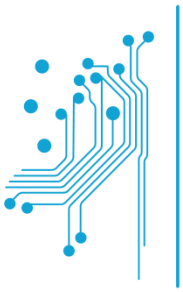


Τμήμα
Μηχανικών
Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κωδικοποίηση Καναλιού Χρησιμοποιώντας Κώδικες Block και Συνελικτικούς Κώδικες

Κυριακίδου Αγγελική
Λόζιου Χριστιάνα

Επιβλέπων Καθηγητής: Μιχαήλ Παρασκευάς

Αντίρριο-Σεπτέμβριος 2015

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, 21/09/2015

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1.

2.

3.

ΠΕΡΙΛΗΨΗ

Εδώ και χρόνια οι ηλεκτρονικοί υπολογιστές διαδραματίζουν σημαντικό ρόλο στην καθημερινότητα των ανθρώπων. Σε πολλές περιπτώσεις οι υπολογιστές, αλλά και η συνεχόμενη εξέλιξή τους, είναι συνυφασμένοι με την ανθρώπινη ζωή, όπως για παράδειγμα στην τηλεϊατρική, τα χειρουργικά ρομπότ, τα στρατιωτικά συστήματα, τις τηλεπικοινωνίες κλπ.

Η ανάγκη για την αξιοπιστία των δεδομένων στις νέες τηλεπικοινωνιακές εφαρμογές, έχει οδηγήσει στην ανάπτυξη και τη βελτιστοποίηση των κωδικών διόρθωσης λαθών. Πρόκειται για συστήματα τα οποία έχουν τη δυνατότητα ανίχνευσης και διόρθωσης λαθών, που εισέρχονται σε τμήματα της πληροφορίας, η οποία μεταφέρεται μέσω τηλεπικοινωνιακών δικτύων λόγω του θορύβου αλλά και από το κανάλι μετάδοσης.

Υπάρχουν πολλές κατηγορίες κωδικών διόρθωσης, οι οποίοι κατατάσσονται σύμφωνα με τη δομή και τη φύση των αλγόριθμων που χρησιμοποιούν. Σκοπός και αντικείμενο της παρούσης πτυχιακής εργασίας είναι η μελέτη και η παρουσίαση των δύο κυριότερων κατηγοριών κωδικών διόρθωσης λαθών, τους συνελικτικούς και γραμμικούς μπλοκ κώδικες.

Λέξεις Κλειδιά : Αποκωδικοποίηση, Κώδικες διόρθωσης λαθών, Μπλοκ κώδικες, Συνελικτικοί κώδικες, Τηλεπικοινωνίες, Hamming,

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα θέλαμε να ευχαριστήσουμε τον καθηγητή μας κ. Μιχαήλ Παρασκευά που δέχτηκε να μας αναλάβει στο τέλος της πτυχιακής μας εργασίας και να μας στηρίξει.

Επίσης την γραμματεία της σχολής που μας βοήθησε όλο αυτόν τον καιρό με τις απορίες και την αγωνία μας, καθώς επίσης και τον κ. Δημήτριο Αμπελιώτη για την ανάθεση του θέματος της πτυχιακής εργασίας.

Τέλος , θέλουμε να ευχαριστήσουμε τις οικογένειες μας για την υπομονή τους και την στήριξη τους όλα αυτά τα χρόνια.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

1. Εισαγωγή

Στην παρούσα πτυχιακή εργασία θα μελετηθούν ορισμένες τεχνικές κωδικοποίησης καναλιού οι οποίες χρησιμοποιούνται είτε από ενσύρματα είτε από ασύρματα τηλεπικοινωνιακά δίκτυα. Εκτός από τις κλασσικές τεχνικές κωδικοποίησης καναλιού θα παρουσιαστούν κυρίως οι σύγχρονες.

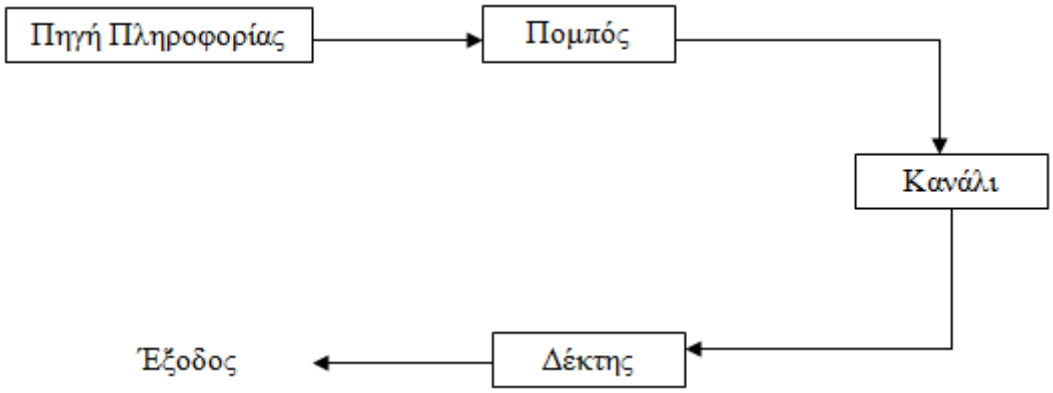
Σε αυτό το εισαγωγικό κεφάλαιο, θα αναφερθούν τα τηλεπικοινωνιακά συστήματα και τα συστήματα επικοινωνίας γενικότερα. Επίσης, θα αναφερθεί η έννοια της πληροφορίας, ο γενικός στόχος των επικοινωνιών είναι η αποστολή ενός μηνύματος από ένα σημείο σε ένα άλλο καθώς και η επιβεβαίωση της αξιόπιστης λήψης του μηνύματος-πληροφορία από έναν παραλήπτη.

1.1 Τηλεπικοινωνίες και συστήματα επικοινωνίας

Από την αρχή της ύπαρξης της ανθρωπότητας δημιουργήθηκε η ανάγκη για επικοινωνία από μακρινές αποστάσεις στο μικρότερο δυνατό χρόνο. Σε κάθε εποχή αναπτύχθηκαν διαφορετικοί τρόπο επικοινωνίας. Τα τελευταία χρόνια, η ανάγκη για αποδοτικά και αξιόπιστα συστήματα επικοινωνίας (κυρίως ψηφιακά) έχει παρουσιάσει μεγάλη εξέλιξη. Δεν είναι τυχαίο ότι η σημερινή εποχή ονομάζεται εποχή των επικοινωνιών.

Είναι σημαντικό, αρχικά, να διαχωριστούν οι έννοιες της επικοινωνίας και των τηλεπικοινωνιών. Όταν υπάρχουν επικοινωνίες σε μακρινή απόσταση, τότε χρησιμοποιείται ο όρος Τηλεπικοινωνίες (από το αρχαίο ελληνικό τηλε). Οι επικοινωνίες σε μεγάλες αποστάσεις λόγω της ανεπάρκειας του μέσου μετάδοσης αναγκαστικά αλλάζουν τη μορφή της πληροφορίας προκειμένου να μπορέσει να μεταφερθεί. Έτσι, στην περίπτωση που η πληροφορία δεν αλλάζει μορφή για να μεταφερθεί, δηλαδή είναι σε μικρές αποστάσεις, τότε ορίζεται ως επικοινωνία, ενώ όταν αλλάζει μορφή για να μεταδοθεί, δηλαδή σε μεγάλες αποστάσεις, χρησιμοποιείται ο όρος της τηλεπικοινωνίας.

Σκοπός των συστημάτων επικοινωνιών είναι η αξιόπιστη μετάδοση της πληροφορίας. Ένα βασικό σύστημα επικοινωνίας αποτελείται από την πηγή πληροφορίας (δηλαδή, την πηγή η οποία παράγει την πληροφορία την οποία θέλουμε να μεταδώσουμε), τον πομπό ο οποίος, με τις κατάλληλες διαδικασίες, μετατρέπει το σήμα σε κατάλληλη μορφή για μετάδοση μέσω του φυσικού καναλιού ή του μέσου μετάδοσης, το κανάλι επικοινωνίας το οποίο αποτελεί το φυσικό μέσο μετάδοσης του σήματος από τον πομπό στο δέκτη. Ως κανάλι επικοινωνίας σε ενσύρματε συνδέσεις μπορεί να είναι κάποιο υλικό μέσο (όπως, καλώδια, οπτικές ίνες και πολλά άλλα) ενώ, στην ασύρματη μετάδοση συνήθως είναι η ατμόσφαιρα. Τέλος, το επικοινωνιακό σύστημα αποτελείται από τον δέκτη ο οποίος έχει ως στόχο, μέσω της λειτουργίας του, την ανάκτηση του μηνύματος από τον πομπό το οποίο και μεταφέρει το σήμα που ελήφθη. (Σχήμα 1.1)



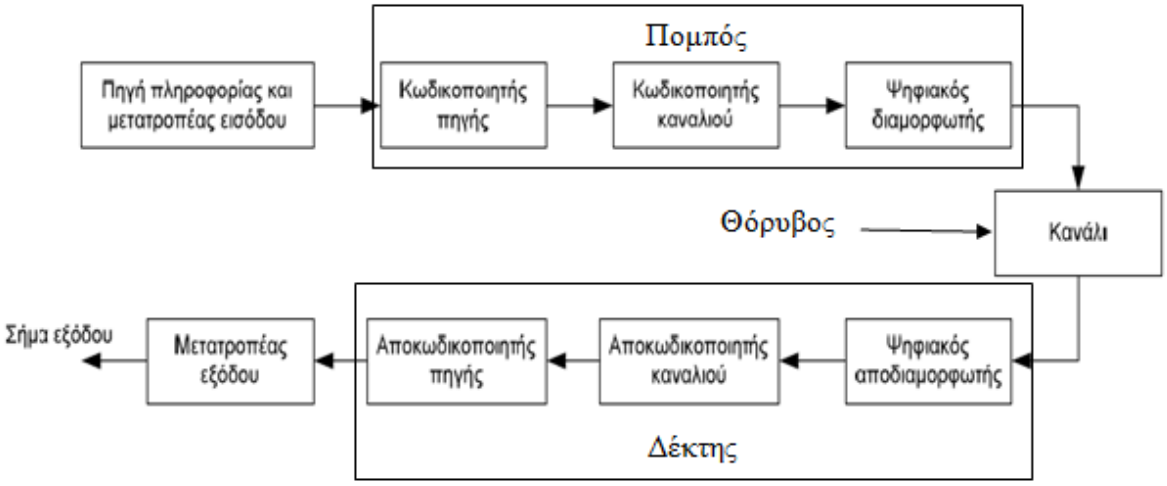
Σχήμα 1.1 Βασικό σύστημα επικοινωνίας

Ένα σύστημα επικοινωνίας μπορεί να είναι είτε ψηφιακό είτε αναλογικό. Τα αναλογικά συστήματα μεταφέρουν αναλογικά σήματα τα οποία είναι κυματομορφές συνεχούς χρόνου και εκπέμπονται από αναλογικές πηγές. (Ένα παράδειγμα αναλογικού σήματος είναι φωνή όπου η πηγή πληροφορίας μπορεί να είναι ο άνθρωπος). Τα αναλογικά σήματα μπορούν να μεταδοθούν απευθείας μέσω διαμόρφωσης φέροντος σε ένα κανάλι επικοινωνίας και να αναδιαμορφώνονται ανάλογα στο δέκτη. Στη σημερινή εποχή, όμως, η έννοια της επικοινωνίας αναφέρεται στη μετάδοση ενός μεγάλου όγκου πληροφοριών ο οποίος συνήθως είναι αποθηκευμένος σε κάποια ψηφιακή μορφή. Υπάρχουν σοβαρά πλεονεκτήματα ώστε ένα αναλογικό σήμα να το μετατρέψουμε σε ψηφιακό καθώς η πιστότητα του σήματος ελέγχεται καλύτερα. Πιο συγκεκριμένα, η ψηφιακή μετάδοση επιτρέπει την «αναγέννηση» του σήματος μετά από μεγάλες αποστάσεις μετάδοσης εξαλείφοντας, πρακτικά, τις

επιδράσεις του θορύβου. Αντίθετα, ο θόρυβος που προστίθεται στην αναλογική μετάδοση ενισχύεται μαζί με το σήμα, ειδικά, αν χρησιμοποιήσουμε ενισχυτές για την ανύψωση της στάθμης του σήματος κατά τη μετάδοση σε μεγάλες αποστάσεις.

Σε ένα ψηφιακό τηλεπικοινωνιακό σύστημα η μετάδοση της πληροφορίας ξεκινάει από την πηγή η οποία μπορεί να είναι κάποιο πρόσωπο όπως ένας ομιλητής μιας οποιασδήποτε συνδιάλεξης ή κάποιο ψηφιακό σύστημα όπως ένας υπολογιστής συνδεδεμένος σε δίκτυο . Η έξοδος της πηγής μπορεί να είναι οποιασδήποτε μορφής σήμα όπως μια κυματομορφή (αναλογικό σήμα) ή μια ακολουθία διακριτών συμβόλων (ψηφιακό σήμα). Η έξοδος της πηγής πρέπει κάθε φορά να μετατραπεί σε μια κατάλληλη μορφή για μετάδοση ανάλογα με το μέσο που χρησιμοποιείται κάθε φορά (οπτικές ίνες, ασύρματες επικοινωνίες, δορυφορικές ζεύξεις). Ο πομπός ο οποίος αποτελείται, συνήθως, από τον κωδικοποιητή πηγής, τον κωδικοποιητή καναλιού και τον διαμορφωτή επιτρέπει την μετατροπή του σήματος από αναλογικό σε ψηφιακό. Ο κωδικοποιητής της πηγής είναι ένα σύστημα το οποίο, αν είναι απαραίτητο, αναλαμβάνει να μετατρέψει σε δυαδικά ψηφία την έξοδο της πηγής. Ενώ, ο κωδικοποιητής του καναλιού είναι ένα σύστημα το οποίο αναλαμβάνει να προσθέσει επιπλέον πληροφορία στην αρχική πληροφορία που έλαβε με στόχο να κάνει το σύστημα πιο αξιόπιστο. Αφού, κατά τη μετάδοση της πληροφορίας μέσω του καναλιού προστίθεται σε αυτή θόρυβος με αποτέλεσμα το σήμα να φτάνει στον δέκτη αλλοιωμένο. Με την επιπλέον πληροφορία του καναλιού ο δέκτης έχει τη δυνατότητα να διορθώσει και να ανακατασκευάσει το σήμα που έλαβε. Το σύστημα του πομπού το οποίο αναλαμβάνει να μετατρέψει το σήμα σε κατάλληλη κυματομορφή ώστε να μπορέσει να μεταφερθεί από το κανάλι είναι ο διαμορφωτής. Κατά γενικό κανόνα, η μορφή της πληροφορία που έχει παραχθεί από τον αποκωδικοποιητή δεν είναι κατάλληλη ώστε να μεταφερθεί στο κανάλι. [1][2]

[1] John G. Proakis, “Digital Communications,” Fourth Edition, Published by McGraw-Hill International Edition.



Σχήμα 1.2 Βασικό ψηφιακό σύστημα τηλεπικοινωνιών

1.2 Θεωρία της πληροφορίας

Η θεωρία της πληροφορίας ως επιστήμη ανήκει στον τομέα των εφαρμοσμένων μαθηματικών και ως στόχο έχει να ορίσει την ποσότητά της (εντροπία). Η θεωρία της πληροφορίας αναπτύχθηκε από τον Κλοντ Σάνον (Claude Elwood Shannon) το 1948 ο οποίος ασχολήθηκε με την πληροφορία με σκοπό να μελετήσει τις επικοινωνίες. [10]

Σύμφωνα, με την θεωρία της πληροφορίας ένα βασικό σύστημα τηλεπικοινωνιών αποτελείται, αρχικά, από τον πομπό ο οποίος, με τη σειρά του, αποτελείται από την πηγή πληροφορίας και τον κωδικοποιητή. Η μορφή της πληροφορίας η οποία θα είναι κατάλληλη να μεταδοθεί παράγεται στην πηγή. Η οργάνωση της πληροφορίας διαχωρίζεται σε μηνύματα πληροφορίας τα οποία θα μετατραπούν σε κωδικά μηνύματα.

Πιο συγκεκριμένα, η πηγή της πληροφορίας παράγει πληροφορία με τη μορφή συμβόλων. Η πληροφορία μετατρέπεται σε σύμβολα έχοντας ως κριτήριο την πιθανότητα εμφάνισης τους στην έξοδο της πηγής πληροφορίας. Η πηγή πληροφορίας οργανώνεται σε αλφάβητο, λέξη πληροφορίας και μηνύματα πληροφορίας. Το αλφάβητο είναι το σύνολο των συμβόλων που χρησιμοποιεί (όπως για παράδειγμα γράμματα, αριθμοί, διαγράμματα, χάρτες). Η λέξη πληροφορίας είναι βραχεία διάταξη του αλφάβητου (όπως για παράδειγμα μια λέξη, π.χ. πιάνο). Ενώ, το μήνυμα πληροφορίας είναι, στην ουσία, η διάταξη των λέξεων πληροφορίας, (για παράδειγμα θα μπορούσε να είναι μια πρόταση, π.χ. το πιάνο είναι ξεκούρδιστο). Κατά

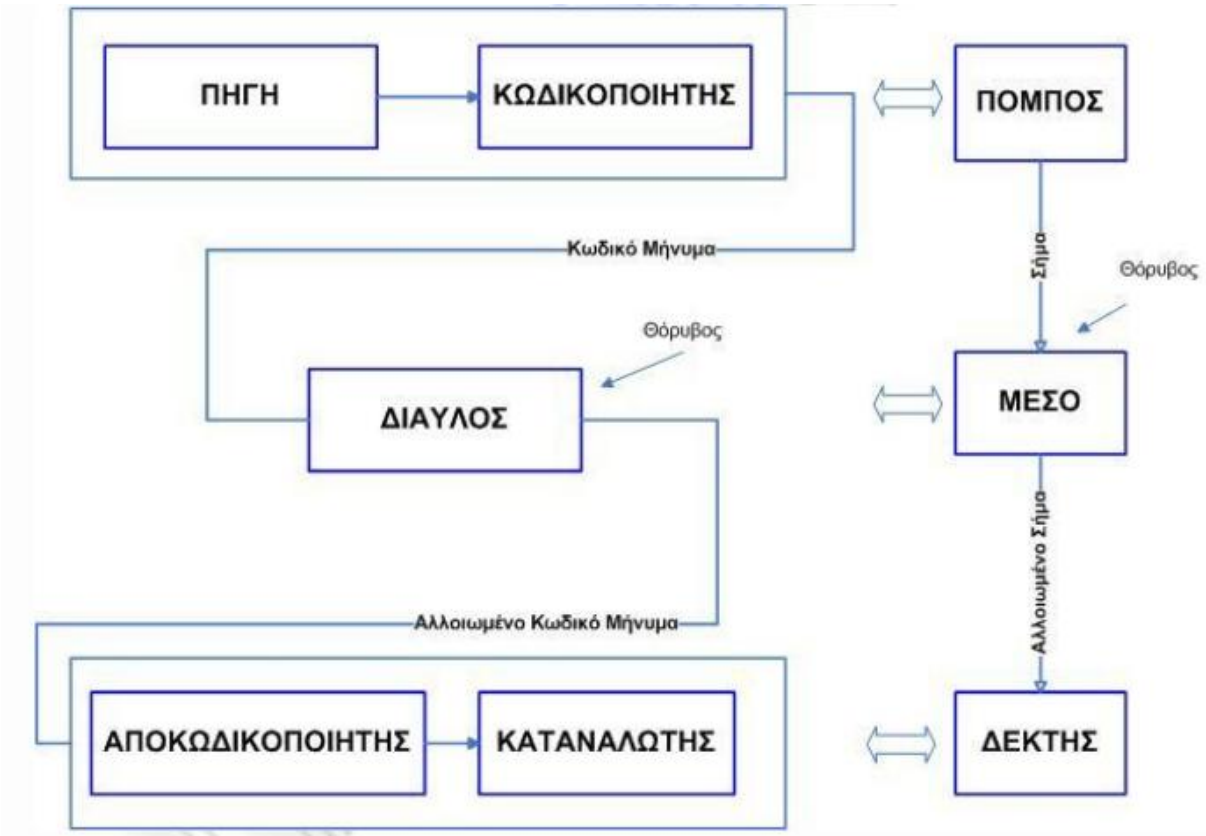
την κωδικοποίηση γίνεται αντικατάσταση συμβόλων πληροφορίας από άλλα κωδικά-σύμβολα με αντικειμενικό σκοπό την βελτιστοποίηση της επικοινωνίας. Η οργάνωση της κωδικοποιημένης πληροφορίας διαχωρίζεται από τις κωδικές λέξεις και τα κωδικά μηνύματα. Κάθε τεχνική κωδικοποίησης μπορεί να εκφραστεί ως κώδικας. Το σύνολο των κωδικών συμβόλων είναι το αλφάβητο του κώδικα, όπου το κλειδί του κώδικα αποτελεί απεικόνιση των συμβόλων στοιχείο προς στοιχείο, κωδικές λέξεις και κωδικά μηνύματα. Στα ψηφιακά συστήματα επικοινωνίας η πιο συνηθισμένη μορφή κωδικοποίησης είναι η δυαδική. Επίσης, απαραίτητο στοιχείο για τον πομπό είναι ο μεταλλάκτης ο οποίος μετατρέπει το κωδικοποιημένο μήνυμα σε σήμα. Το σήμα που παράγει αποτελεί τον υλικό φορέα της πληροφορίας.

Το μέσο που υπάρχει μεταξύ πομπού και δέκτη είναι το κανάλι πληροφορίας (ή δίαυλος πληροφορίας) και διοχετεύει την πληροφορία μεταξύ πομπού και δέκτη. Πιο συγκεκριμένα, κανάλι πληροφορίας είναι αλυσίδα μέσων και συσκευών (π.χ. καλώδια, οπτικές ίνες, κυματοδηγοί) που μεταδίδουν το σήμα. Η χωρητικότητα του καναλιού πληροφορίας είναι ο μέγιστος ρυθμός μετάδοσης της πληροφορίας. Η χωρητικότητα καθορίζει το χρόνο και το κόστος που απαιτούνται για να μεταδοθεί ένα μήνυμα το οποίο μπορεί ταυτόχρονα να περιέχει το κανάλι πληροφορίας. Όταν η πληροφορία διαπερνά το κανάλι είναι πολύ πιθανό να αλλοιωθεί λόγω της παρουσίας θορύβου. Θόρυβος είναι κάθε ανεξέλεγκτη παρεμβολή του καναλιού ο οποίος και προκαλεί αλλοίωση του σήματος και συνεπώς σφάλματα μετάδοσης (απώλεια πληροφορίας).

Τελικά, όταν το μήνυμα φτάσει στο δέκτη δέχεται, αρχικά, κατάλληλη επεξεργασία από τον αποκωδικοποιητή ώστε το σήμα που προκύπτει από την έξοδο του καναλιού να αναπαραχθεί όσο το δυνατόν πιο πιστό αντίγραφο του σήματος στην έξοδο της πληροφορίας.

Στο ακόλουθο Σχήμα 1.3 δίνεται το βασικό διάγραμμα συστήματος τηλεπικοινωνιών με βάση τη θεωρία της πληροφορίας και με όσα αναλύσαμε παραπάνω.[2] [1]

[2] 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.



1.3 Βασικό διάγραμμα συστήματος τηλεπικοινωνιών[3] [12]

[3] Καραμάνου Ευαγ. Δήμητρα "Θεωρία της Πληροφορίας ή Θεωρία των Πληροφοριών Κανάλι – Σύστημα", Διπλωματική εργασία, Πειραιάς, Ιούνιος 2011

ΚΕΦΑΛΑΙΟ 2

ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

2. Θεωρητικό υπόβαθρο

Στο κεφάλαιο αυτό θα αναφέρουμε την προαπαιτούμενη θεωρία για την κατανόηση των επόμενων κεφαλαίων.

2.1 Αριθμητική συστήματος

Ένα αριθμητικό σύστημα είναι ένα σύνολο από ψηφία, τα οποία χρησιμοποιούνται για αρίθμηση και υπολογισμούς. Τα αριθμητικά συστήματα διαχωρίζονται σε δυαδικό, οκταδικό, δεκαδικό (το οποίο είναι και το πιο χρησιμοποιούμενο) και το δεκαεξαδικό.

Το δεκαδικό σύστημα χρησιμοποιεί δέκα ψηφία (τους αριθμούς 0-9) και έχει βάση το 10 καθώς η αξία των ψηφίων εξαρτάται από τις θέσεις τους. Το πρώτο ψηφίο του αριθμού είναι το περισσότερο σημαντικό ψηφίο (Most Significant Digit – MSD), γιατί έχει τη μεγαλύτερη αξία, ενώ το τελευταίο ψηφίο είναι το λιγότερο σημαντικό (Least Significant Digit – LSD) γιατί έχει τη μικρότερη αξία.

Η ανάλυση του δεκαδικού αριθμητικού συστήματος είναι ένας τρόπος κωδικοποίησης που στηρίζεται στη μέθοδο των βαρών. Παραδείγματος χάρη ο αριθμός 1908 νοείται στην πραγματικότητα με πλήθος μονάδων ίσο με :[16]

$$1*10^3+9*10^2+0*10^1+8*10^0$$

Σύμφωνα με τα ανωτέρω, τα βάρη είναι οι αριθμοί 10^3 , 10^2 , 10^1 και 10^0 , με απλά λόγια τα βάρη σχηματίζονται από διαδοχικές δυνάμεις του 10, το οποίο ονομάζεται βάση του συστήματος και το 0 είναι απαραίτητο για να διατηρούνται τα ψηφία στη σωστή θέση. Σε ένα εκθεσιακό σύστημα ένας θετικός αριθμός N παριστάνεται από μια ακολουθία ψηφίων :

$$\alpha_n \, \alpha_{n-1} \ldots \alpha_0 \cdot \alpha_{-1} \ldots \alpha_{-m}$$

η οποία αντιπροσωπεύει πλήθος μονάδων : [15]

$$N = \sum_{i=-m}^{n} \alpha_i \cdot \beta^i$$

όπου :

β είναι η βάση του αριθμού (ακέραιος, $\beta > 1$)

α_i είναι τα ψηφία του αριθμού ($0 \leq \alpha_i < \beta$)

i είναι η τάξη του ψηφίου

n + 1 είναι το πλήθος των ακέραιων ψηφίων

m είναι το πλήθος των κλασματικών ψηφίων.

Η ακολουθία $\alpha_n\ \alpha_{n-1} \ldots \alpha_0$ αποτελεί το ακέραιο μέρος του αριθμού, ενώ η $\alpha_{-1}\ \alpha_{-2} \ldots \alpha_{-m}$ το κλασματικό του μέρος. Το α_n είναι το MSD ενώ το α_{-m} το LSD.

Η μικρότερη βάση που έχει νόημα είναι ο αριθμός 2. Για βάση β=2, το σύστημα ονομάζεται δυαδικό, για β = 3 τριαδικό, για β=8 οκταδικό, για β=10 δεκαδικό κοκ. Όταν β>10 χρειάζονται πρόσθετα σύμβολα για την παράσταση των επιπλέον ψηφίων, συγκεκριμένα για τα ψηφία 10 έως 15 του δεκαεξαδικού συστήματος χρησιμοποιούνται διεθνώς τα πρώτα γράμματα του λατινικού αλφαβήτου, συγκεκριμένα :

Δεκαδικό : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Δεκαεξαδικό : 0,1,2,3,4,5,6,7,8,9,A, B, C, D, E, F

Από την άλλη πλευρά, το δυαδικό σύστημα έχει βάση τον αριθμό 2, επομένως χρησιμοποιεί μόνο δύο ψηφία τα οποία συμβολίζονται με τους χαρακτήρες 0 και 1 και ονομάζονται bits. Το πρώτο ψηφίο του αριθμού είναι το περισσότερο σημαντικό ψηφίο (Most Significant Digit – MSD), γιατί έχει τη μεγαλύτερη αξία, ενώ το τελευταίο ψηφίο είναι το λιγότερο σημαντικό (Least Significant Digit – LSD) γιατί έχει τη μικρότερη αξία.

Παραδείγματος χάρη, τα βάρη των θέσεων του δυαδικού αριθμού 1011 φαίνονται στον ακόλουθο πίνακα :

Βάρη θέσεων δυαδικού αριθμού				
	MSB			**LSB**
Ψηφία	1	0	1	1

Θέση	3	2	1	0
Βάρος	2^3	2^2	2^1	2^0

Άρα ο αντίστοιχος δεκαδικός αριθμός θα είναι :

$$1011 = 1*2^3 + 0*2^2 + 1*2^1 + 1*2^0 = 8+0+2+1 = 11$$

Η μεγαλύτερη αριθμητική τιμή που μπορεί να παρασταθεί από ένα δυαδικό αριθμό μήκους n ψηφίων (bits) είναι $2^n - 1$ γιατί

$$1*2^{n-1} + 1*2^{n-2} + \ldots + 1*2^1 + 1*2^0 + 2^n - 1$$

Οπότε αν n είναι το πλήθος των ψηφίων ενός δυαδικού αριθμού που αντιστοιχεί σ' ένα δεκαδικό αριθμό με d ψηφία τότε :

$$2^n - 1 > 10^d - 1 \text{ και } n = d/\log 10^2 \cong d/0.3$$

Με λίγα λόγια η παράσταση του δυαδικού θα έχει περίπου τριπλάσια ψηφία από αυτή του δεκαδικού. Οι αριθμητικές πράξεις στο δυαδικό σύστημα είναι πιο απλές σε σχέση με αυτές άλλων συστημάτων.

Στον παρακάτω πίνακα παρουσιάζονται οι βασικές πράξεις των μονοψήφιων δυαδικών αριθμών (αριθμοί του ενός bit) :

Πράξεις μονοψηφίων δεκαδικών αριθμών							
Bits		**α+β**		**α-β**		**α*β**	**α/β**
α	**β**	**άθροισμ.**	**Κρατούμ.**	**διαφ.**	**κρατούμ.**		
0	0	0	0	0	0	0	-
0	1	1	0	1	1	0	0
1	0	1	0	1	0	0	-
1	1	1	1	0	0	1	1

2.2Πεδία

Οι αρχές κωδικοποίησης / αποκωδικοποίησης των μη – δυαδικών κωδικών βασίζονται στη θεωρία των Πεπερασμένων Πεδίων (Finite Fields) γνωστά και ως πεδία Galois (Galois Fields ή GF).

Για κάθε πρώτο αριθμό p υπάρχει ένα πεπερασμένο πεδίο GF(p) που περιέχει p στοιχεία. Είναι δυνατό να επεκτείνουμε το GF(p) σε ένα πεδίο με pm στοιχεία, το πεδίο επέκτασης του GF(p) το οποίο συμβολίζεται με $GF(p^m)$, όπου m είναι ένας μη-μηδενικός θετικός ακέραιος αριθμός. Τα στοιχεία του GF(p) είναι υποσύνολο του $GF(p^m)$.

Έστω ότι το πεδίο GF(2) είναι υποπεδίο του πεδίου επέκτασης $GF(2^m)$. Υπάρχουν μοναδικά στοιχεία στο πεδίο επέκτασης, τα οποία συμβολίζονται με α. Κάθε μη- μηδενικό στοιχείο του $GF(2^m)$ μπορεί να αναπαρασταθεί ως μια δύναμη του α. Συγκεκριμένα δημιουργείται ένα πεπερασμένο σύνολο στοιχείων F, αρχίζοντας με τα στοιχεία {0,1,α} και προσθέτονται επιπλέον στοιχεία που προκύπτουν αν πολλαπλασιάζεται κάθε φορά το τελευταίο στοιχείο με α. Οπότε προκύπτει :[4][14]

$$F = \{ 0,1,\alpha,\alpha^2,\ldots., \alpha^j,\ldots\ldots\} = \{ 0,\alpha^0,\alpha^1,\alpha^2,\ldots\ldots\alpha^j,\ldots..\}$$

Για να λάβουμε τα πεπερασμένα στοιχεία του $GF(2^m)$ από το F, επιβάλλουμε έναν κανόνα στο F, όπου λαμβάνουμε μόνο τα δύο πρώτα 2^m αλλά το σύνολο F είναι κλειστό ως προς την πράξη του πολλαπλασιασμού. Η συνθήκη κατά την οποία εξασφαλίζεται το κλειστό της πράξης του πολλαπλασιασμού περιγράφεται από το μη – αναγόμενο (irreducible) πολυώνυμο

$$\alpha\,(2^m-1) + 1 = 0$$

ή

$$\alpha\,(2^m-1) + 1 = \alpha^0$$

Κάθε στοιχείο με δύναμη > ή = του 2^m-1 μπορεί να αναχθεί σε ένα στοιχείο δύναμης < του 2^m-1, σύμφωνα με την επόμενη σχέση :

$$a^{(2^m+n)} = a^{(2^m-1)} \qquad a^{(n+1)} = a^{(n+1)}$$

[4] Θεόδωρος Ρουδας, Σχεδίαση κωδικοποιητή – αποκωδικοποιητή Reed Solomon, Διπλωματική εργασία, Πανεπιστήμιο Πατρών

Με βάση την προηγούμενη σχέση μπορούμε να σχηματίσουμε από τη μη – πεπερασμένη ακολουθία F μια πεπερασμένη ακολουθία F * όπως φαίνεται παρακάτω :

$F^* = \{ 0,1,\alpha,\alpha^2,\ldots, \alpha^{2^m-2}, \alpha^{2^m-1}, \alpha^{2^m},\ldots\} = \{0,1,\alpha, \alpha^2,\ldots, \alpha^{2^m-2}, \alpha^{2m},\alpha^0, \alpha^1, \alpha^2\ldots.\}$

Επομένως καταλήγουμε στο ότι τα στοιχεία του πεπερασμένου πεδίου $GF(2^m)$ είναι τα ακόλουθα :

$$GF(2^m) = \{0,1,\alpha,\alpha^2,\ldots., \alpha^{2^m-2}\}$$

Κάθε ένα από τα 2^m στοιχεία του πεπερασμένου πεδίου, $GF(2^m)$, μπορεί να αναπαρασταθεί από ένα διακριτό πολυώνυμο βαθμού ≥ με το m-1. Ο βαθμός του πολυωνύμου αντιστοιχεί στον εκθέτη της μεγαλύτερης δύναμης και όλα τα μη – μηδενικά στοιχεία του $GF(2^m)$ αναπαριστώνται ως ένα πολυώνυμο $\alpha_i(X)$ στο οποίο τουλάχιστον ένας από τους m συντελεστές είναι μη – μηδενικός.

Για $i = 0,1,2,\ldots.2^m - 2$ ισχύει

$$\alpha^i = \alpha_i (X) = \alpha_{i,0} + \alpha_{i,1} X + \alpha_{i,2} X^2 + \ldots.. + \alpha i,_{m-1} X^{m-1}$$

Σύμφωνα με την ανωτέρω σχέση, ο παρακάτω πίνακας δείχνει την αναπαράσταση των στοιχείων του πεδίου $GF(2^3)$, (Για m=3), που παράγεται από το μη – αναγόμενο πολυώνυμο $f(X) = 1+X+X^3$

Εκθετική αναπαράσταση	**Πολυωνυμική αναπαράσταση Στοιχεία Βάσης**		
	$\mathbf{X^0}$	$\mathbf{X^1}$	$\mathbf{X^2}$
0	0	0	0
α^0	1	0	0
α^1	0	1	0

α^2	0	0	1
α^3	1	1	0
α^4	0	1	1
α^5	1	1	1

Στο τρίτο κεφάλαιο αναλύονται οι γραμμικοί μπλοκ κώδικες, οι οποίοι μπορούν να θεωρηθούν ως προέκταση των γραμμικών δυαδικών κωδικών, όπου τα σύμβολα προέρχονται από το μη – δυαδικό πεδίο GF(2^m).

2.3Θόρυβος

Η προστασία μιας πληροφορίας από το θόρυβο, μπορεί να επιτευχθεί με τη διερεύνηση των σταθμών πλάτους του σήματος ή ακόμη καλύτερα με την κωδικοποίηση. Με την προσθήκη πλεοναζόντων bits στις λέξεις ενός κώδικα, μπορεί να ανιχνευτεί με αρκετή πιθανότητα, το πότε μια λέξη έχει αλλοιωθεί από το θόρυβο αλλά και μέσω της αλλοιωμένης λέξης μπορεί να ανακτηθεί η σωστή πληροφορία.

Ο θόρυβος είναι εγγενής σε κάθε φυσικό σύστημα. Ένα μεγάλο πρόβλημα που παρουσιάζεται κατά τη μετάδοση ή αποθήκευση πληροφοριών, είναι η αλλοίωσή τους λόγω της πανταχού παρουσίας του θορύβου. Οι επιπτώσεις που μπορεί να έχει ο θόρυβος σ’ ένα ψηφιακό σύστημα είναι : [15]

1) καμιά αλλοίωση της κατάστασης των σημάτων, διότι η τρέχουσα στάθμη του θορύβου είναι μέσα στα όρια ανοχής του συστήματος,
2) αλλοίωση ενός ή περισσοτέρων bits μιας λέξης.

Ο θόρυβος από μαθηματικής πλευράς είναι στατιστικό φαινόμενο. Το πλάτος του θορύβου μπορεί να γίνει απεριόριστα μεγάλο και η χρονική συμπεριφορά του να είναι απρόβλεπτη. Η

επίδραση του θορύβου μετράται με την πιθανότητα p να συμβεί ένα λάθος, δηλ. να αλλοιωθεί ένα bit κατά τη μετάδοση μιας λέξης, οπότε η πιθανότητα να συμβούν N λάθη ταυτόχρονα στην ίδια λέξη είναι p^N , δηλαδή πολύ μικρή, άρα η μελέτη των κωδικών θα περιοριστεί κυρίως στην περίπτωση ενός λάθους. [18]

Τέλος, σε έναν κώδικα, ονομάζεται απόσταση Hamming ή αλλιώς απόσταση μεταξύ δύο λέξεών του, το πλήθος των bits που πρέπει να αλλάξουν τιμή για να ταυτιστεί η μια λέξη με την άλλη, για παράδειγμα οι λέξεις 0110 και 0101 έχουν απόσταση 2. Στο επόμενο κεφάλαιο περιγράφονται αναλυτικά οι κώδικες Hamming, οι οποίοι αποτελούν την πρώτη κατηγορία γραμμικών κωδικών που επινοήθηκαν για τη διόρθωση σφαλμάτων.

2.4Hamming

Οι κώδικες Hamming είναι η πρώτη κατηγορία γραμμικών κωδικών που επινοήθηκαν για τη διόρθωση σφαλμάτων, ενώ οι παραλλαγές τους, βρίσκουν ευρεία εφαρμογή στη διαχείριση σφαλμάτων στα συστήματα ψηφιακής επικοινωνίας και αποθήκευσης.

Οι κώδικες Hamming ορίζονται ως εξής : [14]

Μήκος κώδικα : $n = 2^m - 1$

Πλήθος συμβόλων πληροφορίας : $k = 2^m - m - 1$

Πλήθος συμβόλων ελέγχου ισοτιμίας : $n - k = m$

Ικανότητα διόρθωσης σφαλμάτων : $t = 1$ ($d_{min} = 3$)

Η μήτρα ελέγχου ισοτιμίας αυτών των κωδικών αποτελείται από όλα τα μη-μηδενικά m-διάστατα διανύσματα ως στήλες. Σε συστηματική μορφή οι στήλες της μήτρας H διατάσσονται σύμφωνα με τον τύπο

$$H = [\ I_m\ Q\ ]$$

όπου I_m είναι η m x m μοναδιαία μήτρα και η υπο-μήτρα Q αποτελείται από $2m - m - 1$ στήλες, οι οποίες είναι m-διάστατα διανύσματα με βάρος μεγαλύτερο ή ίσο από 2.

Παραδείγματος χάρη, για m = 3, η μήτρα ισοτιμίας του κώδικα Hamming με μήκος 7 μπορεί να αναπαρασταθεί με τη μορφή :

$$H = \begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

Οι στήλες της μήτρας Q μπορούν να διαταχθούν με οποιαδήποτε σειρά, χωρίς αυτό να επηρεάζει την ιδιότητα της απόστασης και την κατανομή του βάρους του κώδικα.

Εφόσον οι στήλες της μήτρας Η είναι μη – μηδενικές και διακριτές, το άθροισμα των δύο στηλών της Η δεν μπορεί να είναι μηδενικό. Με βάση τις ιδιότητες της ελάχιστης απόστασης κώδικα μπλοκ, προκύπτει ότι η ελάχιστη απόσταση ενός κώδικα Hamming είναι 3, επομένως ο κώδικας έχει την ικανότητα να διορθώσει όλα τα πρότυπα λάθους με ένα σφάλμα και να ανιχνεύσει όλα τα πρότυπα λάθους με δύο σφάλματα.

ΚΕΦΑΛΑΙΟ 3

ΚΩΔΙΚΟΠΟΙΗΣΗ

3. Κωδικοποίηση

Η κωδικοποίηση είναι η πιο άμεση εφαρμογή της θεωρίας της πληροφορίας και αποτελεί την πιο σημαντική διαδικασία ενός συστήματος επικοινωνιών. Κατά τη διαδικασία κωδικοποίησης τα αναλογικά σήματα μετατρέπονται σε ψηφιακά και τα ψηφιακά σήματα μετατρέπονται σε τέτοια μορφή ώστε να είναι δυνατή η μετάδοση τους από το φυσικό μέσο.

3.1Κώδικες διόρθωσης

Οι συνελικτικοί κώδικες και οι μπλοκ κώδικες αποτελούν τις δύο μεγαλύτερες κατηγορίες των κωδίκων διόρθωσης λαθών (error-correcting-codes). Η κύρια διαφορά μεταξύ των δύο κατηγοριών είναι ότι στους συνελικτικούς κώδικες, σε αντίθεση με τους μπλοκ κώδικες, υπάρχει μνήμη στον κωδικοποιητή.

3.1.1 Συνελικτικοί κώδικες (Convolution codes)

Οι συνελικτικοί κώδικες άρχισαν να χρησιμοποιούνται κατά τη δεκατετία του 1970 και είναι από τις πρώτες κατηγορίες κωδικοποίησης που εμφανίστηκαν. Χρησιμοποιούνται κυρίως από τηλεπικοινωνιακές ζεύξεις οι οποίες έχουν να αντιμετωπίσουν ισχυρό Gaussian προσθετικό θόρυβο. Βέβαια, με την πάροδο του χρόνου αναπτύχθηκαν διάφορες τεχνικές κωδικοποίησης οι οποίες έχουν πολύ καλυτέρα αποτελέσματα και πιο ευέλικτες τεχνικές.

Οι συνελικτικοί κώδικες αποτελούν γραμμικούς κώδικες όπου η δομή τους σε συνδυασμό με το γεννήτορα πίνακα τους είναι τέτοια που η κωδικοποίηση χρειάζεται πλήθος ψηφιακών φίλτρων τα οποία πρέπει να είναι γραμμικά και χρονικά αμετάβλητα. Από την εκτέλεση της κωδικοποίησης παράγεται η κωδική λέξη η οποία είναι το αποτέλεσμα της δειγματοληψίας που προκύπτει από τις εξόδους των φίλτρων.

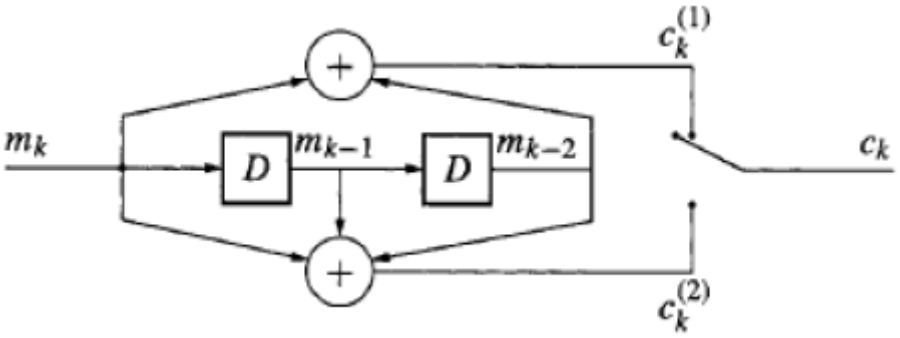
Η βασική αρχή λειτουργίας των συνελικτικών κωδίκων είναι η ύπαρξη μνήμης στον κωδικοποιητή. Δηλαδή, η έξοδος του αποκωδικοποιητή δεν εξαρτάται μόνο από την είσοδο

του την δεδομένη χρονική στιγμή αλλά από προηγούμενες εισόδους. Ο συνελικτικός κωδικοποιητής δέχεται συνεχώς με σύμβολα τα οποία δεν διαχωρίζονται σε μπλοκ ενώ κάθε στιγμή δειγματολειπτούνται οι έξοδοι του κωδικοποιητή που προκύπτουν ως modulo-2 αθροίζοντας το τρέχον σύμβολο με τα προηγούμενα. Επομένως, πρόκειται για κώδικες R=k/n, όπου k (καινούρια σύμβολα μετάβασης) καταχωρητές μετάβασης, ένας για κάθε bit εισόδου πληροφορίας και n (σύμβολα εξόδου) κωδικοποιημένα bit εξόδου ως γραμμικοί συνδυασμοί των περιεχομένων των καταχωρητών και των bit της πληροφορίας εισόδου.[5]

Γενικά, κάθε ακολουθία από σύμβολα $m(x)=[\mathrm{K}\,, m_{-2}, m_{-1}, m_0, m_1, m_2, \mathrm{K}]$ που εισέρχεται στον συνελικτικό κωδικοποιητή μπορεί να περιγραφεί ως μια σειρά δυνάμεων μιας μεταβλητής x με τιμές από ένα πεδίο F. Μια τέτοια ακολουθία μπορεί να περιγραφεί και ως μια σειρά Laurent $m(x)=\sum_{l\ -\infty}^{\infty} m_j x^l$. Το πλήθος όλων των σειρών Laurent στο πεδίο F συμβολίζεται με $F[[x]]$. Άρα, ισχύει ότι $m(x)\in F[[x]]$. Για πολλές εισόδους χρησιμοποιούμε την αναπαράσταση $m^{(1)}(x), m^{(2)}(x)$ για τις επιμέρους ακολουθίες. Η τελική τιμή εισόδου δίνεται από τη σχέση $m(x)=\left[m^{(1)}(x), m^{(2)}(x)\right]\in F[[x]]^2$.

Για να γίνει καλύτερη κατανόηση των συνελικτικών κωδίκων θα εξεταστεί ο κωδικοποιητής του σχήματος 2.1 για ρυθμό R=1/2, που ισούται με παραγωγή 2 bit εξόδου για κάθε bit εισόδου πληροφορίας.

[5] Δημήτριος Νικολός, "Τεχνικές Σχεδίασης Συστημάτων για Εύκολο Έλεγχο της Ορθής τους Λειτουργίας", Παν. Πατρών, Μάρτιος 2009.



Σχήμα 2.1 Διάγραμμα συνελικτικού κωδικοποιητή με ρυθμό R=1/2[6]

Η είσοδος m(x) περνάει ανάμεσα από δύο φίλτρα τα οποία μοιράζονται στοιχεία της μνήμης και παράγουν τις δυο κωδικοποιημένες εξόδους. Ο ρυθμός του κώδικα είναι R=1/2. Οι δυο ακολουθίες που προκύπτουν στην έξοδο interleaved (δηλαδή, στην έξοδο κατά την οποία περνάει μία ακολουθία από σύμβολα και τα συνδυάζει μεταξύ τους) και παράγουν την τελική έξοδο c_k.

$$c_k^{(1)} = m_k + m_{k-2} \text{ και } c_k^{(2)} = m_k + m_{k-1} + m_{k-2}$$

Η σχέση εισόδου-εξόδου μπορεί να αναπαρασταθεί και μέσω συναρτήσεων μεταφοράς. Δηλαδή, $c^{(1)}(x) = g^{(1)}(x)m(x)$ και $c^{(2)}(x) = g^{(2)}(x)m(x)$.

Επίσης, κάθε ακολουθία εισόδου-εξόδου μπορεί να αναπαρασταθεί με πολυώνυμα όπου οι συντελεστές τους ανήκουν στο πεδίο GF(q). Ανάλογα με το πλήθος των bits που αντιστοιχούν σε κάθε σύμβολο της μεταφοράς της ακολουθίας εισόδου. Με τον ίδιο τρόπο γίνεται και η αναπαράσταση των συναρτήσεων μεταφοράς.

Χρησιμοποιώντας τον κωδικοποιητή του σχήματος 2.1 και δεδομένου ότι ένα σύμβολο εισόδου είναι ένα bit. Μια ακολουθία εισόδου $m = \{1,1,0,0,1,0,1\}$, θα έχει τη μορφή $m(x) = 1 + x + x^4 + x^6 \in GF(2)[[X]]$. Οι συναρτήσεις μεταφοράς είναι $g^{(1)}(x) = 1 + x^2$ και $g^{(2)}(x) = 1 + x + x^2$. Έτσι, προκύπτουν οι έξοδοι

[6] Σπουρλής Γεώργιος, "Αρχιτεκτονικές Διόρθωσεις Λαθών βασισμένες σε Κώδικες BCH", Μεταπτυχιακή Διπλωματική εργασία, Πάτρα, Μάρτιος 2012.

$$c^{(1)} = m(x)g^{(1)}(x) = \left(1 + x + x^4 + x^6\right)\left(1 + x^2\right) = 1 + x + x^2 + x^3 + x^4 + x^8$$

$$c^{(2)} = m(x)g^{(2)}(x) = \left(1 + x + x^4 + x^6\right)\left(1 + + x + x^2\right) = 1 + x^3 + x^4 + x^5 + x^7 + x^8$$

Τελικά, οι έξοδοι είναι $c^{(1)}(x) = \{1,1,1,1,1,0,0,0,1\}$ και $c^{(2)}(x) = \{1,0,0,1,1,1,0,1,1\}$.

Γενικά, ένας κωδικοποιητής συνελικτικού κώδικα με ρυθμό R=k/n σχετίζεται με ένα k × n πίνακα συνάρτησης μεταφοράς G(x). Δηλαδή, για το παράδειγμα του συνελικτικού κωδικοποιητή του σχήματος 2.1 ισχύει ότι $G(x) = \left[1 + x^2 \; 1 + x + x^2\right]$. [7]

3.1.2 Μπλοκ κώδικες (block codes)

Οι κώδικες μπλοκ είναι γραμμικοί κώδικες μονοσήμαντης απεικόνισης στοιχείων από ένα σύνολο A σε ένα άλλο σύνολο B. Δηλαδή, σε κάθε στοιχείο του μη κενού συνόλου A αντιστοιχεί ένα και μόνο ένα στοιχείο του μη κενού συνόλου B. Τα στοιχεία του συνόλου A ορίζονται ως λέξεις πληροφορίας (infowords) και τα στοιχεία του συνόλου B ορίζονται ως κωδικές λέξεις (codewords). Οι κωδικές λέξεις σε ένα (n,k) μπλοκ κώδικα c αποτελείται από ένα σύνολο q^k για n διανύσματα όπου, q είναι τα σύμβολα του αλφαβήτου του κώδικα. Ο μπλοκ κωδικοποιητής, ουσιαστικά, αντιστοιχεί ένα μήνυμα από k σύμβολα στις αντίθετες κωδικές λέξεις. Από τη μαθηματική δομή του κώδικα προκύπτει ότι τα n,k είναι επιπλέον σύμβολα για τα όποια ισχύει ότι n>k. Για να είναι δυνατή η διόρθωση λαθών είναι αναγκαίο η απεικόνιση να είναι μονοσήμαντη. Βέβαια, η αντιστοίχηση 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 μία διάταξη χωρίς μνήμη. Αφού, η έξοδος, δηλαδή η κωδική λέξη, δεν εξαρτάται από προηγούμενες εισόδους αλλά μόνο από την είσοδο στη δεδομένη χρονική στιγμή. Ένας μπλοκ κώδικας μπορεί να θεωρηθεί γραμμικός αν και μόνο αν ισχύει ότι στο πεδίο F_q όπου q είναι τα σύμβολα για

[7] M. C. Valenti, “Turbo Codes and Iterative processing”, in Proc. IEEE New Zealand Wireless Commun. Symp. '98, Auckland New Zealand, Nov. 1998.

μήκος n οι κωδικές λέξεις q^k σχηματίζουν ένα διάνυσμα k διαστάσεων. Ο ρυθμός του κώδικα είναι R=k/n, όπου n είναι το μήκος του κώδικα και n η διάσταση του πίνακα. Μια από τις ιδιότητες των γραμμικών κωδίκων είναι ότι αν αθροίσουμε δύο κωδικές λέξεις το αποτέλεσμα θα είναι επίσης μία κωδική λέξη. Σε μία κωδική λέξη ο αριθμός της σε bits που ισούται με τη μονάδα καλείται βάρος Hamming της κωδικής λέξης και συμβολίζεται με το γράμμα w. Η διαφορά των θέσεων στις οποίες ορίζονται δύο κωδικές λέξεις αποτελεί την απόσταση Hamming και συμβολίζεται με το γράμμα d. Σε ένα γραμμικό μπλοκ κώδικα πρέπει το βάρος Hamming να ισούται με την ελάχιστη απόσταση Hamming, δηλαδή $w_{min} = d_{min}$. Επομένως, σε κάθε γραμμικό μπλοκ κώδικα υπάρχει η δυνατότητα διόρθωσης όπου πρέπει να ισχύει ότι διόρθωσης $t \leq (d_{min}-1)/2$.

Κατά τη διαδικασία της κωδικοποίησης τα k σύμβολα του μπλοκ μετατρέπονται σε ένα μπλοκ από n σύμβολα. Έτσι, η ακολουθία των συμβόλων της πληροφορίας είναι $m(x) = [m_0, m_1, m_2, \text{K}, m_k]$ όπου προκύπτει και η κωδική λέξη η οποία εκφράζεται ως $c(x) = [c_0, c_1, c_2, \text{K}, c_k]$. Για την μετατροπή της μιας ακολουθίας στην άλλη χρησιμοποιείται ο γεννήτορας πίνακας του κώδικα G[k × n]. Πολλαπλασιάζοντας τη λέξη της πληροφορίας επί τον γεννήτορα πίνακα του κώδικα λέξη c, δηλαδή c = mG.

Παρατηρούμε, λοιπόν, ότι η παραπάνω διαδικασία κωδικοποίησης, σε σχέση με το υλικό, είναι πιο αποτελεσματική καθώς δεν χρειάζεται να γίνει αποθήκευση q^k διανυσμάτων αλλά αποθηκεύονται μόνο τα k × n στοιχεία του πίνακα G. Στην πραγματικότητα, ο γεννήτορας πίνακας είναι k διανύσματα γραμμικώς ανεξάρτητα μεταξύ τους γραμμικοί συνδυασμοί των οποίων δημιουργούν τον k-διάστατο χώρο διανυσμάτων του κώδικα. Είναι σημαντικό να τονίσουμε ότι η αναπαράσταση των κωδικών λέξεων που παρέχονται με την χρήση του γεννήτορα πίνακα G δεν είναι μοναδική.

Υπάρχει και η περίπτωση ένας κώδικας μπλοκ να μην είναι γραμμικός, αλλά συστηματικός. Ο συστηματικός κωδικοποιητής αποστέλλει το μήνυμα της πληροφορίας χωρίς καμία αλλοίωση στην κωδική λέξη. Η συστηματικότητα μιας κωδικής λέξης εξαρτάται από τον γεννήτορα πίνακα και όχι από τον κώδικα. Οι συστηματικός γεννήτορας πίνακας (δηλαδή, που έχει την ιδιότητα της συστηματικότητας) μπορεί να έχει την εξής μορφή

$$G = \left[P\, I_k \right] = \begin{bmatrix} p_{0,0} & p_{0,1} & \text{L} & p_{0,\text{n}-\text{k}-1} & 1 & 0 & 0 \\ p_{1,0} & p_{1,1} & \text{L} & p_{1,n-k-1} & 0 & 1 & 0 \\ \text{M} & \text{M} & \text{M} & \text{M} & \text{M} & \text{M} & \text{M} \\ p_{k-1.0} & pk-1,1 & \text{L} & p_{k-1,n-k-1} & 0 & 0 & 1 \end{bmatrix}$$

Όπου, ο πίνακας $I_k[k \times k]$ είναι μοναδιαίος και ο P[k × (n-k)] πίνακας παράγει τα σύμβολα ισοτιμίας. Η διαδικασία της κωδικοποίησης είναι $c = m\left[P\, I_k \right] = \left[mP_{\,m} \right]$. Η κωδική λέξη χωρίζεται σε δυο τμήματα από το τμήμα m που περιέχει το μήνυμα το οποίο δεν έχει αλλοιωθεί και από το τμήμα mP που αποτελεί τα σύμβολα ελέγχου ισοτιμίας(parity check symbols).

Δυο γραμμικοί κώδικες οι οποίοι είναι ίδιοι, εκτός από μια μετάθεση μεταξύ κάποιων τμημάτων του κώδικα λέγονται ισοδύναμοι κώδικες. Γεννήτορες πινάκες που αντιστοιχούν σε ισοδύναμους κώδικες προκύπτουν από δυο λειτουργίες, την ανταλλαγή στηλών και τους γραμμικούς συνδυασμούς γραμμών.

Εκτός από τον γεννήτορα πίνακα G σημαντικό ρόλο στους γραμμικούς μπλοκ κώδικες έχει και ο πίνακας ελέγχου ισοτιμίας ο οποίος συμβολίζεται με Η. Ο πίνακας αυτός αποτελείται από n-k διανύσματα n συμβόλων και αποτελεί τον διανυσματικό χώρο για έναν (n,n-k) κώδικα ο οποίος συμβολίζεται ως C_T. Βασική ιδιότητα των πινάκων G και Η είναι ότι είναι ορθογώνιοι μεταξύ τους και συνεπώς ισχύει ότι $GH^T = 0$. Επίσης, οι κωδικές λέξεις αυτού του κώδικα που έχουν πλήθος $2^{\text{n-k}}$ είναι ορθογώνιες με τις λέξεις του κώδικα C και κάθε γραμμή του πίνακα Η είναι ορθογώνια ως προς κάθε έγκυρη κωδική λέξη του κώδικα C. Ο κώδικας C_t ονομάζεται δυικός του κώδικα C. Βάσει αυτών των ιδιοτήτων προκύπτει ότι κάθρε γραμμή του πίνακα Η είναι ορθογώνια ως προς κάθε έγκυρη κωδική λέξη του κώδικα C. Κατά συνέπεια, ο πίνακας Η μας παρέχει n-k σχέσεις τις οποίες θα πρέπει να επαληθεύουν μια κωδική λέξη για να είναι έγκυρη. Αυτή η ιδιότητα μπορεί να χρησιμοποιηθεί στον δέκτη για επαλήθευση ότι η λαμβανόμενη λέξη είναι κωδική λέξη του κώδικα. Η ιδιότητα αυτή μπορεί να εκφραστεί από τη σχέση $cH^T = 0$. Ακόμα έστω ότι ένας γραμμικός μπλοκ

κώδικας έχει πίνακα έλεγχου ισοτιμίας Η. Η ελάχιστη απόσταση d_{min} του κώδικα είναι ίση με τον μικρότερο θετικό αριθμό των στηλών του Η που είναι γραμμικώς εξαρτημένοι. [8]

3.2 Ανίχνευση Λαθών

Για την κατανόηση της λειτουργίας ανίχνευσης λαθών θα θεωρήσουμε ότι έχουμε έναν γραμμικό μπλοκ κώδικα (n,k) και μεταδίδουμε μια κωδική λέξη (του μπλοκ κώδικα) n συμβόλων μέσα από ένα κανάλι προσθετικού θορύβου. Το κανάλι προσθέτει στην κωδική λέξη ένα σφάλμα e, n συμβόλων με αποτέλεσμα να εισέρχεται τελικά στον δέκτη μια λέξη r, n συμβόλων η οποία δεν είναι απαραίτητα έγκυρη κωδική λέξη. Έτσι, μπορούμε να πούμε ότι, ισχύει η σχέση $r = c + e$ με την αριθμητική να είναι στο πεδίο F_q. Το διάνυσμα λάθους e προσθέτει λάθη στις θέσεις όπου τα σύμβολα του έχουν διαφορετική τιμή του μηδενός. Αν κάθε σύμβολο του διανύσματος λάθους είναι μηδέν τότε το κανάλι δεν έχει εισάγει κανένα λάθος. Ως σύνδρομο σφάλματος s ορίζεται το διάνυσμα $s = rH^T$.

Για να είναι μια λέξη έγκυρη κωδική λέξη του κώδικα πρέπει να ισχύει ότι $cH^T = 0$, όπου Η είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα. Επομένως για το σύνδρομο ισχύει ότι $s = rH^T = (c + e)H^T = eH^T$.

Αν, όμως, $s = 0$ τότε η λέξη r που έφτασε στον δέκτη είναι έγκυρη κωδική λέξη. Σε κάθε άλλη περίπτωση γνωρίζουμε ότι σίγουρα υπάρχει λάθος στην λέξη.[9]

[8] Δημήτριος Νικολός, "Τεχνικές Σχεδίασης Συστημάτων για Εύκολο Έλεγχο της Ορθής τους Λειτουργίας", Παν. Πατρών, Μάρτιος 2009. & M. C. Valenti, "Turbo Codes and Iterative processing", in Proc. IEEE New Zealand Wireless Commun. Symp. '98, Auckland New Zealand, Nov. 1998.

[9] Δημήτριος Νικολός, "Τεχνικές Σχεδίασης Συστημάτων για Εύκολο Έλεγχο της Ορθής τους Λειτουργίας", Παν. Πατρών, Μάρτιος 2009.

3.2.1 Δυνατότητες τροποποίησης γραμμικών μπλοκ κωδίκων

Δυνατότητα της επέκτασης με την πρόσθεση ενός επιπλέον πλεονάζοντα όρου, παράγοντας έναν κώδικα (n+1, k, d+1), δηλαδή, έχει ένα επιπλέον σύμβολο ισοτιμίας αλλά και η απόσταση του κώδικα αυξάνει κατά 1. Επίσης, υπάρχει η δυνατότητα μείωσης με την διαγραφή ενός σύμβολου ισοτιμίας έτσι ο κώδικας γίνεται (n-1,k) . Με μείωση κατά p φορές υπάρχει η δυνατότητα για μείωση της απόστασης του κώδικα σε d-p. Επιπρόσθετα, υπάρχει και η δυνατότητα για εξαγωγή με την διαγραφή από τον κώδικα κάποιων κωδικών του λέξεων. Βεβαία αυτό πρέπει να γίνει κατάλληλα αν θέλουμε να παραμείνει γραμμικός ο κώδικάς μας. Η ελάχιστη απόσταση με αυτήν την τροποποίηση μπορεί να αυξηθεί.

Μια άλλη δυνατότητα είναι η αύξηση ενός κώδικα με την πρόσθεση νέων κωδικών λέξεων σε αυτόν. Βέβαια δεν εξασφαλίζεται ότι ο κώδικας που θα προκύψει θα είναι γραμμικός ενώ και η ελάχιστη απόσταση μπορεί να είναι μειωμένη. Επιπλέον, υπάρχει η δυνατότητα για μείωση του μήκους ενός κώδικα με την διαγραφή ενός συμβόλου μηνύματος. Αυτό σημαίνει ότι αφαιρείται μια γραμμή και μια στήλη από τον γεννήτορα πίνακα. Έτσι έχουμε έναν (n-1, k-1) κώδικα. Τέλος, υπάρχει η δυνατότητα για αύξηση του μήκους ενός κώδικα με την πρόσθεση ενός συμβόλου μηνύματος. Αυτό σημαίνει ότι μια γραμμή και μια στήλη προστίθεται στον γεννήτορα πίνακα. Με αυτόν τον τρόπο ένας (n,k) κώδικας γίνεται (n+1, k+1) κώδικας.

3.2.2 Κυκλικοί κώδικες

Οι κυκλικοί κώδικες αποτελούν ένα υποσύνολο των γραμμικών κωδίκων μπλοκ. Πρόκειται για κώδικες που έχουν επιπλέον αλγεβρική δομή για να έχουν αποτελεσματικότερη κωδικοποίηση και αποκωδικοποίηση. Η βάση των κυκλικών κωδίκων είναι οι πράξεις με πολυώνυμα με βασική αλγεβρική δομή το δακτύλιο. Πιο συγκεκριμένα, ένας κυκλικός κώδικας είναι ένας γραμμικός μπλοκ κώδικας με την επιπλέον ιδιότητα ότι σε μια κωδική λέξη c η κυκλική ολίσθηση των ψηφίων της είναι και αυτή κωδική λέξη. Η δομή των κυκλικών κωδίκων βασίζεται στην αναπαράσταση της κωδικής λέξης αλλά και του γεννήτορα πίνακα με πολυώνυμα. Οι κυκλικοί κώδικες κατασκευάζονται με καταχωρητές ολίσθησης. Ένας υλοποιήσιμος κυκλικός κώδικας βασίζεται στο γεγονός ότι το πολυώνυμο

οποιασδήποτε κωδικής λέξης προκύπτει από τον πολλαπλασιασμό του πολυωνύμου γεννήτριας g(p) επί το πολυώνυμο X(p) που αντιστοιχεί στην ακολουθία της πληροφορίας εισόδου.

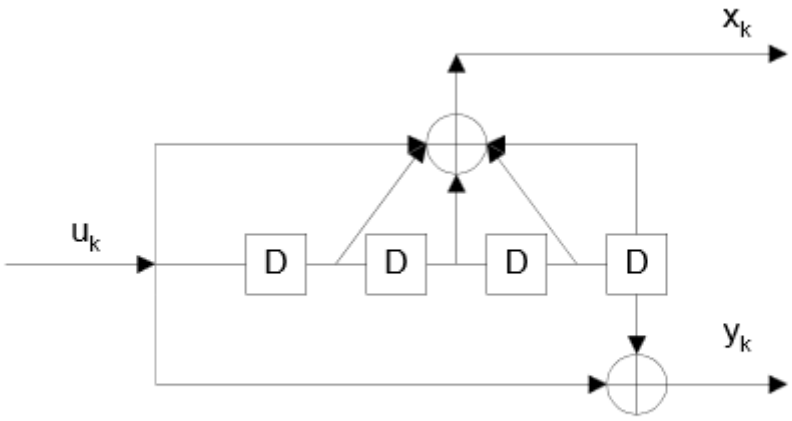
3.2.3 Σύνθετοι κώδικες

Οι σύνθετοι κώδικες βασίζονται σε συνδυασμό απλών κωδικών.. Για την αποκωδικοποίηση ενός σύνθετου κώδικα πραγματοποιείται με την χρήση μεθόδων αποκωδικοποίησης των απλών συνιστωσών κωδίκων. Φυσικά, η αποκωδικοποίηση η οποία προκύπτει δεν είναι τόσο καλή. Ωστόσο, έχει πάρα πολύ ικανοποιητικά αποτελέσματα. Οι πιο σημαντικοί σύνθετοι κώδικες είναι οι turbo κώδικες. Άλλες κατηγορίες είναι οι κώδικες γινομένου και οι αλυσιδωτοί κώδικες. Έχουν γίνει διάφορες μελέτες σε μεθόδους οι οποίες αποσκοπούν στην αύξηση του μήκους των μπλοκ κωδίκων αλλά ταυτόχρονα να μην αυξηθεί η πολυπλοκότητα της αποκωδικοποίησής τους.

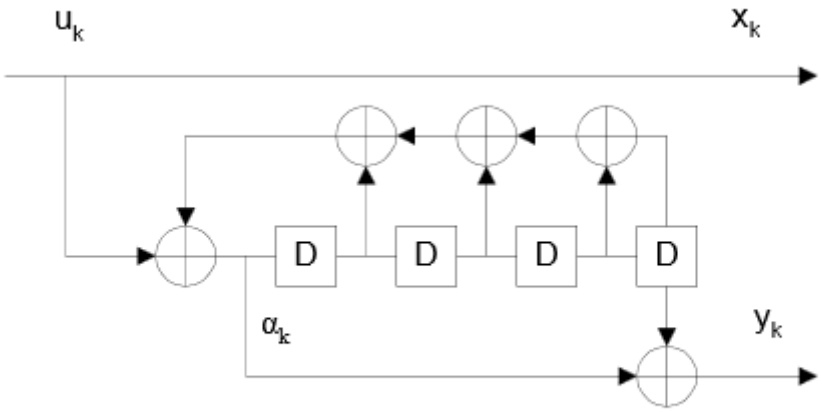
Αναδρομικοί κώδικες (recursive codes)

Οι αναδρομικοί κώδικες χρησιμοποιούν στην είσοδό τους, με κάποιο βρόγχο ανάδρασης, μία ή περισσότερες από τις εξόδους τους. Η είσοδος του καταχωρήτη ολίσθησης δεν είναι bit πληροφορίας u_k αλλά δυαδική μεταβλητή α_k η οποία προκύπτει από τη σχέση $\alpha_k = u_k + \sum_{i=1}^{k-1} g_i a_{k-1}$, όπου $g_i = 1 \; ή \; 0$ ανάλογα με το αν υπάρχει σύνδεση ή όχι. Για τον κώδικα του σχήματος 3.1(b) ισχύει ότι $g = (11111)$. Στην εικόνα εκτός από τον αναδρομικό συστηματικό κώδικα δίνεται και ο μη αναδρομικός συστηματικός κώδικας. [10]

[10] 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.



a) Non recursive-non systematic κωδικοποιητή



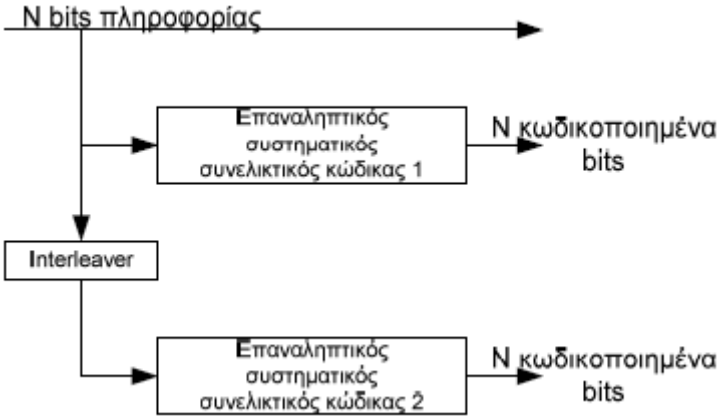
b) Recursive systematic κωδικοποιητή

Σχήμα 3.1 Μορφές κωδικοποίησης [11]

[11] 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.

3.2.4 Κώδικες Turbo

Ένας κωδικοποιητής turbo μπορεί να αποτελείται από δύο επιμέρους κωδικοποιητές συνδεδεμένους παράλληλα. Ένας τέτοιος τρόπος σύνδεσης ονομάζεται παράλληλη αλυσιδωτή κωδικοποίηση (parallel concatenation). Υπάρχουν, όμως, και συστήματα αλυσιδωτής κωδικοποίησης τα οποία συνδέονται σε σειρά (serial concatenation). Ο αριθμός και το είδος των επιμέρους κωδίκων μπορεί να υλοποιηθεί με διάφορους τρόπους, όπως για παράδειγμα να χρησιμοποιήσουμε τρεις ή περισσότερους κώδικες ανάλογα με την περίπτωση. Επιπλέον, έχει αποδειχτεί ότι με τη χρήση περισσότερων από δύο επιμέρους κωδικοποιητών μπορούμε να πετύχουμε καλύτερους turbo κώδικες (multiple turbo codes).[12] Στον turbo κωδικοποιητή έχουν επικρατήσει ως επιμέρους στοιχεία του οι αναδρομικοί συστηματικοί συνελικτικοί (Recursive Systematic Convolution – RSC) κώδικες.



Σχήμα 3.2 Διάγραμμα turbo κωδικοποιητή

Ο λόγος για τον οποίο επιλέγουμε τους RSC κώδικες είναι επειδή έχουν χαμηλές ταχύτητες στις SNR σχέσεις, σε σχέση με τους non-RSC κώδικες. Επιπλέον, σε πληροφορίες που έχουν μικρό βάρος Hamming μπορούν να δώσουν κατά την έξοδό τους κωδικές λέξεις πολύ μεγάλο βάρους. Η ιδιότητα αυτή οφείλεται στο βρόγχο ανάδρασης τον οποίο έχουν, με αποτέλεσμα

[12] D. Divsalar, F. Pollara, "On the Design of Turbo Codes", The Telecommunications and Data Acquisition Progress Report 42-123, July- September 1995, JPL, Pasadena, California, pp. 99-121, November 15, 1995.

όταν βρεθεί μια μονάδα εισόδου, συνεχώς ανακυκλώνεται προκαλώντας, έτσι, μια κωδική λέξη με πολύ μεγάλο βάρος.[13]

Για να κατανοήσουμε περισσότερο έναν turbo κωδικοποιητή θα θεωρήσουμε τον turbo κωδικοποιητή ο οποίος αποτελείται από δύο RSC κώδικες οι οποίοι είναι όμοιοι. Ο πρώτος κωδικοποιητής λειτουργεί απευθείας με την ακολουθία των bit πληροφορίας $u=(u_1,u_2,...,u_N)$ και παράγει δύο ακολουθίες εξόδου x_k, y_{1k}. Ο δεύτερος κωδικοποιητής λειτουργεί με την ίδια ακολουθία εισόδου αφού πρώτα αυτή περάσει από μία συσκευή αναδιάταξης (interleaver).[14]

Ο interleaver λαμβάνει την ακολουθία των bit πληροφορίας και την εξάγει με διαφορετική σειρά σύμφωνα με κάποιον (προ)καθορισμένο κανόνα. Έτσι ο δεύτερος κωδικοποιητής δέχεται τα ίδια bit αλλά με διαφορετική σειρά και παράγει με τη σειρά του την ακολουθία εξόδου y_{2k}. Υποθέτουμε ότι έχουμε ένα κώδικα ρυθμού R= 1/3 όπου οι επιμέρους κώδικες έχουν μνήμη M=4 και οι έξοδοί του δίνονται από τις σχέσεις

$$x_k = u,\ y_{1k} = ug_\alpha / g_b,\ y_{2k} = u' g_\alpha / g_b$$

όπου τα πολυώνυμα είναι $g_\alpha = 10001$ και $g_b = 11111$. Η σχεδίαση των επιμέρους κωδικοποιητών αποτελεί σημαντικό παράγοντα για την συμπεριφορά του turbo κώδικα.[15]

Σε ένα turbo κωδικοποιητή ο ρυθμός διαφοροποιείται ανάλογα με τα διαφορετικά bit της πληροφορίας.

---

[13] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes", Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland, pp. 1064-1070, May 1993.

[14] M. C. Valenti, "Turbo Codes and Iterative processing", in Proc. IEEE New Zealand Wireless Commun. Symp. '98, Auckland New Zealand, Nov. 1998.

[15] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes", Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland, pp. 1064-1070, May 1993.

ΚΕΦΑΛΑΙΟ 4

ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗ

4 Αποκωδικοποίηση

Υπάρχουν δύο κατηγορίες αποκωδικοποιητών. Η μια κατηγορία είναι οι αποκωδικοποιητές πλήρους διόρθωσης λαθών, οι οποίοι έχοντας τη λέξη r την οποία παραλαμβάνουν επιλέγουν την κωδική λέξη c η οποία ελαχιστοποιεί μια συνάρτηση όπως είναι η απόσταση Hamming dH(r,c) και με τη χρήση κατάλληλων δομών όπως οι στάνταρτ πίνακες (standard array) υπάρχει δυνατότητα για πλήρη αποκωδικοποίηση.

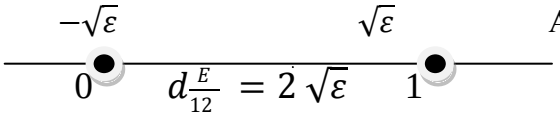
Οι αποκωδικοποιητές αυτού του είδους έχουν πολύ μεγάλη πολυπλοκότητα και απαιτούν πολύ υλικό με αποτέλεσμα να μην είναι δυνατή η χρήση τους στην πράξη. Στη δεύτερη κατηγορία είναι οι αποκωδικοποιητές περιορισμένης δυνατότητας διόρθωσης λαθών, οι οποίοι επιλέγουν την κωδική λέξη c δεδομένης της ληφθείσας λέξης r χρησιμοποιώντας και πάλι τις ίδιες συναρτήσεις με τη διαφορά ότι αρκεί να ισχύει ότι $dH(r,c) \leq t$. Εάν σε έναν τέτοιο αποκωδικοποιητή δεν μπορεί να βρεθεί μια κωδική λέξη, ώστε να ικανοποιεί την συνθήκη αυτή, τότε έχουμε αποτυχία του αποκωδικοποιητή.

Οι σημαντικότεροι τρόποι αποκωδικοποίησης είναι η αποκωδικοποίηση “Soft-Απόφασης” και η αποκωδικοποίηση “Hard-Απόφασης”.

4.1 Soft-Απόφασης

Η φώραση – σήματος η οποία βασίζεται στην Ευκλείδεια απόσταση μεταξύ του λαμβανόμενου και του διαβιβαζόμενου σήματος ονομάζεται αποκωδικοποίηση soft – απόφασης.

Αν χρησιμοποιηθεί δυαδικό PSK [17]



Αστερισμός διαδυκού PSK

Μια κωδική λέξη $C_i = (C_{i1,}C_{i2\ldots,}C_{in,})$ Απεικονίζεται στην ακολουθία

όπου $S_i(t) = \sum_{k=1}^{n} \Psi_{i\kappa}(t - (\kappa - 1)T)$

$$\Psi_{i\kappa\ (t)} = \begin{cases} \Psi\ (t), & C_{i\kappa} = 1 \\ -\Psi\ (t), & C_{i\kappa} = 0 \end{cases}$$

Το σήμα ψ (t) είναι ένα σήμα διάρκειας Τ και ενέργειας ε, όπου είναι ίσο με μηδέν έξω από το διάστημα [0, Τ].

Η Ευκλείδεια απόσταση μεταξύ δύο οποιονδήποτε κυματομορφών σήματος είναι

$$\left(d\ \frac{E}{ij}\right)^2 = \sum_{\substack{1\le k\le n \\ k:\ C_{i\kappa} \neq C_{jk}}}^{n} \left(\pm 2\sqrt{\varepsilon}^{\ 2}\right) = 4d\frac{H}{ij}E$$

Αυτή δίνει μια απλή σχέση μεταξύ Ευκλείδειας και Hamming απόστασης όταν χρησιμοποιείται ένα σήμα σηματοδοσίας PSK (ή οποιοδήποτε άλλο σχήμα αντίποδης σηματοδοσίας).

Η μέση πιθανότητα σφάλματος για δυαδικά αντίποδα σήματα είναι

$P_e = Q\ \mathrm{C}\sqrt{\frac{2e}{No}}$ και επειδή $d^E = 2\sqrt{E}$ έχουμε $P_e = Q\ (\frac{d^E}{\sqrt{2N0}})$

Αν χρησιμοποιηθεί η σχέση μεταξύ Ευκλείδειας και Hamming απόστασης έχουμε

$$\text{P (j λήφθηκε | i στάλθηκε) = Q (}\sqrt{\frac{d\sqrt{\frac{H}{ij}}\ 2E}{No}}\text{)}$$

Η Q(y) είναι μια φθίνουσα συνάρτηση του y. Επίσης $d_{ij} \geq d_{min}$ έτσι έχουμε το ακόλουθο φράγμα στην πιθανότητα σφάλματος ενός συστήματος το οποίο χρησιμοποιεί αντίποδη σηματοδοσία.

$$\text{P (j λήφθηκε | i στάλθηκε) = Q (}\sqrt{\frac{P_{min}\ 2E}{No}}\text{)}$$

Γνωρίζουμε ότι για M – αδικά ορθογώνια σήματα, η πιθανότητα σφάλματος συμβόλου P_M φράσσεται εκ των άνω από το φράγμα ένωσης (union bound)

$$P_M \leq (M - I) \cdot P_2 = (M - 1) \cdot Q(\sqrt{\frac{E_s}{No}}$$

Χρησιμοποιώντας το φράγμα αυτό έχουμε

$$\text{P (σφάλμα | i στάλθηκε)} \leq \text{(M – 1)} \cdot \text{Q (}\sqrt{\frac{d_{min}\ 2E}{No}}\text{)}$$

και αν δεχθούμε ισοπίθανα μηνύματα, έχουμε τελικά για την πιθανότητα σφάλματος

$$P_e \leq (M - 1) \cdot\ Q\ (\sqrt{\frac{d_{min}\ 2E}{No}})$$

Με τον όρο βέλτιστη αποδιαμόρφωση, εννοούμε ότι περνάμε το λαμβανόμενο σήμα r(t) μέσα από μια συστοιχία προσαρμοσμένων φίλτρων για να πετύχουμε ένα λαμβανόμενο διάνυσμα r και κατόπιν βρίσκουμε το πλησιέστερο προς το r σημείο του αστερισμού υπό την έννοια της Ευκλείδειας απόστασης.

Ο τύπος αποκωδικοποίησης που εμπλέκει την εύρεση της ελάχιστης Ευκλείδειας απόστασης καλείται αποκωδικοποίηση soft – απόφασης και απαιτεί υπολογισμούς με πραγματικούς αριθμούς.

Η Ευκλείδεια απόσταση μεταξύ δύο κυματομορφών σήματος είναι :

$$(d^H{}_{ij})^2 \sum_{\substack{1 \leq k \leq n \\ k: C_{ik} \neq C_{jk}}} [\Psi 1\ (t) -\ \Psi_2\ (t)]^2\ dt\ = 2d^H{}_{ij}\ E$$

Το φράγμα στην πιθανότητα σφάλματος ενός συστήματος το οποίο χρησιμοποιεί ορθογώνια σηματοδοσία είναι

$$P\ (\text{ j λήφθηκε} \mid \text{i στάλθηκε }) : Q\ (\ \sqrt{\frac{d_{min}\,E}{N0}}\ )$$

4.2 Hard-Απόφασης

Ένας πιο απλός τρόπος αποκωδικοποίησης είναι η λήψη αποφάσεων ως προς τις συνιστώσες του λαμβανόμενου διανύσματος r, και έπειτα η εύρεση της κωδικής λέξης που βρίσκεται πλησιέστερα σε αυτήν.

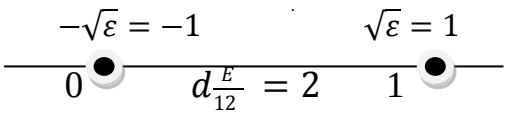
Κατά την αποκωδικοποίηση με hard – απόφαση ακολουθούνται τρία βασικά στάδια :[17]

- Εκτελούμε αποδιαμόρφωση περνώντας το λαμβανόμενο r(t) μέσω των προσαρμοσμένων φίλτρων και δειγματοληπτώντας την έξοδο για να πάρουμε το διάνυσμα r.
- Έπειτα ¨κβαντίζουμε¨ κάθε μια συνιστώσα με τη βοήθεια ενός κατωφλιού για να πάρουμε το δυαδικό διάνυσμα y.
- Αποκωδικοποιούμε βρίσκοντας την κωδική λέξη που είναι εγγύτερη στο y υπό την έννοια απόστασης Hamming.

Παράδειγμα

Κώδικας μπλοκ (3,1) με κωδικές λέξεις 000 και 111 οι οποίες μεταδίδονται με διαμόρφωση δυαδικού PSK με E=1.

Ο αστερισμός του δυαδικού PSK είναι



Αν το λαμβανόμενο διάνυσμα είναι r = (0,5 0,5 -3) η Ευκλείδεια απόσταση του r από τα δύο σημεία (1,1,1) και (-1,-1,-1) είναι αντίστοιχα

$$(\ d_E\ (r,(1,1,1)\ )\ )^2 = (0{,}5)^2 + (4)^2 = 16{,}5$$

$$(d_E\ (r,\ (-1,-1,-1)\ )\ )^2 = (1{,}5)^2 + (1{,}5)^2 + (-2)^2 = 8{,}5$$

Επομένως η soft – απόφαση οδηγεί στην αποκωδικοποίηση του r ως (-1,-1,-1), δηλαδή στην κωδική λέξη 000. Η πλησιέστερη κωδική λέξη υπό την έννοια απόστασης Hamming είναι το 111.

Συμπερασματικά, η αποκωδικοποίηση soft – απόφασης είναι η βέλτιστη μέθοδος και επιτυγχάνει μικρότερη πιθανότητα σφάλματος.

Συστηματικός τρόπος αποκωδικοποίησης με hard – απόφαση :

Μια τυπική διάταξη είναι ένας $2^{n-1} * 2^k$ πίνακας του οποίου τα στοιχεία είναι δυαδικές ακολουθίες μήκους n. Στην πρώτη γραμμή γράφονται όλες οι κωδικές λέξεις c_i $1 \leq i \leq 2^k$, ξεκινώντας από την λέξη c_1

$$c_1, c_2, c_3 \ldots . c_M$$

Από τις υπόλοιπες ακολουθίες μήκους n που δεν έχουν γραφεί στην πρώτη γραμμή, αυτή που έχει το ελάχιστο βάρος, την καλείται e_1 και γράφεται κάτω από την c_1.

C1 C2 C3 …… CM

e1 _ _ …….. _

Κάτω από κάθε μια από τις c_i γράφουμε την $e_i + c_i$ για $2 \leq i \leq M$

C1 C2 C3 …… CM

E_1 e_1+c_2 e_1 + c_3…… e_1 + c_M

Η Τρίτη γραμμή συμπληρώνεται με τον ίδιο τρόπο και η διαδικασία συνεχίζεται μέχρις ότου δεν μείνει καμία δυαδική n – άδα για να ξεκινήσει νέα γραμμή.

ΚΕΦΑΛΑΙΟ 5

ΥΛΟΠΟΙΗΣΗ (implementation)

Περιγραφή της Εφαρμογής Προσομοίωσης

Η κεντρική ιδέα της εφαρμογής που δημιουργήσαμε είναι η υλοποίηση της προσομοίωσης μιας block κωδικοποίησης ενός δυαδικού σήματος και η σύγκριση των αποτελεσμάτων των μεθόδων της SOFT και HARD αποκωδικοποίησης των κωδικών λέξεων, αντίστοιχα. Σκοπός της εφαρμογής είναι η παρατήρηση της αποτελεσματικότητας και της ορθότητας των μεθόδων για διαφορετικά σύνολα στοιχείων εισόδου, διαφορετικούς πίνακες γεννήτορες, διαφορετικές τιμές για την μεταβλητή Eb/No κλπ. Ο αλγόριθμος που θα ακολουθήσουμε για την εν λόγω υλοποίηση αποτελείται συνοπτικά από τα εξής βήματα:

1. Δημιουργία του σήματος εισόδου και αρχικοποίηση όλων των απαραίτητων μεταβλητών και σταθερών, ανάλογα με τις παραμέτρους που επιθυμούμε να εισάγουμε σε κάθε εκτέλεση
2. Παραγωγή των κωδικών λέξεων από τις λέξεις εισόδους με την χρήση του πίνακα γεννήτορα G
3. Διαμόρφωση των κωδικών λέξεων με χρήση του διαμορφωτή BPSK
4. Δημιουργία δείγματος λευκού θορύβου γκαουσιανής κατανομής και πρόσθεση του θορύβου στα διαμορφωμένα δείγματα για την παραγωγή των λαμβανόμενων δειγμάτων
5. Αποκωδικοποίηση των λαμβανόμενων δειγμάτων με SOFT και HARD αποκωδικοποίηση και παραγωγή των λέξεων πληροφορίας
6. Υπολογισμός των διαφορετικών στοιχείων των λέξεων πληροφορίας με τις αντίστοιχες λέξεις εισόδου για κάθε μέθοδο
7. Υπολογισμός της μετρικής BER για κάθε μέθοδο βάσει των αποτελεσμάτων του προηγούμενου βήματος
8. Σύγκριση των δεικτών BER των δύο μεθόδων ως προς τις τιμές του Eb/No και αναπαράστασής τους σε διάγραμμα.

Για την υλοποίηση της εφαρμογής επιλέχθηκε η προγραμματιστική γλώσσα MATLAB. Η εν λόγω επιλογή βασίστηκε στα ιδιαίτερα πλεονεκτήματα της γλώσσας στους μαθηματικούς υπολογισμούς, στους υπολογισμούς μεγάλου όγκου δεδομένων και στην εύχρηστη γραφική αναπαράσταση των αποτελεσμάτων. Επίσης, παρόλο που η γλώσσα MATLAB παρέχει μια πληθώρα έτοιμων και ιδιαίτερα αποτελεσματικών συναρτήσεων για σχεδόν το σύνολο των θεωρητικών υπολογισμών που απαιτούσε το περιεχόμενο της εργασίας (πχ υπολογισμός ευκλείδειας απόστασης, απόστασης Hamming, προσθήκη Gaussian λευκού θορύβου σε σήμα, ακόμα και έτοιμες εφαρμογές Block και άλλων κατηγοριών κωδικοποίησης), ωστόσο επιλέξαμε να εκτελέσουμε από μηδενική βάση σχεδόν όλους τους θεωρητικούς υπολογισμούς.

Αναλυτική περιγραφή των βημάτων του αλγόριθμου της εφαρμογής

1. Εισαγωγή παραμέτρων και αρχικοποίηση μεταβλητών

Ως πρώτο βήμα ορίζουμε τις παραμέτρους της εφαρμογής. Βασική παράμετρος είναι η μεταβλητή x ως παράμετρος της συνάρτησης hammgen(x), βάσει της οποίας παράγεται ο γεννήτορας πίνακας G(k,n) καθώς και τα μήκη εισόδων – κωδικών λέξεων, k και n αντίστοιχα. Ο υπολογισμός γίνεται βάσει της έτοιμης συνάρτησης του MATLAB, και ισχύει ότι $n = 2^x – 1$ και $k = 2^x – x - 1$

```
[~,G,n,k]=hammgen(x);
```

Η συνάρτηση hammgen χρησιμοποιείται για την παραγωγή του γεννήτορα πίνακα και του πίνακα συνδρομών ενός κώδικα block κατηγορίας Hamming. Για μεγαλύτερες τιμές του x παράγεται πίνακας G μεγαλύτερων διαστάσεων και μεγαλύτερες τιμές για τα μεγέθη k και n.

Δεύτερη παράμετρος είναι το όριο (threashold) βάσει του οποίου θα εκτελεστεί η αποδιαμόρφωση της HARD αποκωδικοποίησης. Για την σωστότερη κατανομή των λαμβανόμενων λέξεων στις τιμές 0 και 1 κατά την διαδικασία αποκωδικοποίησης, η τιμή του ορίου πρέπει να ισαπέχει μεταξύ των άκρων του διαστήματος στο οποίο θα κυμαίνονται οι λαμβανόμενες λέξεις. Για παράδειγμα εφόσον επιλέξουμε οι λέξεις να κυμαίνονται στο

συνεχές διάστημα τιμών [0,1] μέσω της κατάλληλης διαμόρφωσης και εύρος θορύβου, η τιμή 0.5 ενδείκνυται για τη μεταβλητή του ορίου.

Η τρίτη παράμετρος είναι ένας ακέραιος αριθμός, βάσει του οποίου υπολογίζεται το μέγιστο πλήθος των λέξεων εισόδου καθώς και των στοιχείων τους. Το πλήθος των στοιχείων N πρέπει να είναι πολλαπλάσιο του k ώστε να μπορούν να παραχθούν N/k λέξεις εισόδου μήκους k, συνεπώς το N υπολογίζεται ως γινόμενο του k με τον αριθμό που επιλέγουμε. Οι τιμές των στοιχείων εισόδου επιλέγουμε να κυμαίνονται στο διάστημα [0.5,1], ωστόσο αυτό δεν είναι ιδιαίτερα σημαντικό καθώς στη συνέχεια θα κανονικοποιηθούν στις τιμές {0,1}.

```
N = 500 * k;
input = rand(1,N)>=0.5;
input = reshape(input,k,N/k);
```

όπου input είναι ο πίνακας λέξεων εισόδου.

2. <u>Κωδικοποίηση εισόδων και παραγωγή κωδικών λέξεων</u>

Για την παραγωγή των κωδικολέξεων χρησιμοποιούμε τον τύπο

$$c = \sum_{i=1}^{k} x_i g_i = xG$$

```
codewords = mod(G*input,2);
codewords = reshape(codewords,1,n*(N/k));
```

Για κάθε στοιχείο του αποτελέσματος επιλέγουμε το υπόλοιπο της διαίρεσης με το 2 ώστε να πετύχουμε κανονικοποίηση στο δυαδικό σύστημα.

3. Διαμόρφωση των κωδικών λέξεων

Για τη διαμόρφωση των κωδικών λέξεων επιλέγουμε την BPSK (Binary Phase-shift Keying) διαμόρφωση, δηλαδή το πλήθος των συμβόλων των διαμορφωμένων στοιχείων είναι $M = 2^l = 2^1 = 2$.

Η αντιστοίχιση από δυαδικά ψηφία σε σύμβολα γίνεται με χρήση του κανόνα

$$x_i = \begin{cases} +1 & v_i = 1 \\ -1 & v_i = 0 \end{cases}$$

και της συνάρτησης CodeModulation

```
mod_codewords = CodeModulation(codewords);
mod_codewords = reshape(mod_codewords,n,length(codewords)/n);
```

όπου

```
function s = CodeModulation(b)
s = zeros(1,length(b));
   for i=1:length(b)
      if(b(i)==1) %Αν το στοιχείο ισούται με 1 του δίνεται η τιμή 1
         s(i) = 1;
      else
         s(1) = -1; %Διαφορετικά του δίνεται η τιμή -1
      end
   end
end
```

4. Προσθήκη θορύβου

Για τη διαδικασία θορυβοποίησης των λέξεων επιλέξαμε το σήμα λευκού θόρυβου γκαουσιανής κατανομής. Η επιλογή της συγκεκριμένης κατηγορίας βασίστηκε στις μαθηματικές ιδιότητες του μοντέλου θορύβου και στο γεγονός ότι χρησιμοποιεί την κανονική κατανομή (Gaussian). Ο θόρυβος παράγεται βάσει της διακύμανσης σ (sigma), η οποία υπολογίζεται για διαφορετικές τιμές του Eb/No.

```
for x = EbN0,
   % Υπολογισμός της διακύμανσης του Gaussian λευκού θορύβου
   sigma=1/(2*Rate*10^(x/10));
   % Παραγωγή του θορύβου
noise=
sqrt(sigma).*
reshape(rand(1,length(codewords)),n,length(codewords)/n);
   % Δημιουργία λαμβανόμενων λέξεων
noised_codewords= mod_codewords + noise;
```

Η μεταβλητή Eb/No δείχνει την ισχύ του συστήματος παραγωγής του σήματος και χρησιμοποιείται συχνά ως δείκτης σύγκρισης για διαφορετικά BER

5. Αποκωδικοποίηση

Για κάθε τιμή του Eb/N0 υλοποιούμε και τους δυο τύπους αποκωδικοποίησης (με τις συναρτήσεις SoftDecode και HardDecode) και υπολογίζουμε το πλήθος των διαφορετικων στοιχείων των πινάκων που μας επιστρέφουν με την αρχική είσοδο

```
% SOFT και HARD αποκωδικοποίηση
soft_decode_info =
```

```
SoftDecode(noised_codewords,mod_codewords,input);
hard_decode_info = HardDecode(noised_codewords,mod_codewords,input,threashold);
```

Για την SOFT αποκωδικοποίηση χρησιμοποιούμε την Ευκλείδια απόσταση ενώ στην HARD αποκωδικοποίηση αποδιαμορφώνουμε τα δείγματα βάσει της σύγκρισης με την μεταβλητή threashold

αν δείγμα > όριο τότε δείγμα =1

αλλιώς δειγμα = 0

και χρησιμοποιούμε την απόσταση Hamming

6. Σύγκριση λέξεων πληροφορίας με είσοδο και υπολογισμός BER

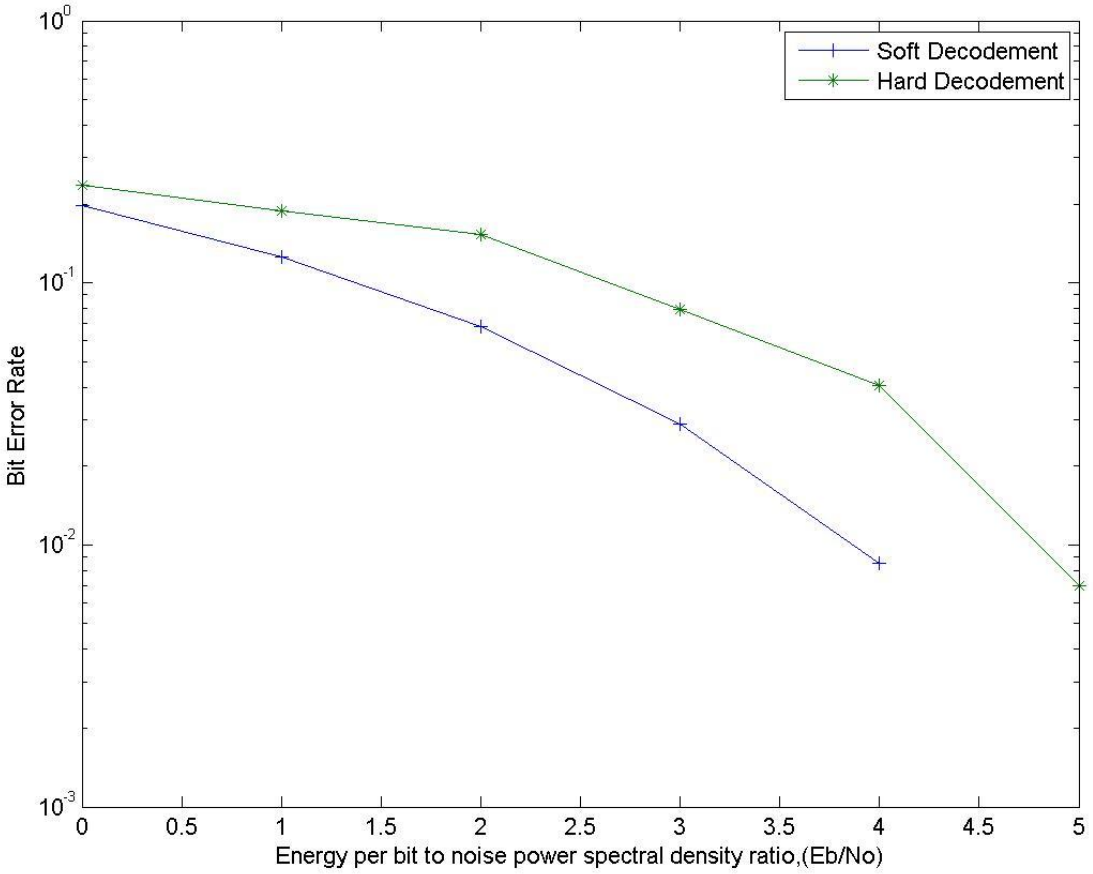
Για να υπολογίσουμε την μετρική BER βάσει της οποίας θα αξιολογήσουμε κάθε μέθοδο αποκωδικοποίησης υπολογίζουμε πρώτα το πλήθος των διαφορετικών στοιχείων μεταξύ του πίνακα λέξεων πληροφορίας και της αρχικής εισόδου και στη συνέχεια διαιρούμε το πλήθος των διαφορετικών στοιχείων με το πλήθος των στοιχείων

```
% Υπολογισμός του BER για κάθε τύπο αποκωδικοποίησης
BER_soft_dec(i) = nnz(input-soft_decode_info)/N;
BER_hard_dec(i) = nnz(input-hard_decode_info)/N;
```

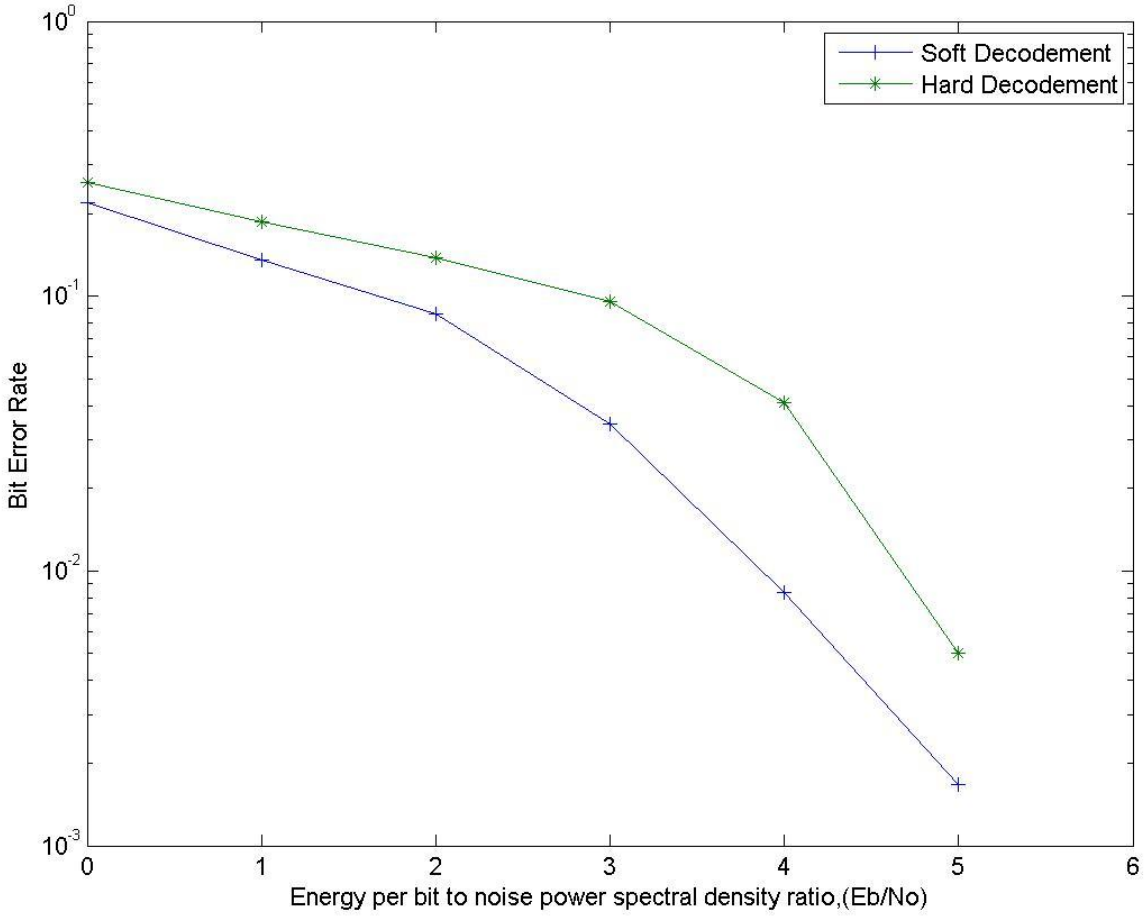
7. Αποτελέσματα

Στο τέλος αναπαριστούμε τα αποτελέσματα σε διάγραμμα. Για την αναπαράσταση των αποτελεσμάτων χρησιμοποιούμε το διάγραμμα semilogy που αντίθετα από το plot παρουσιάζει τις τιμές του πίνακα y λογαριθμημένες.

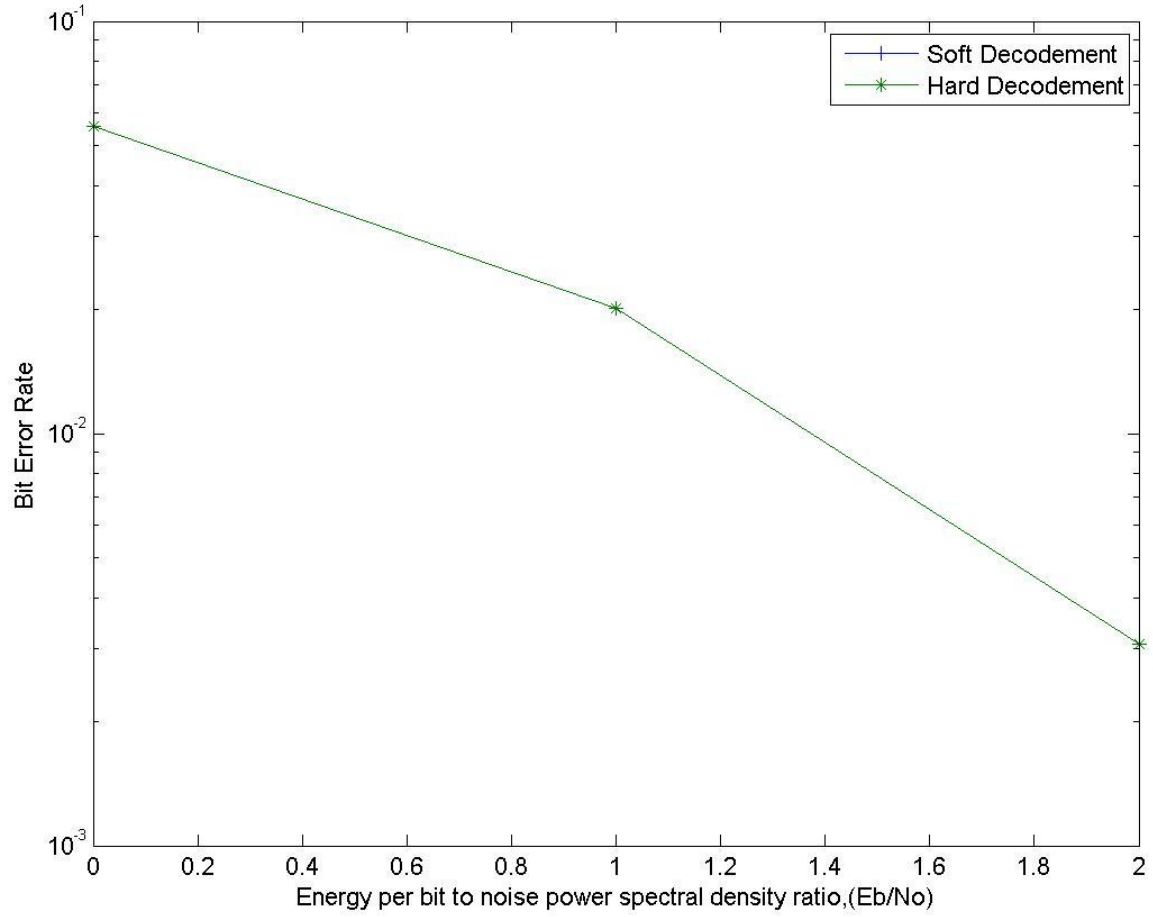
Threashold = 0.5, N = 300 *k



k = 4, n = 7


Soft Decodement
Hard Decodement
Bit Error Rate
Energy per bit to noise power spectral density ratio,(Eb/No)
10^0
10^-1
10^-2
10^-3
0
1
2
3
4
5
6

k = 11, n = 15



k = 26, n = 31

Συμπεράσματα

Από τα παραπάνω διαγράμματα μπορούμε να καταλήξουμε στα εξής συμπεράσματα.

1) Η SOFT αποκωδικοποίηση παρουσιάζει κατά κανόνα πιο ορθά αποτελέσματα από την HARD. Ο βαθμός στον οποίο υπερτερεί εξαρτάται σαφώς από τις τιμές τις οποίες έχουν ένα σύνολο παραμέτρων (k, n, threashold, Eb/No), ωστόσο θεωρείται γενικά πιο αποτελεσματική μέθοδος.

2) Για μεγαλύτερες τιμές του δείκτη Eb/No και οι δυο μέθοδοι αποκωδικοποίησης παρουσιάζουν περισσότερα σωστά αποτελέσματα, μειώνοντας τη συχνότητα λαθών τους.

Αυτό μας δείχνει ότι όσο πιο ισχυρό το σήμα, τόσο καλύτερα τα αποτελέσματα της διαδικασίας αποκωδικοποίησης, ανεξαρτήτως των άλλων παραμέτρων της εφαρμογής

3) Τα αποτελέσματα της αποκωδικοποίησης βελτιώνονται (στην περίπτωση της SOFT φτάνουν το 100% επιτυχίας όπως φαίνεται στο 3ο διάγραμμα όπου το BER πρακτικά είναι 0%) όσο μεγαλώνουν οι τιμές των k και n. Από αυτό μπορούμε να συμπεραίνουμε ότι οι μεγαλύτεροι πίνακες γεννήτορες καθώς και η χρήση μεγαλύτερου μήκους λέξεων αυξάνουν την απόδοση της διαδικασίας κωδικοποίησης – αποκωδικοποίησης.

Γενικά η μέθοδος της SOFT αποκωδικοποίησης δείχνει να παράγει καλύτερα αποτελέσματα από την αντίστοιχη HARD. Ωστόσο η διαφορά απόδοσης μπορεί να καθοριστεί από πολλούς παράγοντες, ενώ ταυτόχρονα η χρήση μεγαλύτερων πινάκων G επίσης βελτιώνει τις συνολικές επιδόσεις της κωδικοποίησης.

ΠΑΡΑΡΤΗΜΑ ΜΕ ΚΩΔΙΚΕΣ

1. function Block()

```
%Παράμετρος για την παραγωγή του γεννήτορα πίνακα G και των k,n
x = 3;

%Όριο για την αποδιαμόρφωση κατά τη διάρκεια της HARD αποκωδικοποίησης
threashold = 0.5;

%Δημιουργία του γεννήτορα πίνακα G και των k,n
[~,G,n,k]=hammgen(x);
G=G';

%Δημιουργία του πλήθους των εισόδων και του πίνακα εισόδων
N= 500 * k;
input = rand(1,N)>=0.5;
input = reshape(input,k,N/k);

%Υπολογισμός του Rate
Rate = k/n;

%Block κωδικοποίηση και υπολογισμός κωδικών λέξεων
codewords = mod(G*input,2);
codewords = reshape(codewords,1,n*(N/k));

% BPSK διαμόρφωση των κωδικών λέξεων
mod_codewords = CodeModulation(codewords);
```

```
mod_codewords = reshape(mod_codewords,n,length(codewords)/n);


% Ορισμός και αρχικοποίηση των μετρικών EbN0(energy per bit to noise power spectral density ratio) και BER (Bit Error Rate) για κάθε
% αποκωδικοποίηση
EbN0=0:1:7;
BER_soft_dec=zeros(1,length(EbN0));
BER_hard_dec=zeros(1,length(EbN0));


% Αποκωδικοποίηση για κάθε τιμή της παραμέτρου Eb/N0
i=1;
for x = EbN0,
    % Υπολογισμός της διακύμανσης του Gaussian λευκού θορύβου
    sigma=1/(2*Rate*10^(x/10));

    % Παραγωγή του θορύβου
    noise=sqrt(sigma).*reshape(rand(1,length(codewords)),n,length(codewords)/n);

    % Δημιουργία λαμβανόμενων λέξεων
    noised_codewords= mod_codewords + noise;

    % SOFT και HARD αποκωδικοποίηση
    soft_decode_info = SoftDecode(noised_codewords,mod_codewords,input);
    hard_decode_info = HardDecode(noised_codewords,mod_codewords,input,threashold);

    % Υπολογισμός του BER για κάθε τύπο αποκωδικοποίησης
    BER_soft_dec(i)=nnz(input-soft_decode_info)/N;
    BER_hard_dec(i)=nnz(input-hard_decode_info)/N;
```

```
    i=i+1;
end

% assignin('base', 'G', G);
% assignin('base', 'input', input);
% assignin('base', 'codewords', codewords);
% assignin('base', 'mod_codewords', mod_codewords);
% assignin('base', 'EbN0', EbN0);
% assignin('base', 'BER_soft_dec', BER_soft_dec);
% assignin('base', 'BER_hard_dec', BER_hard_dec);

%Σύγκριση των BER σε διάγραμμα
close all;
semilogy(EbN0,BER_soft_dec,'-+',EbN0,BER_hard_dec,'-*');
legend('Soft Decodement','Hard Decodement')
%xlabel('E_b/N_0');
xlabel('Energy per bit to noise power spectral density ratio,(Eb/No)');
ylabel('Bit Error Rate');
grid on;
end
```

2. function s = CodeModulation(b)

```
s = zeros(1,length(b));
    for i=1:length(b)
        if(b(i)==1) %Αν το στοιχείο ισούται με 1 του δίνεται η τιμή 1
            s(i) = 1;
        else
            s(1) = -1; %Διαφορετικά του δίνεται η τιμή -1
        end
```

```
    end
end
```

3. function distance = EuclDist(c1,c2)

```
    sum =0;
    for i = 1:length(c1)
        sum = sum + (c1(i)-c2(i))^2;
    end
    distance = sqrt(sum);
end
```

4. function distance = HammDist(c1,c2)

```
    distance =0;
    for i = 1:length(c1)
        if(c1(i)~=c2(i))
            distance = distance + 1;
        end
    end
end
```

5. function info = HardDecode(r,c,b,threashold)

```
    info = zeros(size(b,1),size(b,2));
    for i=1:length(r) %Για κάθε λαμβάνουσα λέξη
        min = Inf;
        index = 1;
        for k=1:size(r,1) %Αποδιαμόρφωση του κάθε στοιχείου βάσει του ορίου
            if(r(k,i)>=threashold)
```

```
            r(k,i) = 1;
        else
            r(k,i) = 0;
        end
    end
    for j=1:length(c) %Για κάθε κωδική λέξη
        distance = HammDist(r(:,i),c(:,j));
        if(distance< min) %Εύρεση της μικρότερης απόστασης Hamming
            min = distance;
            index = j; %Δείκτης της κωδικής λέξης με της μικρότερη απόσταση Hamming
        end
    end
    info(:,i) = b(:,index);%Αντιστοίχηση της αρχικής λέξης από τον αρχικό πίνακα εισόδων
  end
end
```

6. function info = SoftDecode(r,c,b)

```
  info = zeros(size(b,1),size(b,2));
  for i=1:length(r) %Για κάθε λαμβάνουσα λέξη
    min = Inf;
    index = 1;
    for j=1:length(c)  %Για κάθε κωδική λέξη
      distance = EuclDist(r(:,i),c(:,j));
      if(distance< min)   %Εύρεση της μικρότερης ευκλείδιας απόστασης
        min = distance;
        index = j;      %Δείκτης της κωδικής λέξης με της μικρότερη ευκλείδια αποστάση
      end
    end
```

```
        info(:,i) = b(:,index);%Αντιστοίχηση της αρχικής λέξης από τον αρχικό πίνακα εισόδων
    end
end
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] 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.

[2] John G. Proakis, "Digital Communications," Fourth Edition, Published by McGraw-Hill International Edition.

[3] Δημήτριος Νικολός, "Τεχνικές Σχεδίασης Συστημάτων για Εύκολο Έλεγχο της Ορθής τους Λειτουργίας", Παν. Πατρών, Μάρτιος 2009.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes", Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland, pp. 1064-1070, May 1993.

[5] D. Divsalar, F. Pollara, "On the Design of Turbo Codes", The Telecommunications and Data Acquisition Progress Report 42-123, July- September 1995, JPL, Pasadena, California, pp. 99-121, November 15, 1995.

[6] M. C. Valenti "An Introduction to Turbo Codes", Bradley Dept. of Elect. Eng., Virginia Polytechnic Inst. & S.U., unpublished report, May 1996.

(http://www.csee.wvu.edu/~mvalenti/turbo.html)

[7] M. C. Valenti, "Turbo Codes and Iterative processing" , in Proc. IEEE New Zealand Wireless Commun. Symp. '98, Auckland New Zealand, Nov. 1998.

(http://www.csee.wvu.edu/~mvalenti/turbo.html)

[8] Todd K. Moon, "Error Correction Coding – Mathematical Methods and Algorithms", WILEY INTERSCIENCE, A John Wiley & Sons, Inc., Publication, 2005.

[9] Π. Γ. Κωττής, "ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ", Εκδόσεις Τζιόλα, Copyright © 2012.

[10] C. E. Shannon, "A mathematical theory of communication," Bell System Technical

Journal, vol. 27, pp. 379-423 and 623-656, July and October 1948.

[11] W. E. Ryan, "Concatenated Convolutional Codes and Iterative Decoding," available on line.

[12] Καραμάνου Ευαγ. Δήμητρα "Θεωρία της Πληροφορίας ή Θεωρία των Πληροφοριών Κανάλι – Σύστημα", Διπλωματική εργασία, Πειραιάς, Ιούνιος 2011

[13] Σπουρλής Γεώργιος, "Αρχιτεκτονικές Διόρθωσεις Λαθών βασισμένες σε Κώδικες BCH", Μεταπτυχιακή Διπλωματική εργασία, Πάτρα, Μάρτιος 2012.

[14] Θεόδωρος Ρουδος, Σχεδίαση κωδικοποιητή – αποκωδικοποιητή Reed Solomon, Διπλωματική εργασία, , Πανεπιστήμιο Πάτρας.

[15] Παναγιώτης Λιναρδης, Ψηφιακή σχεδίαση Ι, Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2001.

[16] Χαριδημος Θ. Βέργος, Πανεπιστημιακές Παραδόσεις στην Εισαγωγή στα Συστήματα Υπολογιστών, Πανεπιστήμιο Πατρών, Οκτώβριος 2006

[17] Σεραφείμ Καραμπογιάς, Κωδικοποιητής – αποκωδικοποίηση καναλιού, 2013

http://skara.di.uoa.gr/communication_systems/transparency/tranparency2013_Proakis_ch_9.pdf

[18] Θωμάς Καμαλάκης, Οπτικές Επικοινωνίες, Τμήμα Τηλεματικής και Πληροφορικής, Χαροκόπειο Πανεπιστήμιο Αθηνών.