνελικτική διεμπλοκή απαιτεί μόνο την μισή μνήμη.



Εικόνα 27: Διεμπλοκή

4.5 Κώδικες Reed-Solomon

4.5.1 Κώδικες Reed-Solomon

Ο δυαδικός Reed – Solomon κώδικας RS(2r, δ) είναι ένας κυκλικός κώδικας στο GF(2r) (ενώ οι BCH κώδικες είναι στο K = {0, 1}), με πολυώνυμο – γεννήτορα γ(x) = $(\lambda^{m+1}$ + x)$(\lambda^{m+2}$ + x)…$(\lambda^{m+\delta-1}$ + x), όπου m κάποιος ακέραιος και λ πρωτογενές (primitive) στοιχείο του GF(2r). Οι BCH κώδικες περιέχονται ως υποκώδικες στους Reed – Solomon κώδικες. Οι κώδικες Reed-Solomon (R-S) είναι συμβολικοί (μη δυαδικοί) κυκλικοί κώδικες με σύμβολα κατασκευασμένα από ακολουθίες m-bits, όπου m ακέραιος με $m \geq 2$.

• Για τους περισσότερους συμβατικούς κώδικεςR-S(n, k) ισχύει: $(n,k) = (2^m - 1, 2^m - 1 - 2t)$

Όπου: k είναι το πλήθος των συμβόλων δεδομένων που κωδικοποιούνται – n είναι το συνολικό πλήθος των συμβόλων στο block προς κωδικοποίηση (το μήκος block αυτών των κωδικών είναι $n = (2^m-1) - t$)είναι η ικανότητα διόρθωσης του κώδικα, με $\boldsymbol{n - k = 2t}$

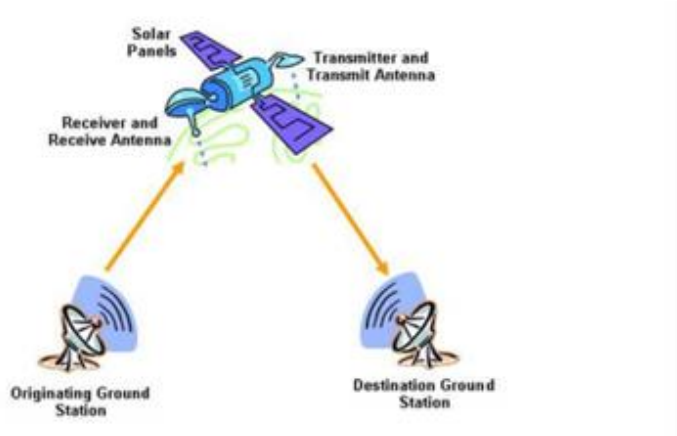
• Το πλήθος των bit ισοτιμίας που πρέπει να χρησιμοποιηθούν για την διόρθωση t λαθών υπολογίζονται από τη σχέση: $t = (d_{\min} - 1)/2 = (n - k)/2$

$$\boldsymbol{t = (d\text{min} - 1)/2 = (n - k)/2}$$

Οι κώδικες $R - S(n,k)$ επιτυγχάνουν τη μεγαλύτερο πιθανή ελάχιστη απόσταση $dmin$ από κάθε γραμμικό κώδικα.

- ✓ Αυτή υπολογίζεται από τη σχέση $dmin = n - k + 1$
- ✓ Ο R-S κωδικοποιητής επεκτείνει ένα block k συμβόλων σε ένα block n συμβόλων προσθέτοντας $(n - k)$ σύμβολα.

Οι κώδικες R-S χρησιμοποιούνται σε πολλές σύγχρονες εφαρμογές όπως: – CDs – Διαστημικές και δορυφορικές επικοινωνίες (π.χ. ο κώδικας R-S(255, 223) ο οποίος αποτελεί standard κώδικα της NASA).

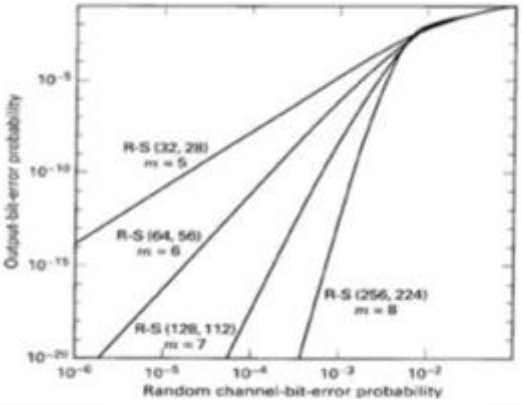


Εικόνα 28: Εικόνα αναπαράστασης χρήσης i

4.5.2 Απόδοση R-S κώδικα σε συνάρτηση του μεγέθους συμβόλου m

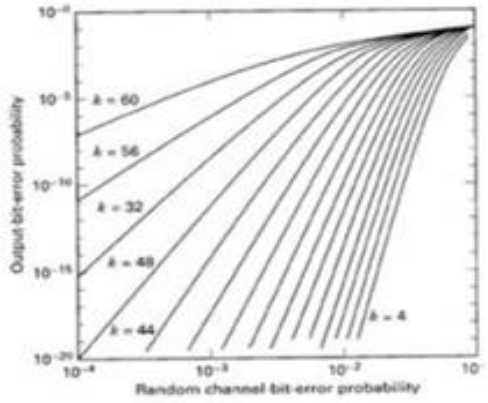
• Οι κώδικες διόρθωσης λαθών γίνονται πιο αποδοτικοί όταν το μέγεθος του block αυξάνεται.

• Εάν υποθέσουμε πως ο ρυθμός του κώδικα διατηρείται σταθερός στα 7/8 και το μέγεθος του block αυξάνεται από n = 32 σύμβολα (m = 5 bits / σύμβολο) σε n= 256 (m = 8 bits / σύμβολο), τότε το μέγεθος του block αυξάνεται από 160 bits σε 2048 bits και η απόδοση διαμορφώνεται όπως στο παρακάτω σχήμα:



Εικόνα 29: Απόδοση Reed-Solomon i

Καθώς τα bit πλεονασμού (n-k) ενός κώδικα R-S αυξάνονται (και άρα μειώνεται ο ρυθμός του κώδικα), αυξάνεται η πολυπλοκότητα υλοποίησης του καθώς και το απαραίτητο εύρος ζώνης.



Εικόνα 29: Απόδοση Reed-Solomon ii

• Το κέρδος από την αύξηση των bit πλεονασμού είναι η βελτίωση του BER, όπως φαίνεται στο παραπανω(Εικονα 29) σχήμα όπου το μήκος του κώδικα διατηρείται σταθερό στα 64 bit και τα πλεονάζοντα σύμβολα αυξάνονται από 4 σε 60.

Κεφάλαιο 5ο
Εφαρμογή σε προγραμματιστικό περιβάλλον Matlab

Στο παρόν κεφάλαιο θα δώσουμε παραδείγματα για τις τεχνικές που είδαμε σε προηγούμενες ενότητες σε προγραμματιστικό περιβάλλον Matlab . Σε κάθε υποενότητα θα υπάρχει και ένα παράδειγμα με τον κώδικα της προσομοίωσης οπου μεσα θα περιέχει και σχόλια για την σωστή κατανόηση των εντολών και συντακτικού. Ακόμη θα υπάρχει και το αποτέλεσμα της προσομοίωσης με συμπεράσματα και σχόλια.

5.1 Μετάδοση και λήψη κωδίκων Reed-Solomon

Στο παρακάτω παράδειγμα θα δείξουμε πως μεταδίδουμε και δεχόμαστε κλασσικούς και συντομευμένους κώδικες Reed – Solomon, με 64-QAM (διαμόρφωση πλάτους) μέσω ενός καναλιού με λευκό Gaussian θόρυβο. Θα συγκρινουμε την αποδοση μεταξύ των κλασσικών και των συντομευμένων κωδίκων.

N: Μέγεθος κωδικολέξης ,

K: Μέγεθος μηνύματος ,

S: Μεγεθος κωδικοποιημένου μηνυματος,

M: Τυπος διαμόρφωσης

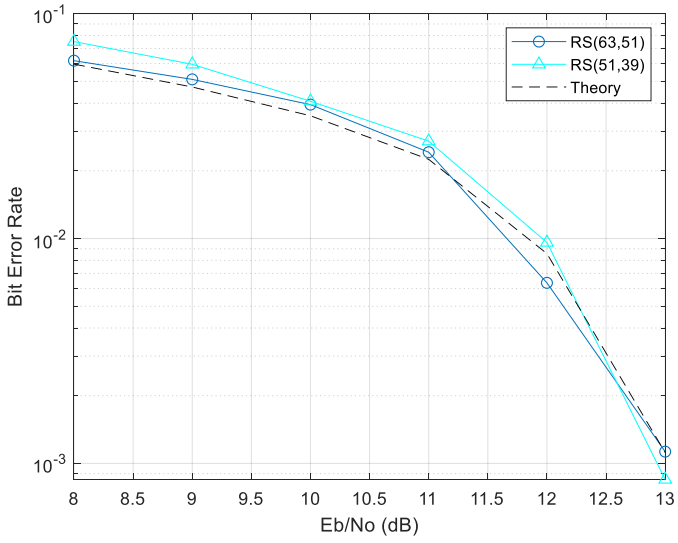
Κώδικας προσομοίωσης:

```
N = 63;  % Μεγεθος κωδικολέξης
K = 51;  % Μέγεθος μηνύματος
S = 39;  % Μειωμένο μεγεθος μηνύματος
M = 64;  % Διαμορφωση
numErrors = 200;
numBits = 1e7;
ebnoVec = (8:13)';
[ber0,ber1] = deal(zeros(size(ebnoVec)));
errorRate = comm.ErrorRate;
rsEncoder = comm.RSEncoder(N,K,'BitInput',true);
rsDecoder = comm.RSDecoder(N,K,'BitInput',true);
rate = K/N;
for k = 1:length(ebnoVec)
    % Μετατροπή του Eb/No σε διαγραμμα θορυβου SNR.
    snrdB = ebnoVec(k) + 10*log10(rate) +
10*log10(log2(M));
    errorStats = zeros(3,1);
    while errorStats(2) < numErrors && errorStats(3)
< numBits
        % Δημιουργία δυαδικών δεδομένων
        txData = randi([0 1],K*log2(M),1);
```

```
        % Κωδικοποίηση
        encData = rsEncoder(txData);
        % Εφαρμογή διαμόρφωσης 64-QAM
        txSig = qammod(encData,M, ...
'UnitAveragePower',true,'InputType','bit');
      % Περνάμε το σημα απο καναλι με Γκαουσιανο
θορυβο
        rxSig = awgn(txSig,snrdB);
        % Αποδιαμορφωση
        demodSig = qamdemod(rxSig,M, ...
'UnitAveragePower',true,'OutputType','bit');
        % Κωδικοποιηση
        rxData = rsDecoder(demodSig);
        % Σφαλματα
        errorStats = errorRate(txData,rxData);
    end
    % Αποθηκευουμε το bit error rate και μηδενιζουμε
τον μετρητη λαθων
    ber0(k) = errorStats(1);
    reset(errorRate)
end
gp = rsgenpoly(N,K,[],0);
rsEncoder = comm.RSEncoder(N,K,gp,S,'BitInput',true);
rsDecoder = comm.RSDecoder(N,K,gp,S,'BitInput',true);
rate = S/(N-(K-S));
for k = 1:length(ebnoVec)
  % Δημιουργουμε έναν Reed-Solomon κωδικοποιητη και
αποκωδικοποιητη με το μηκος του συντομευμενου
μηνυματος S
  % Ακολουθουμε την ιδια διαδικασια για την
δημιουργια κωδικοποιητη -
  % αποκωδικοποιητη με την χρηση του μηνυματος με
μειωμενο μεγεθος
    snrdB = ebnoVec(k) + 10*log10(rate) +
10*log10(log2(M));
    errorStats = zeros(3,1);
    while errorStats(2) < numErrors && errorStats(3)
< numBits
        txData = randi([0 1],S*log2(M),1);
        encData = rsEncoder(txData);
        txSig = qammod(encData,M, ...
'UnitAveragePower',true,'InputType','bit');
        rxSig = awgn(txSig,snrdB);
```

```
        demodSig = qamdemod(rxSig,M, ...
'UnitAveragePower',true,'OutputType','bit');
        rxData = rsDecoder(demodSig);
        errorStats = errorRate(txData,rxData);
    end
    ber1(k) = errorStats(1);
    reset(errorRate)
end
berapprox =
bercoding(ebnoVec,'RS','hard',N,K,'qam',64);
semilogy(ebnoVec,ber0,'o-',ebnoVec,ber1,'c^-
',ebnoVec,berapprox,'k--')
legend('RS(63,51)','RS(51,39)','Theory')
xlabel('Eb/No (dB)')
ylabel('Bit Error Rate')
grid
```

Αποτέλεσμα προσομοιωσης:



Παρατηρούμε ότι παρότι έχουμε μικρότερο κώδικα δεν έχουμε μείωση στην απόδοση και μπορούμε με μικρότερο μέγεθος μηνύματος-πληροφορίας να εχουμε το ιδιο αποτέλεσμα , με χρήση κωδικοποίησης - αποκωδικοποίησης Reed-Solomon.

5.2 Reed-Solomon απλή κωδικοποίηση

Κώδικας προσομοίωσης:

```
m = 3;
n = 2^m - 1;
k = 3;
msg = gf([2 7 3; 4 0 6],m)
code = rsenc(msg,n,k)
```

Αποτέλεσμα προσομοιωσης:

```
msg = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   2   7   3
   4   0   6


code = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   2   7   3   3   6   7   6
   4   0   6   4   2   2   0
```

Η rsenc(msg,n,k) κωδικοποιεί το μήνυμα (msg), οπου είναι ενας πίνακας Galois από σύμβολα με m=3 bits το καθένα ,με τον [n,k] Reed-Solomon κώδικα .Κάθε k - στοιχεία στην γραμμή του πίνακα είναι μια λέξη του μηνύματος ,οπου το αριστερά σύμβολο είναι και το πιο σημαντικό. Το μέγιστο του n ειναι 2^m-1. Αν το n δεν είναι ακριβώς 2^m-1, η rsenc κωδικοποιεί έναν συντομευμένο Reed-Solomon κώδικα. Τα σύμβολα ισοτιμίας βρίσκονται στο τέλος κάθε λέξης στον τελικό πίνακα Galois. Έτσι θέτουμε τις παραμέτρους m και k. Δημιουργούμε 2 μηνύματα με βάση G(8) (Galois Field (2^3)). Έπειτα δημιουργούμε Reed-Solomon κωδικολέξεις. Βλέπουμε ότι είναι συστηματικοι κώδικες και ότι τα πρώτα 3 σύμβολα κάθε σειράς είναι ακριβώς τα στοιχεία του μηνύματος μας msg.

5.3 Διεμπλοκή (Interleaving)

Το ακόλουθο παράδειγμα επεξηγεί πώς ένας block interleaving κωδικοποιήτης βελτιώνει το ποσοστό σφάλματος σε ένα σύστημα επικοινωνίας του οποίου το κανάλι παράγει μια ριπή σφαλμάτων. Ένας τυχαίος interleaver αναδιατάσσει τα bit πολλών κωδικών λέξεων προτού καταστραφούν δύο γειτονικές κωδικές λέξεις η καθεμία από τρία σφάλματα. Τρία σφάλματα υπερβαίνουν τη δυνατότητα διόρθωσης σφαλμάτων του κώδικα Hamming. Ωστόσο, το παράδειγμα δείχνει ότι όταν ο κώδικας Hamming συνδυάζεται με έναν interleaver, αυτό το σύστημα είναι σε θέση να ανακτήσει το αρχικό μήνυμα παρά την έκρηξη 6-bit σφαλμάτων. Η βελτίωση της απόδοσης συμβαίνει επειδή η παρεμβολή κατανέμει αποτελεσματικά τα σφάλματα μεταξύ διαφορετικών κωδικών λέξεων, έτσι ώστε ο αριθμός των σφαλμάτων ανά κωδική λέξη να είναι εντός της ικανότητας διόρθωσης σφαλμάτων του κώδικα.

Κώδικας προσομοίωσης:

(Σχόλια πάνω στον κώδικα)

```
st1 = 27221; st2 = 4831; % Για  τυχαίο αριθμό
n = 7; k = 4; % Παράμετροι για Hamming κώδικα
msg = randi([0 1],k*500,1); % Μηνυμα
code = encode(msg,n,k,'hamming/binary');
% Δημιουργουμε μια ριπή λαθών που θα αλλοιώσει 2
διαδοχικες κωδικολέξεις
errors = zeros(size(code)); errors(n-2:n+3) = [1 1 1
1 1 1];
% Με Διεμπλοκή
inter = randintrlv(code,st2); % Interleave
(διεμπλοκη).
inter_err = bitxor(inter,errors); % Ριπή λαθών
deinter = randdeintrlv(inter_err,st2);
% Αποκωδικοποιηση
decoded = decode(deinter,n,k,'hamming/binary');
disp('Number of errors and error rate, with
interleaving:');
[number_with,rate_with] = biterr(msg,decoded)
% Ποσοστό λαθών
% Χωρίς Διεμπλοκή
code_err = bitxor(code,errors); % Ριπή λαθών
decoded = decode(code_err,n,k,'hamming/binary');
% Αποκωδικοποιηση.
disp('Number of errors and error rate, without
interleaving:');
[number_without,rate_without] = biterr(msg,decoded)
```

Αποτέλεσμα προσομοίωσης:

```
Number of errors and error rate, with interleaving:

number_with =

     0


rate_with =

     0

Number of errors and error rate, without interleaving:

number_without =

     4


rate_without =

    0.0020
```

5.4 Γραμμικός κώδικας μπλοκ

Κώδικας προσομοίωσης:

```
n = 7;
k = 3;
data = randi([0 1],k,1);
pol = cyclpoly(n,k);
parmat = cyclgen(n,pol);
genmat = gen2par(parmat);
encData = encode(data,n,k,'linear/binary',genmat);
encData(3) = ~encData(3);
decData = decode(encData,n,k,'linear/binary',genmat);
numerr = biterr(data,decData)
```

Αποτέλεσμα προσομοίωσης:

```
Single-error patterns loaded in decoding table.  8 rows remaining.
2-error patterns loaded.  1 rows remaining.
3-error patterns loaded.  0 rows remaining.

numerr =

     0
```

Σε αυτό το παράδειγμα παραξαμε ένα τυχαίο δυαδικό μήνυμα ίσο με το μέγεθος του μηνύματος (k) το κωδικοποιήσαμε και εισαγάγαμε σφάλμα στο το 3ο bit του μηνύματος προσομοιώνοντας τον θόρυβο. Έπειτα αποκωδικοποιουμε και παρατηρουμε ότι ο αποκωδικοποιητής κατάφερε να βρει τον σωστό αρχικο αριθμό.

5.5 Κυκλικός κώδικας μπλοκ

Κώδικας προσομοίωσης:

```
n = 7;
k = 3;
data = randi([0 1],k,1);
pol = cyclpoly(n,k);
parmat = cyclgen(n,pol);
genmat = gen2par(parmat);
encData = encode(data,n,k,'linear/binary',genmat);
encData(3) = ~encData(3);
decData = decode(encData,n,k,'linear/binary',genmat);
numerr = biterr(data,decData)
```

Αποτέλεσμα προσομοίωσης:

```
Single-error patterns loaded in decoding table.  1008 rows remaining.
2-error patterns loaded.  918 rows remaining.
3-error patterns loaded.  648 rows remaining.
4-error patterns loaded.  243 rows remaining.
5-error patterns loaded.  0 rows remaining.

numerr =

     0
```

Σε αυτό το παράδειγμα αφού θέτουμε το μήκος της κωδικολέξης και το μήκος του μήνυματος, δημιουργούμε ένα τυχαίο δυαδικό μήνυμα με το ίδιο μήκος. Έπειτα φτιάχνουμε ένα πολυώνυμο κυκλικής γεννήτριας και τον πίνακα ελέγχου ισοτιμίας οπου τον μετατρέπουμε σε έναν γεννήτορα πίνακα. Στην συνέχεια κωδικοποιούμε το μήνυμα με βάση τον γεννήτορα πίνακα και του εισάγουμε ένα σφάλμα στο 3ο bit. Αφού το αποκωδικοποιούμε, παρατηρούμε ότι ο αποκωδικοποιητής κατάφερε να βρεί το σωστό αρχικό μήνυμα.

Βιβλιογραφία

1. https://en.wikipedia.org/wiki/Block_code
2. https://eclass.uop.gr/modules/document/index.php?course=344&openDir=/57fa7e789OdA
3. https://eclass.uop.gr/modules/document/index.php?course=344&openDir=/5802817220Py
4. Επιπλέον υλικό του επιβλέπων καθηγητή (Μιχαήλ Παρασκευά)
5. John G. Proakis and Masoud Salehi, “Communication Systems Engineering,” Second Edition, Published by Pearson Education, Inc, published as PRENTICE HALL, INC, Copyright © 2002 by Prentice-Hall, Inc, Upper Saddle River New Jersey.
6. COVER THOMAS M. THOMAS JOY A. ΣΤΟΙΧΕΙΑ ΤΗΣ ΘΕΩΡΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ
7. https://www.mathworks.com/ (Παραδείγματα)
8. https://www.geeksforgeeks.org/ (Παραδείγματα)