

Τ.Ε.Ι Πελοποννήσου
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

**Μελέτη των κωδικών turbo σε ψηφιακά συστήματα
μετάδοσης βίντεο**

Κυμπούρη Ζαχαρούλα-Μαρία
Πτυχιακή Εργασία

Επιβλέπων Καθηγητής: Βασίλειος Μποζαντζής

Σύμφωνα με απόφαση της Συνέλευσης του ΤΕΙ Πελοποννήσου οι φοιτητές που εκπονούν την πτυχιακή τους εργασία υποχρεούνται να συμπεριλαμβάνουν στις προκαταρκτικές σελίδες της εργασίας τους το παρακάτω κείμενο, υπογεγραμμένο από τους ίδιους.

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Όνομα και Επώνυμο Συγγραφέα (Με Κεφαλαία):

.....

Υπογραφή (Ολογράφως, χωρίς
μονογραφή):

.....

Ημερομηνία (Ημέρα – Μήνας – Έτος):

.....

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1

1.1-Εισαγωγή στα Τηλεπικοινωνιακά Συστήματα.....	4
1.2 – Θεωρία Πληροφορίας.....	11

Κεφάλαιο 2

2.1 – Πρότυπα ψηφιακή μετάδοση βίντεο H.262 και H.264.....	16
2.1.1 - Πρότυπο H.262.....	17
2.1.2 - Πρότυπο H.264.....	23

Κεφάλαιο 3

3.1 - Κωδικοποίηση καναλιού.....	31
3.1.1 – Βασικά στοιχεία Θεωρίας Κωδίκων.....	34
3.2 - Γραμμικοί Κώδικες.....	38
3.3 - Κώδικες LDPC (Low Density Parity Check).....	45
3.4 - Συνελκτικοί κώδικες.....	52
3.5 - Κώδικες τούρμπο.....	61

Κεφάλαιο 4

4.1 – Ιστορία των turbo κωδικών.....	64
4.2 - Turbo MIMO.....	69
4.3 - Χρήση Turbo κωδικών στο πρότυπο IEEE 802.16.....	71
4.4. – Μπλοκ turbo κώδικες (BTC).....	74
4.4.1 – Συνελκτικοί turbo κώδικες (CTC).....	77
4.5 – Άλλες εφαρμογές των turbo κωδικών.....	80

Κεφάλαιο 5

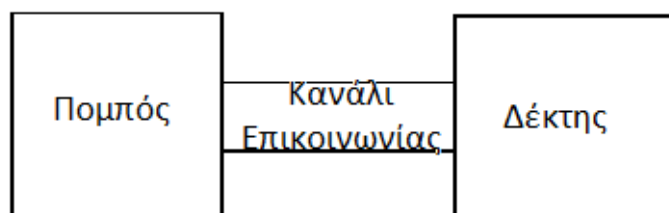
5.1 - Κωδικοποιητής turbo.....	81
5.2 - Iterative Turbo Decoding (επαναληπτικής αποκωδικοποίησης).....	82
5.3 - Variable-sized turbo coding(Κωδικοποίηση μεταβλητού μεγέθους turbo).....	83

Βιβλιογραφία.....	85
--------------------------	-----------

Κεφάλαιο 1

1.1-Εισαγωγή στα Τηλεπικοινωνιακά Συστήματα

Ο εικοστός πρώτος αιώνας έχει χαρακτηριστεί ως η “εποχή της Πληροφορίας”. Ο χαρακτηρισμός αυτός εκφράζει το κύριο χαρακτηριστικό της σημερινής εποχής, το οποίο είναι η αυξημένη ικανότητα πρόσβασης του ανθρώπου σε μεγάλο όγκο πληροφοριών και, κατ' επέκταση, την αυξημένη, συγκριτικά με παλαιότερες “εποχές”, ικανότητα πρόσβασης σε γνώσεις πολλών και ποικίλων πεδίων, καθώς και την δυνατότητα του για την μετάδοση και ανταλλαγή αυτών. Η αυξημένη αυτή ικανότητα πρόσβασης σε διαφόρων ειδών πληροφορίες και μετάδοσης αυτών οφείλεται, κατά κύριο λόγο, στην ραγδαία ανάπτυξη των τηλεπικοινωνιακών τεχνολογιών και των ηλεκτρονικών υπολογιστών, ή αλλιώς, στην “Ψηφιακή Επανάσταση”. Ως “Ψηφιακή Επανάσταση” λογίζεται η περίοδος που ξεκινάει περίπου το δεύτερο μισό του εικοστού αιώνα, με την ανάπτυξη των ηλεκτρονικών συστημάτων και των ολοκληρωμένων κυκλωμάτων, που έκαναν εφικτή την εφεύρεση και ραγδαία εξέλιξη των ψηφιακών ηλεκτρονικών υπολογιστών και την μετάβαση από την αναλογική-μηχανική ηλεκτρική τεχνολογία που μέχρι τότε επικρατούσε, στην ψηφιακή τεχνολογία¹. Τα ολοκληρωμένα κυκλώματα είναι πλέον αναπόσπαστο κομμάτι σχεδόν όλων των ηλεκτρονικών συσκευών που χρησιμοποιούν οι άνθρωποι στην καθημερινότητα τους, από μικροσυσκευές και έξυπνα κινητά τηλέφωνα μέχρι και τις οικιακές συσκευές. Η ραγδαία αυτή εξέλιξη έχει οδηγήσει στην δυνατότητα αλλά και την ανάγκη μετάδοσης και ανταλλαγής μεγάλου όγκου πληροφοριών. Λόγω αυτού έχουν δημιουργηθεί πολλοί τομείς και κλάδοι επιστημών που ασχολούνται με την μελέτη και την βελτίωση της αξιοπιστίας των μεταδιδόμενων πληροφοριών με αποτέλεσμα την μεγάλη εξέλιξη των τηλεπικοινωνιακών συστημάτων και την ανάπτυξη νέων και αποδοτικότερων μεθόδων μετάδοσης.



Σχήμα 1.1 - Στοιχειώδης μορφή Τηλεπικοινωνιακού Συστήματος

¹Λόγω αυτής της μετάβασης ο σημερινός κόσμος χαρακτηρίζεται ως “Ψηφιακός Κόσμος”.

Ένα στοιχειώδες τηλεπικοινωνιακό σύστημα αποτελείται από τον πομπό, το κανάλι μετάδοσης της πληροφορίας και τον δέκτη, όπως φαίνεται στο παραπάνω σχήμα (Σχήμα 1.1). Το είδος και τα βασικά χαρακτηριστικά του πομπού (και κατά συνέπεια και του δέκτη) ποικίλουν και εξαρτώνται από την χρήση για την οποία προορίζεται το σύστημα. Το κανάλι επικοινωνίας μπορεί να είναι είτε κάποιο υλικό για τα ενσύρματα κανάλια επικοινωνίας, όπως ένα μεταλλικό σύρμα ή μία οπτική ίνα είτε και ο ελεύθερος χώρος της ατμόσφαιρας για τα ασύρματα. Όμως, όποιο και να είναι το είδος του πομπού-δέκτη και του καναλιού επικοινωνίας, η πληροφορία, στα σύγχρονα τηλεπικοινωνιακά συστήματα που είναι ηλεκτρικά συστήματα επικοινωνίας², θα μεταδίδεται με μορφή ηλεκτρικού σήματος ή ηλεκτρομαγνητικού κύματος. Οπότε θα πρέπει να είναι διαμορφωμένη κατάλληλα ώστε να μπορεί να μεταδοθεί μέσω του συγκεκριμένου καναλιού επικοινωνίας. Η διαμόρφωση που θα επιλεγεί εξαρτάται από το κανάλι μέσω του οποίου θα μεταδοθεί αλλά και του είδους της πληροφορίας που πρόκειται να μεταδοθεί. Η διαμόρφωση αυτή γίνεται στον πομπό και όταν το σήμα ληφθεί από τον δέκτη αναδιαμορφώνεται ώστε να γίνει η ανάκτηση της μεταδιδόμενης πληροφορίας.

Το πρώτο ηλεκτρικό τηλεπικοινωνιακό σύστημα δημιουργήθηκε από τον Samuel Morse, και ήταν ο τηλέγραφος, του οποίου η πρώτη επίδειξη έγινε το 1837 στις Ηνωμένες Πολιτείες της Αμερικής. Εφτά χρόνια μετά, το Μάιο του 1844, λειτούργησε η πρώτη τηλεγραφική γραμμή, η οποία ένωνε την Washington με την Baltimore. Η μετάδοση της πληροφορίας γινόταν με μεταβλητού μήκους κωδικές λέξεις, που αναπαριστούσαν τα γράμματα του λατινικού αλφαβήτου, τους αραβικούς αριθμούς και κάποια σύμβολα στίξης και ειδικούς χαρακτήρες. Ο κώδικας αυτός επινοήθηκε από τον Morse και ονομάστηκε “κώδικας Morse”. Είναι δυαδικός, με την τελεία (σύντομη τάση) και την παύλα (τάση μεγάλης διάρκειας) και είναι, όπως προαναφέρθηκε, μεταβλητού μήκους κώδικας, με τη μικρότερη να είναι ενός συμβόλου και την μεγαλύτερη να είναι έξι συμβόλων (με εξαίρεση το σήμα σφάλματος που είναι 8 τελείες). Οι στιγμές (τελείες) και οι άλλες γραμμές (παύλες) αντιστοιχούν σε ηλεκτρικά κύματα. Η διάρκεια της στιγμής λαμβάνεται ως μονάδα. Χρονικά, η στιγμή (τελεία) αντιστοιχεί στο 1/6 του δευτερολέπτου. Η γραμμή έχει διάρκεια τρεις φορές μεγαλύτερη (δηλαδή μισό δευτερόλεπτο). Η απόσταση μεταξύ των λέξεων είναι ίση με επτά στιγμές. Η απόσταση μεταξύ των γραμμάτων είναι ίση με τρεις στιγμές, η απόσταση μεταξύ των ίδιων γραμμάτων είναι ίση με μια στιγμή. Ο κώδικας αυτός είναι ο πρώτος

²Ο χαρακτηρισμός ως “ηλεκτρικά” τα ξεχωρίζει από παλαιότερα συστήματα επικοινωνιών όπως το ταχυδρομείο και ένα σύστημα σηματοφόρων που χρησιμοποιούνταν μέχρι και τα μέσα του δεκάτου ενάτου αιώνα.

ψηφιακός κώδικας που επινοήθηκε, μιας και το ηλεκτρικό σήμα που μεταδιδόταν είχε μόνο δύο πιθανές τιμές, την ύπαρξη “1” ή όχι “0” τάσης, και κατάλληλος συνδυασμός αυτών σχημάτιζε το κάθε γράμμα, και υπήρξε ο πρόδρομος των μεθόδων ψηφιακής κωδικοποίησης οι οποίες αναπτύχθηκαν πολλά χρόνια μετά και χρησιμοποιούνται μέχρι και σήμερα στα σύγχρονα μέσα τηλεπικοινωνιών.

Το τηλεπικοινωνιακό αυτό σύστημα ήταν το επικρατέστερο, μέχρι την ανάπτυξη και διάδοση μίας εφεύρεσης, η οποία εξακολουθεί να είναι από τα κυρίαρχα τηλεπικοινωνιακά μέσα, το τηλέφωνο. Το 1876 ο Alexander Graham Bell κατοχύρωσε ευρεσιτεχνία για την εφεύρεση της τηλεφωνίας και το 1877 ίδρυσε την πρώτη τηλεφωνική εταιρία, την “Bell Telephony Company”. Το σήμα το οποίο χρησιμοποιούσε ήταν αναλογικό και η πληροφορία που μεταφερόταν ήταν κατάλληλα διαμορφωμένα, από ηχητικά κύματα, ηλεκτρικά σήματα. Οι υπηρεσίες που παρείχαν, οι πρώτες παραλλαγές συστημάτων τηλεφωνίας ήταν σχετικά απλές και για αποστάσεις μερικών εκατοντάδων μιλίων, λόγω κακής ποιότητας ήχου αλλά και μεγάλης απόσβεσης του σήματος. Τις επόμενες δύο δεκαετίες όμως, με τη βοήθεια των εφευρέσεων του μικροφώνου άνθρακα και του επαγωγικού πηνίου έγιναν σημαντικές πρόοδοι και στην ποιότητα αλλά και στην εμβέλεια των υπηρεσιών. Ειδικά μετά το 1906 και την εφεύρεση της τριόδου ενισχύτριας λυχνίας (λυχνία κενού) από τον Lee De Frost, κατέστη δυνατή η τοποθέτηση ενισχυτών σήματος στα τηλεφωνικά συστήματα και η εμβέλεια αλλά και η ποιότητα των υπηρεσιών άρχισε να αυξάνεται πολύ.

Η Τηλεγραφία και η Τηλεφωνία άρχισαν ως ενσύρματα τηλεπικοινωνιακά συστήματα. Παράλληλα όμως με αυτά, αναπτύχθηκαν και εξελίχθηκαν και τα αντίστοιχα ασύρματα. Η ανάπτυξή τους έγινε εφικτή με την θεμελίωση της Ηλεκτρομαγνητικής θεωρίας από τον Maxwell. Αλλά η αρχή έγινε το 1820, όπου ο Oersted σε μία εργασία του απέδειξε τη στενή σχέση μεταξύ ηλεκτρικού και μαγνητικού πεδίου, παράγοντας μαγνητικό πεδίο από ένα ηλεκτρικό. Εν συνεχεία, στις 29 Αυγούστου 1831 ο Micheal Faraday κάνει επίδειξη της μαγνητικής επαγωγής, παράγοντας ηλεκτρικό ρεύμα κινώντας έναν μαγνήτη κοντά σε έναν αγωγό, φέρνοντας την ανθρωπότητα ένα βήμα πιο κοντά στην Ηλεκτρομαγνητική θεωρία, η οποία διατυπώθηκε το 1864 από τον James C. Maxwell και επαληθεύτηκε πειραματικά από τον Hertz το 1887. Προέβλεπε την ύπαρξη ηλεκτρομαγνητικής ακτινοβολίας, η οποία είναι η ακτινοβολία που χρησιμοποιούν τα ασύρματα συστήματα τηλεπικοινωνιών μέχρι και σήμερα. Τα σήματα αυτού του είδους αναφέρονται με τον όρο “ραδιοσήματα”, με τον οποίο ορίζονται τα σήματα που μεταδίδονται με ραδιοκύματα. Τα ραδιοκύματα είναι τα ηλεκτρομαγνητικά κύματα με συχνότητες από 0.3Hz μέχρι 300MHz και χρήση αυτών γίνεται

από τα επίγεια ασύρματα τηλεπικοινωνιακά δίκτυα³. Στα ασύρματα συστήματα τηλεπικοινωνιών μεγάλο ρόλο στην ανάπτυξη τους έπαιξε η εφεύρεση της διόδου κενού, το 1904 από τον Fleming και της τριόδου λυχνίας (λυχνία κενού) από τον Lee De Frost το 1906, η οποία, όπως προαναφέρθηκε, συνετέλεσε και στην εξέλιξη της Τηλεφωνίας, βελτιώνοντας τον λόγο απόσταση προς ποιότητα, αυξάνοντας εντυπωσιακά την εμβέλεια. Εκτός όμως αυτού, η λυχνία κενού έθεσε τις βάσεις και έκανε δυνατή την ανάπτυξη της ραδιοφωνίας καθιστώντας εφικτή την πρώτη διαμόρφωση ηλεκτρομαγνητικού κύματος, την διαμόρφωση AM (amplitude modulation- διαμόρφωση πλάτους).

Όπως προαναφέρθηκε, η μεταφορά της πληροφορίας γινόταν (και γίνεται!) με την μετάδοση και λήψη κατάλληλα διαμορφωμένου ηλεκτρομαγνητικού κύματος το οποίο φέρει την πληροφορία και ονομάζεται φέρον κύμα (carrier). Η γενική μορφή ενός ηλεκτρομαγνητικού κύματος δίνεται από την εξίσωση:

$$E(t) = A \cdot \sin(\omega t + \varphi)(1.1.1)$$

όπου το A είναι το πλάτος, το ω είναι η κυκλική συχνότητα και το φ η φάση του κύματος. Και σε ένα από τα τρία αυτά χαρακτηριστικά μεγέθη των ηλεκτρομαγνητικών κυμάτων γίνεται η διαμόρφωση σύμφωνα με το σήμα πληροφορίας που είναι επιθυμητό να μεταδοθεί. Αν μεταβάλλεται το πλάτος του κύματος ανάλογα με το σήμα δεδομένων, η πληροφορία περιέχεται σε αυτό και η διαμόρφωση είναι η AM διαμόρφωση που προαναφέρθηκε. Οπότε το πλάτος του κύματος γίνεται συνάρτηση του χρόνου και η γενική μορφή της εξίσωσης του φέροντος θα είναι:

$$C(t) = A(t) \cdot \sin(\omega t + \varphi)(1.1.2)$$

Αν το σήμα της πληροφορίας διαμορφώνει κατάλληλα την συχνότητα του φέροντος, τότε η διαμόρφωση ονομάζεται “διαμόρφωση συχνότητας” (FM-frequency modulation) η οποία δημιουργήθηκε το 1933 και έγινε δημοφιλής και αναπτύχθηκε εμπορικά μετά τον Δεύτερο Παγκόσμιο Πόλεμο. Στην περίπτωση αυτή η συχνότητα του κύματος γίνεται συνάρτηση του χρόνου και η γενική μορφή της εξίσωσης του φέροντος θα είναι:

$$C(t) = A \cdot \sin(\omega(t) \cdot t + \varphi)(1.1.3)$$

³Τα κύματα συχνοτήτων μεγαλύτερων των 300MHz (μέχρι συχνότητα 300GHz) ονομάζονται “μικροκύματα” και χρησιμοποιούνται στις δορυφορικές επικοινωνίες.

Τέλος, αν το μέγεθος που μεταβάλλεται σύμφωνα με το σήμα πληροφορίας είναι η φάση του κύματος, τότε η διαμόρφωση ονομάζεται “διαμόρφωση φάσης” (PM-phase modulation) και η φάση του κύματος γίνεται συνάρτηση του χρόνου, με την γενική μορφή της εξίσωσης του κύματος να είναι:

$$C(t) = A \cdot \sin(\omega t + \varphi(t))(1.4)$$

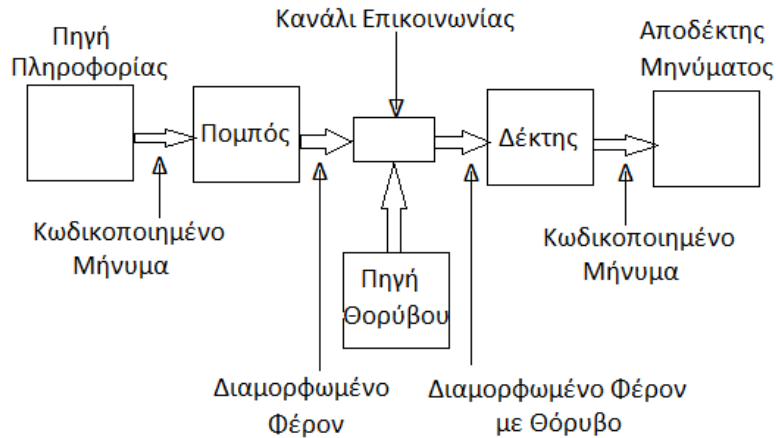
Οι παραπάνω διαμορφώσεις αφορούν την διαμόρφωση του ηλεκτρομαγνητικού σήματος που θα σταλεί από τον πομπό και θα ληφθεί από τον δέκτη και χρησιμοποιούνται από όλα τα ασύρματα τηλεπικοινωνιακά συστήματα. Ένα τέτοιο σύστημα, όπως και ένα ενσύρματο τηλεπικοινωνιακό σύστημα, έχει σχεδιαστεί για να στέλνει το μήνυμα (ή πληροφορία) που δημιουργείται από μία πηγή προς έναν ή περισσότερους προορισμούς και, σε οποιοδήποτε είδος και να ανήκει, θα έχει μία συγκεκριμένη δομή και κάποιες βασικές βαθμίδες, όπως φαίνεται στο παρακάτω σχήμα (Σχήμα 1.2) στο οποίο παρουσιάζεται ένα τέτοιο σύστημα. Η πορεία της πληροφορίας θα είναι η εξής: αρχικά από την πηγή της πληροφορίας θα μετατραπεί κατάλληλα με κάποια μορφή κωδικοποίησης ώστε να εισέλθει στον πομπό, στον οποίο θα διαμορφωθεί το φέρον έτσι ώστε να σταλεί, μέσω του καναλιού επικοινωνίας, στον δέκτη. Ο δέκτης, αφού το αποδιαμορφώσει θα το προωθήσει στον μετατροπέα εξόδου όπου θα λάβει χώρα η αποκωδικοποίηση του σήματος και η έξοδος του θα είναι η αρχική πληροφορία. Ανάλογα με το είδος της πληροφορίας που είναι επιθυμητό να μεταδοθεί και το είδος του καναλιού που θα χρησιμοποιηθεί θα επιλεγεί και η κατάλληλη κωδικοποίηση του σήματος και διαμόρφωση του φέροντος. Για παράδειγμα, στην ραδιοφωνική μετάδοση AM, η πληροφορία που μεταδίδεται είναι ήχος. Οπότε ο ήχος θα μετατραπεί σε ηλεκτρικό σήμα το οποίο στην συνέχεια θα εισέλθει στον πομπό. Ο πομπός θα είναι ένας ετερόδυνος ραδιοπομπός που θα διαμορφώσει κατά πλάτος το φέρον ηλεκτρομαγνητικό κύμα. Το κανάλι επικοινωνίας θα είναι η ατμόσφαιρα και ο δέκτης θα είναι ένας ετερόδυνος ραδιοδέκτης, ο οποίος θα αποδιαμορφώσει το ηλεκτρομαγνητικό κύμα κατά πλάτος. Τέλος, το ηλεκτρικό σήμα θα μετατραπεί ξανά σε ήχο μέσω ενός ηχείου και ο παραλήπτης θα ακούσει το ηχητικό σήμα που μετέδωσε ο ραδιοσταθμός. Ανάλογα, λοιπόν, με το κανάλι που έχουμε και το είδος του σήματος που θέλουμε να μεταφέρουμε θα έχουμε και διαφορετικό είδος πομπού, αλλά η βασική αρχή λειτουργίας όλων θα είναι η κατάλληλη επεξεργασία του σήματος που θα εισαχθεί στο κανάλι επικοινωνίας.

Με τον όρο “κανάλι επικοινωνίας” ορίζεται το φυσικό μέσο μέσω του οποίου θα

μεταδοθεί το φέρον σήμα. Για τις ενσύρματες τηλεπικοινωνίες το κανάλι επικοινωνίας μπορεί να είναι κάποιο μεταλλικό σύρμα ή κάποια οπτική ίνα. Για τις ασύρματες τηλεπικοινωνίες το κανάλι θα είναι η ατμόσφαιρα (ελεύθερος χώρος). Και, ειδικά στην περίπτωση που το κανάλι επικοινωνίας είναι ο ελεύθερος χώρος, αυτό θα είναι κοινό σε πολλά Τηλεπικοινωνιακά Συστήματα, κάτι που συμβαίνει όμως και σε πολλά ενσύρματα κανάλια. Για τον λόγο αυτό έχουν αναπτυχθεί τεχνικές μετάδοσης πολλών σημάτων μέσα από το ίδιο κανάλι, που ονομάζονται “Μέθοδοι Πολύπλεξης⁴” και οι οποίες αποσκοπούν στην καλύτερη αξιοποίηση των κοινών καναλιών επικοινωνίας αλλά και του ηλεκτρομαγνητικού φάσματος. Οι τεχνικές αυτές θα αναφερθούν συνοπτικά γιατί πιο αναλυτική αναφορά σε αυτές ξεφεύγει από τα πλαίσια της παρούσας εργασίας.

- **FDMA (Frequency Division Multiple Access – Πολλαπλή Πρόσβαση με Διαίρεση Συχνοτήτων) :** Η πολλαπλή πρόσβαση επιτυγχάνεται με την χρήση συγκεκριμένου εύρους συχνοτήτων, μοναδικό για κάθε Τηλεπικοινωνιακό Σύστημα που χρησιμοποιεί το συγκεκριμένο κανάλι. Όλα τα σήματα μεταδίδονται ταυτόχρονα μέσω του ίδιου καναλιού και ο διαχωρισμός των σημάτων μπορεί να γίνει με χρήση ενός φίλτρου στον δέκτη.
- **TDMA (Time Division Multiple Access - Πολλαπλή Πρόσβαση με Διαίρεση Χρόνου):** Κάθε σύστημα μπορεί να χρησιμοποιεί το κανάλι για συγκεκριμένο χρονικό διάστημα στην διάρκεια του οποίου δεν το χρησιμοποιεί κανένα άλλο σύστημα. Στην τεχνική αυτή δεν υπάρχει περιορισμός στο εύρος συχνοτήτων που μπορεί να χρησιμοποιεί κάθε σύστημα.
- **CDMA (Code Division Multiple Access – Πολλαπλή Πρόσβαση με Διαίρεση Κώδικα):** Η τεχνική αυτή χρησιμοποιείται αποκλειστικά στα ψηφιακά Τηλεπικοινωνιακά Συστήματα. Στο κανάλι επικοινωνίας μεταδίδονται ταυτόχρονα πολλά σήματα, τα οποία μπορούν να χρησιμοποιούν όλο το ηλεκτρομαγνητικό φάσμα (χωρίς περιορισμό εύρους συχνοτήτων). Κάθε σήμα όμως θα έχει μία συγκεκριμένη και μοναδική (για το συγκεκριμένο κανάλι) κωδικοποίηση, δίνοντας στο δέκτη τη δυνατότητα να αναγνωρίσει ανάμεσα σε πολλά σήματα, το επιθυμητό σήμα.

⁴Με τον όρο “Πολύπλεξη” περιγράφεται η μετάδοση διαφορετικών σημάτων πληροφορίας μέσω του ίδιου καναλιού επικοινωνίας, ή αλλιώς, μέσα από την ίδια φυσική ζεύξη.



Σχήμα 1.2 - Διάγραμμα Τηλεπικοινωνιακού Συστήματος

Τα σύγχρονα Τηλεπικοινωνιακά Συστήματα χρησιμοποιούν συνδυασμό περισσότερων από μία από τις παραπάνω τεχνικές πολύπλεξης. Όμως, οποιοδήποτε και να είναι το κανάλι επικοινωνίας και ο τρόπος πολύπλεξης που χρησιμοποιείται, όποιο φυσικό μέσο και να χρησιμοποιηθεί, θα έχει ένα κύριο χαρακτηριστικό. Θα προκαλεί κάποιες αλλοιώσεις στο σήμα που μεταδίδεται μέσω αυτού, με τυχαίο τρόπο, λόγω ποικίλων φαινομένων όπως η απόσβεση του σήματος, οι αλληλεπιδράσεις του με άλλα ηλεκτρομαγνητικά σήματα είτε της ατμόσφαιρας είτε κάποιου άλλου τηλεπικοινωνιακού συστήματος που χρησιμοποιεί το ίδιο κανάλι⁵, ανάλογα με το μέσον. Δηλαδή θα προσθέτει κάποιο θόρυβο στο σήμα το οποίο διαδίδεται μέσω αυτού, όπως φαίνεται και στο παραπάνω σχήμα (Σχήμα 1.2). Ο θόρυβος αυτός θα προκαλεί δυσκολίες στην πιστή αναπαραγωγή της αρχικής πληροφορίας και, αν είναι πολύ ισχυρός, μέχρι και απώλεια της μεταδιδόμενης πληροφορίας. Για τον λόγο αυτό πρέπει να γίνει προσεκτικός σχεδιασμός του τηλεπικοινωνιακού συστήματος που θα χρησιμοποιηθεί, κατάλληλος για το είδος του σήματος που είναι επιθυμητό να μεταδοθεί και για το κανάλι επικοινωνίας που θα χρησιμοποιηθεί. Στα σύγχρονα τηλεπικοινωνιακά συστήματα τα οποία είναι ψηφιακά, ένα από τα σημαντικότερα αντικείμενα μελέτης είναι ο τρόπος ή η μέθοδος κωδικοποίησης του σήματος (που είναι και το αντικείμενο της παρούσας εργασίας) έτσι ώστε να αυξάνεται η αξιοπιστία της πληροφορίας που μεταδίδεται αλλά και να αυξάνεται η ικανότητα μετάδοσης μεγαλύτερου όγκου πληροφορίας ενός τηλεπικοινωνιακού συστήματος. Με την μελέτη του αντικείμενου αυτού ασχολείται ο κλάδος της “Θεωρίας Πληροφορίας” (που είναι τμήμα των εφαρμοσμένων μαθηματικών).

⁵Ειδικά στις περιπτώσεις των τεχνικών FDMA και CDMA, για ένα σήμα, τα υπόλοιπα σήματα που μεταδίδονται από το ίδιο κανάλι αποτελούν θόρυβο για το σήμα αυτό.

1.2 – Θεωρία Πληροφορίας

Ο κλάδος της “Θεωρίας Πληροφορίας” άρχισε να αναπτύσσεται το δεύτερο μισό του εικοστού αιώνα. Ιδρυτής της θεωρείται ο Claude Elwood Shannon ο οποίος με την εργασία του “A mathematical theory of Communication” που δημοσίευσε το 1948 έθεσε τις βάσεις για την ανάπτυξη του κλάδου αυτού. Η αρχή όμως είχε γίνει το 1928 με τον ορισμό της “ποσότητας πληροφορίας” από τον Hartley βάσει της οποίας οποιαδήποτε πληροφορία αποτελείται από την διαδοχική επιλογή συμβόλων ή λέξεων από ένα πλήρες προκαθορισμένο “αλφάβητο” ή “λεξιλόγιο” (όπως παραδείγματος χάριν είναι ο κώδικας Morse που αναφέρθηκε στην προηγούμενη ενότητα). Ένα χρόνο αργότερα, το 1929, ο Szilard συνέδεσε την πληροφορία με την θερμοδυναμική εντροπία, έννοια πολύ βασική στην θεωρία πληροφορίας.

Η ροή πληροφορίας συνίσταται στην εκπομπή μηνυμάτων (ή συμβόλων τα οποία συνθέτουν το μήνυμα) σύμφωνα με το προκαθορισμένο “λεξιλόγιο” που αναφέρθηκε παραπάνω και το οποίο αποτελεί τον κώδικα επικοινωνίας μεταξύ δύο οντοτήτων (παραδείγματος χάριν συστήματος πομπού-δέκτη). Όταν τα σύμβολα ή οι λέξεις που χρησιμοποιούνται αποτελούνται από ακολουθίες δυαδικών ψηφίων, τότε το σύστημα είναι σύστημα ψηφιακής επικοινωνίας. Μονάδα μέτρησης της μεταδιδόμενης πληροφορίας στα συστήματα αυτά είναι το δυαδικό ψηφίο (binary digit⁶). Έστω ότι το γεγονός που απεικονίζεται από το μεταδιδόμενο σύμβολο M_i εμφανίζεται με πιθανότητα (για τον δέκτη) ίση με P_i . Τότε, το ποσό πληροφορίας που περιέχει το σύμβολο M_i ορίζεται ίσο με:

$$I_i = \log_2 \frac{1}{P_i} = -\log_2 P_i \quad (1.2.1)$$

Οι βασικές ιδιότητες του παραπάνω ορισμού είναι:

- Αν το γεγονός που απεικονίζεται από το σύμβολο M_i είναι απίθανο (για τον δέκτη) η πληροφορία που φέρει είναι άπειρη.
- Αν το γεγονός που απεικονίζεται από το σύμβολο M_i είναι γνωστό (στον δέκτη) η πληροφορία που φέρει είναι μηδενική.

⁶ Αρχικά το “δυαδικό ψηφίο” ονομαζόταν “binit”. Αργότερα συντάθηκε στον όρο “bit” ο οποίος επικράτησε και είναι ο όρος που θα χρησιμοποιηθεί στην συνέχεια της εργασίας.

- Η πληροφορία που μεταφέρεται από δύο σύμβολα που απεικονίζουν ανεξάρτητα γεγονότα είναι ίση με το άθροισμα των επί μέρους πληροφοριών⁷.

Η μέση πληροφορία που μεταφέρεται ανά σύμβολο, ή αλλιώς, η εντροπία H , της πηγής είναι ίση με:

$$H = \sum_{i=1}^M P_i \cdot \log_2 \frac{1}{P_i} \quad (1.2.2)$$

και όταν $P_i=1/M$ για $i=1,2,3,\dots,M$ τότε η εντροπία μεγιστοποιείται και γίνεται ίση με:

$$H_{max} = \log_2 M \quad (1.2.3)$$

και για δυαδικό σύστημα με ισοπίθανα ψηφία η μέγιστη εντροπία θα είναι ίση με 1.

Στο δυαδικό σύστημα, ένα μήνυμα είναι, όπως προαναφέρθηκε, μία αλληλουχία δυαδικών ψηφίων. Αν ο ρυθμός μετάδοσης τους είναι ίσος με B bit/second τότε ο μέσος ρυθμός πληροφορίας θα ισούται με $B \cdot H$ bits. Με την συνήθη κωδικοποίηση σε M δυαδικές λέξεις μήκους $\log_2 M$ η κάθε μία (παραδείγματος χάριν στον κώδικα ASCII με $M=128$ ή $M=256$) ο ρυθμός μετάδοσης θα είναι ίσος με $B \cdot \log_2 M$. Άρα ο ρυθμός μετάδοσης θα ταυτίζεται με τον μέσο ρυθμό πληροφορίας μόνος όταν έχουμε μέγιστη εντροπία της πηγής. Σε οποιαδήποτε άλλη περίπτωση θα είναι μικρότερος. Και ο λόγος του μέσου ρυθμού μετάδοσης πληροφορίας προς τον ρυθμό μετάδοσης συμβόλου αποτελεί ένα ποιοτικό μέτρο του κάθε κώδικα και ορίζεται ως “απόδοση” (efficiency) του κώδικα. Η μεγιστοποίηση της απόδοσης των κωδίκων είναι ένα από τα βασικά αντικείμενα μελέτης της θεωρίας πληροφοριών έτσι ώστε να χρησιμοποιούνται κωδικές μέγιστης απόδοσης. Οι κωδικές αυτοί αφορούν, όπως προαναφέρθηκε, την πηγή πληροφορίας και οι μέθοδοι που χρησιμοποιούνται ονομάζονται “κωδικοποίηση πηγής πληροφορίας⁸”. Για κωδικές που χρησιμοποιούν λέξεις σταθερού μήκους, η μεγιστοποίηση της απόδοσης τους επιτυγχάνεται όταν τα σύμβολα που χρησιμοποιούνται έχουν την ίδια πιθανότητα. Αν δεν συμβαίνει αυτό

⁷ Αν έχουμε δύο σύμβολα M_1 και M_2 που απεικονίζουν μη ανεξάρτητα γεγονότα, η πληροφορία που θα περιέχουν θα δίνεται από την σχέση: $I_{i,j} = -\log_2 P(i,j)$ όπου $P(i,j)$ η συνδυασμένη πιθανότητα των γεγονότων αυτών.

⁸ Στα σύγχρονα τηλεπικοινωνιακά δίκτυα που είναι ψηφιακά, το σήμα κωδικοποιείται και πριν εισέλθει στο κανάλι επικοινωνίας. Η μέθοδος αυτή ονομάζεται “κωδικοποίηση καναλιού”, η οποία θα μελετηθεί στο επόμενο κεφάλαιο.

(να μην είναι τα σύμβολα ισοπίθανα) μία από τις μεθόδους αύξησης της απόδοσης του κώδικα είναι η χρήση λέξεων μεταβλητού μήκους.

Βασική συνεισφορά της θεμελίωσης της θεωρίας Πληροφορίας από τον Shannon (και ένα από τα βασικά αντικείμενα μελέτης της εργασίας του) ήταν η εύρεση των θεμελιωδών ορίων της επεξεργασίας ενός σήματος σε εφαρμογές όπως η συμπίεση δεδομένων (κωδικοποίηση πηγής) ή η κωδικοποίηση και αποστολή δεδομένων σε ένα κανάλι επικοινωνίας (κωδικοποίηση καναλιού) ώστε να έχουμε τον λιγότερο δυνατό θόρυβο και την μεγαλύτερη δυνατή αξιοπιστία στην μετάδοση των δεδομένων. Στα πλαίσια αυτού ορίστηκε ένα μέγεθος, η “χωρητικότητα καναλιού”. Το μέγεθος αυτό μας δείχνει ποιος είναι ο μέγιστος ρυθμός μετάδοσης δεδομένων σε ένα κανάλι επικοινωνίας με λευκό προσθετικό θόρυβο Γκάους⁹ (AWGN-Additive White Gaussian Noise) και για τον υπολογισμό του χρησιμοποιείται το θεώρημα του Shannon, η μαθηματική έκφραση του οποίου είναι:

$$C = B \cdot \log_2 \left(1 + \frac{S}{N} \right) \quad (1.2.4)$$

όπου το C είναι η χωρητικότητα του καναλιού, το B αναπαριστά το εύρος ζώνης συχνοτήτων που μπορεί να διέλθει μέσω αυτού και ο λόγος S/N (που ονομάζεται και SNR- Signal-to-noise Ratio¹⁰) είναι ο λόγος του σήματος πληροφορίας προς τον θόρυβο του καναλιού. Έτσι, γνωρίζοντας τα παραπάνω χαρακτηριστικά για ένα κανάλι επικοινωνίας μπορεί να υπολογιστεί η χωρητικότητά του. Το θεώρημα του Shannon λέει ότι είναι δυνατόν να επινοηθεί ένα κανάλι επικοινωνίας μέσω του οποίου ένα σύστημα επικοινωνίας θα μεταδίδει πληροφορία με μία αυθαίρετα μικρή πιθανότητα σφάλματος δεδομένου ότι ο ρυθμός μετάδοσης δεδομένων R θα είναι ίσος ή μικρότερος από τον ρυθμό C, δηλαδή την χωρητικότητά του καναλιού. Σύμφωνα με την απόδειξη του θεωρήματος του Shannon, ο ρυθμός μετάδοσης δεδομένων που προβλέπεται από τον παραπάνω τύπο δεν μπορεί να επιτευχθεί στα πραγματικά τηλεπικοινωνιακά συστήματα και το μεγαλύτερο ποσοστό που

⁹Είναι ένα είδος θορύβου που πρώτοξετάστηκε από τον μαθηματικό Carl Friedrich Gauss, από τον οποίο πήρε και το όνομα του. Καλείται “προσθετικός” γιατί προστίθεται στο κανάλι επικοινωνίας και “λευκός” γιατί σε όλες τις συχνότητες έχει την ίδια ενέργεια οπότε σε οποιαδήποτε συχνότητα και αν μεταδίδεται το σήμα, ο θόρυβος που θα του προστεθεί θα έχει το ίδιο πλάτος.

¹⁰Ο λόγος σήματος προς θόρυβο (S/N), ως λόγος ισχύων των αντίστοιχων σημάτων είναι αδιάστατη ποσότητα ενώ όταν εκφράζεται σαν SNR, εκφράζεται σε μονάδες deciBell (dB) και δίνεται από την σχέση $SNR = 10 \cdot \log_{10} \left(\frac{S}{N} \right)$.

έχει καταφέρει να φτάσει ο άνθρωπος είναι το 95% της χωρητικότητας αυτής. Όσο πιο κοντά στο όριο που θέτει το θεώρημα του Shannon είναι ο ρυθμός μετάδοσης που χρησιμοποιείται, τόσο μεγαλύτερη θα είναι η πιθανότητα σφάλματος και αν ξεπεραστεί το όριο αυτό, η πιθανότητα σφάλματος της μεταδιδόμενης πληροφορίας τείνει στην μονάδα και η μετάδοση της πληροφορίας καθίσταται αναξιόπιστη.

Το ζητούμενο από ένα τηλεπικοινωνιακό σύστημα είναι να μπορεί να μεταδώσει τον μέγιστο δυνατό όγκο πληροφορίας με την μέγιστη δυνατή ταχύτητα και την ελάχιστη δυνατή πιθανότητα σφάλματος. Οπότε κατά την σχεδίαση του θα πρέπει να ληφθούν υπόψιν όλα τα παραπάνω και να καθοριστεί ο ρυθμός μετάδοσης της πληροφορίας σύμφωνα με το θεώρημα του Shannon. Για την μείωση του σφάλματος, μπορεί να μειωθεί ο ρυθμός μετάδοσης του συστήματος, κάτι όμως που θα οδηγήσει στην μείωση του όγκου των μεταδιδόμενων δεδομένων και άρα του μεταδιδόμενου όγκου πληροφορίας. Μπορεί να αυξηθεί το εύρος συχνοτήτων που χρησιμοποιείται αλλά αυτή η αύξηση θα οδηγήσει σε αύξηση του θορύβου. Μπορεί να αυξηθεί η ενέργεια του σήματος ώστε να αυξηθεί ο λόγος σήματος προς θόρυβο αλλά αυτό θα οδηγήσει (σε κανάλια επικοινωνίας που χρησιμοποιούν μεθόδους πολύπλεξης FDMA ή/και CDMA) στην αύξηση του θορύβου καναλιού για τα υπόλοιπα σήματα που μεταδίδονται μέσω του ίδιου καναλιού. Οπότε πρέπει να επιλεγούν όλα τα παραπάνω χαρακτηριστικά ενός συστήματος κατάλληλα έτσι ώστε το σύστημα αυτό να είναι όσο πιο αποδοτικό και αξιόπιστο γίνεται για την εφαρμογή για την οποία προορίζεται.

Ένας από τους τρόπους αύξησης του ρυθμού μεταδιδόμενης πληροφορίας είναι η μείωση του όγκου δεδομένων που περιέχουν την πληροφορία αυτή και η κωδικοποίηση πηγής αποσκοπεί στην επίτευξη του στόχου αυτού. Μία από τις πρώτες τεχνικές κωδικοποίησης πηγής ήταν η δειγματοληψία του σήματος που οδήγησε στις ψηφιακές επικοινωνίες. Με τον όρο “δειγματοληψία” ορίζεται η λήψη δειγμάτων ενός αναλογικού σήματος ανά τακτά χρονικά διαστήματα T_s , οπότε έχουμε ψηφιοποίηση του αναλογικού αυτού σήματος. Για να μπορεί ένα σήμα που δειγματοληπτείται να ανακτηθεί, το θεώρημα δειγματοληψίας ορίζει ένα μέγιστο χρονικό διάστημα μεταξύ κάθε δείγματος (ή αλλιώς, έναν ελάχιστο ρυθμό δειγματοληψίας) $T_s \leq \frac{1}{f_M}$, όπου f_M η υψηλότερη συχνότητα του αναλογικού σήματος. Αφού από το συνεχές σήμα λαμβάνουμε και μεταδίδονται μόνο οι τιμές του ανά T_s επιτυγχάνεται σημαντική μείωση του όγκου του σήματος που περιέχει την πληροφορία, δίνοντας την δυνατότητα επίτευξης του ίδιου ρυθμού μετάδοσης πληροφορίας με πολύ μικρότερο ρυθμό μετάδοσης δεδομένων οπότε και μικρότερη πιθανότητα σφάλματος καθιστώντας το σύστημα πιο αξιόπιστο. Και αυτός είναι ένας από τους λόγους που τα

σύγχρονα τηλεπικοινωνιακά συστήματα είναι ψηφιακά και έγινε η μετάβαση από τις αναλογικές στις ψηφιακές τεχνολογίες που αναφέρθηκε στην αρχή της εργασίας.

Εκτός όμως από την δειγματοληψία, η οποία αφορά τα αναλογικά σήματα και την μετατροπή τους σε ψηφιακά, μέθοδοι και τεχνικές κωδικοποίησης πηγής έχουν αναπτυχθεί και για τα ψηφιακά σήματα οι οποίες αποσκοπούν όμως, κατά κύριο λόγο, στον ίδιο στόχο: την μείωση του όγκου των δεδομένων που απαιτείται για μία συγκεκριμένη ποσότητα πληροφορίας. Ανάλογα με το είδος των δεδομένων, υπάρχουν και οι αντίστοιχες τεχνικές και, ειδικά στην περίπτωση των πολυμέσων¹¹, οι τεχνικές αυτές είναι πολλές και ποικίλες. Οι τεχνικές αυτές, εκτός της καλύτερευσης της μετάδοσης των δεδομένων χρησιμοποιούνται και γιατί μειώνουν τον απαιτούμενο χώρο αποθήκευσης για τις πληροφορίες, ειδικά στις περιπτώσεις δεδομένων ήχου, εικόνας και βίντεο, όπου το ζητούμενο είναι να έχουμε την μέγιστη δυνατή πληροφορία στον ελάχιστο δυνατό όγκο δεδομένων λόγω περιορισμών του μεγέθους των μέσων αποθήκευσης των δεδομένων.

Μία από τις πιο διαδεδομένες τέτοιες τεχνικές είναι το πρότυπο ψηφιακής κωδικοποίησης ήχου MPEG-1 Audio Layer 3 (3^ο Επίπεδο Ήχου του προτύπου MPEG-1), γνωστό και ως MP3. Η βασική αρχή του προτύπου αυτού είναι η αποτελεσματική συμπίεση αρχείων ήχου μέσω ενός αλγόριθμου ο οποίος μειώνει δραστικά τον όγκο των ψηφιακών δεδομένων (δηλαδή των δεδομένων μετά την ψηφιοποίηση του αναλογικού ήχου) που απαιτούνται για την αποθήκευση του ήχου που περιέχει το αρχείο, ο οποίος όμως συνεχίζει να ακούγεται σαν πιστή αναπαραγωγή του αρχικού ασυμπίεστου περιεχομένου από τους περισσότερους ακροατές¹² το οποίο εφευρέθηκε από μία ομάδα Γερμανών μηχανικών του ιδρύματος Fraunhofer και τυποποιήθηκε με βάση το πρότυπο ISO/IEC το 1991.

Το πρότυπο MP3 ανήκει στην γενική μέθοδο συμπίεσης και μετάδοσης βίντεο MPEG¹³ και έχουν υπάρξει πολλές εκδόσεις της και συνεχίζουν να αναπτύσσονται καινούριες, οι οποίες ακολουθούν τις τεχνολογικές εξελίξεις μέσω αποθήκευσης και

¹¹Συνδυασμός ψηφιακών δεδομένων πολλαπλών μορφών, δηλαδή κειμένου, γραφικών εικόνας, κινούμενης εικόνας (animation), ήχου και βίντεο, για την αναπαράσταση, παρουσίαση, αποθήκευση, μετάδοση και επεξεργασία πληροφοριών.

¹²Μία από τις τεχνικές που χρησιμοποιούνται για την συμπίεση είναι η αποκοπή των υψηλών συχνοτήτων, δηλαδή τον περιορισμό του εύρους ζώνης του σήματος, τις οποίες δεν “ακούν” οι περισσότεροι άνθρωποι και για τον λόγο αυτό γίνεται η διάκριση της πιστότητας για του περισσότερους ακροατές.

¹³Το ακρωνύμιο MPEG από το οποίο έχουν πάρει το όνομα τους οι οικογένειες προτύπων αυτές προέρχεται από το όνομα της ομάδας εργασίας της ISO/IEC Moving Picture Experts Group αντικείμενο μελέτης της οποίας είναι η ανάπτυξη και προτυποποίηση μεθόδων συμπίεσης και μετάδοσης βίντεο.

μετάδοσης δεδομένων. Κάθε έκδοση του MPEG περιέχει πολλά πρότυπα (ή μεθόδους κωδικοποίησης) και επίπεδα, όπως φάνηκε και στα παραπάνω όπου το πρότυπο MP3 είναι το 3^ο επίπεδο ήχου του προτύπου MPEG-1. Η έκδοση αυτή είχε σχεδιαστεί για CD-ROM, του οποίου η μέγιστη χωρητικότητα είναι 800MBytes και η ταχύτητα μεταφοράς 1.5 Mbps (Mbit per second). Η επόμενη έκδοση ήταν η MPEG-2 η οποία σχεδιάστηκε για DVD υψηλής ποιότητας (απλός DVD δίσκος έχει χωρητικότητα που κυμαίνεται στα 4,7GByte) με ταχύτητα μεταφοράς από 4 μέχρι 9 Mbps και αρχικά υιοθετήθηκε από συστήματα εκπομπής ψηφιακής τηλεόρασης υψηλής ευκρίνειας. Μία άλλη πολύ σημαντική MPEG έκδοση¹⁴ είναι η τέταρτη έκδοση, MPEG-4 η οποία σχεδιάστηκε για εφαρμογές με μικρό εύρος ζώνης συχνοτήτων ώστε να μπορεί να μεταδίδονται δεδομένα βίντεο μέσω καναλιών επικοινωνίας περιορισμένων δυνατοτήτων (ρυθμών μετάδοσης δεδομένων) και περιέχει κάποια από τα πιο ευρέως χρησιμοποιούμενα πρότυπα (ή μεθόδους κωδικοποίησης) δύο από τα οποία είναι το MPEG-4 μέρος 2 (χρησιμοποιείται από πολλές τεχνικές κωδικοποίησης όπως τα DivX, Xvid, Nero Digital και 3ivx) και το MPEG-4 μέρος 10 που είναι η μέθοδος κωδικοποίησης που χρησιμοποιείται και στην Ελλάδα από το υπάρχον σύστημα ψηφιακής τηλεόρασης.

Κεφάλαιο 2

2.1 – Πρότυπα ψηφιακή μετάδοση βίντεο H.262 και H.264

Δύο από τις πιο διαδεδομένες μεθόδους ψηφιακής κωδικοποίησης και μετάδοσης βίντεο είναι οι H.262 και H.264 στα οποία θα γίνει εκτενής αναφορά στις επόμενες παραγράφους. Ανήκουν στην κατηγορία “συστάσεων¹⁵” ψηφιακής κωδικοποίησης και μετάδοσης βίντεο H.26x που αναπτύσσονται από την ομάδα Visual Coding Experts Group (VCEG) της ITU-T τα οποία αναπτύχθηκαν σε συνεργασία με την ομάδα MPEG και για τον λόγο αυτό ανήκουν και στην οικογένεια των MPEG προτύπων, με το πρότυπο H.262 να ονομάζεται και MPEG-2 μέρος 2 και το H.264¹⁶ MPEG-4 μέρος 10.

¹⁴Αναφορά σε άλλες MPEG εκδόσεις ξεφεύγει από τα πλαίσια της παρούσας εργασίας και δεν θα γίνει.

¹⁵Τα “αποτελέσματα” των εργασιών των ομάδων της ITU ονομάζονται “συστάσεις” (Recommendations) και είναι αντίστοιχα με τα πρότυπα που εκδίδονται από τις ομάδες του οργανισμού ISO.

¹⁶Το πιο πρόσφατο πρότυπο της συνεργασίας των δύο αυτών ομάδων είναι το H.265 ή MPEG-H μέρος 2 που εκδόθηκε το 2013, στο οποίο όμως δεν θα γίνει περαιτέρω αναφορά

2.1.1 - Πρότυπο H.262

Το H.262 (ή MPEG-2 μέρος 2) είναι παρόμοιο με αντίστοιχα πρότυπα του MPEG-1 με τις ειδοποιές διαφορές να είναι δύο: πρώτον ότι παρέχει υποστήριξη για βίντεο με interlaced¹⁷ μορφή (η τεχνική αυτή κωδικοποίησης χρησιμοποιείται στα συστήματα τηλεόρασης NTSC, PAL και SECAM) και δεύτερον ότι έχει πολύ καλύτερη απόδοση για ρυθμούς μετάδοσης μεγαλύτερους των 3Mbps. Όμως, έχει πολύ κακή απόδοση για ρυθμούς μετάδοσης μικρότερους από 1Mbps. Έχουν αναπτυχθεί και εκδοθεί τρεις, όπως φαίνεται και στον παρακάτω πίνακα (πίνακας 2.1), όπου παρατίθενται λεπτομέρειες σχετικά με το έτος έκδοσης, το έτος τελευταίας αναθεώρησης, το πρότυπο ISO/IEC καθώς και την σύσταση ITU-T που αντιστοιχεί στην κάθε μία.

Έκδοση	Έτος έκδοσης	Τελευταία αναθεώρηση	ISO/IEC πρότυπο	ITU-T σύσταση
Πρώτη έκδοση	1995	2000	ISO/IEC 13818-2:1996	H.262 (07/95)
Δεύτερη έκδοση	2000	2010	ISO/IEC 13818-2:2000	H.262 (02/00)
Τρίτη έκδοση	2013		ISO/IEC 13818-2:2013	H.262 (02/12)

Πίνακας 2.1 – Εκδόσεις του H.262/MPEG-2 part 2

Όπως αναφέρθηκε παραπάνω, το H.262 σχεδιάστηκε για εφαρμογές συμπίεσης και μετάδοσης βίντεο υψηλής ποιότητας. Οπότε, η εικόνα την οποία σχεδιάστηκε να μπορεί να διαχειριστεί και να μεταδώσει θα είναι εικόνα από κάμερα υψηλής ευκρίνειας όπου με τον όρο αυτό χαρακτηρίζονται οι κάμερες οι οποίες παρέχουν ανάλυση εικόνας υψηλής ευκρίνειας 1080p δηλαδή η οριζόντια ανάλυση της εικόνας θα είναι 1080 γραμμές από pixels¹⁸ και για μία αναλογία 16:9, η κατακόρυφη θα είναι 1920 γραμμές και θα αποτελείται

¹⁷Ο όρος αποδίδεται στα ελληνικά ως πεπλεγμένη ή διεπλεγμένη μορφή και περιγραφή της μορφής αυτής θα γίνει παρακάτω. Στο υπόλοιπο μέρος της εργασίας θα χρησιμοποιηθεί ο αγγλικός όρος.

¹⁸Οι ψηφιοποιημένες εικόνες χωρίζονται σε εικονοστοιχεία (pixels) όπου κάθε pixel περιέχει πληροφορία χρώματος. Έτσι, όσο πιο πολλά pixels έχει μία εικόνα, τόσο καλύτερη ανάλυση έχει. Το μέγεθος, σε μονάδες δεδομένων, που μπορεί να έχει ένα pixel εξαρτάται από το πόσες αποχρώσεις (τιμές χρωμάτων) μπορεί να έχει.

συνολικά από 2073600 pixels. Ο ελάχιστος ρυθμός εικόνων ανά δευτερόλεπτο ώστε το ανθρώπινο μάτι να καταλαβαίνει κίνηση είναι 24 εικόνες το δευτερόλεπτο. Τέλος, για μία εικόνα με πολύ καλή ποιότητα χρωμάτων (Truecolor: 16,777,216 τιμές χρώματος) κάθε pixel θα έχει μέγεθος 3 byte ($2^8 * 2^8 * 2^8 = 16,777,216$). Οπότε, μία τέτοια κάμερα θα παράγει βίντεο το οποίο, για ένα δευτερόλεπτο (24 εικόνες) θα έχει μέγεθος $24 * 1920 * 1080 * 3 = 149,299,200$ bytes το δευτερόλεπτο. Το μέγεθος αυτό είναι υπερβολικά μεγάλο για να μεταδοθεί μέσω ενός καναλιού επικοινωνίας κάποιου τηλεπικοινωνιακού δικτύου. Οπότε ο όγκος των δεδομένων αυτών θα πρέπει να συμπιεστεί πολύ ώστε να μπορεί να μεταδοθεί με τους ρυθμούς που υποστηρίζει το H.262 οι οποίοι είναι, όπως προαναφέρθηκε, από 4 μέχρι 9 Mbps. Για την επίτευξη του στόχου αυτού η κωδικοποίηση H.262 χρησιμοποιεί διάφορες τεχνικές/τρόπους.

Ένας πρώτος τέτοιος τρόπος μείωσης του όγκου των δεδομένων αυτών είναι η χρήση της interlaced μορφής βίντεο που αναφέρθηκε παραπάνω. Αρχικά, χωρίζεται κάθε εικόνα σε δύο πεδία, όπου το ένα θα περιέχει τα δεδομένα των pixel που βρίσκονται στις άρτιες γραμμές της εικόνας και το άλλο στις περιττές περιττές γραμμές. Η διαδικασία αυτή γίνεται κατά την διάρκεια της κωδικοποίησης και αποθηκεύεται ή μεταδίδεται ένα από αυτά για κάθε εικόνα, εναλλάξ. Κατά την διαδικασία της αποκωδικοποίησης απεικονίζονται τα πεδία που λήφθηκαν και δημιουργούν στο ανθρώπινο μάτι την εντύπωση της πλήρους κινούμενης εικόνας για τον ρυθμό λήψης εικόνων ανά δευτερόλεπτο που χρησιμοποιούνται στα τηλεοπτικά δίκτυα (50 στο Ευρωπαϊκό πρότυπο PAL και 59.94 στο Αμερικάνικο NTSC). Οπότε με τον τρόπο αυτό μειώνεται στο μισό ο όγκος δεδομένων που πρέπει να μεταδοθεί. Όμως το H.262 υποστηρίζει μόνο την interlaced μορφή βίντεο αλλά και την progressive μορφή¹⁹, στην οποία κάθε εικόνα είναι ένα πλήρες πλαίσιο και μεταδίδονται όλα τα pixels.

Ένας άλλος είναι η κωδικοποίηση του κάθε pixel σε τρεις τιμές από τις οποίες η μία αναπαριστά την φωτεινότητα του συγκεκριμένου pixel και οι άλλοι δύο περιέχουν πληροφορίες χρώματος. Λόγω του χαρακτηριστικού του ανθρώπινου ματιού να καταλαβαίνει καλύτερα λεπτομέρειες φωτεινότητας από ότι λεπτομέρειες χρώματος, μπορούν να αγνοηθούν κάποιες τιμές χρώματος, δηλαδή να έχουμε “υποδειγματοληψία” (ανάλογα με την εφαρμογή ή/και την τεχνική που χρησιμοποιείται, ο λόγος υποδειγματοληψίας ποικίλει²⁰) και οι τιμές του χρώματος των pixel που αγνοήθηκαν να οριστούν κατά την αποκωδικοποίηση

¹⁹Ένα μη interlaced βίντεο χαρακτηρίζεται ως ‘προοδευτικά σαρωμένο’ (progressively scanned) ή ‘ακολουθιακά σαρωμένο’ (sequentially scanned) βίντεο.

²⁰Οι πιο συνηθισμένες δομές υποδειγματοληψίας είναι οι 4:2:2 και 4:2:0. Το 4:2:2 σημαίνει ότι η πληροφορία χρώματος υποδειγματοληπτείται στην οριζόντια διάσταση με ένα συντελεστή 2 σε σχέση με την φωτεινότητα, ενώ το 4:2:0 σημαίνει ότι υποδειγματοληπτείται στην οριζόντια και στην κάθετη διάσταση με ένα συντελεστή 2 σε σχέση με την φωτεινότητα.

σύμφωνα με τις τιμές των γειτονικών τους pixel, με αποτέλεσμα να μειωθεί ο όγκος των δεδομένων που μεταδίδονται.

Συμπληρωματικά με τα παραπάνω, το MPEG-2 χρησιμοποιεί και δύο τεχνικές συμπίεσης του όγκου των δεδομένων οι οποίες στηρίζονται στον ορισμό τριών ειδών πλαισίων στα οποία μπορεί να κωδικοποιηθεί (συμπιεστεί) μία εικόνα²¹: τα intra-coded frames (ενδο-κωδικοποιημένα πλαίσια) ή I-frames, τα predictive-coded frames (πλαίσια με κωδικοποίηση πρόβλεψης) ή P-frames και τα bidirectionally-predictive-coded frames (πλαίσια με κωδικοποίηση αμφίδρομης πρόβλεψης) ή B-frames. Στην πρώτη τεχνική χρησιμοποιείται ο διακριτός μετασχηματισμός συνημιτόνου (Discrete Cosine Transform – DCT) και στην δεύτερη η πρόβλεψη αντισταθμισμένης κίνησης (motion-compensated).

Ένα I-frame είναι ένα πλαίσιο από pixels το οποίο αντιστοιχεί σε μία κωδικοποιημένη πλήρη και ανεξάρτητη εικόνα (χωρίς αναφορά σε άλλες εικόνες). Το πλαίσιο αυτό διαιρείται σε μικρά μπλοκ των 8*8 pixels (8 pixels σε 8 γραμμές) και σε κάθε τέτοιο μπλοκ εκτελείται ένας DCT δύο διαστάσεων έτσι ώστε να παραχθεί ένας πίνακας από DCT συντελεστές. Το αποτέλεσμα είναι να μετατραπούν οι τιμές μεταβλητών χώρου σε τιμές μεταβλητών συχνότητας, χωρίς όμως να έχουμε κάποια αλλαγή της περιεχόμενης πληροφορίας. Η κωδικοποιημένη εικόνα μπορεί να αποκωδικοποιηθεί εφαρμόζοντας τον αντίστροφο διακριτό μετασχηματισμό συνημιτόνου. Ο λόγος για τον οποίο γίνεται ο μετασχηματισμός αυτός είναι το γεγονός ότι οι τιμές που αντιστοιχούν στις υψηλότερες συχνότητες θα είναι κοντά στο μηδέν. Εφαρμόζοντας κβαντισμό²² μηδενίζονται οι υψηλές συχνότητες κάτι που αν και προκαλεί κάποια απώλεια πληροφορίας (η αποκωδικοποίηση των κβαντισμένων τιμών παράγει μία εικόνα όμοια με την αρχική στην ευκρίνεια αλλά με λίγο λιγότερες αποχρώσεις). Στην συνέχεια, οι πίνακες των κβαντισμένων συντελεστών συμπίεζονται με τα εξής βήματα: μετά τον κβαντισμό έχουν μηδενιστεί, όπως προαναφέρθηκε, οι τιμές αρκετών συντελεστών του κάθε πίνακα, οι οποίες θα βρίσκονται σε μία από τις γωνίες του πίνακα. Αρχίζοντας από την αντίθετη γωνία, ακολουθώντας μία διαγώνια ζιγκ-ζαγκ πορεία, οι τιμές των συντελεστών που περιέχει ο πίνακας μετατρέπονται σε γραμμικές ακολουθίες τιμών στις οποίες εφαρμόζεται κωδικοποίηση με χρήση κώδικα μεταβλητού μήκους, όπου οι συνεχόμενες

²¹Τα πλαίσια αυτά είναι κοινά σε όλα τα MPEG πρότυπα με την διαφορά ότι στο MPEG-1 οριζόταν ένα ακόμα είδος πλαισίου, το D-frame, που ήταν παρόμοιο με το I-frame που θα περιγραφεί παρακάτω αλλά πολύ χαμηλότερης ποιότητας, το οποίο δεν συμπεριλήφθηκε στα επόμενα πρότυπα.

²²Η μέθοδος του κβαντισμού είναι η μετατροπή των συνεχών τιμών ενός μεγέθους σε διακριτές. Επιλέγονται κάποιες συγκεκριμένες τιμές, οι στάθμες κβαντισμού, και αντικαθίστανται η συνεχής τιμές των αρχικών δεδομένων με την πλησιέστερη στάθμη κβαντισμού στην κάθε μία.

μηδενικές τιμές αναπαρίστανται σε μία κωδική λέξη με την επόμενη μη μηδενική τιμή με αποτέλεσμα την μείωση του όγκου των δεδομένων που θα μεταδοθούν με χρήση του DCT, η οποία χρησιμοποιεί μόνο τα I-frame.

Η δεύτερη τεχνική και τα τρία είδη πλαισίων που ορίζονται στο MPEG. Στηρίζεται στην λογική ότι σε ένα βίντεο, οι τιμές χρώματος και φωτεινότητας που θα περιέχει μία αλληλουχία εικόνων δεν είναι, γενικά, ανεξάρτητες η μία με την άλλη αλλά έχουμε χρονική επανάληψη της πληροφορίας και γίνεται μία προσπάθεια “πρόβλεψης” της εικόνας που πρόκειται να κωδικοποιηθεί βάσει μίας προηγούμενης εικόνας “αναφοράς”. Ως εικόνες ή πλαίσια αναφοράς χρησιμοποιούνται τα I-frames, τα οποία παράγονται συνήθως ανά 15 πλαίσια. Βάσει λοιπόν των εικόνων αναφοράς, για τα άλλα δύο είδη πλαισίων κωδικοποιείται η μεταβολή της θέσης του κάθε 8*8 μπλοκ στα οποία είναι χωρισμένη η εικόνα και μεταδίδονται τα απαραίτητα δεδομένα για την κίνηση αυτή και όχι όλα τα δεδομένα του κάθε μπλοκ, μειώνοντας πολύ τον όγκο των μεταδιδόμενων δεδομένων (λόγω αυτού η τεχνική αυτή μπορεί να χαρακτηριστεί και, εν μέρει, διαφορεική κωδικοποίηση, με την έννοια ότι κωδικοποιούνται, όπως θα δειχθεί παρακάτω, όχι τα ίδια τα δεδομένα αλλά διαφορές αυτών και συγκεκριμένα της θέσης τους). Τα είδη αυτά και ο τρόπος με τον οποίο κωδικοποιούνται τα δεδομένα των εικόνων στις οποίες αντιστοιχούν είναι:

P-frames: Μπορούν να χρησιμοποιήσουν κάποιο προηγούμενο I-frame ή P-frame για “αντιστάθμιση κίνησης” και ενδέχεται να χρησιμοποιηθούν σαν αναφορά από κάποιο άλλο P-frame ή B-frame. Για την κωδικοποίηση του κάθε μπλοκ σε ένα P-frame μπορεί είτε να κωδικοποιηθούν τα δεδομένα κίνησης ενός μπλοκ του πλαισίου που χρησιμοποιεί σαν αναφορά είτε να κωδικοποιηθούν απευθείας τα δεδομένα της εικόνας ανεξάρτητα. Και επειδή στις περισσότερες περιπτώσεις δεν έχουμε πολύ έντονες αλλαγές μεταξύ των κοντινών εικόνων ενός βίντεο, για τα περισσότερα μπλοκ μεταδίδονται μόνο δεδομένα κίνησης επιτυγχάνοντας μεγάλη μείωση της χρονικής και χωρικής επανάληψης πληροφορίας που είναι κοινή σε αυτό και στο πλαίσιο αναφοράς, με αποτέλεσμα τα P-frames να προσφέρουν σημαντικά αυξημένη συμπίεση σε σχέση με τα I-frames.

B-frames: Κωδικοποιούνται με την ίδια λογική αντιστάθμισης κίνησης με τα P-frames με την διαφορά ότι μπορούν να χρησιμοποιήσουν, εκτός από κάποιο προηγούμενο, και κάποιο επόμενο I-frame ή P-frame για τον υπολογισμό της κίνησης αντιστάθμισης, και προσφέρουν τον υψηλότερο βαθμό συμπίεσης. Για να μπορεί όμως να χρησιμοποιηθεί η “προς τα πίσω πρόβλεψη”, δηλαδή να χρησιμοποιηθεί ένα μελλοντικό πλαίσιο σαν πλαίσιο αναφοράς κατά την αποκωδικοποίηση, θα πρέπει να υπάρχει το πλαίσιο αυτό στον αποκωδικοποιητή. Για τον λόγο αυτό, ο κωδικοποιητής αναδιατάσσει τα μεταδιδόμενα

πλαίσια από την φυσική τους σειρά έτσι ώστε ένα B-frame να μεταδίδεται μετά τα πλαίσια που χρησιμοποιεί ως πλαίσια αναφοράς. Αυτό εισάγει μια καθυστέρηση αναδιάταξης, η οποία εξαρτάται από τον αριθμό των διαδοχικών B-frames, καθυστέρηση όμως που αντισταθμίζεται από την αυξημένη δυνατότητα συμπίεσης των δεδομένων των πλαισίων αυτών.

Ένα H.262 σύστημα χρησιμοποιεί έναν συνδυασμό των παραπάνω τεχνικών επιτυγχάνοντας και μεγάλη συμπίεση των δεδομένων αλλά και σχετικά μικρή απώλεια πληροφορίας. Τα χαρακτηριστικά αυτά το καθιστούν χρήσιμο σε πολλές εφαρμογές, από κινητές συσκευές μέχρι επεξεργασία βίντεο υψηλής ευκρίνειας. Κάθε όμως τέτοια εφαρμογή δεν χρησιμοποιεί όλες τις τεχνικές και τα χαρακτηριστικά του προτύπου αυτού. Για τον λόγο αυτό ορίζονται διάφορα “προφίλ” και “επίπεδα” του H.262. Με κάθε διαφορετικό προφίλ ορίζεται ένα σύνολο χαρακτηριστικών, όπως είναι παραδείγματος χάριν το είδος των πλαισίων που θα χρησιμοποιηθούν, η δυνατότητα τρισδιάστατων βίντεο και το είδος της διαμόρφωσης των χρωμάτων που θα χρησιμοποιηθεί, δημιουργώντας έτσι διαφορετικές “εκδόσεις” του. Με κάθε επίπεδο ορίζονται τα όρια της μνήμης και της επεξεργαστικής ισχύος που απαιτούνται από ένα σύστημα καθώς και ο μέγιστος ρυθμός δεδομένων και το μέγεθος και ο ρυθμός των πλαισίων. Έτσι, κάθε εφαρμογή που χρησιμοποιεί το H.262 μπορεί να επιλέξει το προφίλ και το επίπεδο που είναι καταλληλότερο για το είδος αυτής για να χρησιμοποιήσει χωρίς να είναι απαραίτητο να υλοποιήσει όλα τα διαθέσιμα χαρακτηριστικά του. Ακόμα, δηλώνοντας το προφίλ και το επίπεδο που χρησιμοποιεί μπορεί να ενημερώσει δυνητικούς χρήστες για τις δυνατότητες της.

Συντ/φία	Όνομα	Τύποι πλαισίων	Υποδ/ληψία	Αναλογίες απεικόνισης	Intra DC ακρίβεια ²³
SP	Simple profile	I, P	4:2:0	4:3 ή 16:9	8, 9, 10
MP	Main profile	I, P, B	4:2:0	4:3 ή 16:9	8, 9, 10
SNR	SNR Scalable profile	I, P, B	4:2:0	4:3 ή 16:9	8, 9, 10
Spatial	Spatially Scalable profile	I, P, B	4:2:0	4:3 ή 16:9	8, 9, 10

²³Το μέγεθος αυτό δηλώνει το πλήθος των bits που χρησιμοποιείται για την κβάντωση των DCT συντελεστών.

HP	High profile	I, P, B	4:2:2 ή 4:2:0	4:3 ή 16:9	8, 9, 10, 11
422	4:2:2 profile	I, P, B	4:2:2 ή 4:2:0	4:3 ή 16:9	8, 9, 10, 11
MVP	Multi-view profile	I, P, B	4:2:0	4:3 ή 16:9	8, 9, 10

Πίνακας 2.2 – Προφίλ του H.262/MPEG-2 part 2

Στον παραπάνω πίνακα (πίνακα 2.2) παρατίθενται τα διαθέσιμα προφίλ του H.262 και στον παρακάτω (πίνακας 2.3) τα επίπεδα που έχουν οριστεί. Το επίπεδο και το προφίλ που υποστηρίζει κάθε εφαρμογή ή και συσκευή δηλώνεται ως profile @ level. Για παράδειγμα ένα μηχάνημα αναπαραγωγής DVD που υποστηρίζει μέχρι και το κύριο προφίλ και το κύριο επίπεδο θα το δήλωνε ως “MP@ML” το οποίο στην ουσία περιγράφει τα χαρακτηριστικά της κωδικοποίησης των DVD δίσκων που μπορεί να έχει κάποιος ώστε να αναπαραχθεί σωστά από το συγκεκριμένο μηχάνημα.

Συντομο- γραφία	Όνομα	Ρυθμός πλαισίων (Hz)	Μέγιστη οριζόντια ανάλυση	Μέγιστη κάθετη ανάλυση	Μέγιστο πλήθος δειγμάτων φωτεινότητας ανά δευτερόλεπτο	Μέγιστος ρυθμός δεδομένων στο κύριο προφίλ (Mbit/s)
LL	Low Level	23.976, 24, 25, 29.97, 30	352	288	3,041,280	4
ML	Main Level	23.976, 24, 25, 29.97, 30	720	576	10,368,000, εκτός του High profile, όπου είναι 14,475,600 για 4:2:0 και 11,059,200 για 4:2:2	15
H-14	High 1440	23.976, 24, 25, 29.97, 30,	1440	1152	47,001,600, εκτός του High profile με 4:2:0, όπου είναι	60

		50, 59.94, 60			62,668,800	
HL	High Level	23.976, 24, 25, 29.97, 30, 50, 59.94, 60	1920	1152	62,668,800, εκτός του High profile με 4:2:0, όπου είναι 83,558,400	80

Πίνακας 2.3 – Επίπεδα του H.262/MPEG-2 part 2

2.1.2 - Πρότυπο H.264

Το H.264 είναι ένα πρότυπο που προορίζεται να υποστηρίζει τις πιο αποτελεσματικές τεχνικές συμπίεσης βίντεο που ήταν διαθέσιμες, με την πρώτη ολοκληρωμένη έκδοση να δημοσιεύεται τον Μάιο του 2003. Σχεδιάστηκε έτσι ώστε, χωρίς συμβιβασμούς στην ποιότητα της εικόνας, ένας κωδικοποιητής H.264 να μπορεί να μειώσει το μέγεθος ενός ψηφιακού αρχείου βίντεο περισσότερο από 80% σε σύγκριση με την Motion JPEG μέθοδο και 50% περισσότερο από ότι με το πρότυπο MPEG-4 μέρος 2. Αυτό σημαίνει ότι απαιτείται για ένα αρχείο βίντεο πολύ μικρότερο εύρος ζώνης δικτύου και αποθηκευτικός χώρος, χαρακτηριστικό που προσδίδει στο πρότυπο αυτό την ευελιξία να υποστηρίξει μια ευρεία ποικιλία εφαρμογών με πολύ διαφορετικές απαιτήσεις ρυθμού bit. Για παράδειγμα, στις εφαρμογές που μεταδίδουν ψυχαγωγικά βίντεο, όπως η δορυφορική και η καλωδιακή τηλεόραση και τα συστήματα αναπαραγωγής δίσκων DVD, το H.264 θα είναι σε θέση να προσφέρει επιδόσεις από 1 έως 10 Mbps με υψηλή όμως καθυστέρηση, όπου όμως ενδιαφέρει περισσότερο ο υψηλός ρυθμός μετάδοσης, ενώ για υπηρεσίες τηλεπικοινωνιών μπορεί να προσφέρει ρυθμούς δεδομένων μικρότερους του 1 Mbps με χαμηλή καθυστέρηση, όπου στις εφαρμογές αυτές οι οποίες χαρακτηρίζονται και ως “εφαρμογές πραγματικού χρόνου” και απαιτούν να είναι όσο δυνατόν πιο μικρή η καθυστέρηση. Οπότε τα αποτελέσματα από κωδικοποιητές που χρησιμοποιούν το ίδιο πρότυπο συμπίεσης μπορεί να ποικίλει, επειδή ο σχεδιαστής ενός κωδικοποιητή μπορεί να επιλέξει να εφαρμόσει διαφορετικά σύνολα εργαλείων που ορίζονται από το πρότυπο αυτό, που δεν είναι άλλα από τα προφίλ που αναφέρθηκαν και στην περίπτωση του H.262, ανάλογα με την εφαρμογή για

την οποία προορίζεται²⁴.

Ως μέλος της οικογένειας πρωτοκόλλων MPEG αλλά και της ομάδας συστάσεων H.26x έχει πολλά κοινά στον τρόπο λειτουργίας με το H.264 που αναφέρθηκε στην προηγούμενη ενότητα και για τον λόγο αυτό δεν θα γίνει αναφορά στα κοινά τους χαρακτηριστικά. Η περιγραφή της λειτουργίας και του τρόπου με τον οποίο επιτυγχάνεται η συμπίεση των δεδομένων στην μέθοδο αυτή θα περιοριστεί στην αναφορά των καινοτόμων χαρακτηριστικών που εισήγαγε αυτή, με αναφορά και στις διαφορές μεταξύ των H.262 και H.264. Και τα χαρακτηριστικά αυτά είναι που οφείλονται για την δυνατότητα πιο αποδοτικής συμπίεσης και την μεγαλύτερη ευελιξία ώστε να είναι κατάλληλο για ποικίλες εφαρμογές κωδικοποίησης και μετάδοσης βίντεο. Κάποια από τα κύρια χαρακτηριστικά αναφέρονται παρακάτω.

Ένα από αυτά είναι η μέθοδος αντιστάθμισης κίνησης πολλαπλών εικόνων (Χρησιμοποιώντας προηγούμενες κωδικοποιημένες εικόνες πιο αποδοτικά, επιτρέπει την χρήση μέχρι και 16 πλαισίων ως πλαίσια αναφοράς (ή 32 πλαίσια στην περίπτωση της interlaced κωδικοποίησης). Στα προφίλ που υποστηρίζουν μη IDR-πλαίσια, τα περισσότερα επίπεδα (στις λεπτομέρειες των προφίλ και των επιπέδων θα γίνει αναφορά παρακάτω) καθορίζουν ότι θα πρέπει να υποστηρίζει το σύστημα προσωρινή μνήμη ικανή να επιτρέπει την χρήση τουλάχιστον 4-5 πλαισίων αναφοράς στην μέγιστη ανάλυση, χαρακτηριστικό που στα προηγούμενα πρότυπα το όριο ήταν συνήθως 1, ή στην περίπτωση των B-frames δύο. Αυτό προσφέρει μέτρια βελτίωση του ρυθμού δεδομένων και της ποιότητας στις περισσότερες των περιπτώσεων, όμως σε κάποιες περιπτώσεις, όπως η επαναλαμβανόμενη κίνηση ή η αποκάλυψη περιοχών του φόντου σε ένα βίντεο προσφέρει μεγάλη μείωση του ρυθμού δεδομένων διατηρώντας την διαύγεια την εικόνας.

Το μέγεθος των μπλοκ στα οποία χωρίζεται κάθε πλαίσιο είναι μεταβλητό, με το μεγαλύτερο να ορίζεται σε 16*16 pixels και το μικρότερο 4*4 pixels, δίνοντας την δυνατότητα την επιλογή του μεγέθους στον αλγόριθμο ώστε, ανάλογα με την περίπτωση, να επιλεγεί το κατάλληλο καθώς και την επιλογή περισσότερων του ενός μεγέθους στην πρόβλεψη για ένα μπλοκ. Το μέγεθος που θα χρησιμοποιηθεί για την πρόβλεψη μπλοκ απόχρωσης θα είναι μικρότερο από αυτό που θα χρησιμοποιηθεί για ένα μπλοκ φωτεινότητας λόγω της υποδειγματοληψίας που εφαρμόζεται στα πρώτα. Και για την πρόβλεψη αυτή,

²⁴Τα οποία ισχύουν και για τον αποκωδικοποιητή ο οποίος πρέπει να είναι σχεδιασμένος να υποστηρίζει το προφίλ βάσει του οποίου έχουν κωδικοποιηθεί τα δεδομένα που είναι προς αποκωδικοποίηση. Για τον λόγο αυτό επειδή οι αποκωδικοποιητές είναι επιθυμητό να μπορούν λαμβάνουν και να αποκωδικοποιούν σήματα από ποικίλους κωδικοποιητές, είναι πιο πολύπλοκοι κυκλωματικά.

μπορούν να χρησιμοποιηθούν περισσότερα από ένα διανύσματα κίνησης, με μέγιστο πλήθος να ορίζονται τα 32 για την περίπτωση ενός B μακρομπλόκ που κατασκευάζεται από δεκαέξι 4*4 διαιρέσεις. Και κάθε ένα διάνυσμα κίνησης για κάθε 8*8, ή μεγαλύτερη διαίρεση, μπορεί να χρησιμοποιήσει σημείο από διαφορετική εικόνα αναφοράς από τα υπόλοιπα.

Εκτός των παραπάνω, χρησιμοποιείται ακρίβεια ενός τετάρτου του pixel για αντιστάθμιση κίνησης, καθιστώντας ικανή την ακριβέστερη μετακίνηση της κινούμενης περιοχής και για ανάλυση χρώματος με υποδειγματοληψία 4:2:0 (που είναι αρκετά συνηθισμένη) χρησιμοποιείται πλέγμα μεγέθους ενός ογδού του pixel, μειώνοντας κατά πολύ τον όγκο των δεδομένων, σχετικά με τα άλλα πρότυπα, χωρίς να έχει απώλειες ποιότητας εικόνας. Τέλος, χωρική πρόβλεψη κίνησης βάσει των άκρων των γειτονικών μπλοκ για “ενδο-κωδικοποίηση” και όχι μόνο βάσει των DC συντελεστών που αναφέρθηκαν στο H.262 (ή της πρόβλεψης μετασχηματισμού συνημιτόνου που χρησιμοποιείται από το H.263v2). Αυτό περιλαμβάνει ποικίλα μεγέθη μπλοκ φωτεινότητας, 16*16, 8*8 και 4*4, που όμως σε κάθε περίπτωση μπορεί να χρησιμοποιηθεί ένας από τους παραπάνω τύπους για κάθε μακρομπλόκ.

Οπότε, από όσο μπορεί κάποιος να παρατηρήσει από την παραπάνω περιγραφή των ιδιαίτερων χαρακτηριστικών της τεχνικής πρόβλεψης κίνησης που χρησιμοποιείται, αποτελεί μία καλή εξέλιξη της τεχνικής του H.262 και του H.263. Για τον λόγο αυτό δεν θα γίνει περαιτέρω αναλυτική περιγραφή των βελτιώσεων που έγιναν σε κάθε χαρακτηριστικό των μεθόδων αλλά θα παρατεθούν μόνο τα κύρια χαρακτηριστικά (πίνακας 2.4) για την περιγραφή των χαρακτηριστικών που υποστηρίζει το κάθε προφίλ (αντίστοιχα με τα προφίλ που αναφέρθηκαν στο H.262).

Τα κύρια προφίλ που έχουν οριστεί για χρήσεις σε εφαρμογές δισδιάστατων μη βαθμωτών βίντεο είναι:

Constrained Baseline Profile (CBP): Χρήση κυρίως για εφαρμογές χαμηλού κόστους όπως εφαρμογές κινητών συσκευών και βίντεο-συνδιασκέψεων. Αντιστοιχεί σε χαρακτηριστικά που είναι κοινά στο Baseline, το Main και το High προφίλ.

Baseline Profile (BP): Χρήση κυρίως σε εφαρμογές χαμηλού κόστους που απαιτούν πρόσθετη αντοχή στις απώλειες δεδομένων και χρησιμοποιείται σε εφαρμογές κινητών συσκευών και βίντεο-συνδιασκέψεων. Περιέχει όλα τα χαρακτηριστικά του Constrained Baseline προφίλ που αναφέρθηκε παραπάνω, με τρεις πρόσθετες δυνατότητες που αυξάνουν την ανοχή του συστήματος στις απώλειες δεδομένων.

Extended Profile (XP): Προοριζόταν για εφαρμογές μετάδοσης βίντεο συνεχής ροής πραγματικού χρόνου (streaming) και έχει, σχετικά με τα υπόλοιπα, υψηλές δυνατότητες

συμπύεσης και μερικά πρόσθετα χαρακτηριστικά για την εναλλαγή του χρησιμοποιούμενου server καθώς και την αντοχή στην απώλεια δεδομένων.

Main Profile (MP): Προορίζεται για χρήση κυρίως σε μετάδοση ψηφιακής τηλεόρασης κανονικής ευκρίνειας ενώ για τις εφαρμογές ψηφιακής τηλεόρασης υψηλής ευκρίνειας έχει οριστεί το High προφίλ που αναφέρεται στη συνέχεια.

High Profile (HiP): Το κύριο προφίλ για εφαρμογές broadcasting (μετάδοση δεδομένων σε πολλούς χρήστες ταυτόχρονα), όπως παραδείγματος χάριν εφαρμογές τηλεόρασης υψηλής ευκρίνειας, καθώς και για εφαρμογές αποθήκευσης σε δίσκους (υιοθετήθηκε από τις εφαρμογές των δίσκων Blu-ray)

Progressive High Profile (PhiP): Παρόμοιο με το παραπάνω High προφίλ, αλλά χωρίς να υποστηρίζει χαρακτηριστικά κωδικοποίησης τομέα.

High 10 Profile (Hi10P): Εφαρμόζεται πάνω από το High προφίλ παρέχοντας του μέχρι και 10 bits ανά δείγμα για την ακρίβεια αποκωδικοποίησης εικόνας.

High 4:2:2 Profile (Hi422P): Εφαρμόζεται πάνω από το High προφίλ παρέχοντας πρόσθετες δυνατότητες υποστήριξης 4:2:2 υποδειγματοληψίας, χρησιμοποιώντας μέχρι και 10 bits ανά δείγμα για την ακρίβεια αποκωδικοποίησης εικόνας.

High 4:4:4 Predictive Profile (Hi444PP): Το προφίλ αυτό λειτουργεί πάνω από το High 4:2:2 που αναφέρθηκε παραπάνω, υποστηρίζοντας μέχρι και 4:4:4 υποδειγματοληψία χρώματος, μέχρι 14 bits ανά δείγμα, αποδοτική κωδικοποίηση περιοχής χωρίς απώλειες καθώς και την δυνατότητα κωδικοποίησης κάθε εικόνας ως τρία ανεξάρτητα επίπεδα χρώματος.

Πίνακας 2.4 - Προφίλ του H.264

Χαρακτηριστικό	CBP	BP	XP	MP	ProHiP	HiP	Hi10P	Hi422P	Hi444PP
Bit depth ²⁵ (ανά δείγμα)	8	8	8	8	8	8	8~10	8~10	8~14
Υποδειγματοληψία	4:2:0	4:2:0	4:2:0	4:2:0	4:2:0	4:2:0	4:2:0	4:2:0/ 4:2:2	4:2:0/4:2:2/ 4:4:4
Ευέλικτη διάταξη μακρομπλοκ (FMO)	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι

²⁵Πλήθος bits που χρησιμοποιείται για την περιγραφή του χρώματος.

Αυθαίρετη διάταξη των slices (ASO)	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Πλεονάζουσες slices (RS)	Όχι	Ναι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Καταμερισμός δεδομένων	Όχι	Όχι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
SI και SP slices	Όχι	Όχι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι
Interlaced κωδικοποίηση (PicAFF, MBAFF)	Όχι	Όχι	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι	Ναι
B slices	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
CABAC κωδικοποίηση εντροπίας	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
4:0:0 (Μονοχρωματικό)	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι
8×8 vs. 4×4 μετασχηματιστική προσαρμοστικότητα	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι
Πίνακες κβάντωσης βαθμίδων	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι
Διαχωρισμός Cb και Cr QP ελέγχου	Όχι	Όχι	Όχι	Όχι	Ναι	Ναι	Ναι	Ναι	Ναι
Ξεχωριστή κωδικοποίηση επίπεδου χρώματος	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι
Κωδικοποίηση	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι

πρόβλεψης χωρίς απώλειες									
-----------------------------	--	--	--	--	--	--	--	--	--

Τα επιμέρους χαρακτηριστικά που υποστηρίζει το κάθε προφίλ φαίνονται πιο αναλυτικά στον παραπάνω πίνακα (πίνακας 2.4). Η αριστερή κάθετη στήλη αναφέρει τα κύρια χαρακτηριστικά του H.264 και η πάνω οριζόντια τα διαθέσιμα προφίλ, δημιουργώντας τον πίνακα 2.4 ο οποίος, για κάθε προφίλ, δίνει πληροφορίες για τα χαρακτηριστικά που υποστηρίζει και, στις δύο πρώτες περιπτώσεις, πληροφορίες των χαρακτηριστικών αυτών.

Και όπως είδαμε και για το H.262, έχουν οριστεί και τα αντίστοιχα επίπεδα ποιότητας για κάθε προφίλ, τα οποία φαίνονται στον παρακάτω πίνακα (πίνακας 2.5) όπου αναφέρονται τα διαθέσιμα προφίλ με τα κύρια χαρακτηριστικά τους που είναι η μέγιστη ταχύτητα κωδικοποίησης, ο μέγιστος ρυθμός πλαισίων και ο μέγιστος ρυθμός βίντεο για επίπεδα κωδικοποίησης βίντεο VCL, με τις τιμές δειγματοληψίας φωτεινότητας και μακρομπλόκ που αντιστοιχούν (αναφορικά με τα δύο πρώτα χαρακτηριστικά) και την τιμή που έχει για κάποια επιλεγμένα προφίλ, όσον αφορά το τρίτο.

Όπως φάνηκε και από τα παραπάνω, οι εφαρμογές για τις οποίες είναι κατάλληλο το H.264 ποικίλουν. Κάποια χαρακτηριστικά παραδείγματα είναι οι εφαρμογές βίντεο υψηλής ευκρίνειας, όπως οι δίσκοι Blu-ray που αναφέρθηκαν παραπάνω, η τηλεόραση υψηλής ευκρίνειας, η αποθήκευση βίντεο στο διαδίκτυο (π.χ. YouTube), τα τρίτης γενιάς κινητής τηλεφωνίας, διάφορα λογισμικά, όπως το QuickTime, το Macromedia Flash και κάποιες εφαρμογές του λειτουργικού συστήματος Mac OS X της Apple Computer, και σε κονσόλες παιχνιδιών βίντεο όπως το PlayStation 3.

Πίνακας 2.5 – Επίπεδα του H.264

Επίπεδο	Μέγιστη ταχύτητα κωδικοποίησης		Μέγιστος ρυθμός πλαισίων		Μέγιστος ρυθμός βίντεο για επίπεδο κωδικοποίησης βίντεο (VCL) kbps		
	Δείγματα φωτεινότητας ανά δευτερόλεπτο	Macroblocks ανά δευτερόλεπτο	Δείγματα φωτεινότητας	Macroblocks	Baseline, Extended και Main Profiles	High Profile	High 10 Profile
1	380,160	1,485	25,344	99	64	80	192

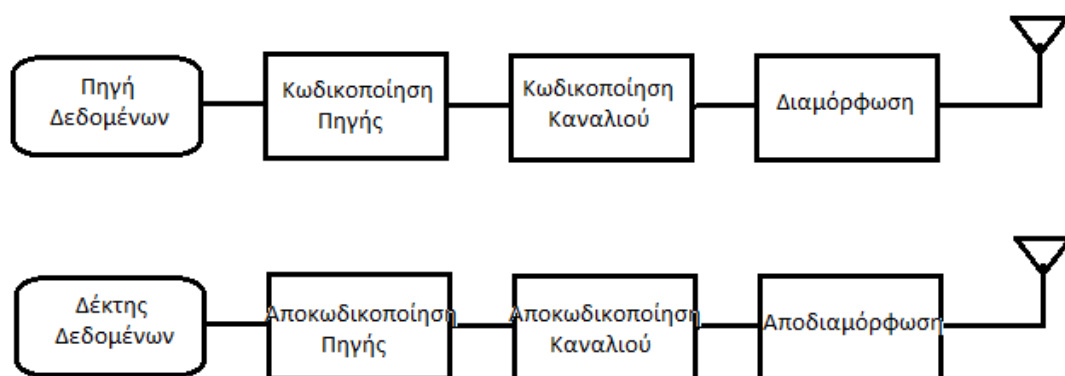
1b	380,160	1,485	25,344	99	128	160	384
1.1	768,000	3,000	101,376	396	192	240	576
1.2	1,536,000	6,000	101,376	396	384	480	1,152
1.3	3,041,280	11,880	101,376	396	768	960	2,304
2	3,041,280	11,880	101,376	396	2,000	2,500	6,000
2.1	5,068,800	19,800	202,752	792	4,000	5,000	12,000
2.2	5,184,000	20,250	414,720	1,620	4,000	5,000	12,000
3	10,368,000	40,500	414,720	1,620	10,000	12,500	30,000
3.1	27,648,000	108,000	921,600	3,600	14,000	17,500	42,000
3.2	55,296,000	216,000	1,310,720	5,120	20,000	25,000	60,000
4	62,914,560	245,760	2,097,152	8,192	20,000	25,000	60,000
4.1	62,914,560	245,760	2,097,152	8,192	50,000	62,500	150,000
4.2	133,693,440	522,240	2,228,224	8,704	50,000	62,500	150,000
5	150,994,944	589,824	5,652,480	22,080	135,000	168,750	405,000
5.1	251,658,240	983,040	9,437,184	36,864	240,000	300,000	720,000
5.2	530,841,600	2,073,600	9,437,184	36,864	240,000	300,000	720,000

Κεφάλαιο 3

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, τα σύγχρονα τηλεπικοινωνιακά συστήματα είναι ψηφιακά συστήματα. Ένα σχηματικό διάγραμμα ενός τέτοιου συστήματος με τα στοιχεία στα οποία έχει γίνει (και στην περίπτωση της κωδικοποίησης καναλιού ή κωδικοποίηση διαύλου) παρουσιάζεται στο παρακάτω σχήμα (σχήμα 3.1). Οπότε τα δεδομένα που καλούνται να διαχειριστούν και να μεταδώσουν τα τηλεπικοινωνιακά αυτά συστήματα είναι σε δυαδική μορφή, την γλώσσα των υπολογιστών. Η δυαδική μορφή των δεδομένων προσδίδει μία αντοχή στα σφάλματα που μπορεί να προκύψουν στην μετάδοση τους, συγκριτικά με την περίπτωση όπου μεταδίδονται αναλογικά δεδομένα²⁶. Παραμένει

²⁶Ο θόρυβος που προστίθεται, όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, υπάρχει σε όλα τα κανάλια επικοινωνίας. Στα αναλογικά σήματα ο θόρυβος θα αλλάξει την τιμή του σήματος η οποία είναι συνεχής και άρα δύσκολα ανιχνεύσιμη η αλλαγή της από τον δέκτη. Στα ψηφιακά, επειδή οι καταστάσεις είναι ή “0” ή “1” ο δέκτης μπορεί πιο εύκολα να “διακρίνει” το θορυβώδες σήμα και να διορθώσει κάποιες περιπτώσεις αλλοίωσης του.

όμως το πρόβλημα του θορύβου που προστίθεται, ειδικά στις περιπτώσεις όπου απαιτείται μεγάλη ταχύτητα μετάδοσης για μεγάλους όγκους δεδομένων, όπως δείχνει και το θεώρημα του Shannon που υπολογίζει τον μέγιστο ρυθμό μετάδοσης δεδομένων C πληροφορίας με μία αυθαίρετα μικρή πιθανότητα σφάλματος δεδομένου ότι ο ρυθμός μετάδοσης δεδομένων R θα είναι ίσος ή μικρότερος από τον ρυθμό C , δηλαδή την χωρητικότητα του καναλιού (εξίσωση 1.2.4). Ο θόρυβος αυτός, όπως προαναφέρθηκε, οφείλεται σε πολλές και ποικίλες αιτίες και προκαλεί αλλοίωση των δεδομένων που λαμβάνει ο δέκτης. Για την αντιμετώπιση του προβλήματος αυτού και την μεγιστοποίηση της αξιοπιστίας των τηλεπικοινωνιακών συστημάτων έχουν αναπτυχθεί πολλές τεχνικές²⁷, όπως οι μέθοδοι πολύπλεξης που έχουν ως στόχο την μεγιστοποίηση της εκμετάλλευσης των καναλιών επικοινωνίας και οι μέθοδοι κωδικοποίησης πηγής μέσω της οποίας συμπιέζεται ο όγκος των δεδομένων που απαιτείται για την μετάδοση της πληροφορίας. Μία από τις πιο ανεπτυγμένες τέτοιες τεχνικές, η οποία εφαρμόζεται, όπως φαίνεται και στο σχήμα 3.1 μετά την κωδικοποίηση πηγής και πριν την διαμόρφωση του σήματος είναι η κωδικοποίηση καναλιού (ή κωδικοποίηση διαύλου) με την οποία ασχολείται ο κλάδος των μαθηματικών, “Θεωρία Κωδίκων”. Οι προσπάθειες των ερευνητών που ασχολούνται με τον κλάδο αυτόν αποσκοπούν στην σχεδίαση και υλοποίηση κωδικών οι οποίοι να έχουν την δυνατότητα να λειτουργούν όσο πιο κοντά στο όριο Shannon είναι δυνατόν. Η επίτευξη του στόχου αυτού, σύμφωνα με τον Shannon, μπορεί να επιτευχθεί κατασκευάζοντας έναν τυχαίο κώδικα (randomly constructed code) με πολύ μεγάλο μέγεθος, n , και για τον λόγο αυτό κατασκευάζονταν όλο και πιο “ογκώδεις” και πολύπλοκοι κώδικες.



Σχήμα 3.1 - Μπλοκ Διάγραμμα Σύγχρονου Τηλεπικοινωνιακού Συστήματος

²⁷Περαιτέρω ανάλυση των τεχνικών που ήδη αναφέρθηκαν ή και αναφορά άλλων ξεφεύγει από τα πλαίσια της παρούσας εργασίας και δεν θα γίνει, εκτός από την περίπτωση της κωδικοποίησης καναλιού που είναι το θέμα που θα απασχολήσει το υπόλοιπο μέρος της.

3.1 - Κωδικοποίηση καναλιού

Με τον όρο “Κωδικοποίηση Καναλιού” αναφέρονται οι διάφορες τεχνικές κωδικοποίησης των δεδομένων που είναι να μεταδοθούν έτσι ώστε να επιτευχθεί μείωση του θορύβου του καναλιού επικοινωνίας²⁸. Με τον τρόπο αυτό μειώνεται η απαιτούμενη ισχύς του σήματος που μεταδίδεται για την ίδια πιθανότητα σφάλματος με την περίπτωση που δεν έχουμε μείωση του θορύβου και η μείωση αυτή της ισχύος, υπολογισμένη σε dB, καλείται “Κέρδος Κωδικοποίησης”. Η μεγάλη διαφορά με την κωδικοποίηση πηγής είναι ότι, σε αντίθεση με την κωδικοποίηση πηγής η οποία πετυχαίνει συμπίεση των δεδομένων και αύξηση του ρυθμού μετάδοσης πληροφορίας, οι κώδικες που χρησιμοποιούνται στην κωδικοποίηση καναλιού αυξάνουν τον όγκο των δεδομένων που μεταδίδονται, μειώνοντας τον μέγιστο δυνατό ρυθμό μετάδοσης πληροφορίας, αυξάνοντας όμως την αξιοπιστία των λαμβανομένων δεδομένων. Για την επίτευξη του στόχου αυτού προστίθενται κάποια ψηφία τα οποία χρησιμοποιούνται για την ανίχνευση ή και διόρθωση λαθών που μπορεί να προκύψουν από τον θόρυβο του καναλιού επικοινωνίας και κάθε κώδικας που χρησιμοποιείται στην κωδικοποίηση καναλιού ορίζει το πλήθος των προστιθέμενων ψηφίων καθώς και το ρόλο που έχει το κάθε ένα από αυτά, όπως θα φανεί και παρακάτω όπου θα γίνει περιγραφή τέτοιων κωδικών.

Η απλούστερη τεχνική που μπορεί να υλοποιηθεί ώστε να μπορεί ο δέκτης να αναγνωρίζει και να διορθώνει τυχόν λάθη στο λαμβανόμενο σήμα είναι η πολλαπλή αποστολή των ίδιων δεδομένων. Ο πομπός δημιουργεί ένα πλήθος αντιγράφων του σήματος που πρόκειται να μεταδοθεί και το αποστέλλει μαζί με τα αντίγραφα του (το πλήθος των αντιγράφων εξαρτάται από τον σχεδιαστεί του συστήματος). Οι κώδικες που χρησιμοποιούνται στην τεχνική αυτή ονομάζονται “επαναληπτικοί κώδικες”²⁹ (repetition codes). Το σύστημα το οποίο προορίζεται να λάβει τα δεδομένα αυτά σχεδιάζεται έτσι ώστε να μπορεί να κάνει κάποια σύγκριση στα δεδομένα που λαμβάνει. Ένας τέτοιος τρόπος είναι το σύστημα στον δέκτη να “διαβάζει” τα εισερχόμενα ψηφία σε N-αδες (όπου N το πλήθος

²⁸Με τον όρο “μείωση του θορύβου” στην ουσία εννοείται η μεγιστοποίηση της προστασίας των δεδομένων από το θόρυβο ώστε να μην αλλοιώνονται τα μεταδιδόμενα δεδομένα και την μεγιστοποίηση της αξιοπιστίας του συστήματος.

²⁹Η μελέτη των επαναληπτικών κωδικών ξεφεύγει από τα πλαίσια της εργασίας αυτής και δεν θα γίνει αναλυτική περιγραφή τους αλλά απλή αναφορά της λογικής στην οποία στηρίζονται.

των αντιγράφων που στέλνονται) και σε περίπτωση που βρεθούν διαφορές στις τιμές των ψηφίων (μιας και τα N ψηφία που συγκρίνει αντιστοιχούν στο ίδιο κομμάτι πληροφορίας και άρα πρέπει να είναι όλα ίδια) μπορεί να συμπεράνει ότι σε κάποιο ψηφίο παρουσιάστηκε ένα σφάλμα. Μετά την ανίχνευση σφάλματος ο δέκτης είτε μπορεί να αιτηθεί επαναποστολή των συγκεκριμένων δεδομένων ή για την περίπτωση που το πλήθος ψηφίων είναι μεγαλύτερο του 2 μπορεί, μέσω ενός κυκλώματος πλειοψηφίας³⁰, να κάνει διόρθωση του σφάλματος. Με τον τρόπο αυτό μπορεί να γίνει ανίχνευση και διόρθωση εσφαλμένου ψηφίου, αρκεί τα ψηφία (σε κάθε περίπτωση σύγκρισης ψηφίων) που εμφανίζουν σφάλμα να μην είναι περισσότερα από $N/2$ και όσο μεγαλύτερη είναι η τιμή του N (δηλαδή όσο περισσότερα αντίγραφα του μηνύματος πληροφορίας στέλνονται) τόσο μικραίνει η πιθανότητα σφάλματος. Η τεχνική αυτή έχει το μεγάλο μειονέκτημα ότι αυξάνει πολύ τον όγκο των δεδομένων που μεταδίδονται και συγκεκριμένα, αφού κάθε μήνυμα αποστέλλεται N φορές, αυξάνει τον όγκο των δεδομένων N φορές, καθιστώντας την τεχνική αυτή πολύ δαπανηρή από άποψη πόρων και για τον λόγο αυτό δεν χρησιμοποιείται ευρέως.

Μία άλλη τεχνική ανίχνευσης σφαλμάτων προβλέπει την προσθήκη ψηφίων τα οποία, με κατάλληλο τρόπο, να μπορούν να δώσουν πληροφορίες στον δέκτη σχετικά με την αξιοπιστία των λαμβανομένων δεδομένων, χωρίς να απαιτείται η παραπάνω πολλαπλή αποστολή των ίδιων δεδομένων. Το πιο απλό και διαδεδομένο παράδειγμα ενός τέτοιου μοντέλου κωδικοποίησης είναι ο κώδικας ASCII (American Standard Code for Information Interchange) που χρησιμοποιείται για την κωδικοποίηση των χαρακτήρων που χρησιμοποιούνται για την αναπαράσταση ενός κειμένου. Ο κώδικας αυτός χρησιμοποιεί οκτώ ψηφία από τα οποία τα επτά περιέχουν την πληροφορία και το όγδοο είναι ψηφίο ελέγχου. Τα επτά δυαδικά ψηφία μπορούν να αναπαραστήσουν μέχρι $2^7=128$ “καταστάσεις” (δηλαδή να αναπαρίστανται μέχρι 128 χαρακτήρες). Ανάλογα με τον χαρακτήρα που κωδικοποιείται, δημιουργείται μία αλληλουχία από οκτώ ψηφία, με το όγδοο ψηφίο να παίρνει κατάλληλη τιμή έτσι ώστε το πλήθος των μονάδων (“1”) της αλληλουχίας να είναι είτε περιττό (συστήματα περιττής ισοτιμίας) είτε άρτιος (άρτιας ισοτιμίας) και ονομάζεται “ψηφίο ισοτιμίας” (parity bit). Ελέγχοντας ο δέκτης το πλήθος των μονάδων της αλληλουχίας που έλαβε μπορεί να ανιχνεύσει περιττό πλήθος σφαλμάτων³¹, χωρίς όμως να έχει την δυνατότητα διόρθωσης των σφαλμάτων, και να στείλει στον πομπό σήμα σφάλματος

³⁰Ένα ψηφιακό κύκλωμα ή σύστημα πλειοψηφίας είναι ένα ψηφιακό συνδυαστικό κύκλωμα του οποίου η έξοδος εξαρτάται από το αν θα έχει περισσότερα ψηφία “1” ή “0” στην είσοδο του.

³¹Στην περίπτωση που συμβεί άρτιο πλήθος σφαλμάτων ο δέκτης θα αναγνωρίσει τα δεδομένα σαν σωστά γιατί το πλήθος των μονάδων θα είναι αυτό που ανέμενε.

ζητώντας την επανάληψη της αποστολής των συγκεκριμένων δεδομένων, χαρακτηριστικά που αποτελούν τα μεγαλύτερα μειονεκτήματα του κώδικα αυτού.

Ένα παράδειγμα κωδικοποίησης ASCII με κωδικοποίηση άρτιας ισοτιμίας φαίνεται στον παρακάτω πίνακα (πίνακας 3.1) όπου στην πρώτη στήλη φαίνεται ο χαρακτήρας που θα μεταδοθεί (το μήνυμα είναι το “SOS!”), στην δεύτερη ο δεκαδικός συμβολισμός του στο ASCII, στην τρίτη ο δυαδικός συμβολισμός του χαρακτήρα (επτά ψηφία) και στην τελευταία η αλληλουχία των ψηφίων που θα μεταδοθεί (οκτώ ψηφία). Οπότε, στην περίπτωση του “S” του οποίου ο δυαδικός συμβολισμός είναι “1010011” (τέσσερις μονάδες), το ψηφίο ισοτιμίας θα οριστεί να έχει την τιμή “0” έτσι ώστε το πλήθος των μονάδων να παραμείνει άρτιο ενώ στην περίπτωση του “O” του οποίου ο δυαδικός συμβολισμός είναι “1001111” (πέντε μονάδες) το ψηφίο ισοτιμίας θα πάρει την τιμή “1” έτσι ώστε το πλήθος των μονάδων να γίνει άρτιο.

Χαρακτήρας	Δεκαδικός Συμβολισμός:	Δυαδικός Συμβολισμός:	Αλληλουχία ψηφίων:
S	83	1010011	1010011 0
O	79	1001111	1001111 1
S	83	1010011	1010011 0
!	33	0100001	0100001 0

Πίνακας 3.1 – ASCII κωδικοποίηση άρτιας ισοτιμίας

Η συγκεκριμένη κωδικοποίηση δεν αυξάνει πολύ τον όγκο των μεταδιδόμενων δεδομένων μιας και μόνο το 1/8 των μεταδιδόμενων ψηφίων είναι ψηφία ελέγχου (δηλαδή έχουμε αύξηση των δεδομένων κατά ~14.3%). Οι κώδικες που χρησιμοποιούν την λογική αυτή με ένα ψηφίο ισοτιμίας ανά αλληλουχία ψηφίων (ή κωδική λέξη) ονομάζονται κώδικες SPC (Single Parity Check codes) και το ψηφίο ισοτιμίας προκύπτει, ανάλογα με το αν χρησιμοποιείται άρτια ή περιττή ισοτιμία, μέσω κάποιου μηχανισμού σύνθεσης των ψηφίων της κωδικής λέξης που θα μεταδοθεί και μπορούν να ανιχνεύσουν, όπως προαναφέρθηκε, περιττό πλήθος σφαλμάτων, χωρίς να υπάρχει η δυνατότητα διόρθωσης των σφαλμάτων που θα ανιχνευθούν. Με χρήση όμως περισσότερων ψηφίων ισοτιμίας (ή γενικότερα, όπως θα αναφερθεί παρακάτω, περισσότερων ψηφίων ελέγχου) είναι δυνατόν να ανιχνεύονται περισσότερα σφάλματα καθώς και να γίνεται διόρθωση των σφαλμάτων που ανιχνεύονται. Πρώτη τέτοια απόπειρα έγινε από τον Richard Hamming το 1946 ο οποίος, βασιζόμενος

στην σκέψη ότι αν ο δέκτης ήταν σε θέση να αναγνωρίσει κάποιο λάθος, τότε ίσως να μπορούσε να το διορθώσει κιόλας. Αυτό όμως δεν ήταν εφικτό με μετάδοση μόνο των ψηφίων που είναι απαραίτητα για την μετάδοση κάποιας πληροφορίας και θα έπρεπε να προστεθούν και κάποια πλεονάζοντα ψηφία ως ψηφία ελέγχου μέσω των οποίων θα γίνεται ο εντοπισμός τυχόν λαθών και, ίσως, η διόρθωση τους. Ο πρώτος κώδικας που σχεδιάστηκε (από τον ίδιο από τον οποίο πήρε και το όνομα του: “Κώδικας Hamming”³²) χρησιμοποιούσε, ανά τέσσερα ψηφία πληροφορίας, τρία ψηφία ελέγχου, επιτυγχάνοντας τον εντοπισμό και την διόρθωση ενός λανθασμένου ψηφίου στον δέκτη.

Στα επόμενα χρόνια και με τον κώδικα Hamming να έχει εγκαινιάσει τους κώδικες διόρθωσης λαθών, η Θεωρία Κωδίκων αναπτύχθηκε πολύ. Ποικίλες τεχνικές κωδικοποίησης σχεδιάστηκαν και υλοποιήθηκαν και, για κάθε τέτοια τεχνική αναπτύχθηκαν αρκετοί κώδικες με αποτέλεσμα το πλήθος και το είδος των κωδικών που χρησιμοποιούνται στην κωδικοποίηση καναλιού να είναι αρκετά μεγάλος. Ο βασικός στόχος όλων αυτών των κωδικών είναι η αποτελεσματική και αξιόπιστη επικοινωνία μέσω των διαθέσιμων θορυβωδών καναλιών επικοινωνίας. Για να είναι όμως ένας τέτοιος κώδικας αποτελεσματικός (η επικοινωνία να είναι αποτελεσματική) θα πρέπει να έχει όσο το δυνατόν λιγότερες απαιτήσεις για την υλοποίησή του σε υλισμικό (hardware), χρόνο και κόστος έτσι ώστε να είναι δυνατή η μεταφορά του μέγιστου δυνατού όγκου πληροφορίας με το μικρότερο δυνατό κόστος. Για να είναι αξιόπιστος πρέπει να έχει αυξημένη ικανότητα ανίχνευσης και διόρθωσης λαθών κατά την λήψη των δεδομένων από τον δέκτη. Για να μπορούν να ποσοτικοποιηθούν οι έννοιες της αποδοτικότητας και της αξιοπιστίας κάθε κώδικα έχουν οριστεί ο “Βαθμός Πληροφορίας” (information ή transmission rate) και ο “Βαθμός Διόρθωσης Λαθών” (error correcting rate). Όμως, για να μπορέσουμε να ορίσουμε τις ποσότητες αυτές θα πρέπει πρώτα να γίνει μία μικρή εισαγωγή στην Θεωρία Κωδίκων.

3.1.1 – Βασικά στοιχεία Θεωρίας Κωδίκων

Ένας κώδικας C είναι ένα σύνολο από r διακριτά στοιχεία, έστω το σύνολο $A = \{a_1, a_2, a_3, \dots, a_n\}$. Το σύνολο αυτό αποτελεί το “αλφάβητο” του κώδικα και τα επί μέρους στοιχεία του ονομάζονται κωδικοσύμβολα ή κωδικολέξεις. Οι κωδικές λέξεις είναι μία

³²Παρακάτω θα γίνει εκτενής αναφορά στον κώδικα Hamming.

ακολουθία ψηφίων και το πλήθος τους αποτελεί το μήκος της κωδικής αυτής λέξης. Το μήκος αυτό ποικίλει μεταξύ των διαφόρων κωδικών και, αν είναι όλες οι κωδικές λέξεις του αλφαβήτου ενός κώδικα ίδιου μήκους, τότε ο κώδικας αυτός ανήκει στους “Μπλοκ Κώδικες”³³ και το μήκος των κωδικών λέξεων ονομάζεται “μήκος του κώδικα”. Οπότε η επικοινωνία επιτυγχάνεται όταν και ο πομπός και ο δέκτης είναι γνώστες του αλφαβήτου που χρησιμοποιεί ο κώδικας που χρησιμοποιείται και μία πρώτη ανίχνευση σφαλμάτων μπορεί να επιτευχθεί αν ο δέκτης λάβει μία ακολουθία ψηφίων η οποία δεν ανήκει στο αλφάβητο του κώδικα. Αν το μήκος ενός κώδικα είναι n (δηλαδή κάθε κωδική λέξη αποτελείται από n ψηφία) και το κάθε ψηφίο μπορεί να πάρει m πιθανές τιμές (αν τα ψηφία που χρησιμοποιούνται είναι δυαδικά, τότε $m=2$), τότε το πλήθος των πιθανών κωδικών λέξεων που μπορεί να περιέχει το αλφάβητο του κώδικα αυτού θα είναι m^n . Το πλήθος των κωδικών λέξεων που περιέχει το αλφάβητο του κώδικα (όχι όλων των πιθανών κωδικών λέξεων αλλά μόνο αυτών που χρησιμοποιούνται) αποτελεί το μέγεθος του.

Οι κωδικές λέξεις που περιέχει το αλφάβητο ενός τέτοιου κώδικα C θα περιέχει τα ψηφία που περιέχουν την πληροφορία και κάποια ψηφία ελέγχου. Αν το μήκος του κώδικα είναι n και τα ψηφία που περιέχουν την πληροφορία είναι k , τότε ο κώδικας αυτός θα συμβολίζεται ως $C(n,k)$. Έτσι, ο παραπάνω κώδικας Hamming θα συμβολίζεται ως $H(7,4)$ ενώ ο κώδικας ASCII ως $A(8,7)$.

Δύο σημαντικές έννοιες της θεωρίας κωδικών είναι το “Βάρος Hamming”, ή απλά βάρος μίας κωδικής λέξης, και η “Απόσταση Hamming”. Έστω v και w δύο κωδικές λέξεις του αλφαβήτου ενός κώδικα. Τότε, το βάρος Hamming θα είναι μία ποσότητα η οποία ορίζεται ως το πλήθος των εμφανίσεων του ψηφίου “1” και συμβολίζεται με $w_t(v)$. Οπότε, το βάρος της κωδικής λέξης $v=“110111”$ θα είναι: $w_t(110111) = 5$ ενώ της $w=“000010”$ θα είναι $w_t(000010) = 1$. Για κάθε κώδικα, ορίζεται το ελάχιστο βάρος κώδικα το οποίο θα είναι το ελάχιστο βάρος Hamming των κωδικών λέξεων του αλφαβήτου του, εξαιρώντας την κωδική λέξη (αν περιέχεται στο αλφάβητο) που αποτελείται μόνο από μηδενικά. Ως απόσταση Hamming μεταξύ των λέξεων v και w ορίζεται το πλήθος των διαφορετικών ψηφίων που περιέχουν οι λέξεις αυτές, συγκρίνοντας τα ψηφία των αντίστοιχων θέσεων, οπότε η απόσταση d των παραπάνω λέξεων θα είναι

³³Οι “Μπλοκ κώδικες” (block) είναι οι κώδικες των οποίων τα δεδομένα που μεταφέρουν την πληροφορία αποστέλλονται σε ομάδες ή πακέτα, όπως ο κώδικας ASCII που αναφέρθηκε παραπάνω και του οποίου το μήκος είναι 8 bit.

$$d(v, w) = d(110111, 000010) = 4 \quad (3.1.1)$$

και για κάθε κώδικα υπολογίζεται μία ελάχιστη απόσταση d που θα είναι η μικρότερη απόσταση μεταξύ δύο διαφορετικών κωδικών λέξεων. Ένας κώδικας C μήκους n , μεγέθους M και ελάχιστης απόστασης $d(C)$, αναφέρεται ως (n, M, d) -κώδικας και τα n, M, d καλούνται “παράμετροι του κώδικα”.

Όταν ο δέκτης δεχθεί μία ακολουθία ψηφίων η οποία δεν ανήκει στο αλφάβητο του κώδικα αυτού, όπως προαναφέρθηκε, ανιχνεύει την είσοδο αυτή σαν λανθασμένη. Ανάλογα με την υλοποίηση του συστήματος επικοινωνίας, μπορεί να σταλθεί ένα μήνυμα λάθους στον πομπό ώστε να γίνει επανάληψη της αποστολής των δεδομένων ή μπορεί να χρησιμοποιηθεί μία διαδικασία για την επιλογή της κωδικής λέξης που στάλθηκε, η οποία ονομάζεται “Αποκωδικοποίηση Μέγιστης Πιθανότητας” και είναι ένας τρόπος διόρθωσης λαθών. Οι εκδοχές της διαδικασίας αυτής είναι δύο: η “Πλήρης αποκωδικοποίηση μέγιστης πιθανότητας” (ΠΑΜΠ) και η “Ατελής αποκωδικοποίηση μέγιστης πιθανότητας” (ΑΑΜΠ). Και οι δύο εκδοχές χρησιμοποιούν την απόσταση Hamming, ελέγχοντας ποια ή ποιες κωδικές λέξεις του αλφαβήτου έχουν την ελάχιστη απόσταση από την λέξη που λήφθηκε. Αν είναι μία η λέξη και η απόσταση της είναι μικρή τότε επιλέγεται αυτή και αποκωδικοποιείται η πληροφορία. Αν όμως δεν είναι μία η λέξη αλλά περισσότερες, τότε στην πρώτη εκδοχή (ΠΑΜΠ) επιλέγεται, βάση προκαθορισμένων κριτηρίων μία από τις πιθανές λέξεις ενώ στην δεύτερη εκδοχή (ΑΑΜΠ) στέλνεται μήνυμα λάθους στον πομπό και γίνεται αίτηση επανάληψης της αποστολής των συγκεκριμένων δεδομένων. Η επανάληψη της μετάδοσης μπορεί να συμβεί, όταν χρησιμοποιείται η ΑΑΜΠ και στην περίπτωση που η λέξη με την μικρότερη απόσταση είναι μοναδική αλλά η απόσταση αυτή είναι μεγάλη.

Ο “Βαθμός Πληροφορίας” ή απλά “Βαθμός” ενός κώδικα είναι ένας αριθμός μέσω του οποίου μπορεί να μετρηθεί το ποσοστό κάθε κωδικής λέξης από την οποία αποτελείται η πληροφορία. Ο βαθμός αυτός, για έναν κώδικα C μήκους n ορίζεται, για κώδικες με ψηφία που μπορούν να λάβουν r τιμές, από την σχέση:

$$R(C) = \frac{1}{n} \cdot \log_r M \quad (3.1.2)$$

όπου M το πλήθος των κωδικών λέξεων που χρησιμοποιεί ο κώδικας. Στην περίπτωση που ο κώδικας στον οποίο αναφέρεται η παραπάνω σχέση (εξίσωση 3.1.1) είναι δυαδικός, τότε $1 \leq M \leq 2^n$ (θεωρώντας ότι περιέχεται τουλάχιστον μία κωδική λέξη στο αλφάβητο του) και ο

βαθμός πληροφορίας $R(C)$ θα είναι μεταξύ του 0 και του 1, με την τιμή 0 να αντιστοιχεί σε κώδικα του οποίου το αλφάβητο περιέχει μόνο μία κωδική λέξη και 1 για την περίπτωση που περιέχονται όλες οι πιθανές λέξεις στο αλφάβητο. Οπότε, ο βαθμός πληροφορίας εκφράζει την αναλογία της “καθαρής” πληροφορίας σε σχέση με το μήκος του κώδικα.

Τέλος, ως βαθμός διόρθωσης λαθών ορίζεται η ποσότητα $\delta(C)$ η οποία για έναν (n, M, d) - κώδικα υπολογίζεται από την σχέση:

$$\delta(C) = \frac{d-1}{2n} \quad (3.1.3)$$

Οι παραπάνω ποσότητες, για έναν κώδικα Hamming $H(n, h)$ του οποίου η ελάχιστη απόσταση είναι $d=3$ και το μέγεθος του $M=r^{n-h}$, θα είναι

$$\begin{aligned} R(C) &= \frac{1}{n} \cdot \log_r r^{n-h} = 1 - \frac{h}{n} \\ \delta(C) &= \frac{3-1}{2n} = \frac{1}{n} \end{aligned} \quad (3.1.4)$$

Από τις παραπάνω σχέσεις (σχέσεις 3.1.4) παρατηρούμε ότι όσο μεγαλώνει το n τόσο πλησιάζει ο βαθμός πληροφορίας στην μονάδα. Όμως, όσο μεγαλώνει το n μικραίνει ο βαθμός διόρθωσης λαθών. Αντίστροφα, όσο μικραίνει το n μεγαλώνει ο βαθμός διόρθωσης λαθών αλλά μικραίνει ο βαθμός πληροφορίας. Οπότε κατά τον σχεδιασμό ενός κώδικα θα πρέπει να γίνει ένας συμβιβασμός μεταξύ των μεγεθών αυτών και να βρεθεί το μέγιστο μέγεθος M , δηλαδή το μέγιστο βαθμό πληροφορίας που να δίνει όμως τον βέλτιστο βαθμό διόρθωσης λαθών. Αν για κάποιον κώδικα υπάρχει, τότε αυτό συμβολίζεται με $A_1(n, d)$ και ο κώδικας καλείται “βέλτιστος κώδικας” (optimal code). Η εύρεση των τιμών αυτών είναι γνωστή ως “Το κεντρικό πρόβλημα της θεωρίας κωδίκων”³⁴.

Τέλος, σε κάθε σύστημα που χρησιμοποιείται για την κωδικοποίηση καναλιού γίνονται μετρήσεις της απόδοσης του συστήματος με διάφορες τεχνικές, με την πιο διαδεδομένη να είναι η τροφοδότηση δεδομένων στην είσοδο και ο έλεγχος της εξόδου για την δεδομένη αυτή είσοδο. Μετά τις μετρήσεις μπορεί να αξιολογηθεί η απόδοση του

³⁴Παραδείγματα τιμών του $A_1(n, d)$ μπορούν να βρεθούν στον σύνδεσμο: www.eng.tau.ac.il/~litsyn/tableand/index.html

συστήματος με διάφορους τρόπους³⁵, από τους οποίους οι πιο συχνά χρησιμοποιούμενοι είναι:

- Ο ρυθμός λανθασμένων κωδικών λέξεων (WER-word error rate) που εκφράζει τον ρυθμό με τον οποίο εμφανίζεται στην έξοδο διαφορετική λέξη από αυτήν της εισόδου.
- Ο ρυθμός λανθασμένων ψηφίων (BER-bit error rate) που εκφράζει τον ρυθμό με τον οποίο εμφανίζεται στην έξοδο διαφορετικό ψηφίο από αυτό της εισόδου.
- Το σύνολο των λανθασμένων ψηφίων σε μία λέξη.
- Το σύνολο των φορών που ο αποκωδικοποιητής απέτυχε να αποκωδικοποιήσει την κωδική λέξη που έλαβε.

Ανάλογα με τα ιδιαίτερα χαρακτηριστικά του κάθε κώδικα έχουν δημιουργηθεί πολλές κατηγορίες. Ήδη αναφέρθηκαν οι κατηγορίες των μπλοκ κωδικών, στην οποία θα ανήκουν οι κώδικες των οποίων τα δεδομένα στέλνονται σε διακεκριμένες ακολουθίες ψηφίων, και οι επαναληπτικοί κώδικες. Στις επόμενες παραγράφους του κεφαλαίου αυτού θα αναφερθούν και οι Γραμμικοί Κώδικες (οι Μπλοκ Κώδικες ανήκουν στην κατηγορία αυτή), οι Κώδικες LDPC (Low Density Parity Check), οι Συνελικτικοί Κώδικες και τέλος, οι Κώδικες Turbo, στους οποίους θα γίνει εκτενέστερη αναφορά στο επόμενο κεφάλαιο. Στις αναφορές που θα γίνουν στις κατηγορίες αυτές, αν δεν υπάρχει σαφής αναφορά στο είδος του κώδικα, οι κώδικες θα θεωρούνται δυαδικοί.

3.2 - Γραμμικοί Κώδικες

Η κατηγορία των Γραμμικών Κωδικών είναι πολύ μεγάλη και περιέχει και κώδικες που ανήκουν σε πολλές άλλες κατηγορίες, όπως οι Μπλοκ Κώδικες που προαναφέρθηκαν, οι κώδικες LDPC (που ανήκουν στους Μπλοκ κώδικες), οι Συνελικτικοί Κώδικες καθώς και οι Turbo Κώδικες και για τον λόγο αυτό θα γίνει εκτενής αναφορά στα χαρακτηριστικά της

³⁵Οι τρόποι που αναφέρονται αφορούν τα συστήματα κωδικοποίησης-αποκωδικοποίησης καναλιού, μιας και αυτό είναι το θέμα την εργασίας και για τον λόγο αυτό δεν θα γίνει αναφορά σε άλλους τρόπους/τεχνικές/έννοιες που χρησιμοποιούνται για την αξιολόγηση της απόδοσης ενός συστήματος επικοινωνίας, όπως ο λόγος SNR που αναφέρθηκε παραπάνω.

κατηγορίας αυτής καθώς αυτά θα ισχύουν και για τις κατηγορίες κωδίκων που θα αναφερθούν στην συνέχεια. Αντίστοιχα, για τους γραμμικούς κώδικες θα ισχύουν όσα αναφέρθηκαν παραπάνω σχετικά με τους κώδικες Κωδικοποίησης Καναλιού. Θα υπάρχει ένα απολύτως ορισμένο σύνολο στοιχείων A θα αντιστοιχίζεται με (απεικονίζεται σε) κάποια πληροφορία η οποία θα ανήκει σε ένα σύνολο B . Η απεικόνιση αυτή θα είναι απαραίτητα μονοσήμαντη. Τα στοιχεία του συνόλου A είναι οι κωδικές λέξεις και του συνόλου B οι “λέξεις πληροφορίας” (infowords). Τα στοιχεία του συνόλου B , οι λέξεις πληροφορίας, μπορεί να έχουν ποικίλες μορφές, ανάλογα με το είδος της πληροφορίας που είναι επιθυμητό να μεταδοθεί. Τα στοιχεία του συνόλου A όμως θα είναι ακολουθίες ψηφίων και το πλήθος τους θα είναι το μέγεθος του κώδικα και θεωρώντας ότι η κάθε κωδική λέξη του αλφαβήτου του κώδικα αποτελείται από n ψηφία³⁶ (με τα q ψηφία να περιέχουν την πληροφορία) πληροφορίας, οι κωδικές λέξεις θα είναι ακολουθίες n ψηφίων, με μέγιστο πλήθος ή μέγεθος κώδικα, q^k . Ο κωδικοποιητής θα αντιστοιχίζει κάθε στοιχείο του συνόλου B σε ένα στοιχείο του συνόλου A και ο αποκωδικοποιητής θα εκτελεί την αντίστροφη διαδικασία.

Για να είναι ένας τέτοιος κώδικας γραμμικός, θα πρέπει το σύνολο των στοιχείων του αλφαβήτου του, ή αλλιώς του συνόλου A , q^k να σχηματίζουν ένα k -διάστατο διάνυσμα, υποχώρο του χώρου διανυσμάτων όλων των πιθανών q^n συνδυασμών των n ψηφίων, από όπου προκύπτει και μία από τις βασικότερες ιδιότητες (αλλά και απαιτήσεις ώστε ένας κώδικας να ανήκει στην κατηγορία αυτή) των γραμμικών κωδίκων, που είναι το γεγονός ότι το άθροισμα οιονδήποτε δύο κωδικών λέξεων θα είναι επίσης κωδική λέξη. Έτσι, ένας κώδικας του οποίου το αλφάβητο είναι $A_1 = \{00, 11\}$ θα είναι γραμμικός γιατί τα αθροίσματα όλων των πιθανών συνδυασμών κωδικών του λέξεων:

$$\begin{array}{l} 00 + 00 = 00 \quad 11 + 11 = 00 \\ 00 + 11 = 11 \quad 11 + 00 = 11 \end{array} \quad (3.2.1)$$

ανήκουν στο A_1 ενώ ένας κώδικας με αλφάβητο $A_2 = \{00, 10, 11\}$ δεν θα είναι γραμμικός γιατί το αποτέλεσμα του αθροίσματος των στοιχείων του είναι:

³⁶Όταν ένας κώδικας έχει σταθερό μήκος κωδικής λέξης, ο κώδικας αυτός ανήκει στην κατηγορία των Μπλοκ κωδίκων, όπως προαναφέρθηκε. Οπότε στα παρακάτω παραδείγματα, που αναφέρονται σε κώδικες σταθερού μήκους κωδικής λέξης αφορούν τους Μπλοκ κώδικες και η χρήση τους γίνεται γιατί, αφενός οι τεχνικές και τα συμπεράσματα για τα οποία χρησιμοποιούνται αφορούν γενικά τους Γραμμικούς κώδικες και, αφετέρου, οι LDPC κώδικες στους οποίους θα γίνει αναφορά σε επόμενη παράγραφο ανήκουν στην κατηγορία των Μπλοκ κωδίκων.

$$\begin{array}{lll}
00 + 00 = 00 & 11 + 11 = 00 & 10 + 10 = 00 \\
00 + 11 = 11 & 11 + 00 = 11 & 00 + 10 = 10(3.2.2) \\
10 + 00 = 10 & 10 + 11 = 01 & 11 + 10 = 01
\end{array}$$

και η κωδική λέξη 01 που είναι το αποτέλεσμα των αθροισμάτων 10+11 και 11+01 δεν ανήκει στο A_2 . Ο αριθμός n ονομάζεται μήκος του κώδικα ενώ ο k διάσταση του κώδικα, με τον ρυθμό του κώδικα να ορίζεται ως

$$R = \frac{k}{n} \quad (3.2.3)$$

Μία άλλη βασική ιδιότητα των γραμμικών κωδίκων είναι ότι η ελάχιστη απόσταση Hamming ισούται με το ελάχιστο βάρος Hamming, κάτι που αποτελεί σημαντικό πλεονέκτημα των γραμμικών κωδίκων γιατί έτσι, κάθε απόσταση Hamming μπορεί να γραφεί σαν βάρος κάποιας κωδικής λέξης και άρα η ελαχιστοποίηση γίνεται πάνω στα ίδια σύνολα.

Η διαδικασία κωδικοποίησης των δεδομένων στην ουσία είναι η μετατροπή των λέξεων πληροφορίας k ψηφίων στις αντίστοιχες κωδικές λέξεις n ψηφίων:

$$m = [m_0, m_1, m_2, \dots, m_k] \rightarrow c = [c_0, c_1, c_2, \dots, c_n] \quad (3.2.4)$$

Όταν οι τιμές των n και k είναι σχετικά μικρές, η παραπάνω μετατροπή–αντιστοίχιση μπορεί να γίνει μέσω ενός κατάλληλου πίνακα που θα αντιστοιχίζει κάθε ένα από τα 2^k διανύσματα πληροφορίας σε μία κωδική λέξη μήκους n . Όταν όμως τα n και k είναι μεγάλα, οι διαστάσεις ενός τέτοιου πίνακα είναι πρακτικά απαγορευτικές και έτσι υπάρχει η ανάγκη ανάπτυξης ενός γεννήτορα μηχανισμού για τη διαδικασία κωδικοποίησης. Δεδομένης αυτής της ανάγκης, η ύπαρξη γραμμικότητας σε αυτόν τον μηχανισμό βοηθά πολύ στην απλοποίηση της διαδικασίας και η μετατροπή αυτή πραγματοποιείται με την βοήθεια ενός $k \times n$ πίνακα, G , ο οποίος ονομάζεται “Γεννήτορας Πίνακας” του κώδικα, πολλαπλασιάζοντας την λέξη πληροφορίας με τον Γεννήτορα Πίνακα, πράξη της οποίας ο μαθηματικός τύπος φαίνεται στην παρακάτω σχέση (σχέση 3.2.5):

$$c = m \cdot G \quad (3.2.5)$$

Για να είναι όμως ένας πίνακας G γεννήτορας πίνακας για κάποιο γραμμικό κώδικα C πρέπει οι γραμμές του G είναι γραμμικά ανεξάρτητες, δηλαδή η τάξη του πίνακα G ³⁷ να είναι ίση με το πλήθος των γραμμών του. Και επειδή οι ισοδύναμοι πίνακες³⁸ ως προς τις γραμμές έχουν την ίδια τάξη, αν υπάρχει ένας πίνακας ισοδύναμος του G , τότε και αυτός θα είναι Γεννήτορας Πίνακας του γραμμικού κώδικα C . Από τα παραπάνω γίνεται φανερό ότι, έχοντας έναν Γεννήτορα Πίνακα ενός κώδικα C , μπορεί να παραχθεί ένα πλήθος άλλων Γεννητόρων Πινάκων πραγματοποιώντας ακολουθίες πράξεων στις γραμμές του G . Για κάθε έναν Γεννήτορα Πίνακα, G_i , που παράγεται, η διαδικασία της κωδικοποίησης θα περιγράφεται με την σχέση 3.2.5, και κάθε λέξη πληροφορίας θα αντιστοιχίζεται σε μία κωδική λέξη, όπως και στην αρχική περίπτωση, με την διαφορά ότι η κωδική λέξη στην οποία θα αντιστοιχεί κάθε Γεννήτορας Πίνακας G_i μία συγκεκριμένη πληροφορία δεν θα είναι απαραίτητα η ίδια.

Η σχέση 3.2.5 που εκφράζει την διαδικασία κωδικοποίησης των δεδομένων είναι ένας απλός πολλαπλασιασμός πινάκων. Η διαδικασία αυτή είναι αρκετά απλή να υλοποιηθεί μιας και δεν απαιτείται ο κωδικοποιητής και ο αποκωδικοποιητής να περιλαμβάνουν πολλά κυκλώματα μνήμης μιας και για κάθε λέξη πληροφορίας χρειάζεται μόνο ο Γεννήτορας Πίνακας για να κωδικοποιηθεί και αντίστοιχα για κάθε κωδική λέξη για να αποκωδικοποιηθεί.

Η μορφή και το μέγεθος της κωδικής αυτής λέξης ποικίλει, όπως προαναφέρθηκε, ανάλογα με το είδος του κώδικα και το σύστημα για το οποίο προορίζεται. Μία τέτοια μορφή αναφέρθηκε στην περίπτωση του κώδικα ASCII, όπου τα επτά πρώτα ψηφία κάθε κωδικής λέξης αποτελούσαν την λέξη πληροφορίας και το όγδοο ήταν το ψηφίο ισοτιμίας. Κώδικες που έχουν αυτό το χαρακτηριστικό, δηλαδή μέσα στην κωδική λέξη, είτε στην αρχή της είτε στο τέλος της, να υπάρχει αναλλοίωτη η λέξη πληροφορίας, ονομάζονται “Συστηματικοί Κώδικες” (Systematic codes) και ο Γεννήτορας Πίνακας τους μπορεί να έχει την μορφή (θεωρώντας ότι σε κάθε κωδική λέξη η λέξη πληροφορίας είναι στο τέλος της) :

³⁷Ως “τάξη” ενός πίνακα ορίζεται ο αριθμός των γραμμικά ανεξάρτητων στηλών ή γραμμών του πίνακα αυτού.

³⁸Δύο πίνακες χαρακτηρίζονται ως “ισοδύναμοι” ως προς τις γραμμές (γραμμικά ισοδύναμοι) αν και μόνο αν ο ένας μπορεί να παραχθεί από τον άλλον με μία ακολουθία στοιχειωδών πράξεων στις γραμμές του δεύτερου.

$$G = [P, I_k] = \begin{bmatrix} p_{0,0} & p_{0,1} & p_{0,2} & \dots & p_{0,n-k-1} & 1 & 0 & \dots & 0 \\ p_{1,0} & p_{1,1} & p_{1,2} & \dots & p_{1,n-k-1} & 0 & 1 & \dots & 0 \\ p_{2,0} & p_{2,1} & p_{2,2} & \dots & p_{2,n-k-1} & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ p_{k-1,0} & p_{k-1,1} & p_{k-1,2} & \dots & p_{k-1,n-k-1} & 0 & 0 & \dots & 1 \end{bmatrix} \quad (3.2.6)$$

όπου ο I_k είναι ένας μοναδιαίος $k \times k$ πίνακας και ο P ένας $k \times n-k$ πίνακας μέσω του οποίου θα παράγονται τα ψηφία ισοτιμίας. Συνδυάζοντας τις δύο τελευταίες σχέσεις (3.2.5 και 3.2.6) έχουμε ότι, αν ένας Γεννήτορας Πίνακας είναι Συστηματικός, η κωδικοποίηση θα περιγράφεται με την παρακάτω σχέση (σχέση 3.2.7)

$$c = m \cdot [P, I_k] = [m \cdot P, m] \quad (3.2.7)$$

όπου φαίνεται ότι η κωδική λέξη αποτελείται από δύο μέρη: το πρώτο μέρος, αρχή της κωδικής λέξης στο οποίο βρίσκονται τα ψηφία ελέγχου και το δεύτερο μέρος της κωδικής λέξης, στο τέλος της, όπου περιέχεται αναλλοίωτη η λέξη πληροφορίας. Το ιδιαίτερο αυτό χαρακτηριστικό των Συστηματικών Κωδίκων αποτελεί πολύ σημαντικό πλεονέκτημα για την αποκωδικοποίηση μιας και, στην περίπτωση που υπάρξει σφάλμα στην μετάδοση των δεδομένων, αν ο δέκτης χρησιμοποιήσει την τεχνική Αποκωδικοποίησης Μέγιστης Πιθανότητας και “συμπεράνει” την κωδική λέξη που θα έπρεπε να λάβει, μπορεί να ανακτήσει την λέξη πληροφορίας αφού θα περιέχεται μέσα στην κωδική αυτή λέξη, όπως δείχθηκε και με την σχέση 3.2.7 .

Ένας πίνακας που παίζει σημαντικό ρόλο στους Γραμμικούς Κώδικες και συνδέεται με τον Γεννήτορα Πίνακα είναι ο Πίνακας Ελέγχου Ισοτιμίας (parity check matrix), ο οποίος συμβολίζεται με H . Ο πίνακας αυτός, για την περίπτωση ενός (n,k) κώδικα, είναι ένας $(n - k) \times n$ πίνακας ο οποίος προκύπτει από τον Γεννήτορα Πίνακα G , βάσει της παρακάτω σχέσης (σχέση 3.2.8):

$$G \cdot H^T = 0 \quad (3.2.8)$$

όπου ο πίνακας H^T είναι ο ανάστροφος πίνακας του H ³⁹. Ο πίνακας H μπορεί να θεωρηθεί ότι αποτελεί τον διανυσματικό χώρο για έναν $(n,n-k)$ κώδικα ο οποίος συμβολίζεται ως C_1 . Οι

³⁹Ως “Ανάστροφος” πίνακας A^T ενός πίνακα A ορίζεται ο πίνακας που προκύπτει αν οι στήλες του A γίνουν γραμμές και οι γραμμές του στήλες.

κωδικές του λέξεις θα είναι 2^{n-k} (το πλήθος τους) και θα είναι ορθογώνιες με τις κωδικές λέξεις του C, οπότε και κάθε γραμμή του πίνακα H θα είναι ορθογώνια ως προς κάθε έγκυρη κωδική λέξη του C. Ο κώδικας C_t ονομάζεται “Δυϊκός”⁴⁰ του κώδικα C και αν ο Γεννήτορας Πίνακας του C από τον οποίο προκύπτει ο H είναι συστηματικός, τότε βάσει των σχέσεων 3.2.6, 3.2.7 και 3.2.8 και των ιδιοτήτων του H που προαναφέρθηκαν, προκύπτει ότι η μορφή του πίνακα H θα είναι παρόμοια με του G (σχέση 3.2.9):

$$\begin{aligned}
 H &= \begin{bmatrix} 1, & 0, & \dots, & 0, & p_{0,0}, & p_{0,1}, & p_{0,2}, & \dots, & p_{0,n-k-1} \\ 0, & 1, & \dots, & 0, & p_{1,0}, & p_{1,1}, & p_{1,2}, & \dots, & p_{1,n-k-1} \\ 0, & 0, & \dots, & 0, & p_{2,0}, & p_{2,1}, & p_{2,2}, & \dots, & p_{2,n-k-1} \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0, & 0, & \dots, & 1, & p_{k-1,0}, & p_{k-1,1}, & p_{k-1,2}, & \dots, & p_{k-1,n-k-1} \end{bmatrix} \\
 &= [I_{n-k}, P] \quad (3.2.9)
 \end{aligned}$$

και ότι, λόγω της ορθογωνικότητας μεταξύ του H και των κωδικών λέξεων του C, προκύπτει η σχέση 3.2.10 η οποία αποτελεί σχέση ελέγχου εγκυρότητας των δεδομένων που λαμβάνονται από τον δέκτη γιατί, μιας και θα ισχύει για όλες τις έγκυρες κωδικές λέξεις του C, αρκεί να επαληθεύεται για κάποια κωδική λέξη που έλαβε ο δέκτης για να την θεωρήσει έγκυρη.

$$c \cdot H^T = m \cdot G \cdot H^T = 0 \quad (3.2.10)$$

Η παραπάνω ιδιότητα μπορεί να χρησιμοποιηθεί και για την ανίχνευση λαθών στον δέκτη. Αρχικά, υποθέτουμε ότι έχουμε έναν Γραμμικό Μπλοκ κώδικα (n,k) και ότι μεταδίδουμε μία κωδική λέξη του, c, n συμβόλων, μέσω ενός καναλιού με προσθετικό θόρυβο. Το κανάλι αυτό θα προσθέσει στην κωδική λέξη που διέρχεται μέσω αυτού ένα σφάλμα, e, n συμβόλων, με αποτέλεσμα ο δέκτης να λάβει μία λέξη, r, n συμβόλων, της οποίας όμως τα σύμβολα δεν είναι απαραίτητα τα σύμβολα που εστάλησαν από τον πομπό, λόγω του προαναφερθέντος θορύβου. Η κωδική αυτή λέξη μπορεί να εκφραστεί μαθηματικώς από την σχέση 3.2.11:

⁴⁰Για δύο κώδικες που είναι Δυϊκοί, έστω C και C_t , θα ισχύει ότι ο Γεννήτορας Πίνακας του C θα είναι ο Πίνακας Ελέγχου Ισοτιμίας του C_t και ο Πίνακας Ελέγχου Ισοτιμίας του C θα είναι ο Γεννήτορας Πίνακας του C_t .

$$r = c + e(3.2.11)$$

Ορίζοντας την έννοια του “Συνδρόμου Σφάλματος”, s , ίση με το διάνυσμα

$$s = r \cdot H^T(3.2.12)$$

και συνδυάζοντας την με την σχέση 3.2.10, προκύπτει ότι:

$$s = r \cdot H^T = (c + e) \cdot H^T = e \cdot H^T(3.2.13)$$

και με χρήση της σχέσης αυτής, υπολογίζοντας ο δέκτης την τιμή του συνδρόμου σφάλματος μπορεί να γνωρίζει αν η λέξη μεταδόθηκε χωρίς να αλλοιωθεί από τον θόρυβο ή όχι. Στην περίπτωση που $s=0$, τότε η λέξη που έφθασε στον δέκτη είναι έγκυρη ενώ αν $s \neq 0$ υπάρχει σίγουρα κάποιο λάθος.

Στην περίπτωση που βρεθεί ότι υπάρχει κάποιο σφάλμα στην κωδική λέξη που έλαβε ο δέκτης, ανάλογα με τον αποκωδικοποιητή που περιέχει, μπορεί να γίνει διόρθωση του σφάλματος. Ανάλογα με την “ικανότητα” του κάθε αποκωδικοποιητή να διορθώνει τα πιθανά σφάλματα, οι αποκωδικοποιητές χωρίζονται σε δύο μεγάλες κατηγορίες, τους αποκωδικοποιητές πλήρους διόρθωσης λαθών και τους αποκωδικοποιητές περιορισμένης δυνατότητας διόρθωσης λαθών.

Οι αποκωδικοποιητές της πρώτης κατηγορίας, δοσμένης της λέξης r και στην περίπτωση που το σύνδρομο σφάλματος είναι διάφορο του μηδενός (δηλαδή η r περιέχει σφάλματα) μπορούν να “βρουν” την σωστή κωδική λέξη, αποκωδικοποιώντας πλήρως την μεταδιδόμενη πληροφορία. Για να το επιτύχουν αυτό η πιο συνηθισμένη τεχνική είναι η ελαχιστοποίηση κάποιου σχετικού μεγέθους, όπως είναι η απόσταση Hamming που αναφέρθηκε παραπάνω, μέσω της οποίας μπορεί να επιλεγεί η κωδική λέξη c που μεταδόθηκε και με χρήση κατάλληλων δομών, όπως είναι οι τυπικοί πίνακες (standard array) έχουν την δυνατότητα για πλήρη αποκωδικοποίηση. Όμως, επειδή η παραπάνω διαδικασία είναι αρκετά πολύπλοκη και απαιτεί σημαντική υπολογιστική ικανότητα από τον αποκωδικοποιητή, ο αποκωδικοποιητής αυτός θα είναι αρκετά πολύπλοκος και θα απαιτείται πολύ υλικό για την κατασκευή του, καθιστώντας την κατηγορία αυτή των αποκωδικοποιητών ασύμφορη για τις συνηθισμένες περιπτώσεις χρήσης.

Η δεύτερη κατηγορία, οι αποκωδικοποιητές περιορισμένης δυνατότητας διόρθωσης

σφαλμάτων, είναι αρκετά πιο απλοί σαν κυκλώματα και έχουν πολύ μικρότερες απαιτήσεις σε υλικό για την κατασκευή τους, και για τον λόγο αυτό οι αποκωδικοποιητές της κατηγορίας αυτής χρησιμοποιούνται στις περισσότερες εφαρμογές. Η διόρθωση των σφαλμάτων της κωδικής λέξης γίνεται με πιο απλούς μηχανισμούς, σχετικά με τους μηχανισμούς που χρησιμοποιούνται από την πρώτη κατηγορία, με πιο χαρακτηριστική τεχνική την χρήση της απόστασης Hamming, με την διαφορά ότι στην περίπτωση αυτή δεν γίνεται προσπάθεια ελαχιστοποίησης της αλλά απλά ελέγχεται αν είναι μικρότερη από μία συγκεκριμένη τιμή, t , δηλαδή $d_H(r,c) \leq t$. Η ειδοποιός διαφορά είναι το ότι, στην πρώτη περίπτωση έχουμε ελαχιστοποίηση κάποιας τιμής (παραδείγματος χάριν η απόσταση Hamming), οπότε θα έχουμε πάντα λύση και πάντα θα καταλήγει ο αποκωδικοποιητής σε μία κωδική λέξη η οποία θα είναι η κωδική λέξη που μεταδόθηκε μέσω του θορυβώδους καναλιού ενώ, στην δεύτερη περίπτωση, αν η ελάχιστη απόσταση Hamming για την ληφθείσα κωδική λέξη δεν είναι μικρότερη από την προκαθορισμένη τιμή t δεν μπορεί ο αποκωδικοποιητής να αποκωδικοποιήσει την εσφαλμένη κωδική λέξη και έχουμε αποτυχία του αποκωδικοποιητή. Για τον λόγο αυτό οι αποκωδικοποιητές της κατηγορίας αυτής ονομάζονται “αποκωδικοποιητές περιορισμένης δυνατότητας διόρθωσης σφαλμάτων”.

3.3 - Κώδικες LDPC (Low Density Parity Check)

Οι κώδικες LDPC (Low Density Parity Check - Χαμηλής Πυκνότητας⁴¹ Έλεγχος Ισοτιμίας) είναι Γραμμικοί Μπλοκ κώδικες διόρθωσης σφαλμάτων. Ως τέτοιοι, έχουν τα χαρακτηριστικά που περιγράφηκαν στην προηγούμενη παράγραφο. Το βασικό τους χαρακτηριστικό είναι ότι κατασκευάζονται βάσει ενός πίνακα ελέγχου ισοτιμίας H , ο οποίος αποτελείται από λίγα μη μηδενικά στοιχεία (“1” για την περίπτωση των δυαδικών (binary) κωδίκων της κατηγορίας αυτής που είναι και οι κώδικες που θα χρησιμοποιηθούν σε παραδείγματα) σχετικά με το μέγεθος του πίνακα, διάσπαρτα ανάμεσα σε πολλά μηδενικά (“0”). Έχουν δηλαδή μικρή πυκνότητα μη μηδενικών στοιχείων στον πίνακα ισοτιμίας τους, από όπου προέρχεται και το όνομα της κατηγορίας αυτής. Αρχικά παρουσιάστηκαν από τον Robert Gallager, ο οποίος, το 1962, στην διδακτορική του διατριβή στο πανεπιστήμιο MIT

⁴¹Η πυκνότητα ενός πίνακα ορίζεται ως:

$$\text{Πυκνότητα πίνακα} = \frac{\text{πλήθος μηδενικών στοιχείων του πίνακα}}{\text{συνολικό πλήθος στοιχείων του πίνακα}} \quad (2.3.f)$$

(Massachusetts Institute of Technology) παρουσίασε, για πρώτη φορά, τα πλεονεκτήματα της χρήσης Γραμμικών Μπλοκ κωδικών που περιγράφονται από έναν αραιό πίνακα ισοτιμίας. Ένα από τα πλεονεκτήματα αυτά είναι ότι, λόγω της χαμηλής πυκνότητας του πίνακα ισοτιμίας, οι κώδικες αυτοί είναι επιδεκτικοί σε διάφορους αλγόριθμους επαναληπτικής αποκωδικοποίησης (iterative decoding), πλεονέκτημα που είναι από τους κύριους λόγους της αλματώδης ανάπτυξης των κωδικών της κατηγορίας αυτής.

Αν και η επαναληπτική αποκωδικοποίηση που παρουσίασε ο Gallager στην ίδια εργασία δεν ήταν βέλτιστη, σε σχέση με άλλες μορφές αποκωδικοποίησης, όπως η MAP⁴² (Maximum A Posteriori) αποκωδικοποίηση, επέτρεπε την πρακτική υλοποίηση κωδικών μεγάλου μήκους⁴³ ($n \sim 10$), οι οποίοι όμως δεν παρουσιάζουν πολύ μεγάλη πολυπλοκότητα, καθιστώντας την υλοποίηση τους εφικτή σε πραγματικά συστήματα, και μπορούν να φθάσουν πολύ κοντά (εώς και μερικά εκατοστά του dB) στο όριο Shannon με την απόδοση τους να χαρακτηρίζεται σχεδόν βέλτιστη. Όμως, παρά την μειωμένη πολυπλοκότητα, για το μέγεθος τους, που παρουσίαζε το είδος αυτό των κωδικών που εισήχθησαν από τον Gallager, λόγω περιορισμένης υπολογιστικής ισχύος των ηλεκτρονικών υπολογιστών της δεκαετίας του 1960 και των επόμενων δεκαετιών, δεν είχαν μεγάλη αποδοχή, με την αλματώδη ανάπτυξη τους να αρχίζει το 1995⁴⁴, χρονιά που οι D. MacKay και R. Neal παρουσίασαν, μέσω προσομοίωσης, τα σημαντικά οφέλη της χρήσης τέτοιων κωδικών (συγκεκριμένα για του δυαδικούς Μπλοκ κώδικες LDPC) και ειδικά την ικανότητα τους να λειτουργούν κοντά στο όριο Shannon για το δυαδικό συμμετρικό κανάλι (Binary Symmetric Channel-BSC) και για το BI-AWGN (δυαδικό κανάλι λευκού προσθετικού θορύβου). Η ικανότητα αυτή χαρακτηρίζει τους κώδικες αυτής της κατηγορίας και τους turbo κώδικες που θα αναφερθούν στην συνέχεια της παρούσας εργασίας, χαρακτηριστικό που οδήγησε στο να γίνουν οι δύο αυτές κατηγορίες οι πιο ανεπτυγμένες και ευρέως χρησιμοποιούμενες κατηγορίες κωδικών στις περισσότερες εφαρμογές. Παραδείγματος χάριν, οι LDPC κώδικες έχουν υιοθετηθεί από

⁴²Η μέθοδος της MAP αποκωδικοποίησης στηρίζεται στον υπολογισμό της πιθανότητας κάθε συμβόλου και στην μεγιστοποίηση της πιθανότητας αυτής και βασίζεται στην χρήση trellis διαγραμμάτων.

⁴³Ο πίνακας ισοτιμίας του κώδικα που παρουσιάστηκε από τον Gallager ήταν μεγέθους περίπου 500 στηλών.

⁴⁴Πολύ σημαντική για την ανάπτυξη των LDPC κωδικών ήταν και η δουλειά του Michael Tanner το 1981, ο οποίος εισήγαγε μία νέα ερμηνεία των κωδικών αυτών (η οποία όμως έχει πιο γενική ισχύ και αφορά και άλλες κατηγορίες κωδικών) με την χρήση διμερών γραφημάτων, των γραφημάτων ή γράφων Tanner που θα αναφερθούν και χρησιμοποιηθούν παρακάτω, και την περιγραφή ενός μεγάλου κώδικα ως σύνθεση μικρότερων και απλούστερων κωδικών, χρησιμοποιώντας την επαναληπτικότητα για την μείωση της πολυπλοκότητας.

διάφορα πρότυπα επικοινωνιών, με πιο χαρακτηριστικά τα πρότυπα DVB-S2 (IEEE80216.e, IEEE802.3an(10BASE-T) κ.α.).

Η επίδοση των κωδικών αυτών εξαρτάται σημαντικά από την σχεδίαση του χαμηλής πυκνότητας πίνακα ισοτιμίας, H , καθώς και από τον αλγόριθμο αποκωδικοποίησης που θα χρησιμοποιηθεί και για τον λόγο αυτό η εισαγωγή τους από τον Gallager έγινε μαζί με την παρουσίαση της επαναληπτικής μεθόδου αποκωδικοποίησης. Η χαμηλή πυκνότητα του πίνακα ισοτιμίας διευκολύνει, όπως προαναφέρθηκε, την εφαρμογή της επαναληπτικής αποκωδικοποίησης, η οποία επαναληπτική κωδικοποίηση είναι αυτή που μειώνει σημαντικά την πολυπλοκότητα της αποκωδικοποίησης, σχετικά με αντίστοιχους κώδικες ίδιου μεγέθους αλλά μεγαλύτερης πυκνότητας πίνακα ελέγχου ισοτιμίας. Με κατάλληλη σχεδίαση και υλοποίηση των παραπάνω μπορούν να επιτευχθούν τιμές πολύ κοντά στο όριο Shannon. Έχουν σχεδιαστεί αρκετοί αλγόριθμοι για την κατασκευή κωδικών LDPC οι οποίοι έχουν το παραπάνω χαρακτηριστικό, με πιο χαρακτηριστικούς τους αλγόριθμους Progressive Edge Growth (PEG) και Improved PEG.

Ένας LDPC κώδικας, εκτός της χαμηλής πυκνότητας του πίνακα ελέγχου ισοτιμίας του (και του επαναληπτικού τρόπου αποκωδικοποίησης), έχει όλα τα χαρακτηριστικά των Γραμμικών Μπλοκ κωδικών που αναφέρθηκαν στην προηγούμενη παράγραφο (παράγραφος 3.2). Έχουν δηλαδή έναν Γεννήτορα πίνακα G , διαστάσεων $k \times n$, ο οποίος θα μετατρέπει το μήνυμα m μήκους k σε μία κωδικοποιημένη ακολουθία, c , μήκους n , μέσω της σχέσης 3.2.5 που παρουσιάστηκε στην παραπάνω ανάλυση των Γραμμικών κωδικών (παράγραφος 3.2), που θα είναι η έξοδος του κωδικοποιητή και η ακολουθία που θα σταλεί από τον πομπό.

$$c = m \cdot G(3.2.5)$$

Τα χαρακτηριστικά του πίνακα αυτού θα είναι αυτά που προαναφέρθηκαν στην παράγραφο 3.2 και θα συνδέεται με τον πίνακα ελέγχου ισοτιμίας μέσω της σχέσης 3.2.8:

$$G \cdot H^T = 0(3.2.8)$$

και ο έλεγχος ισοτιμίας θα γίνεται σύμφωνα με την σχέση 3.2.10:

$$c \cdot H^T = m \cdot G \cdot H^T = 0(3.2.10)$$

Ο πίνακας ισοτιμίας των κωδικών αυτών, όπως προαναφέρθηκε, έχει πολύ μεγάλη σημασία και επηρεάζει καθοριστικά τα χαρακτηριστικά και τις επιδόσεις του κάθε κώδικα, και για τον λόγο αυτό γίνεται προσεκτική σχεδίαση του. Για έναν κώδικα με διαστάσεις Γεννήτορα πίνακα $k \times n$ ο πίνακας H θα έχει διαστάσεις $(n - k) \times n$. Οι βασικές παράμετροι του πίνακα αυτού είναι:

- Το πλήθος, m , των γραμμών του πίνακα H που ισούται με $n-k$, όπου, όπως δείχθηκε στην παράγραφο 3.2, κάθε γραμμή θα αποτελεί και μία εξίσωση ελέγχου ισοτιμίας. Οπότε η αύξηση της τιμής του m ενισχύει τις δυνατότητες ανίχνευσης και διόρθωσης λαθών του κώδικα.
- Το πλήθος, n των στηλών του πίνακα H , που αποτελεί το μήκος του μεγέθους του μπλοκ του κώδικα και αύξηση του επιφέρει βελτίωση στις επιδόσεις του κώδικα.
- Ο βαθμός του πίνακα H ($\text{rank}H$), ο οποίος θα ισούται το πλήθος των γραμμικά ανεξάρτητων γραμμών του πίνακα. Θεωρώντας ότι όλες οι γραμμές του πίνακα είναι γραμμικά ανεξάρτητες, οπότε $\text{rank}H=m$, ορίζεται ο ρυθμός σχεδιασμού (design rate) r του κώδικα αυτού ως: $r = \frac{n-m}{n}$ (3.3.1). Αυτός θα αποτελεί και τον ελάχιστο πιθανό ρυθμό του κώδικα αυτού, γιατί στην πραγματικότητα κάποιες γραμμές θα είναι γραμμικά εξαρτημένες και οπότε ο πραγματικός ρυθμός του κώδικα αυτού θα είναι: $R = \frac{k}{n} = \frac{n-\text{rank}H}{n}$ (3.3.2) και αφού $\text{rank}H \leq m$, θα ισχύει ότι $R \geq r$, μη την ισότητα να ισχύει στην περίπτωση που ο πίνακας H είναι full rank (πλήρους βαθμού: πίνακες που δεν έχουν γραμμικά εξαρτημένες γραμμές) πίνακας.
- Κατανομή βαρών (weight distribution) του πίνακα που ορίζεται ως το πλήθος των μη μηδενικών στοιχείων κάθε γραμμής και κάθε στήλης. Τα βάρη των γραμμών συμβολίζονται ως w_r και των στηλών ως w_c .

Η τελευταία παράμετρος του πίνακα ελέγχου ισοτιμίας είναι ειδοποιός για τους LDPC κώδικες και τους χωρίζει σε δύο μεγάλες κατηγορίες. Η πρώτη είναι οι κανονικοί ή ομαλοί (regular) κώδικες, των οποίων τα βάρη όλων των γραμμών του είναι ίσα, όπως και τα βάρη των στηλών του, και η κατηγορία αυτή προτάθηκε από τον Gallager, ο οποίος ανέδειξε και τις βασικές ιδιότητες της κατηγορίας αυτής που είναι ότι η πιθανότητα λάθους είναι αντιστρόφως ανάλογη με το μέγεθος n του κώδικα (μειώνεται εκθετικά με την αύξηση του n) και ότι η ελάχιστη απόσταση είναι ανάλογη με το μέγεθος του κώδικα. Έτσι λοιπόν, σε έναν πίνακα ελέγχου ισοτιμίας θα πρέπει, εκτός του σταθερού βάρους γραμμών w_r και στηλών w_c ,

να ισχύουν οι σχέσεις $w_r \ll n$ και $w_c \ll m$ για να θεωρείται ο πίνακας ως χαμηλής πυκνότητας⁴⁵ και ο πίνακας ισοτιμίας να μην έχει περισσότερα από ένα μη μηδενικά στοιχεία στην ίδια θέση σε οποιοδήποτε γραμμές ή και στήλες έτσι ώστε να γίνεται όσο δυνατόν μεγαλύτερο το μήκος κύκλου (έννοια που θα αναφερθεί παρακάτω) και να αποφεύγεται η περίπτωση όπου το μήκος να είναι 4. Ακόμα, σε έναν κανονικό LDPC κώδικα, θα ισχύει η σχέση:

$$n \cdot w_r = m \cdot w_c \quad (3.3.3)$$

από την οποία, σε συνδυασμό με την σχέση 3.2.1, προκύπτει ότι ο ρυθμός σχεδίασης θα δίνεται από την σχέση:

$$r = \frac{n - m}{n} = 1 - \frac{m}{n} = 1 - \frac{w_c}{w_r} \quad (3.3.4)$$

και, επομένως για τον πραγματικό ρυθμό του κώδικα θα ισχύει ότι:

$$R \leq 1 - \frac{w_c}{w_r} \quad (3.3.5)$$

Ένας πίνακας χαμηλής πυκνότητας ελέγχου ισοτιμίας με τα παραπάνω χαρακτηριστικά παρουσιάζεται στην σχέση 3.3.6, όπου ο πίνακας είναι 15x5, το βάρος των γραμμών είναι 6 και το βάρος των στηλών είναι 2, με την πυκνότητα του πίνακα να είναι, σύμφωνα με την σχέση 2.3.f.2 ίση με $\frac{w_r}{n} = \frac{6}{15} = \frac{2}{5} = \frac{w_c}{m}$ ⁴⁶. Οπότε, για τον κώδικα που θα αντιστοιχεί στον πίνακα ελέγχου ισοτιμίας της σχέσης 3.3.6, για τον ελάχιστο ρυθμό ισχύει ότι $R \leq 1 - \frac{w_c}{w_r} = 1 - \frac{2}{6} = \frac{2}{3}$.

⁴⁵Η πυκνότητα θα δίνεται από την σχέση: $\text{πυκνότητα πίνακα} = \frac{w_r}{n} = \frac{w_c}{m}$ 2.3. f. 2

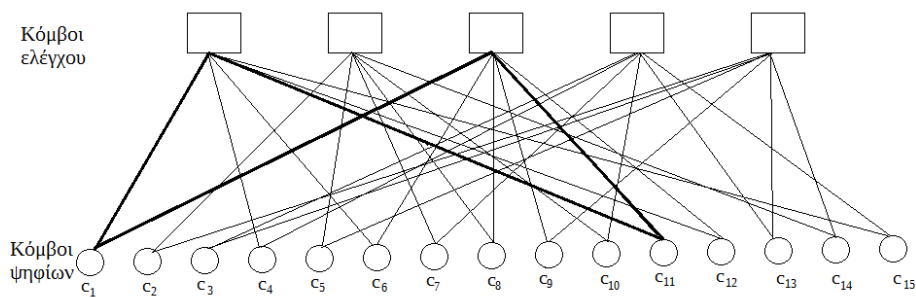
⁴⁶Η πυκνότητα αυτή δεν είναι ιδιαίτερα μικρή λόγω του μικρού μεγέθους που έχει ο πίνακας, ο οποίος σχεδιάστηκε για την καλύτερη εποπτεία των παραπάνω εννοιών και δεν αντιστοιχεί σε πραγματικό κώδικα (όπως προαναφέρθηκε, οι πίνακες ελέγχου ισοτιμίας των κωδικών αυτών έχουν πολύ μεγάλο πλήθος στοιχείων, με χαρακτηριστικό μέγεθος τις περίπου 500 στήλες που είχε ο αρχικός LDPC κώδικας που παρουσίασε ο Gallager).

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad (3.3.6)$$

Εκτός όμως από την περιγραφή των LDPC κωδικών με χρήση των παραπάνω πινάκων, ένα άλλο χρήσιμο εργαλείο αναπαράστασης ενός τέτοιου κώδικα είναι με τα διμερή γραφήματα που παρουσίασε ο Michael Tanner, τους γράφους Tanner (υποσημείωση 44) οι οποίοι μπορούν να αναπαραστήσουν γραφικά τις εξισώσεις ισοτιμίας που περιγράφονται από τον πίνακα ελέγχου ισοτιμίας. Οι εξισώσεις αυτές, για την περίπτωση του παραπάνω πίνακα H θα είναι:

$$\begin{aligned} c_1 \cdot c_4 \cdot c_6 \cdot c_{12} \cdot c_{11} \cdot c_{15} &= 0 \\ c_2 \cdot c_5 \cdot c_7 \cdot c_8 \cdot c_{10} \cdot c_{14} &= 0 \\ c_1 \cdot c_6 \cdot c_8 \cdot c_9 \cdot c_{11} \cdot c_{12} &= 0 \quad (3.3.7) \\ c_3 \cdot c_4 \cdot c_7 \cdot c_{10} \cdot c_{13} \cdot c_{15} &= 0 \\ c_2 \cdot c_3 \cdot c_5 \cdot c_9 \cdot c_{13} \cdot c_{14} &= 0 \end{aligned}$$

Ο γράφος Tanner, είναι ένα γράφημα το οποίο αποτελείται από κόμβους ψηφίων (bit nodes) το πλήθος των οποίων είναι ίσο με το πλήθος των στηλών του πίνακα ελέγχου ισοτιμίας του κώδικα τον οποίο αναπαριστά, και κόμβους ελέγχου (check nodes) το πλήθος των οποίων είναι ίσο με το πλήθος των γραμμών του πίνακα. Κάθε κόμβος ψηφίου αναπαριστά ένα ψηφίο της κωδικοποιημένης λέξης και κάθε κόμβος ελέγχου έναν έλεγχο ισοτιμίας. Τα δύο είδη αυτά των κόμβων τα ενώνουν γραμμές, ανάλογα με τις εξισώσεις ισοτιμίας που αντιστοιχούν στον κώδικα που αναπαριστά ο κάθε γράφος, με κάθε κόμβο ελέγχου να ενώνεται με εκείνους τους κόμβους ψηφίων των οποίων τα ψηφία χρησιμοποιούνται στην εξίσωση ισοτιμίας που αντιστοιχεί στον συγκεκριμένο κόμβο ελέγχου, ή, αν χρησιμοποιείται ο πίνακας ελέγχου ισοτιμίας για την κατασκευή του γράφου, κάθε κόμβος ελέγχου θα ενώνεται με τους κόμβους ψηφίων που αντιστοιχούν στα μη μηδενικά στοιχεία της γραμμής του πίνακα. Οπότε, για την περίπτωση του παραπάνω πίνακα H (σχέση 3.3.6) ο αντίστοιχος γράφος θα είναι αυτός που παρουσιάζεται στο παρακάτω σχήμα (σχήμα 3.2).



Σχήμα 3.2 - Γράφος Tanner για τον πίνακα H της σχέσης 3.3.6 (ή τις εξισώσεις 3.3.7)

Όπως φαίνεται από την παραπάνω αναπαράσταση (σχήμα 3.2) κάθε κόμβος ελέγχου ενώνεται με έξι κόμβους ψηφίων, όσο είναι και το βάρος των γραμμών του πίνακα ελέγχου ισοτιμίας του κώδικα που αναπαριστά, και κάθε κόμβος ψηφίων με 2 κόμβους ελέγχου, όσο είναι και το βάρος των στηλών του αντίστοιχου πίνακα H. Οι παρατηρήσεις αυτές είναι σύμφωνες με την παραπάνω περιγραφή του συγκεκριμένου τύπου διαγραμμάτων. Μία ακόμα σημαντική παράμετρος των γράφων Tanner είναι το ελάχιστο μήκος κλειστού μονοπατιού, το οποίο είναι ίσο με τις ακμές ενός μονοπατιού το οποίο ξεκινάει και καταλήγει στον ίδιο κόμβο και ονομάζεται *girth*. Στον γράφο του σχήματος 3.2 το ελάχιστο αυτό μήκος είναι 4, με ένα τέτοιο κλειστό μονοπάτι να αναπαρίσταται με τις έντονες γραμμές, που είναι και η ελάχιστη τιμή που μπορεί να πάρει η παράμετρος αυτή σε έναν οποιοδήποτε γράφο Tanner.

Στους κώδικες LDPC, οι καλύτερες επιδόσεις παρατηρούνται όταν αυτοί συνδυαστούν με αλγόριθμο αποκωδικοποίησης *belief-propagation*, όπου η πιθανότητα κάθε ψηφίου διαδίδεται μέσω των ακμών του γράφου Tanner και χρησιμοποιείται για την ανανέωση της πιθανότητας των άλλων ψηφίων ως εξωτερική πληροφορία και έχει δειχθεί ότι όσο πιο πολύ “εξωτερική” πληροφορία είναι διαθέσιμη, τόσο αυξάνεται η επίδοση του κώδικα. Σε περίπτωση που το *girth* είναι μικρό, η πληροφορία αυτή επιστρέφει σύντομα στον αρχικό της κόμβο και το ποσό της “εξωτερικής πληροφορίας που περιέχει είναι μικρό. Συνεπώς, η παράμετρος αυτή είναι πολύ σημαντική και είναι από τα χαρακτηριστικά ενός LDPC κώδικα που γίνονται προσπάθειες βελτιστοποίησης, με την προσπάθεια, στην προκειμένη περίπτωση, να προσανατολίζεται στην μεγιστοποίηση της.

3.4 - Συνελικτικοί κώδικες

Μία από τις μεγαλύτερες και παλαιότερες⁴⁷ κατηγορίες κωδικών διόρθωσης λαθών που αναπτύχθηκαν είναι οι συνελικτικοί κώδικες. Λόγω του ότι είναι από τις πρώτες κατηγορίες που εμφανίστηκαν και με το πέρασμα του χρόνου έχουν αναπτυχθεί πολλοί αλγόριθμοι αποκωδικοποίησης με πολύ καλές επιδόσεις καθώς και αποδοτικές αρχιτεκτονικές, χρησιμοποιούνται ευρύτατα και είναι από τις μεγαλύτερες κατηγορίες κωδικών διόρθωσης λαθών. Με τον όρο “Συνέλιξη” ορίζεται η μαθηματική διαδικασία μέσω της οποίας μπορεί να συνδεθεί η κρουστική απόκριση ενός LTI (Linear Time Invariant-Γραμμικό Χρονικά Ανεξάρτητο) συστήματος συνεχούς χρόνου με την απόκριση του για οποιαδήποτε διέγερση, η οποία ονομάζεται “Συνάρτηση Μεταφοράς”. Ο χαρακτηρισμός των κωδικών που ανήκουν στην κατηγορία αυτή στηρίζεται στο γεγονός ότι, όπως θα φανεί παρακάτω, στους κώδικες αυτούς, την σχέση εισόδου-εξόδου ενός κωδικοποιητή (ή αποκωδικοποιητή) μπορούμε να την αναπαραστήσουμε με μία Συνάρτηση Μεταφοράς, περιγράφοντας το σύστημα αυτό ως ένα LTI σύστημα.

Όπως αναφέρθηκε παραπάνω, οι κώδικες αυτοί είναι Γραμμικοί Κώδικες οι οποίοι έχουν τέτοια δομή (αναφορικά με τον γεννήτορα πίνακα) ώστε η κωδικοποίηση των δεδομένων (και η αποκωδικοποίηση τους) να απαιτεί ένα πλήθος ψηφιακών γραμμικών, χρονικά ανεξάρτητων φίλτρων και η κωδική λέξη που προκύπτει να είναι το αποτέλεσμα της δειγματοληψίας των εξόδων των φίλτρων αυτών, όπως και η έξοδος ενός LTI ψηφιακού συστήματος. Η πληροφορία δεν χωρίζεται σε δομές δεδομένων συγκεκριμένου πλήθους συμβόλων και τα επιπλέον παραγόμενα σύμβολα της κωδικής λέξης δεν εξαρτώνται αποκλειστικά από τα σύμβολα πληροφορίας, όπως συμβαίνει στους Μπλοκ κώδικες που αναφέρθηκαν παραπάνω. Ο κωδικοποιητής τροφοδοτείται συνεχώς με σύμβολα (χωρίς αυτά να χωρίζονται σε blocks) και κάθε χρονική στιγμή οι έξοδοι του κωδικοποιητή, που προκύπτουν ως modulo-2 άθροιση⁴⁸ του συμβόλου της κάθε χρονικής στιγμής με σύμβολα προηγούμενων χρονικών στιγμών, δειγματοληπτούνται. Λόγω της χρήσης συμβόλων από προηγούμενες χρονικές στιγμές, οι κωδικοποιητές που χρησιμοποιούνται είναι συστήματα με μνήμη, σε αντίθεση με τους Μπλοκ κώδικες. Για τον ορισμό του ρυθμού στους κώδικες της

⁴⁷Οι συνελικτικοί κώδικες εφευρέθηκαν το 1954 από τον Elias και η αλγεβρική τους θεωρία αναλύθηκε από τον Forney αρκετά χρόνια αργότερα.

⁴⁸Ως “modulo-2 άθροιση” ορίζεται η πράξη της οποίας το αποτέλεσμα θα είναι “0” αν το αποτέλεσμα της άθροισης είναι άρτιο και “1” αν είναι περιττό.

κατηγορίας αυτής χρησιμοποιείται το πλήθος των καινούριων συμβόλων εισόδου k σε δεδομένα χρονικά διαστήματα, τα οποία παράγουν n σύμβολα εξόδου. Οπότε ο ρυθμός του κώδικα εκφράζεται μαθηματικώς από την σχέση 3.2.3 που ορίστηκε παραπάνω:

$$R = \frac{k}{n} \quad (3.2.3)$$

όπου όμως τα k και n δεν είναι η διάσταση και το μήκος του κώδικα, αντίστοιχα, αλλά το πλήθος των συμβόλων εισόδου και το πλήθος των συμβόλων που παράγονται στην έξοδο, αντίστοιχα. Τυπικά, ο ρυθμός ενός κώδικα διατηρείται σταθερός, δεδομένου ότι μπορεί να αυξάνει η τάξη της μνήμης ώστε να αντισταθμίζεται ο θόρυβος του διαύλου. Αυτό σημαίνει ότι αυξάνεται η πολυπλοκότητα του αλγορίθμου, όπως θα αναφερθεί και παρακάτω, για να χρησιμοποιηθούν περισσότερα ψηφία πλεονασμού. Για την εύρεση του κατάλληλου αλγορίθμου λαμβάνονται υπόψιν και χρησιμοποιούνται τα παραπάνω, έτσι ώστε να διατηρείται ο ρυθμός κοντά στην μονάδα και να αυξάνει η ικανότητα διόρθωσης λαθών. Συγκεκριμένα, κώδικες διόρθωσης λαθών ρυθμού μεγαλύτερου του 0.9 χρησιμοποιούνται κυρίως για εφαρμογές μαγνητικής αποθήκευσης, όπου η πυκνότητα της πληροφορίας στο μαγνητικό μέσο περιορίζεται κυρίως από το χρησιμοποιούμενο υλικό και την ταχύτητα μετάδοσης, ενώ για εφαρμογές επικοινωνίας δεδομένων, όπου η αξιοπιστία των μεταδιδόμενων δεδομένων είναι σημαντική, βάρος δίνεται στις διορθωτικές ικανότητες. Τέλος για πολύ θορυβώδεις διαύλους χρησιμοποιούνται συνήθως κώδικες με ρυθμό $1/2$ ή και μικρότερο.

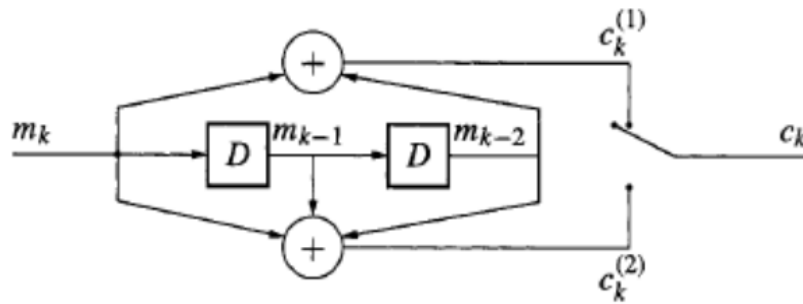
Ένα ακόμα μέγεθος που ορίζεται στους Συνελκτικούς αλγόριθμους είναι το μήκος εξαναγκασμού (constraint length) το οποίο συμβολίζεται με “ K ” και είναι ίσο με το πλήθος των στοιχείων μνήμης με πρόσθεση της μονάδας. Η φυσική σημασία του μεγέθους αυτού είναι το πλήθος των διακριτών χρονικών στιγμών που χρειάζεται ο κωδικοποιητής για να εξάγει το ψηφίο εξόδου που θα αντιστοιχεί σε ένα συγκεκριμένο ψηφίο εισόδου, θεωρώντας ότι ο χρόνος που απαιτείται από ένα ψηφίο να διέλθει μέσω ενός στοιχείου μνήμης είναι μία χρονική στιγμή.

Κάθε ακολουθία από σύμβολα $m(x)=[\dots m_{-2}, m_{-1}, m_0, m_1, m_2, m_3, m_4, \dots]$ που εισέρχεται στον κωδικοποιητή ενός συνελκτικού κώδικα μπορεί να περιγραφεί ως μία δυναμοσειρά της μεταβλητής x με τιμές σε ένα πεδίο τιμών F , π.χ. μία δυναμοσειρά Laurent, σύμφωνα με την παρακάτω σχέση:

$$m(x) = \sum_{l=-\infty}^{\infty} m_l \cdot x^l \quad (3.4.1)$$

και το πλήθος όλως των παρόμοιων τέτοιων σειρών στο πεδίο F αποτελεί ένα πεδίο που ορίζεται ως $F[[x]]$. Οπότε θα ισχύει ότι $m(x) \in F[[x]]$ και για την περίπτωση που έχουμε πολλαπλές εισόδους στον κωδικοποιητή, κάθε μία θα αποτελεί μία ακολουθία $m^{(i)}(x)$, με την τελική να εκφράζεται από την παρακάτω σχέση:

$$m(x) = [m^{(1)}(x)m^{(2)}(x)\dots m^{(i-1)}(x)m^{(i)}(x)] \in F[[x]]^i \quad (3.4.2)$$



Σχημα 3.3 - Συνελκτικός Κωδικοποιητής με ρυθμό $R = 1/2$

Σύμφωνα με τον ορισμό του ρυθμού κώδικα που έγινε παραπάνω, ένας κωδικοποιητής ο οποίος δέχεται ένα σύμβολο σαν είσοδο και παράγει δύο σύμβολα στην έξοδο, θα έχει ρυθμό κώδικα $R=1/2$. Ένας τέτοιος κωδικοποιητής παρουσιάζεται στο παραπάνω σχήμα (σχήμα 3.3). Η είσοδος $m(x)$ διέρχεται μέσω των δύο φίλτρων που μοιράζονται στοιχεία μνήμης και παράγονται οι δύο κωδικοποιημένες έξοδοι, $c_k^{(1)}$ και $c_k^{(2)}$, οι οποίες πολυπλέκονται και παράγουν την τελική έξοδο c_k . Οι $c_k^{(1)}$ και $c_k^{(2)}$ του παρακάτω κωδικοποιητή μπορούν να εκφραστούν μαθηματικώς από τις σχέσεις 3.4.3:

$$c_k^{(1)} = m_k + m_{k-2} \text{ και } c_k^{(2)} = m_k + m_{k-1} + m_{k-2} \quad (3.4.3)$$

τις οποίες μπορούμε να αναπαραστήσουμε μέσω σχέσεων συναρτήσεων μεταφοράς $g^{(1)}(x)$ και $g^{(2)}(x)$ ως εξής:

$$c_k^{(1)}(x) = g^{(1)}(x)m(x) \text{ και } c_k^{(2)}(x) = g^{(2)}(x)m(x) \quad (3.4.4)$$

και κάθε ακολουθία εισόδου και εξόδου μπορεί να αναπαρασταθεί με ένα πολυώνυμο (όπως και οι συναρτήσεις μεταφοράς), οι συντελεστές του οποίου θα ανήκουν στο πεδίο GF(q), ανάλογα με το πλήθος των bits που αντιστοιχούν σε κάθε σύμβολο της ακολουθίας εισόδου. Για καλύτερη εποπτεία των παραπάνω, θα χρησιμοποιηθεί σαν παράδειγμα ο κωδικοποιητής του παραπάνω σχήματος (σχήμα 3.3), θεωρώντας ότι η ακολουθία εισόδου είναι η $m = \{1,1,0,0,1,0,1\}$ (κάθε bit αποτελεί και ένα σύμβολο). Έτσι, η ακολουθία αυτή θα αναπαρίσταται από την σχέση 3.4.5:

$$m(x) = 1 + x + x^4 + x^6 \quad (3.4.5)$$

και οι συναρτήσεις μεταφοράς θα είναι οι:

$$g^{(1)}(x) = 1 + x^2 \text{ και } g^{(2)}(x) = 1 + x + x^2 \quad (3.4.6)$$

οπότε οι έξοδοι που προκύπτουν, σύμφωνα με τις σχέσεις 3.4.4 θα είναι:

$$\begin{aligned} c^{(1)}(x) &= g^{(1)}(x)m(x) = (1 + x^2)(1 + x + x^4 + x^6) = 1 + x + x^2 + x^3 + x^4 + x^8 \\ c^{(2)}(x) &= g^{(2)}(x)m(x) = (1 + x + x^2)(1 + x + x^4 + x^6) = 1 + x^3 + x^4 + x^5 + x^7 + x^8 \end{aligned} \quad (3.4.7)$$

και τελικά, από την παραπάνω ακολουθία εισόδου m παράγονται οι έξοδοι:

$$c^{(1)} = 1,1,1,1,1,0,0,0,1 \text{ και } c^{(2)} = 1,0,0,1,1,1,0,1,1 \quad (3.4.8)$$

Οι συναρτήσεις μεταφοράς της κάθε εξόδου του κωδικοποιητή ενός Συνελκτικού κώδικα ρυθμού $R=k/n$ μπορούν να εκφραστούν ως μία γενική συνάρτηση μεταφοράς του συστήματος μέσω ενός πίνακα $G(x)$ ⁴⁹ διαστάσεων $k \times n$, ο οποίος, αναφορικά με το παραπάνω παράδειγμα, θα είναι:

$$G(x) = [1 + x^2, 1 + x + x^2] \quad (3.4.9)$$

Στο παράδειγμα αυτό οι επιμέρους συναρτήσεις μεταφοράς είναι πολυωνυμικές. Οι

⁴⁹Ο αντίστοιχος Γεννήτορας πίνακας που αναφέρθηκε στην παράγραφο 3.2, που όμως στους Συνελκτικούς κώδικες αναφέρεται ως “πίνακας συνάρτησης μεταφοράς”.

κωδικοποιητές που έχουν αυτό το χαρακτηριστικό λέγονται FIR (Finite Impulse Response-Πεπερασμένης Κρουστικής Απόκρισης) (κατά αναλογία με τα αντίστοιχα ψηφιακά συστήματα) ή feed-forward κωδικοποιητές ενώ οι κωδικοποιητές των οποίων οι επιμέρους συναρτήσεις μεταφοράς είναι κλασματικές⁵⁰, ονομάζονται IIR (Infinite Impulse Response-Άπειρης Κρουστικής Απόκρισης) ή feedback κωδικοποιητές.

Στην παράγραφο 3.2 αναφέρθηκε η έννοια των Συστηματικών Κωδικών οι οποίοι είναι κώδικες των οποίων η είσοδος του εμφανίζεται στην έξοδο με την ίδια μορφή, όπου δείχθηκε ότι ένα τμήμα της κωδικής λέξης θα είναι η είσοδος (στην αρχή ή στο τέλος της κωδικής λέξης) και το άλλο τμήμα θα αποτελεί τα ψηφία πλεονασμού. Για να είναι ένας Συνελκτικός κώδικας Συστηματικός, θα πρέπει ο πίνακας της συνάρτησης μεταφοράς να έχει μορφή παρόμοια με της σχέσης 3.2.6, δηλαδή να είναι:

$$G(x) = [G_k I_k] \quad (3.4.10)$$

και για έναν κώδικα ρυθμού $R=2/3$ ενός feedback συστήματος θα είναι:

$$G(x) = \begin{bmatrix} 1 & 0 & \frac{x}{1+x^3} \\ 0 & 1 & \frac{x^2}{1+x^3} \end{bmatrix} \quad (3.4.11)$$

Ο κώδικας της παραπάνω σχέσης (σχέση 3.4.11) έχει κλασματικούς όρους συνάρτησης μεταφοράς και ο κωδικοποιητής του θα χαρακτηρίζεται ως IIR ή feedback κωδικοποιητής. Για κάθε τέτοιο κώδικα θα υπάρχει ο ισοδύναμος του, ένας κώδικας που θα παράγει την ίδια ακολουθία στην έξοδο για την ίδια ακολουθία εισόδου, του οποίου οι όροι θα είναι πολωνυμικοί, με την διαφορά ότι πιθανόν να μην είναι συστημικός. Για να είναι ένας κώδικας με πίνακα συνάρτησης μεταφοράς $G_2(x)$ ισοδύναμος με κάποιον άλλο, με πίνακα συνάρτησης μεταφοράς $G_1(x)$ θα πρέπει να υπάρχει πίνακας $T(x)$ ο οποίος να είναι μη αντιστρέψιμος και για τον οποίο να ισχύει η παρακάτω σχέση (σχέση 3.4.12):

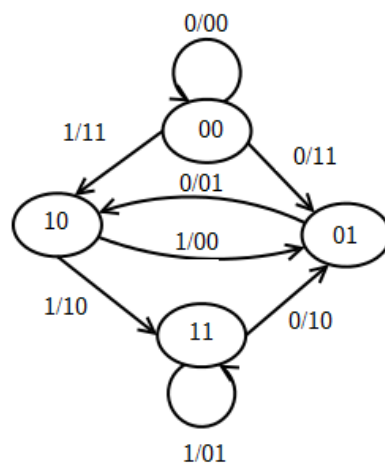
$$G_1(x) = T(x)G_2(x) \quad 3.4.12$$

Τέτοιοι ισοδύναμοι κώδικες μπορεί να υπάρχουν αρκετοί, κάτι που δίνει την

⁵⁰Ο αριθμητής και ο παρανομαστής των συναρτήσεων αυτών μεταφοράς όμως θα είναι πολωνυμικές.

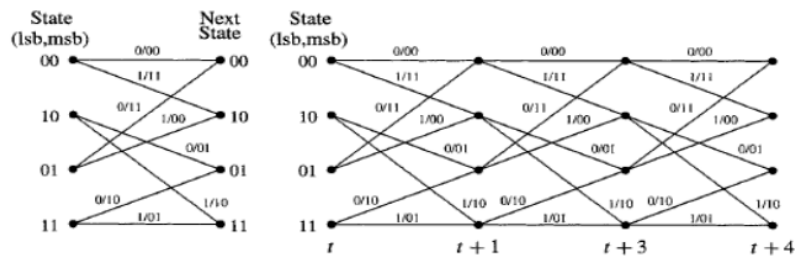
δυνατότητα στον κατασκευαστή ενός κωδικοποιητή ή αποκωδικοποιητή ενός τέτοιου συστήματος να επιλέξει τον πιο κατάλληλο για την συγκεκριμένη υλοποίηση. Παραδείγματος χάριν, μία πρώτη επιλογή θα ήταν ο κώδικας αυτός ο οποίος απαιτεί λιγότερα στοιχεία μνήμης για να απαιτείται λιγότερο υλικό για την κατασκευή του κωδικοποιητή (και του αποκωδικοποιητή).

Κάθε τέτοιος κωδικοποιητής (και αποκωδικοποιητής), μιας και υπάρχει η προαναφερθείσα αντιστοιχία των κωδικών της κατηγορίας αυτής με τα ψηφιακά συστήματα, μπορεί να χαρακτηριστεί ως μία μηχανή καταστάσεων (state machine) και ως τέτοια, μπορούν να παραχθούν τα διαγράμματα καταστάσεων, τα οποία θα αναπαριστούν τις σχέσεις μεταξύ των καταστάσεων κάποιας χρονικής στιγμής και της επόμενης. Για κωδικοποιητή με n στοιχεία μνήμης, μπορεί αν υπάρχουν 2^n πιθανές καταστάσεις και ένα τέτοιο διάγραμμα καταστάσεων, το οποίο αντιστοιχεί στον κωδικοποιητή του σχήματος 3.3 παρουσιάζεται στο παρακάτω σχήμα (σχήμα 3.4).



Σχήμα 3.4 - Διάγραμμα καταστάσεων για $G(x) = [1 + x^2, 1 + x + x^2]$

Η σύνδεση όμως μεταξύ των καταστάσεων μπορεί να αναπαρασταθεί και με χρήση γράφου. Ενώνοντας πολλούς τέτοιους γράφους, δημιουργείται ένας γράφος που ονομάζεται trellis και ο οποίος έχει την δυνατότητα της αναπαράστασης πολλών χρονικών στιγμών. Η αναπαράσταση ενός απλού γράφου και ενός trellis γράφου παρουσιάζεται στο παρακάτω σχήμα (σχήμα 3.5).



Σχήμα 3.5 - Γράφος και Trellis γράφος για $G(x) = [1 + x^2, 1 + x + x^2]$

Για την αποκωδικοποίηση των συνελκτικών κωδικών έχουν προταθεί αρκετοί αλγόριθμοι, μερικοί από τους οποίους θα αναφερθούν παρακάτω. Μεταξύ των σημαντικότερων τέτοιων αλγορίθμων είναι ο αλγόριθμος Viterbi, βασική αρχή του οποίου είναι η μεγιστοποίηση της πιθανοφάνειας της ακολουθίας⁵¹. Μια παραλλαγή αυτού του αλγορίθμου είναι ο αλγόριθμος SOVA (Soft Output Viterbi Algorithm), ο οποίος μπορεί να παρέχει και μια ένδειξη της αξιοπιστίας των αποκωδικοποιημένων συμβόλων που προκύπτουν. Ένας άλλος αλγόριθμος αποκωδικοποίησης είναι ο BCJR ο οποίος ανήκει στους MAP (Maximum A Posteriori) αλγορίθμους και ο οποίος υπολογίζει τις πιθανότητες των αποκωδικοποιημένων ψηφίων. Οι παραπάνω αλγόριθμοι είναι βέλτιστοι αλγόριθμοι. Υπάρχουν και μερικώς βέλτιστοι αλγόριθμοι αποκωδικοποίησης οι οποίοι παρουσιάζουν αρκετό ενδιαφέρον, μιας και παρουσιάζουν πολύ καλά χαρακτηριστικά απόδοσης και χαμηλών απαιτήσεων σε υπολογιστική πολυπλοκότητα και για τον λόγο αυτό θα γίνει αναφορά σε επόμενο κεφάλαιο.

Ένας από τους σημαντικότερους αλγόριθμους που χρησιμοποιούνται για την υλοποίηση συνελκτικών αποκωδικοποιητών είναι, όπως προαναφέρθηκε, ο αλγόριθμος Viterbi, ο οποίος χρησιμοποιείται σε ένα μεγάλο εύρος τηλεπικοινωνιακών εφαρμογών. Είναι βέλτιστος, όσον αφορά την μεγιστοποίηση της πιθανοφάνειας της ακολουθίας εξόδου από τα δεδομένα εισόδου και είναι ένας αλγόριθμος “συντομότερης διαδρομής”, ανάλογο με αυτόν του Dijkstra, καθώς υπολογίζει την συντομότερη διαδρομή χρησιμοποιώντας το διάγραμμα trellis του κάθε κώδικα. Σε κάθε κωδικοποιημένη ακολουθία (c_1, c_2, c_3, \dots) που παράγεται από τον κωδικοποιητή θα αντιστοιχεί μία συγκεκριμένη διαδρομή διαμέσου του

⁵¹Ως συνάρτηση πιθανοφάνειας ενός τυχαίου δείγματος X από τον πληθυσμό $(X, f(x; \theta), \theta = (\theta_1, \theta_2, \theta_3, \theta_4, \dots, \theta_m) \in \Theta)$ ορίζεται η ποσότητα $L(\theta) = \prod_{i=1}^n f(x_i; \theta)$, $\theta \in \Theta$, η οποία εκφράζει το πόσο πιθανοφανείς, ή διαφορετικά, πόσο σύμφωνες με το συγκεκριμένο δείγμα $X=x$ είναι οι διάφορες τιμές της παραμέτρου θ και στην περίπτωση του αλγορίθμου Viterbi χρησιμοποιείται ορίζοντας ως X την ακολουθία εισόδου και ως θ την ακολουθία εξόδου.

διαγράμματος trellis του κωδικοποιητή. Η ακολουθία όμως που θα λάβει ο δέκτης, εξαιτίας των φαινομένων θορύβου, θα είναι παραμορφωμένη και δεν θα αντιστοιχεί ακριβώς σε κάποιο μονοπάτι στο trellis διάγραμμα. Ο αλγόριθμος Viterbi θα υπολογίσει όλα τα πιθανά μονοπάτια του διαγράμματος trellis και θα επιλέξει αυτό που είναι κοντινότερο στην ληφθείσα ακολουθία σύμφωνα με την συνάρτηση πιθανότητας που χρησιμοποιείται από το εκάστοτε μοντέλο καναλιού, με την συνάρτηση αυτή, για την περίπτωση καναλιού με προσθετικό θόρυβο, να είναι η ευκλείδεια απόσταση. Όσο μεγαλύτερη είναι η ληφθείσα ακολουθία, τόσο καλύτερα θα είναι τα αποτελέσματα που θα δίνει ο αλγόριθμος αυτός. Η συνάρτηση πιθανοφάνειας που καλείται ο αλγόριθμος να μεγιστοποιήσει ονομάζεται $f(r|x)$ και εκφράζεται από την σχέση:

$$f(r | x) = f(r_0^{L-1} | x_0^{L-1}) = f(r_0, r_1, r_2, \dots, r_{L-1} | x_0, x_1, x_2, \dots, x_{L-1})$$

$$= \prod_{t=0}^{L-1} f(r_t | x_t) \quad (3.4.13)$$

όπου με r συμβολίζεται η ακολουθία που έλαβε ο αποκωδικοποιητής και με x τα σύμβολα εισόδου του κωδικοποιητή. Κάθε φορά υπολογίζεται το μονοπάτι του trellis διαγράμματος το οποίο μεγιστοποιεί την συνάρτηση αυτή και είναι και το συντομότερο, και αποθηκεύεται στην μνήμη του αποκωδικοποιητή.

Η πολυπλοκότητα του αλγορίθμου αυτού αυξάνεται εκθετικά συναρτήσει του πλήθους των καταστάσεων. Ακόμα, το όριο πιθανότητας για την κωδικοποίηση καναλιού στους κώδικες αυτούς προβλέπει ότι για η βελτιστοποίηση της απόδοσης τους επιτυγχάνεται με την αύξηση της μνήμης. Και αφού το πλήθος των καταστάσεων είναι ανάλογο με τις διαθέσιμες μνήμες του κυκλώματος, έπεται ότι η πολυπλοκότητα του αλγορίθμου είναι ανάλογη με την πολυπλοκότητα του κυκλώματος. Οπότε, κατά την σχεδίαση του αλγορίθμου πρέπει να γίνουν κάποιοι συμβιβασμοί και δεν είναι πάντα εφικτό να επιτευχθεί το επιθυμητό επίπεδο απόδοσης γιατί θα απαιτεί το κύκλωμα του αποκωδικοποιητή να έχει πολύ μνήμη, κάτι που αυξάνει και το κόστος υλικού αλλά και τον απαιτούμενο χρόνο για την ολοκλήρωση των υπολογισμών, το πλήθος των οποίων, στον αλγόριθμο Viterbi, είναι ανεξάρτητο από το επίπεδο θορύβου. Για τους λόγους αυτούς, αν και ο αλγόριθμος αυτός είναι βέλτιστος, έχουν αναπτυχθεί και χρησιμοποιούνται σε πολλές εφαρμογές αλγόριθμοι οι οποίοι, αν και δεν είναι βέλτιστοι, έχουν μικρότερη πολυπλοκότητα υλικού και απαιτούν λιγότερες πράξεις, ανάλογα με το επίπεδο του θορύβου. Οι αλγόριθμοι αυτοί υπερέχουν στην απλότητα και την

ταχύτητα αλλά είναι υποδεέστεροι στην απόδοση, μιας και δεν καταλήγουν πάντα στην μέγιστη δυνατή τιμή της συνάρτησης πιθανοφάνειας. Οι κώδικες των αλγορίθμων αυτών χρησιμοποιούν διαγράμματα δέντρων για την αναπαράσταση τους και κάθε φορά επιλέγεται το ανάλογο μονοπάτι-κλαδί, ανάλογα με την απόφαση που παίρνεται για κάθε σύμβολο, σύμφωνα με κάποιες συναρτήσεις που χρησιμοποιούν για την μέτρηση της πιθανοφάνειας ώστε να είναι σε θέση να καταλήξουν στο βέλτιστο μονοπάτι.

Ένας τέτοιος αλγόριθμος είναι ο αλγόριθμος Z-J, ο οποίος δημιουργήθηκε από τους A.J. Viterbi και K. Zigangirov. Η λειτουργία του βασίζεται στην χρήση μίας λίστας στην οποία αποθηκεύονται όλα τα μερικά μονοπάτια, η οποία είναι ταξινομημένη έτσι ώστε το μονοπάτι που βελτιστοποιεί την συνάρτηση πιθανοφάνειας να είναι στην κορυφή της (φθίνουσα σειρά). Σε κάθε βήμα του αλγορίθμου, εξετάζεται το μονοπάτι που βρίσκεται στην κορυφή και υπολογίζονται για τα 2^k μονοπάτια που προκύπτουν από αυτό (απόγονοι) η τιμή της συνάρτησης πιθανοφάνειας. Στην συνέχεια τα μονοπάτια αυτά τοποθετούνται στην λίστα με φθίνουσα σειρά (όπως και τα προηγούμενα μονοπάτια που ήταν αποθηκευμένα στην λίστα) και συνεχίζει η εκτέλεση του αλγορίθμου με την επόμενο βήμα, επαναλαμβάνοντας την παραπάνω διαδικασία μέχρι να φθάσει σε κάποιον κόμβο (φύλλο στο διάγραμμα δέντρου) και να τερματίσει ο αλγόριθμος.

Ένας άλλος αλγόριθμος που ανήκει στην κατηγορία αυτή είναι ο αλγόριθμος του Fano. Η διαφορά με τον προηγούμενο είναι ότι η λίστα που χρησιμοποιεί αυτός δεν περιέχει όλα τα πιθανά μονοπάτια αλλά μόνο ένα κάθε φορά, διατηρώντας μία τιμή κατωφλίου, T . Για να προχωρήσει στο δέντρο, πρέπει η τιμή της συνάρτησης να αυξάνεται. Αν σε κάποιο μονοπάτι η τιμή της συνάρτησης είναι μικρότερη της τιμής κατωφλίου T , τότε ο αλγόριθμος επιστρέφει στον προηγούμενο κόμβο και υπολογίζει εκ νέου την τιμή της συνάρτησης. Οπότε είναι ένας αλγόριθμος λογικής depth-first⁵².

Τέλος, μία παραλλαγή του αλγορίθμου Viterbi είναι ο αλγόριθμος M (SOMA-Soft Output M-Algorithm). Ο αλγόριθμος αυτός διατηρεί σε λίστα M μονοπάτια και σε κάθε βήμα το πλήθος των μονοπατιών γίνεται $M \cdot 2^k$ μονοπάτια, όπου k το πλήθος των ψηφίων εισόδου, υπολογίζει την τιμή της συνάρτησης όπως και στον αλγόριθμο Viterbi και τα M καλύτερα μονοπάτια τοποθετούνται στην λίστα για το επόμενο βήμα, κρατώντας στο τέλος ως βέλτιστο μονοπάτι εκείνο με την καλύτερη τιμή. Οπότε, ενώ στον αλγόριθμο Viterbi κάθε φορά

⁵²Οι αλγόριθμοι λογικής depth-first search (αναζήτηση κατά βάθος) πραγματοποιούν την διάσχιση ή αναζήτηση της διαδρομής ή μονοπατιού σε ένα διάγραμμα δέντρου ή σε ένα γράφημα ξεκινώντας από την ρίζα και εξερευνούν όσο το δυνατόν περισσότερο κατά μήκος κάθε κλαδί του δέντρου μέχρι να φθάσουν σε αδιέξοδο.

υπολογίζονται όλα τα πιθανά μονοπάτια, στον M αλγόριθμο υπολογίζονται μόνο τα μονοπάτια που αντιστοιχούν στα M καλύτερα μονοπάτια του κάθε βήματος, καθιστώντας τον αλγόριθμο αυτό ταχύτερο από τον Viterbi.

3.5 - Κώδικες τούρμπο

Όπως αναφέρθηκε στην αρχή του παρόντος κεφαλαίου, η κωδικοποίηση καναλιού (ή κωδικοποίηση διαύλου) είναι από τα σημαντικότερα εργαλεία για την αύξηση της αποδοτικότητας και της αποτελεσματικότητας της επικοινωνίας των σύγχρονων συστημάτων επικοινωνιών, οι οποίες μειώνονται λόγω των περιορισμών της ισχύος και του διαθέσιμου εύρους ζώνης των συστημάτων αυτών. Οπότε, το ζητούμενο είναι η επίτευξη μεγάλου κέρδους κωδικοποίησης για συγκεκριμένη απόδοση φάσματος, το οποίο, σύμφωνα με τον Shannon μπορεί να επιτευχθεί κωδικοποιώντας την ακολουθία δεδομένων σε μεγάλα κομμάτια (Μπλοκς-Blocks), ο οποίος όρισε ότι το μέγιστο δυνατό κέρδος κωδικοποίησης για δεδομένο ρυθμό και μεγέθους block περιορίζεται από το όριο της μέγιστης χωρητικότητας καναλιού, όπως αναφέρθηκε και στο πρώτο κεφάλαιο της παρούσας εργασίας (σχέση 3.2.4). Αυτός είναι και ο στόχος του σχεδιασμού των κωδικών που αναφέρθηκαν παραπάνω, όπως και των κωδικών turbo.

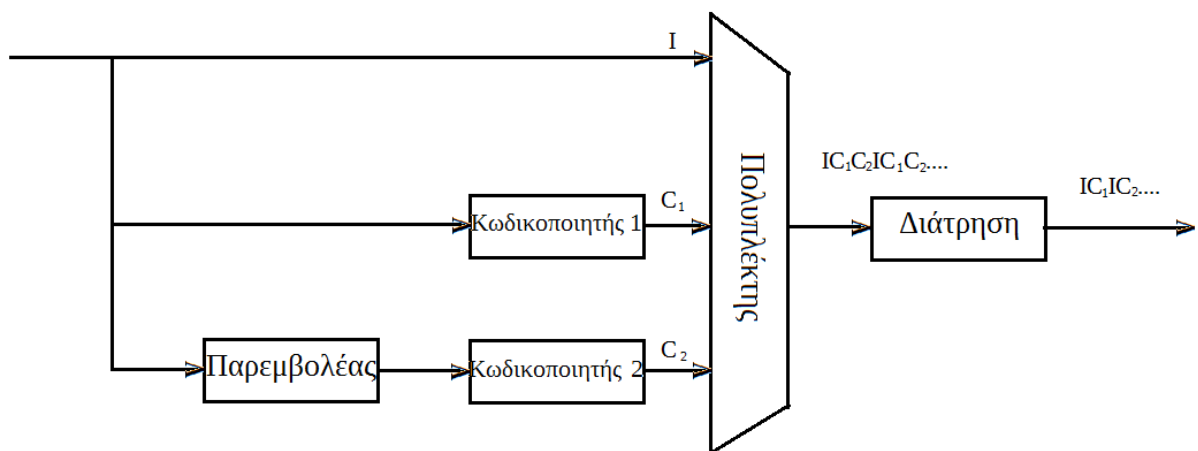
Οι κώδικες turbo άρχισαν να αναπτύσσονται το 1990-1991 και η πρώτη εργασία που παρουσίαζε το συγκεκριμένο είδος κωδικών εκδόθηκε το 1993⁵³ από τους Calude Berrou⁵⁴, Alain Glavieux και Punya Thitimajshima. Οι κώδικες αυτοί έφεραν “επανάσταση” στην θεωρία Πληροφοριών και στις τεχνικές κωδικοποίησης καναλιού, εισάγοντας μία καινοτόμα προσέγγιση στην δυνατότητα διόρθωσης λαθών, η οποία μπορούσε να παρέχει επικοινωνία με πολύ μικρή πιθανότητα σφάλματος μετάδοσης των δεδομένων, και μάλιστα σε ρυθμούς μετάδοσης δεδομένων και απόδοσης μεταδιδόμενης ισχύος πολύ μεγαλύτερους από αυτούς που μπορούσαν να υποστηρίξουν οι υπάρχοντες κώδικες, προσεγγίζοντας τα απόλυτα όρια απόδοσης. Όπως και στις κατηγορίες κωδικών που παρουσιάστηκαν παραπάνω, έτσι και στους turbo κώδικες οι παραλλαγές τους είναι πολλές, ανάλογα με την εφαρμογή για την οποία προορίζονται. Για όποια όμως εφαρμογή και αν προορίζονται, όλες οι υλοποιήσεις

⁵³Τίτλος εργασίας: “Near Shannon Limit Error-correcting Coding and Decoding: Turbo-Codes”.

⁵⁴Ο οποίος στις 23 Απριλίου 1991 κατοχύρωσε την πατέντα των turbo κωδικών ως ο μοναδικός εφευρέτης τους.

turbo κωδικοποιητών και αποκωδικοποιητών θα στηρίζονται σε μία διαδικασία η οποία είναι μία παραλλαγή της συνελκτικής κωδικοποίησης γνωστή ως επαναληπτική συστηματική συνελκτική κωδικοποίηση RSC (Recursive Systematic Convolutional). Για τον λόγο αυτό, και για την αρτιότερη παρουσίαση τους, στην παράγραφο αυτή θα γίνει αναφορά σε μία απλή περίπτωση κωδικοποιητή -αποκωδικοποιητή και στο επόμενο κεφάλαιο θα αναφερθούν συγκεκριμένες εφαρμογές στις οποίες χρησιμοποιούνται οι κώδικες αυτοί.

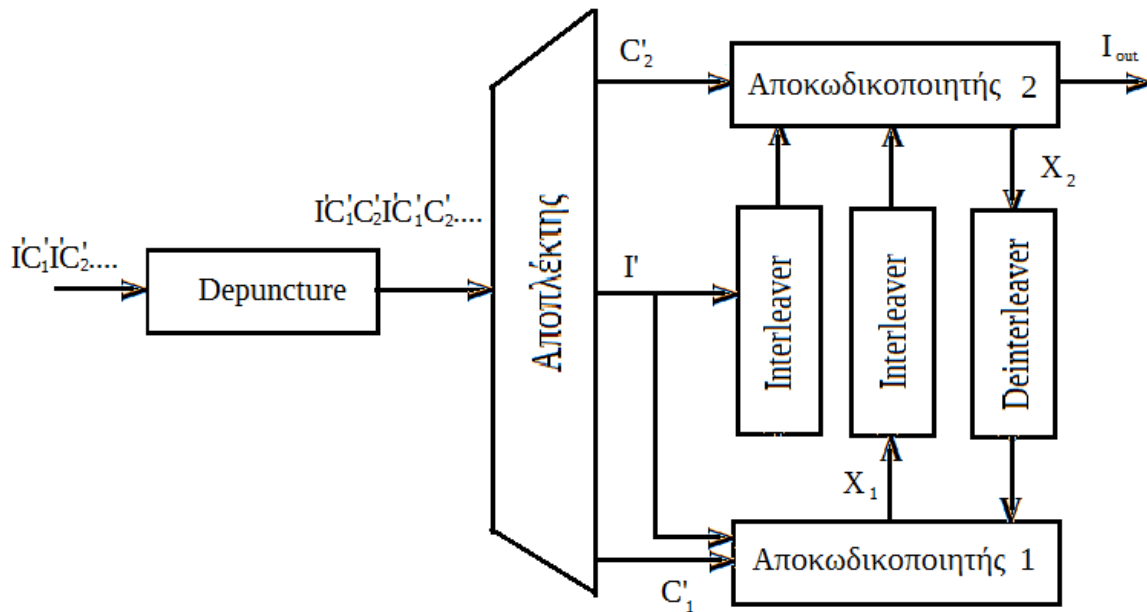
Ένα παράδειγμα γενικού διαγράμματος turbo κωδικοποιητή απεικονίζεται στο παρακάτω σχήμα (σχήμα 3.6) . Ο κωδικοποιητής αυτός, που αποτελείται από δύο όμοιους κωδικοποιητές, από τους οποίους, ο πρώτος (κωδικοποιητής 1) δέχεται σαν είσοδο του την ακολουθία I των ψηφίων δεδομένων εισόδου του turbo κωδικοποιητή και για κάθε ψηφίο της I παράγει ένα ψηφίο ελέγχου (check bit), C_1 . Το ίδιο κάνει και ο κωδικοποιητής 2, ο οποίος όμως δέχεται την ακολουθία των ψηφίων εισόδου I με διαφορετική διάταξη των ψηφίων στο χρόνο, η οποία επιτυγχάνεται με χρήση του “Παρεμβολέα” (Interleaver), και για κάθε ψηφίο που δέχεται ως είσοδο παράγει ένα ψηφίο ελέγχου, C_2 . Η έξοδος του κάθε αποκωδικοποιητή, στην συνέχεια, πολυπλέκεται, μέσω του “Πολυπλέκτη”, με τα ψηφία εισόδου I , οπότε θα παραχθεί, για κάθε ψηφίο εισόδου I_i , η ακολουθία $I_i C_{i,1} C_{i,2}$. Έτσι, η ακολουθία αυτή θα έχει ρυθμό κωδικοποίησης $1/3$. Όμως, μετά τον πολυπλέκτη και πριν την έξοδο του turbo κωδικοποιητή παρεμβάλλεται ένα κύκλωμα, το οποίο αλλάζει την ακολουθία εξόδου του πολυπλέκτη, επιλέγοντας μόνο τα μισά ψηφία ελέγχου, επιτυγχάνοντας ρυθμό κωδικοποίησης $1/2$. Η διαδικασία αυτή ονομάζεται “διάτρηση” (puncturing) και η τελική ακολουθία εξόδου του turbo κωδικοποιητή μπορεί να είναι $I_1 C_{1,1} I_2 C_{2,2} I_3 C_{3,1} I_4 C_{4,2} \dots$, όπου το $C_{3,1}$ είναι το ψηφίο ελέγχου που παράχθηκε από τον κωδικοποιητή 1 για το ψηφίο I_3 και το $C_{4,2}$ το ψηφίο ελέγχου του δεύτερου κωδικοποιητή για το I_4 .



Σχήμα 3.6 - Turbo Κωδικοποιητής

Στον αποκωδικοποιητή λαμβάνει χώρα η αντίστροφη διαδικασία. Ένα γενικό διάγραμμα ενός turbo αποκωδικοποιητή παρουσιάζεται στο παρακάτω σχήμα (σχήμα 3.7). Τα λαμβανόμενα δεδομένα, $I'_1C'_{1,1}I'_2C'_{2,2}I'_3C'_{3,3}I'_4C'_{4,2} \dots$, υπόκεινται σε μία διεργασία αντίστροφης της διάτρησης, την *departuring*, τα δεδομένα εξόδου της οποίας θα είναι η ακολουθία εισόδου της με την προσθήκη των υπολειπόμενων ψηφίων ελέγχου, είτε με μία διαδικασία εκτίμησης είτε θέτοντας την τιμή του ίση με “0”. Έτσι, για κάθε ψηφίο εισόδου I'_i , μετά την αντίστροφη διάτρηση, εξάγονται τρία ψηφία, τα $I'_iC'_{i,1}C'_{i,2}$. Τα ψηφία αυτά αποπλέκονται μέσω του “αποπλέκτη”. Ο πρώτος αποκωδικοποιητής, “αποκωδικοποιητής 1”, δέχεται ως είσοδο το ψηφίο ελέγχου $C'_{i,1}$ και παράγει το ψηφίο διόρθωσης $X_{i,1}$. Το ψηφίο αυτό, μαζί με το ψηφίο εισόδου I'_i , τροφοδοτούνται, μέσω παρεμβολέων, ώστε να πραγματοποιηθεί η αντίστοιχη αναδιάταξη ψηφίων που πραγματοποιήθηκε στον turbo κωδικοποιητή, στον αποκωδικοποιητή 2, ο οποίος, συνδυάζοντας τα με το ψηφίο ελέγχου $C'_{i,2}$ παράγει το ψηφίο διόρθωσης $X_{i,2}$. Το ψηφίο αυτό τροφοδοτείται στον αποκωδικοποιητή 1, αφού πραγματοποιηθεί η αντίστροφη διεργασία αναδιάταξης (*Deinterleaving*), και μετά από κάποιες επαναλήψεις παράγεται το τελικό ψηφίο εξόδου, $I_{i,out}$.

Το παραπάνω παράδειγμα αποτελεί ένα γενικό παράδειγμα εφαρμογής των κωδικών turbo. Περιέχει όλα τα κύρια χαρακτηριστικά της λειτουργίας των κωδικών turbo, με σημαντικότερο να είναι η επαναληπτική αποκωδικοποίηση, χαρακτηριστικό που προσδίδει στους κώδικες turbo την υψηλή απόδοση και την μεγάλη ικανότητα για διόρθωση των τυχόν λανθασμένων ψηφίων. Στο επόμενο κεφάλαιο θα γίνει εκτενέστερη αναφορά στο είδος αυτό, όπου, μετά από μία συνοπτική ιστορική αναδρομή, θα γίνει αναφορά σε συγκεκριμένες εφαρμογές, οι οποίες αποτελούν τις πιο σύγχρονες εφαρμογές των κωδικών αυτών σε τηλεπικοινωνιακά συστήματα.



Σχήμα 3.7 - Turbo Αποκωδικοποιητής

Κεφάλαιο 4

Στο προηγούμενο κεφάλαιο έγινε μία σύντομη περιγραφή των turbo κωδικών. Στο παρόν κεφάλαιο θα γίνει εκτενέστερη περιγραφή του είδους αυτού των κωδικών με αναφορά σε εφαρμογές στις οποίες χρησιμοποιούνται, αφού προηγηθεί μία σύντομη ιστορική αναδρομή στην εξέλιξη των κωδικών αυτών.

4.1 – Ιστορία των turbo κωδικών

Όπως αναφέρθηκε παραπάνω, η κωδικοποίηση διαύλου (ή καναλιού) είναι από τους κυριότερους τομείς που εξελίσσονται για την μείωση των σφαλμάτων των δεδομένων που μεταδίδονται μέσω ενός τηλεπικοινωνιακού δικτύου. Και ειδικά η ανάπτυξη μεθόδων διόρθωσης λανθασμένων ψηφίων αποτελεί έναν από τους βασικούς τομείς ανάπτυξης της θεωρίας Πληροφοριών, κλάδος που θεωρείται ότι άρχισε να αναπτύσσεται μετά το 1948, με την εισαγωγή της από τον Claude E. Shannon. Μέχρι τα πρώτα χρόνια της δεκαετίας του 1950, οι περισσότεροι ερευνητές προσανατολιζόνταν στο να δημιουργηθεί ένα καλό

θεωρητικό υπόβαθρο και του κλάδου της θεωρίας Πληροφορίας αλλά και στην δημιουργία του απαραίτητου μαθηματικού υποβάθρου για την δημιουργία κωδικών με αυξημένη ικανότητα διόρθωσης λαθών. Στην επόμενη δεκαετία, αναπτύχθηκαν αρκετοί τέτοιοι κώδικες, και στην δεκαετία του 1970 σχεδιάστηκαν πολλές οικογένειες (ή κατηγορίες) κωδικών μεγάλου μήκους, οι οποίοι είχαν βελτιωμένα χαρακτηριστικά απόδοσης από τους ήδη υπάρχοντες, κάποιες από τις οποίες αναφέρθηκαν στο προηγούμενο κεφάλαιο. Τέλος, στην δεκαετία του 1980 έλαβαν χώρα πολλές υλοποιήσεις των παραπάνω κατηγοριών, περνώντας από την θεωρητική ενασχόληση με τους κώδικες αυτούς στην πρακτική τους εφαρμογή.

Ανάλογα με την εφαρμογή, σχεδιάστηκαν αρκετοί κωδικοποιητές και αποκωδικοποιητές, οι οποίοι υλοποιούσαν κάποια από τις κατηγορίες κωδικών που είχαν ήδη σχεδιαστεί. Πολλοί από τους κώδικες που υλοποιήθηκαν εξελίχθηκαν ανάλογα με την εφαρμογή, έτσι ώστε να επιτευχθεί η βέλτιστη υλοποίηση τους για την συγκεκριμένη εφαρμογή. Οι κύριοι στόχοι ήταν:

- Η επίτευξη καλύτερου κέρδους κωδικοποίησης
- Η μείωση της πολυπλοκότητας της αποκωδικοποίησης και
- Η ικανότητα της υποστήριξης διαφόρων τηλεπικοινωνιακών τεχνολογιών ή η ικανότητα συνεργασίας τέτοιων τεχνολογιών.

Βασικότερος όμως όλων των στόχων της ανάπτυξης νέων τηλεπικοινωνιακών συστημάτων είναι η ικανότητα αυτών να λειτουργούν όσο πιο κοντά γίνεται στο θεωρητικό όριο του Shannon που αναφέρθηκε σε προηγούμενο κεφάλαιο. Κάποιες από τις κατηγορίες κωδικών που είχαν πολύ καλά αποτελέσματα ήταν οι block Κώδικες, οι κώδικες Hamming, οι Συνελικτικοί κώδικες και ο αλγόριθμος Viterbi, και άλλοι. Η “επανάσταση” στην θεωρία Πληροφορίας έγινε στις αρχές της δεκαετίας του 1990, με την αρχή της ανάπτυξης και του σχεδιασμού των κωδικών turbo, και συγκεκριμένα το 1993, χρονιά που δημοσιεύθηκε η εργασία των Claude Berrou, Alain Glavieux και Punya Thitimajshima, στην οποία παρουσιάστηκε για πρώτη φορά η εφεύρεση μίας καινοτόμου μεθόδου κωδικοποίησης με αυξημένη ικανότητα ελέγχου λαθών. Η μέθοδος αυτή είχε την ικανότητα να παρέχει πρακτικώς επικοινωνία χωρίς λάθη ή να εξασφαλίζει πολύ βελτιωμένο κέρδος κωδικοποίησης, συγκριτικά με τους ήδη υπάρχοντες κώδικες. Για τον λόγο αυτό, η μέθοδος αυτή ενέπνευσε τον σχεδιασμό πολλών παρόμοιων μεθόδων, πολλές από τις οποίες έχουν εξέχοντα ρόλο στα σύγχρονα τηλεπικοινωνιακά συστήματα, όπως θα δειχθεί στις επόμενες παραγράφους όπου θα παρουσιαστούν κάποιες από τις εφαρμογές των κωδικών turbo.

Οι τρεις επιστήμονες που εισήγαγαν τους κώδικες turbo, άρχισαν να εργάζονται πάνω στον Soft-Output Viterbi αλγόριθμο (SOVA), έναν αλγόριθμο που στηριζόταν στις εργασίες του G. Battail⁵⁵ του 1987 και των J. Hagenauer και P. Hoeher⁵⁶ του 1989, οι οποίες εργασίες στηρίζονταν στις προγενέστερες εργασίες των A.J. Viterbi⁵⁷, και G.D. Forney⁵⁸. Ο αρχικός τους προσανατολισμός ήταν η κυκλωματική υλοποίηση του SOVA με χρήση της τεχνολογίας MOS τρανζίστορ, με τον απλούστερο δυνατό τρόπο. Κατά την διάρκεια των εργασιών τους, παρατήρησαν ότι ο αλγόριθμος SOVA μπορούσε να θεωρηθεί ως ένας ενισχυτής του λόγου σήματος προς θόρυβο (SNR). Αυτό θα μπορούσε να θεωρηθεί και ως η γένεση της ιδέας των turbo κωδικών, μιας και αποτέλεσε το έναυσμα για την χρήση τεχνικών ανάδρασης, που χρησιμοποιούν κατά κόρον οι ενισχυτές, σε μία μέθοδο κωδικοποίησης καναλιού. Για την διερεύνηση της σημασίας της παραπάνω ιδέας, εξέλιξαν τον παραπάνω ενισχυτή, ή την δική τους έκδοση του SOVA, έτσι ώστε να επιτύχουν μεγάλο κέρδος, βασιζόμενοι στην ιδέα της επαναληπτικής κωδικοποίησης. Τα πρώτα πειράματα υλοποιούσαν μία σειριακή αλληλουχία δύο συνελκτικών κωδικών και στην συνέχεια επικεντρώθηκαν στην παράλληλη σύνδεση τέτοιων συστημάτων. Αναφορικά με την αποκωδικοποίηση, δύο παράλληλοι αποκωδικοποιητές που θα λειτουργούν με το ίδιο ρολόι συμπίπτει με την υλοποίηση παράλληλων κυκλωμάτων και τον διαμοιρασμό στα παράλληλα αυτά κυκλώματα του σήματος ρολογιού. Μία τέτοια παράλληλη σύνδεση θα έχει νόημα μόνο όταν ο κώδικας που υλοποιείται είναι συστηματικός και για τον λόγο αυτό τελικά χρησιμοποιήθηκαν επαναληπτικοί συστηματικοί συνελκτικοί κώδικες.

Την εποχή που άρχισαν να θεμελιώνονται οι κώδικες turbo (1989), ο Punya Thitimajshima, ο οποίος ήταν υποψήφιος διδάκτορας, άρχισε να συνεργάζεται με τους άλλους δύο επιστήμονες. Το αντικείμενο της δικής του έρευνας αφορούσε την ανάλυση των ιδιοτήτων της απόστασης και της πιθανότητας λάθους των RPSC⁵⁹ κωδικών και της δυνατότητας αυτών σε παράλληλη ή σειριακή σύνδεση αλληλουχίας. Έτσι, άρχισε η

⁵⁵G. Battail, "Pondération des symboles d'écodés par l'algorithme de Viterbi" (στα Γαλλικά), Ann. T'el'ecommun., Fr., 42, N 1-2, pp. 31-38, Ιανουάριος 1987

⁵⁶J. Hagenauer and P. Hoeher, "A Viterbi algorithm with soft-decision outputs and its applications", Proc. of Globecom '89, Dallas, Texas, pp. 47.11-47.17, Νοέμβριος 1989.

⁵⁷A. J. Viterbi, "Convolutional codes and their performance in communication systems," IEEE Trans. Com. Technology, vol. COM-19, No. 15, pp. 751-772, Οκτώβριος 1971

⁵⁸G. D. Forney, "The Viterbi algorithm," Proc. IEEE, vol. 61, N 3, pp. 268-278, Μάρτιος 1973.

⁵⁹**Recursive Punctured Systematic Convolutional** : Επαναληπτικών Συστηματικών Συνελκτικών κωδικών με χρήση της διάρτησης που αναφέρθηκε στο προηγούμενο κεφάλαιο

κατασκευή των πρώτων turbo κωδικών, η οποία, για την αντιμετώπιση των προβλημάτων που παρουσιάζονταν, ειδικά αναφορικά με την στάθμιση των συστημάτων, ο SOVA αντικαταστάθηκε τελικά από τον αλγόριθμο Bahl-Cocke-Jelinek-Raviv⁶⁰ (BCJR). Το πρώτο πείραμα με το νέο αυτό είδος κωδικών πραγματοποιήθηκε το 1991, και με την θεμελίωση κάποιων ήδη γνωστών τεχνικών όρων, όπως είναι η εξωτερική πληροφορία, η επαναληπτική αποκωδικοποίηση, οι αναδρομικοί συστηματικοί συνελκτικοί κώδικες, η παράλληλη αλληλουχία συστημάτων και η μη κανονική παρεμβολή (non-regular interleaving), η δημιουργία των turbo κωδικών αποτελούσε πλέον γεγονός.

Εκτός της εργασίας του 1993 που προαναφέρθηκε, δύο είναι οι σημαντικότερες δημοσιεύσεις που αφορούν τους κώδικες turbo, οι οποίες δημοσιεύθηκαν μετά το 1993. Η πρώτη είναι ένα κομμάτι της διατριβής του Punya Thitimajshima⁶¹, που παρουσιάστηκε από τον ίδιο στο συνέδριο της IEEE, Globecom το 1995, με τίτλο “Recursive Systematic Convolutional codes and application”⁶² (Αναδρομικοί Συστηματικοί κώδικες και εφαρμογές). Έναν χρόνο μετά, τον Οκτώβριο του 1996, οι Claude Berrou and Alain Glavieux δημοσίευσαν ένα άρθρο στο “Transactions on Communications” της IEEE, με τίτλο “Near optimum error correcting coding and decoding: turbo-codes”⁶³ (σχεδόν βέλτιστης διόρθωσης σφαλμάτων κωδικοποίηση και αποκωδικοποίηση: κώδικες turbo).

Όπως αναφέρθηκε και παραπάνω, μετά την παρουσίαση τους το 1993, οι κώδικες turbo έχουν κεντρίσει το ενδιαφέρον πολλών ερευνητών, με αποτέλεσμα να δημιουργούνται συνεχώς νέοι τεχνολογικοί τομείς έρευνας και να εφευρίσκονται νέοι τρόποι βελτίωσης της απόδοσης τους. Επιπροσθέτως, η ιδέα στην οποία στηρίζονται οι κώδικες αυτοί συνδυάζονται με άλλες τεχνολογίες επικοινωνιών έτσι ώστε να βελτιώνεται η απόδοση των συστημάτων που χρησιμοποιούνται. Μερικά τέτοια παραδείγματα είναι:

- Turbo μπλοκ κώδικες: Οι μπλοκ κώδικες είχαν ήδη αναπτυχθεί όταν πρωτοπαρουσιάστηκαν οι κώδικες turbo. Έτσι, δημιουργήθηκε ένα νέο είδος επαναληπτικών

⁶⁰L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate,” IEEE Trans. Inform. Theory, IT-20, pp. 248-287, Μάρτιος 1974.

⁶¹Ο τίτλος της διατριβής του είναι: “Les codes Convolutifs Rkursifs Systmatiques et leur application la concatenation parallele”, και κατατέθηκε στο l’Universit de Bretagne Occidentale (UBO).

⁶²Punya Thitimajshima, “Recursive Systematic Convolutional codes and application to parallel concatenation,” IEEE Globecom’95, Singapore, pp.2267-2272.

⁶³Claude Berrou and Alain Glavieux, “Near optimum error correcting coding and decoding: turbo-codes,” IEEE Transactions on Communications, vol.11, no.10, Οκτώβριος 1996.

αλγορίθμων αποκωδικοποίησης για τους μπλοκ κώδικες το οποίο βασιζόταν στην soft⁶⁴ αποκωδικοποίηση και την soft απόφαση για την στάθμη των δεδομένων εξόδου των συνισταμένων κωδικών. Έτσι, δημιουργήθηκε μία νέα γενιά μεθόδων κωδικοποίησης με υψηλότερο ρυθμό κώδικα.

- Turbo Εξισορρόπηση: Μία άλλη πολύ σημαντική επίδραση που είχαν οι κώδικες turbo σε υπάρχουσες τεχνολογίες ήταν η χρήση τους στην εξισορρόπηση καναλιού (channel equalization). Στην ουσία αποτελεί μία επαναληπτική τεχνική η οποία εμφανίζει πολύ καλή απόδοση για εφαρμογές επικοινωνιών μέσω καναλιών που έχουν έντονο το φαινόμενο της διασυμβολικής παρεμβολής (ISI – Inter Symbol Interference), όπως είναι το ασύρματο κανάλι πολλαπλών διαδρομών που χρησιμοποιούν τα συστήματα ασύρματων επικοινωνιών και άλλα κανάλια που χρησιμοποιούν τα διάφορα συστήματα, τα οποία είναι περιορισμένου εύρους ζώνης συχνοτήτων.
- Κώδικες turbo για πολλαπλά επίπεδα ή turbo trellis κωδικοποιημένη διαμόρφωση (TTCM): Οι κώδικες turbo συνδυάζονται με διαμορφώσεις υψηλής φασματικής απόδοσης ή σηματοδότησης υψηλότερης τάξης (όχι δυαδικής) για την επίτευξη των παραπάνω στόχων και το αποτέλεσμα αυτού του συνδυασμού είναι η διαμόρφωση TTCM.
- Εφαρμογή των κωδικών turbo στα συστήματα πολλαπλών κεραιών για την βελτίωση του ρυθμού μετάδοσης δεδομένων καθώς και της αξιοπιστίας της επικοινωνίας μέσω των καναλιών που χρησιμοποιούν οι ασύρματες επικοινωνίες, τα οποία προκαλούν έντονα το φαινόμενο των αποσβέσεων στο μεταδιδόμενο σήμα.
- Κώδικες LDPC (Low Density Parity Check): Οι κώδικες LDPC που αναφέρθηκαν στο προηγούμενο κεφάλαιο, εφευρέθηκαν το 1962. Όμως, κατά την εποχή που αναπτύσσονταν οι κώδικες turbo, οι LDPC είχαν σχεδόν εγκαταλειφθεί. Οι ερευνητές που ασχολούνταν με τους κώδικες turbo άρχισαν να ερευνούν και τους LDPC κώδικες, εξελίσσοντας την μέθοδο κωδικοποίησης που χρησιμοποιούσαν αυτοί, με την βοήθεια των

⁶⁴Με τον όρο “soft” αναφέρονται οι κώδικες και οι αλγόριθμοι οι οποίοι, αναφορικά με την αποκωδικοποίηση, δεν καθορίζουν απόλυτα τα ψηφία που αποκωδικοποιούν, παρέχοντας στο σύστημα μεγαλύτερη ευελιξία αναφορικά με την ανίχνευση και διόρθωση λαθών, σε αντίθεση με τους αποκωδικοποιητές των οποίων η απόφαση για τα ψηφία που αποκωδικοποιούν είναι απόλυτη (hard). Οι hard-decision αποκωδικοποιητές δίνουν ως έξοδο την “απόφαση” τους αναφορικά με το ποιο ψηφίο αποκωδικοποίησαν, και στους δυαδικούς αποκωδικοποιητές θα έχει τιμή “0” ή “1”, ενώ οι soft-decision θα μπορούν να χρησιμοποιούν λαμβανόμενα δεδομένα τιμών μεταξύ αυτών, αντλώντας πληροφορίες αναφορικά με την πιθανότητα του να είναι εσφαλμένα τα δεδομένα αυτά, κάνοντας καλύτερη πρόβλεψη (ή αποφασίζοντας πιο σωστά) για την πραγματική τιμή των δεδομένων που λαμβάνουν, έχοντας πολύ καλύτερη απόδοση σε συστήματα με έντονο θόρυβο.

κωδικών turbo, έτσι ώστε να επιτύχουν υψηλότερο κέρδος κωδικοποίησης. Έτσι, επαναφέρθηκαν οι LDPC κώδικες μέσω των turbo κωδικών, επιτυγχάνοντας απόδοση πολύ κοντά στο όριο Shannon.

Οι κώδικες turbo (ή αλλιώς, οι αρχές ή μέθοδοι των κωδικών turbo) και οι μεταγενέστεροι τέτοιο κώδικες έχουν υλοποιηθεί επιτυχώς σε πολλά σύγχρονα τηλεπικοινωνιακά συστήματα που χρησιμοποιούν διάφορες τεχνολογίες. Ένα πολύ χαρακτηριστικό παράδειγμα, στο οποίο θα γίνει εκτενέστερη αναφορά σε επόμενη παράγραφο, είναι η χρήση τους σε συστήματα πολλαπλών χρηστών ή αλλιώς, MIMO (Multiple-Input Multiple-Output) συστήματα, που έχει ως αποτέλεσμα την υψηλότερη φασματική απόδοση καθώς και την αύξηση της χωρητικότητας των δικτύων που χρησιμοποιούν τέτοια συστήματα και συνδυάζεται με την τεχνική πολλαπλής πρόσβασης OFDM (Orthogonal-Frequency Division Multiplexing), μία μέθοδο που μπορεί να επιτύχει ψηφιακή μετάδοση μέσω αποσβεστικών καναλιών μετάδοσης υψηλής ταχύτητας μετάδοσης δεδομένων.

4.2 - Turbo MIMO

Η τεχνική χρήσης πολλαπλών κεραιών MIMO (Multiple Input-Multiple Output) έγινε εφικτή με την ανάπτυξη των στοιχειοκεραιών και την ενσωμάτωση της στα συστήματα ασύρματων επικοινωνιών. Η χρήση της τεχνικής MIMO έχει την δυνατότητα να παρέχει αυξημένη χωρητικότητα δικτύων και ποικιλόμορφο κέρδος των συστημάτων αυτών, συγκριτικά με τα συστήματα που χρησιμοποιούν μόνο μία κεραία. Όμως, η πολυπλοκότητα των απαιτούμενων υπολογισμών για μία βέλτιστη μέθοδο συνδυασμένης ανίχνευσης και αποκωδικοποίησης τέτοιων συστημάτων αυξάνει εκθετικά συναρτήσει πολλών παραγόντων, ένας από τους οποίους είναι το μέγεθος της δέσμης, καθιστώντας δύσκολη την πρακτική υλοποίηση τέτοιων συστημάτων.

Με χρήση όμως μεθόδων επαναληπτικής ανίχνευσης και αποκωδικοποίησης, στις οποίες το στάδιο της ανίχνευσης αποσυνδέεται αποδοτικά από το στάδιο της αποκωδικοποίησης καναλιού, καθιστώντας την πολυπλοκότητα ανεξάρτητη από το μέγεθος της δέσμης, μπορεί να επιτευχθεί απόδοση κοντά στην βέλτιστη. Στον επαναληπτικό δέκτη,

οι εξωτερικές πληροφορίες από την έξοδο του ανιχνευτή τροφοδοτούνται στον αποκωδικοποιητή καναλιού (ή και αντίθετα, από τον κωδικοποιητή καναλιού στον ανιχνευτή), επιτρέποντας στην επαναληπτική διεργασία να μπορεί να καθορίσει την πορεία που θα ακολουθήσει, ανάλογα με το λαμβανόμενο θορυβώδες σήμα και τους περιορισμούς που θέτει ο χρησιμοποιούμενος κώδικας. Για τον λόγο αυτό, και ο ανιχνευτής αλλά και ο αποκωδικοποιητής καναλιού θα πρέπει να χρησιμοποιούν την μέθοδο SISO (Soft-Input Soft-Output) έτσι ώστε να μπορούν να δέχονται (και να παράγουν στην έξοδο τους) soft-decision δεδομένα, τα οποία, όπως προαναφέρθηκε, θα περιέχουν και πληροφορίες αναφορικά με την αξιοπιστία τους.

Η παραπάνω γενική ιδέα για τα MIMO συστήματα έχει το θετικό ότι μπορεί να κάνει χρήση των υπάρχοντων turbo κωδικών (ή κωδικών που στηρίζονται στις αρχές αυτών), αρκεί να έχει εισαχθεί ο κώδικας προς χρήση στο MIMO κανάλι. Η αρχιτεκτονική αυτή ονομάζεται Turbo-MIMO και το κύριο χαρακτηριστικό αυτής είναι ότι η απόδοση του συστήματος, αναφορικά με την δυνατότητα διόρθωσης λαθών που μπορεί αυτό να επιτύχει, αυξάνεται ανάλογα με το πλήθος των επαναλήψεων του βρόγχου ανιχνευτής-αποκωδικοποιητής και είναι πολύ υψηλότερη από ένα αντίστοιχο MIMO σύστημα που δεν χρησιμοποιεί επαναληπτικές μεθόδους, όπως το V-BLAST.

Μία διαμόρφωση που χρησιμοποιείται από τέτοια συστήματα είναι η ST-BICM (Space-time bit-interleaved coded modulation) η οποία είναι μία μέθοδος σχεδιασμού υψηλής απόδοσης MIMO συστημάτων, στην οποία τα ψηφία της εξόδου του κωδικοποιητή καναλιού είναι ανεξάρτητα διαμοιρασμένα μεταξύ των διαθέσιμων κεραιών, με στόχο την μεγιστοποίηση του επιμέρους κέρδους. Στα συστήματα αυτά, οι πληροφορίες του χρήστη κωδικοποιούνται πρώτα, χρησιμοποιώντας έναν προκαθορισμένο γραμμικό μπλοκ κώδικα, ή έναν κώδικα trellis καναλιού. Η ροή των δεδομένων αυτών, με χρήση ενός δυαδικού παρεμβολέα, μετατίθεται κατάλληλα, είτε τυχαία είτε βέλτιστα, ανάλογα με τις απαιτήσεις του συστήματος. Η ροή αυτή, η οποία είναι κωδικοποιημένη και έχει υποστεί παρεμβολή, μετατρέπεται από σειριακή σε παράλληλη και διαχωρίζεται σε υπο-ροές, κάθε μία από τις οποίες διαμορφώνεται κατάλληλα σε μία ακολουθία από PSK ή QAM σύμβολα και εκπέμπεται από διαφορετική κεραία. Η επεξεργασία των λαμβανόμενων σημάτων ακολουθεί μία επαναληπτική πορεία, στην οποία τα λαμβανόμενα δεδομένα ανταλλάσσονται μεταξύ του ανιχνευτή και του αποκωδικοποιητή καναλιού με διαδοχικές διαδικασίες αντίστροφης παρεμβολής (de-interleaved) και επανάληψης της παρεμβολής (re-interleaved). Τα συστήματα αυτά (ST-BICM συστήματα) έχουν πολύ καλή απόδοση σε περιβάλλον αποσβέσεων Rayleigh, επιτυγχάνοντας παράλληλα μικρή πολυπλοκότητα των απαραίτητων

υπολογισμών στον δέκτη.

Η πολυπλοκότητα του δέκτη, όταν αυτός χρησιμοποιεί επαναληπτικές μεθόδους, καθορίζεται από την πολυπλοκότητα των επιμέρους διαδικασιών της ανίχνευσης και της αποκωδικοποίησης. Λόγω της ύπαρξης μεθόδων κωδικοποίησης καναλιού οι οποίες έχουν πολύ καλή απόδοση και μικρή πολυπλοκότητα, όπως είναι οι κώδικες turbo τεσσάρων καταστάσεων, η πολυπλοκότητα των αποκωδικοποιητών δεν είναι μεγάλη. Οπότε, μεγαλύτερης σημασίας είναι η πολυπλοκότητα της μεθόδου ανίχνευσης που θα χρησιμοποιεί το σύστημα αυτό. Αν χρησιμοποιηθεί ως σύστημα ανίχνευσης ένας (MAP) Maximum A posteriori Probability) ανιχνευτής, που χρησιμοποιεί την βέλτιστη μέθοδο ανίχνευσης, τότε η πολυπλοκότητα αυτού θα είναι ανάλογη με το πλήθος των κωδικοποιημένων ψηφίων που μεταδίδονται παράλληλα ανά διάρκεια συμβόλου, γεγονός που συχνά καθιστά απαγορευμένη την χρήση ενός τέτοιου συστήματος για πρακτικά MIMO συστήματα. Όμως, μπορούν να χρησιμοποιηθούν άλλες μέθοδοι, οι οποίες αν και δεν είναι οι βέλτιστες, λόγω της χρήσης των επαναλήψεων, μπορούν να έχουν πολύ καλές επιδόσεις, όπως η μέθοδος SIC-MMSE (Successive Interference Cancellation - Minimum Mean-Square-Error), η μέθοδος με χρήση ενός ανιχνευτή iterative tree search (ITS) καθώς και η χρήση ενός ανιχνευτή list sphere.

4.3 - Χρήση Turbo κωδικών στο πρότυπο IEEE 802.16

Μία από τις πιο σύγχρονες εφαρμογές των turbo κωδικών είναι αυτή που υλοποιείται στα πρότυπα 802.16 της IEEE. Τα πρότυπα αυτά αφορούν την τεχνολογία ασύρματης δικτύωσης WiMax, εξέλιξη της οποίας έχει γίνει αποδεκτή ως τεχνολογία τέταρτης γενιάς (4G) για τα δίκτυα κινητής τηλεφωνίας και είναι από τις υποψήφιες τεχνολογίες και για την επόμενη γενιά, την 5G, της οποίας αναμένεται να ολοκληρωθεί η προτυποποίηση το 2020. Έτσι, οι εφαρμογές που θα περιγραφούν στην παράγραφο αυτή αφορούν την υλοποίηση των κωδικών turbo στα 4G δίκτυα κινητής τηλεφωνίας. Τα δίκτυα αυτά έχουν την δυνατότητα χρήσης ποικίλων ζωνών συχνοτήτων, οι οποίες, βάσει των χαρακτηριστικών τους, χωρίζονται σε δύο μεγάλες κατηγορίες.

Η πρώτη κατηγορία περιέχει τις συχνότητες 10 – 66 GHz. Στις συχνότητες αυτές, το μήκος του κύματος είναι μικρό και διαδίδεται σε ευθεία κατεύθυνση, με αποτέλεσμα να υπόκειται σε μεγάλο βαθμού αποσβέσεις από τα φυσικά εμπόδια που μπορεί να συναντήσει.

Για τον λόγο αυτό, ο πομπός και ο δέκτης πρέπει να “βλέπονται” μεταξύ τους (line of sight) και το σήμα να μην ακολουθεί πολλαπλές διαδρομές. Έτσι, η χρήση ενός φέροντος ταιριάζει αρκετά για την επικοινωνία στις συχνότητες αυτές. Το πρότυπο που καθορίζει τον τρόπο αυτό επικοινωνίας ονομάζεται “WirelessMAN-SC” (Wireless Metropolitan Area Network – Single Carrier) και μπορεί να χρησιμοποιεί και τους δύο διαθέσιμους τρόπους πολύπλεξης, την πολύπλεξη συχνότητας (Frequency Division Duplexing (FDD)) και την πολύπλεξη χρόνου (Time Division Duplexing (TDD)). Η πολλαπλή πρόσβαση επιτυγχάνεται με την μέθοδο πολλαπλής πρόσβασης με διαίρεση χρόνου (Time Division Multiple Access (TDMA)) και την μέθοδο ανάθεσης μετά από αίτηση (demand assigned multiple access (DAMA)) για την αποστολή δεδομένων από τον χρήστη (Uplink). Για την λήψη δεδομένων από τον χρήστη (Downlink) χρησιμοποιείται η πολύπλεξη χρόνου, όπου τα δεδομένα μεταδίδονται ταυτόχρονα προς όλους τους χρήστες.

Η κωδικοποίηση διόρθωσης λαθών χρησιμοποιεί την μέθοδο Reed-Solomon, σε συνδυασμό είτε με κάποιον μπλοκ συνελκτικό κώδικα είτε σε συνδυασμό με κάποιον κώδικα μονού ψηφίου ισοτιμίας, όπως και με κάποιον turbo μπλοκ κώδικα (BTC - Block Turbo Code). Οι κωδικοποιημένες ακολουθίες χαρτογραφούνται σε ακολουθίες QPSK, 16-QAM ή 64-QAM συμβόλων και στην συνέχεια εκπέμπονται. Λόγω των χαρακτηριστικών του σήματος στις συγκεκριμένες συχνότητες, τα παραπάνω αφορούν κεραιές του δικτύου οι οποίες είναι τοποθετημένες σε εξωτερικούς χώρους, ψηλότερα του μέσου ύψους του περιβάλλοντος στο οποίο είναι τοποθετημένες.

Η δεύτερη κατηγορία συχνοτήτων είναι οι συχνότητες από 2 μέχρι 11 GHz. Στις συχνότητες αυτές, το σήμα δεν επηρεάζεται όσο το σήμα υψηλότερων συχνοτήτων, και για τον λόγο αυτό οι συχνότητες αυτές χρησιμοποιούνται όταν δεν είναι εφικτό η κεραία να είναι ορατή από όλους τους χρήστες (Line of Sight), όπως παραδείγματος χάριν όταν είναι τοποθετημένη εντός ενός κτηρίου, ή όταν οι χρήστες βρίσκονται εντός ενός κτιρίου. Και στις δύο περιπτώσεις, το σήμα θα φθάνει στον δέκτη μέσω πολλαπλών διαδρομών, καθιστώντας την αντιμετώπιση των δια συμβολικών παρεμβολών (ISI) μείζονος σημασίας, είτε χρησιμοποιείται ένα φέρον είτε πολλαπλά. Ανάλογα με την μέθοδο, οι πιθανές περιπτώσεις είναι οι παρακάτω τέσσερις:

- WirelessMAN-SCa: Η μετάδοση των πληροφοριών γίνεται με χρήση ενός φέροντος στο πεδίο του χρόνου και η διόρθωση λαθών εφαρμόζεται με συνεχόμενη Reed-Solomon μέθοδο με χρήση ενός πρακτικού κώδικα Trellis κωδικοποιημένης διαμόρφωσης (Trellis Coded Modulation - TCM) έτσι ώστε να επιτυγχάνεται ρυθμός συνελκτικού κώδικα 1/2. Με χρήση της μεθόδου της διάτρησης στο εσωτερικό του TCM κώδικα μπορούν να επιτευχθούν

διάφοροι ρυθμοί κώδικα. Στα συστήματα αυτά μπορούν να υποστηριχθεί και η μη χρήση διόρθωσης λαθών για διαμόρφωση QPSK, με την δυνατότητα χρήσης κωδικών Block Turbo Code (BTC) και Convolutional Turbo Code (CTC).

Στον δέκτη, η εξισορρόπηση στο πεδίο των συχνοτήτων εφαρμόζεται για την μείωση των δια συμβολικών παρεμβολών. Μπορεί να χρησιμοποιηθεί είτε γραμμική εξισορρόπηση είτε εξισορρόπηση με χρήση ανάδρασης. Το μεγάλο πλεονέκτημα της μεθόδου αυτής είναι ότι, λόγω της χρήσης ενός φέροντος δεν παρουσιάζονται προβλήματα αυτοπαρεμβολών, όπως παρουσιάζονται στην χρήση της OFDM που θα αναφερθεί παρακάτω και με χρήση γραμμικής εξισορρόπησης, η πολυπλοκότητα του συστήματος είναι αντίστοιχη ενός συστήματος που χρησιμοποιεί την OFDM χωρίς κωδικοποίηση. Τέλος, ένα ακόμα σημείο στο οποίο η χρήση ενός φέροντος υπερέχει της χρήσης μη κωδικοποιημένης OFDM μεθόδου είναι το ότι, με χρήση ενός φέροντος, ο διαχωρισμός συχνοτήτων είναι δεδομένος ενώ στην OFDM μέθοδο απαιτείται κωδικοποίηση μεταξύ των υπο-φερόντων για την επίτευξη του διαχωρισμού συχνοτήτων.

- **WirelessMAN-OFDM:** Η μέθοδος αυτή, σε αντίθεση με την προηγούμενη που χρησιμοποιούσε ένα φέρον, εφαρμόζει την μέθοδο πολύπλεξης με ορθογωνική διαίρεση συχνοτήτων με μετασχηματισμό 256 σημείων με 200 διαθέσιμα υπο-φέροντα. Η μέθοδος διόρθωσης λαθών είναι μία διαδοχική Reed-Solomon με έναν συνελκτικό κώδικα κατάλληλο για τον συγκεκριμένο ρυθμό που έχει υποστεί διάτρηση (RCPC-*Rate-Compatible Punctured Convolutional Code*), με δυνατότητα χρήσης ενός BTC και ενός CTC κώδικα. Το πλεονέκτημα της περίπτωσης αυτής είναι ότι η μέθοδος OFDM, όταν ο ρυθμός κώδικα είναι μικρός, έχει καλύτερες επιδόσεις από την αντίστοιχη μέθοδο μονού φέροντος, έχοντας μικρή πολυπλοκότητα δέκτη. Ακόμα, η μέθοδος αυτή επηρεάζεται πολύ λιγότερο από τις διακυμάνσεις της φάσης του σήματος λόγω του θορυβώδους περιβάλλοντος.
- **WirelessMAN-OFDMA:** Στην περίπτωση αυτή χρησιμοποιείται η μέθοδος πολλαπλής πρόσβασης OFDMA (*Orthogonal Frequency Division Multiple Access*) με μετασχηματισμό 2048 σημείων με διαθέσιμα 1702 υποφέροντα. Η OFDMA χωρίζει το διαθέσιμο εύρος ζώνης σε ομάδες συνεχών υποφερόντων, δημιουργώντας έτσι κάποια υπο-κανάλια επικοινωνίας, κάθε ένα από τα οποία αποτελείται από ένα υποφέρον από κάθε ομάδα. Όπως και στην μέθοδο OFDM, η διόρθωση λαθών υλοποιείται με τον συνδυασμό της Reed-Solomon μεθόδου με έναν RCPC κώδικα, με δυνατότητα χρήσης ενός BTC ή CTC. Σαν μέθοδος έχει όλα τα πλεονεκτήματα της OFDM, με το πρόσθετο χαρακτηριστικό της καλύτερης απόρριψης των παρεμβολών, καθιστώντας την κατάλληλη για χρήση σε

περιβάλλοντα όπου γειτονικές κεραιές χρησιμοποιούν τις ίδιες συχνότητες.

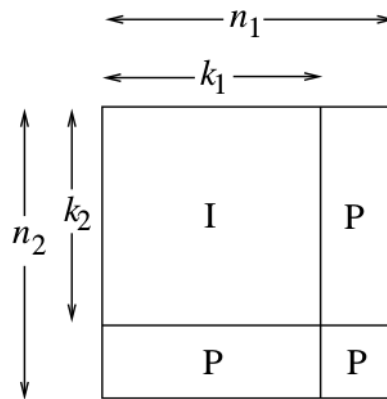
- **WirelessHUMAN (Wireless High-speed Unlicensed Metropolitan Area Networks):** Τα συστήματα που ανήκουν στην κατηγορία αυτή θα ανήκουν και σε μία από τις τρεις παραπάνω κατηγορίες, αναφορικά με τον τρόπο λειτουργίας τους, με την διαφορά ότι θα έχουν την δυνατότητα να χρησιμοποιούν διαφορετικές ζώνες συχνοτήτων, ανάλογα με την διαθεσιμότητα του περιβάλλοντος στο οποίο έχουν τοποθετηθεί.

Στην παραπάνω ανάλυση, αναφέρθηκαν δύο είδη κωδικών που χρησιμοποιούνται από τα πρότυπα 802.16, οι BTC και οι CTC, στους οποίους, λόγω της μεγάλης σημασίας αυτών, θα γίνει πιο εκτενής αναφορά στις επόμενες παραγράφους.

4.4. – Μπλοκ turbo κώδικες (BTC)

Η πρώτη κατηγορία κωδικών που χρησιμοποιούνται από τα πρότυπα IEEE 802.16 είναι οι μπλοκ turbo κώδικες (Block turbo code-BTC) ή, όπως αλλιώς είναι γνωστοί, οι turbo product κώδικες (TPC). Οι κώδικες αυτοί αρχικά είχαν επιλεγεί ως εναλλακτική μέθοδος διόρθωσης καθόν στα WirelessMAN-SC. Η κωδική λέξη ενός τέτοιου TPC κώδικα παρουσιάζεται στο παρακάτω σχήμα (σχήμα 4.1). Όπως φαίνεται, αποτελείται από μία δισδιάστατη διάταξη ψηφίων, από τα οποία η περιοχή όπου θα περιέχεται η πληροφορία θα έχει μέγεθος $k_1 \times k_2$. Κάθε στήλη και κάθε γραμμή της διάταξης αυτής θα κωδικοποιείται μέσω συστηματικού μπλοκ κώδικα ρυθμού k_1/n_1 και k_2/n_2 αντίστοιχα. Τα ψηφία ισοτιμίας προστίθενται στα ψηφία πληροφορίας στις αντίστοιχες γραμμές ή στήλες και, συνήθως η αποκωδικοποίηση γίνεται πρώτα στις στήλες και μετά στις γραμμές. Κάθε στήλη των ψηφίων ισοτιμίας των τελευταίων $n_1 - k_1$ στηλών κωδικοποιείται από τον κωδικοποιητή στηλών και τα πρόσθετα ψηφία ισοτιμίας που παράγονται τοποθετούνται στην αντίστοιχη στήλη. Έτσι, η τελική κωδική λέξη που θα παραχθεί από τον TPC κώδικα θα είναι μεγέθους $n_1 \times n_2$ και ο ρυθμός κώδικα θα είναι ίσος με $k_1 k_2 / n_1 n_2$. Στην γενικότερη περίπτωση, μπορεί η παραπάνω διάταξη να έχει περισσότερες των δύο διαστάσεις, και στην περίπτωση αυτή θα υπάρχουν αντίστοιχο πλήθος κωδικοποιητών με το πλήθος των διαστάσεων της κωδικής λέξης. Η αποκωδικοποίηση θα ξεκινάει από το πρώτο ψηφίο της πρώτης γραμμής της κωδικής λέξης και θα συνεχίσει μέχρι να φθάσει στο τελευταίο ψηφίο της διάταξης αυτής. Στα παραπάνω

δεν έγινε καμία αναφορά σε παρεμβολή των ψηφίων που κωδικοποιούνται, αλλά κάλλιστα θα μπορούσε να χρησιμοποιηθεί και η τεχνική αυτή, με έναν παρεμβολέα να διαβάζει τα ψηφία σειρά-σειρά, ξεκινώντας από το πρώτο ψηφίο της πρώτης σειράς.



Σχήμα 4.1 - TPC Κωδική λέξη

Η επαναληπτική αποκωδικοποίηση ενός TPC κώδικα εφαρμόζει soft μορφής αποκωδικοποίηση για κάθε σειρά και στην συνέχεια, την soft αυτή έξοδο του την τροφοδοτεί στον αποκωδικοποιητή στηλών. Η διαδικασία αυτή συνεχίζει μέχρι την ικανοποίηση κάποιου προκαθορισμένου κριτηρίου και η έξοδος του αποκωδικοποιητή θα είναι η έξοδος ενός από τους δύο επιμέρους αποκωδικοποιητών, όποιου είναι σε λειτουργία όταν ικανοποιηθεί το κριτήριο τερματισμού του αλγορίθμου που χρησιμοποιείται. Το πλεονέκτημα του είδους αυτού κωδικών, των BTC ή TPC, είναι ότι ο κώδικας που κωδικοποιεί την κάθε διάσταση συνήθως έχει απόλυτα καθορισμένη αλγεβρική δομή, με αποτέλεσμα να είναι εφικτή η αποκωδικοποίηση των δεδομένων αυτών με χρήση soft αλγεβρικής αποκωδικοποίησης, μέθοδος που απαιτεί μικρότερη πολυπλοκότητα συγκριτικά με άλλες μεθόδους αποκωδικοποίησης όπως η αποκωδικοποίηση μέγιστης πιθανότητας. Εκτός όμως αυτού, το είδος αυτό των turbo κωδικών έχει και άλλα πλεονεκτήματα, αναφορικά με τους CTC, τα κυριότερα των οποίων είναι:

- Οι TPC κώδικες έχουν μεγάλη ελάχιστη απόσταση Hamming. Η ελάχιστη αυτή απόσταση Hamming είναι το γινόμενο της ελάχιστης απόστασης των επιμέρους διαστάσεων και, αφού η απόσταση Hamming επηρεάζει τις επιδόσεις του κώδικα σε συνθήκες μικρού σφάλματος, δηλαδή για υψηλό SNR ή πολύ χαμηλό BER, οι TPC κώδικες επηρεάζονται λιγότερο από τους CPC που θα παρουσιαστούν στην συνέχεια.
- Η διαδικασία του σχεδιασμού της κωδικής λέξης έτσι ώστε να “χωράει” στο διαθέσιμο πλαίσιο είναι εύκολη. Συνήθως αυτό επιτυγχάνεται με την σύμπτυξη λίγων σειρών

και λίγων στηλών, κάτι που είναι αντίστοιχο με την προσθήκη μηδενικών των σειρών και των στηλών αυτών, τα οποία δεν θα μεταδοθούν. Για την περίπτωση αυτή, μιας και τα ψηφία εισόδου μπορεί να έχουν και μηδενικές τιμές, ο κωδικοποιητής θα πρέπει να γνωρίζει το πλήθος των ψηφίων που είναι για κωδικοποίηση σε κάθε σειρά και σε κάθε στήλη, και δεν χρειάζεται η χρήση της διάτρησης (Puncturing) στα δεδομένα αυτά.

- Η ανάλυση της επίδοσης των TPC κωδικών είναι ευκολότερη από την περίπτωση των CTC, λόγω της πλήρως καθορισμένης αλγεβρικής τους δομής, που αναφέρθηκε παραπάνω. Αυτό μπορεί να είναι πολύ χρήσιμο κατά την σχεδίαση του συστήματος, ώστε να επιλεγθεί ο κατάλληλος για τις απαιτήσεις του συστήματος, κώδικας.
- Ο λανθάνων χρόνος των TPC κωδικών είναι μικρότερος των CTC. Αυτό σημαίνει ότι, για δεδομένο χρόνο κωδικοποίησης, ο TPC κώδικας μπορεί να χρησιμοποιήσει μεγαλύτερο πλήθος επαναλήψεων, αυξάνοντας έτσι τις επιδόσεις του.
- Ολοκληρωμένα κυκλώματα που να υλοποιούν του TPC κώδικες είναι πολύ πιο εύκολο να βρεθούν, μιας και η πολυπλοκότητα των κωδικών αυτών είναι μικρότερη από τους CTC.

Για την υλοποίηση των WirelessMAN-SC προτείνεται ένας εκτεταμένος κώδικας Hamming ως συστατικό του TPC δύο διαστάσεων (οι κώδικες στηλών και γραμμών που προαναφέρθηκαν). Ο εκτεταμένος αυτός Hamming κώδικας προέρχεται από έναν Hamming κώδικα με προσθήκη ενός ψηφίου ελέγχου ισοτιμίας και με τον κώδικα αυτό, η ελάχιστη απόσταση Hamming του TPC κώδικα αυξάνεται πολύ, με πολύ μικρή πρόσθετη απαιτούμενη πολυπλοκότητα. Στο παράδειγμα του συστήματος WirelessMAN-SC, ο εκτεταμένος Hamming κώδικας ορίζεται ως (32,26) κώδικας, ο οποίος προέρχεται από έναν (31,26) Hamming κώδικα με προσθήκη ενός ψηφίου ελέγχου ισοτιμίας. Η ελάχιστη απόσταση του (31,26) Hamming κώδικα είναι 3, οπότε αντίστοιχα του δισδιάστατου TPC θα είναι 9. Με την προσθήκη ενός ψηφίου ισοτιμίας, η ελάχιστη απόσταση του (32,26) Hamming κώδικα γίνεται 4 και η αντίστοιχη απόσταση του TPC κώδικα θα είναι 16, η οποία είναι μεγάλη αύξηση συγκριτικά με την πολυπλοκότητα που προσθέτει το ένα ψηφίο ελέγχου ισοτιμίας.

4.4.1 – Συνελκτικοί turbo κώδικες (CTC)

Όπως αναφέρθηκε και παραπάνω, οι συνηθισμένοι CTC έχουν σχετικά μικρή ελάχιστη απόσταση Hamming με αποτέλεσμα να επηρεάζονται αρνητικά από την διαδικασία της διάτρησης. Όμως αυτό δεν συμβαίνει με τους CTC που δεν είναι δυαδικοί. Επί προσθέτως, η ιδέα των tail-biting συνελκτικών κωδικών έχει εφαρμοστεί στους CTC, βελτιώνοντας την απόδοση φάσματος των κωδικών αυτών, λύνοντας το πρόβλημα των ψηφίων ουράς που χρησιμοποιούνται για τον τερματισμό της κατάστασης του κωδικοποιητή.

Η μέθοδος Tail-Biting αντιμετωπίζει κάποια μειονεκτήματα των συνηθισμένων μη επαναληπτικών συνελκτικών κωδικών, οι οποίοι συνήθως προσθέτουν ένα πλήθος μηδενικών ψηφίων, έτσι ώστε να εξασφαλίσουν ότι η κατάσταση τερματισμού θα είναι μηδενική. Το πλήθος αυτών θα είναι ίσο με το πλήθος των στοιχείων μνήμης του κωδικοποιητή, έστω m . Αυτό έχει σαν αποτέλεσμα την απώλεια φασματικής απόδοσης, μιας και αυτά τα μηδενικά δεν περιέχουν πληροφορία. Η μέθοδος tail-biting εξαλείφει το μειονέκτημα αυτό, θεωρώντας ότι τα τελευταία m ψηφία αποτελούν την αρχική κατάσταση του κωδικοποιητή, δημιουργώντας έτσι έναν κώδικα του οποίου η αρχική και η τελική κατάσταση είναι η ίδια. Αν και ο αποκωδικοποιητής δεν γνωρίζει τίποτε σχετικά με την αρχική και την τελική κατάσταση, μπορεί να υποθέσει κάθε δυνατή κατάσταση ως την αρχική και τελική και να βρεί την ακολουθία μέγιστης απόστασης. Όπως όμως αναφέρθηκε παραπάνω, η μέθοδος αυτή μπορεί αν χρησιμοποιηθεί μόνο σε μη επαναληπτικούς κώδικες, γιατί στους επαναληπτικούς, η τελική κατάσταση εξαρτάται από όλη την ακολουθία δεδομένων, και το να υποθεθεί ότι η αρχική και τελική κατάσταση είναι η ίδια θα οδηγήσει σε λανθασμένη διαδικασία αποκωδικοποίησης.

Για χρήση με τους επαναληπτικούς συνελκτικούς κώδικες, έχει αναπτυχθεί μία παραλλαγή της μεθόδου tail-biting η οποία περιέχει έναν επαναληπτικό κώδικα, και ονομάζεται κυκλικός συνελκτικός κώδικας (Circular convolutional code). Η κυκλική κωδικοποίηση εξασφαλίζει το ότι, μετά την ολοκλήρωση της κωδικοποίησης, η τελική κατάσταση καταλήγει στην αρχική κατάσταση. Η κατάσταση αυτή ονομάζεται “κυκλική κατάσταση” και θα υπάρχει μόνο όταν το μήκος της ακολουθίας των ψηφίων πληροφορίας, N , δεν είναι πολλαπλάσιο του γεννήτορα. Για την εύρεση της αρχικής κατάστασης, αυτή προ-κωδικοποιείται στην ακολουθία των ψηφίων πληροφορίας με την μηδενική αρχική κατάσταση. Η τελική κατάσταση στην οποία θα καταλήξει με τον τρόπο αυτό, έστω S_N^0 θα χρησιμοποιηθεί για την εύρεση της αρχικής S_c κατάστασης σύμφωνα με την παρακάτω

εξίσωση (σχέση 4.1):

$$S_c = (I + G^N)^{-1} S_N^0 (4.1)$$

όπου G είναι ο γεννήτορας πίνακας. Στις πρακτικές εφαρμογές, η κατάσταση S_c μπορεί να βρεθεί μέσα από έναν προκαθορισμένο πίνακα. Μιας και οι κώδικες CTC αποτελούνται από δύο επιμέρους κώδικες, η παραπάνω προ-κωδικοποίηση θα πρέπει να εφαρμοστεί δύο φορές ώστε να προστεθούν τα δεδομένα των αρχικών καταστάσεων και των δύο κωδικοποιητών.

Μία άλλη κατηγορία CTC κωδικών που αναφέρθηκε παραπάνω είναι οι turbo κώδικες που δεν είναι δυαδικοί. Οι κώδικες αυτοί έχουν περισσότερα του ενός ψηφία ως είσοδο κάθε χρονική στιγμή. Αυτό μπορεί να επιτευχθεί και με την χρήση δυαδικών turbo κωδικών που λειτουργούν σε αλληλουχία παράλληλα με επαναληπτικούς συστηματικούς συνελκτικούς κώδικες συνθέτοντας ένα σύστημα δύο κωδικοποιητών, ενός παρεμβολέα (interleaver) και, ανάλογα με το αν χρειάζεται για την εφαρμογή για την οποία υλοποιείται το συγκεκριμένο σύστημα, ένα σύστημα διάτρησης. Ο παρεμβολέας έχει μοναδική δομή η οποία εισάγει “τοπική αταξία” στα δεδομένα εισόδου. Για παράδειγμα, αν μία είσοδος δύο ψηφίων εισέλθει στον κωδικοποιητή την ίδια χρονική στιγμή, ο παρεμβολέας μεταθέτει την θέση τους ως ζευγάρι και αλλάζει την θέση των ψηφίων αυτών για κάθε άρτιο διάστημα. Η διαδικασία αυτή, και ειδικά το δεύτερο κομμάτι της, είναι απαραίτητη έτσι ώστε να αυξηθεί η τυχαιότητα της ακολουθίας που έχει υποστεί την παρεμβολή, μιας και η παρεμβολή στα ζευγάρια οδηγεί σε αρκετά κανονική δομή, έτσι ώστε να μπορεί να διαχειριστεί τα σφάλματα μικρού βάρους. Έτσι, οι μη δυαδικοί turbo κώδικες απαιτούν παρεμβολή δύο βημάτων.

Πολλοί CTC συνδυάζουν τις παραπάνω μεθόδους (ή βασικές ιδέες) έτσι ώστε να έχουν όσο περισσότερα πλεονεκτήματα είναι δυνατόν. Κάποια από τα σημαντικότερα αυτών είναι:

- Οι CTC έχουν καλύτερη σύγκλιση από του BTC και τους κλασικούς turbo κώδικες. Η δομή των CTC μειώνει την συσχέτιση μεταξύ εξόδων από δύο συνδυαστικούς κωδικοποιητές, και έχουν και καλύτερη επίδοση κέρδους.
- Οι CTC έχουν μεγαλύτερη ελάχιστη απόσταση Hamming από τους κλασικούς turbo κώδικες λόγω της παρεμβολής δύο επιπέδων και για τον λόγο αυτό έχουν μικρότερο σφάλμα.
- Αν και η μέθοδος της διάτρησης είναι αναγκαία στους CTC, φαίνεται ότι έχουν μεγαλύτερη ανένεια σε αυτήν και, όσον αφορά τις μη δυαδικές δομές, απαιτείται μικρότερη διάτρηση των ψηφίων ισοτιμίας, αυξάνοντας έτσι την επίδοση των κωδικών υψηλού ρυθμού κώδικα.
- Για την περίπτωση των μη δυαδικών κωδικών, μιας και εισέρχονται περισσότερα του ενός ψηφία σε κάθε χρονική στιγμή στον κωδικοποιητή, ο λανθάνων χρόνος μειώνεται.

- Έχει παρατηρηθεί ότι οι CTC έχουν αντοχή στην χρήση τεχνικών αποκωδικοποίησης που δεν είναι οι βέλτιστες, όπως η Max-Log-MAP. Αυτό οφείλεται στο γεγονός ότι το μέγεθος του μπλοκ είναι μικρότερο στους μη δυαδικούς turbo κώδικες, κάτι που οδηγεί σε μικρότερης πολυπλοκότητας δέκτες.
- Συγκριτικά με του BTC, οι CTC απαιτούν μικρότερο όγκο δεδομένων για την μηνυματοδοσία στο MAC επίπεδο.

Οι CTC κώδικες καθορίζονται από τα πρότυπα IEEE 802.16 ως μία προαιρετική μέθοδος κωδικοποίησης για τις συχνότητες 2-11GHz. Χρησιμοποιεί διπλό δυαδικό κυκλικό επαναληπτικό συστηματικό συνελκτικό κώδικα, του οποίου το ψηφίο ελέγχου ισοτιμίας Y παράγεται από το πολυώνυμο $1+D^2+D^3$ και το πολυώνυμο που παράγει τον βρόγχο ανάδρασης είναι το $1+D+D^3$. Αν θεωρήσουμε ότι τα δύο ψηφία που εισέρχονται ταυτόχρονα στον κωδικοποιητή είναι (A,B), τότε η παρεμβολή θα γίνει σε δύο στάδια, όπως προαναφέρθηκε, τα οποία θα είναι:

- Αρχικά θα αλλάξει η θέση των ψηφίων για κάθε άρτιο διάστημα και θα γίνει (B,A) και
- Έστω ότι η διεύθυνση του ζευγαριού j είναι i , αυτή θα υπολογιστεί ως εξής:

$$ifj \bmod 4 = 0 \text{ ή } 1, i = (P_0 \cdot j + 1)_{\bmod N}$$

$$ifj \bmod 4 = 2 \text{ ή } 3, i = (P_0 \cdot j + 1 + \frac{N}{4})_{\bmod N} \quad (4.2)$$

Τέλος, πρέπει να τονιστεί ότι η σύγκριση των CTC με τους BTC, αν και έγινε παραπάνω, είναι γενικά πολύ δύσκολη. Και οι δύο κατηγορίες έχουν τα πλεονεκτήματα και τα μειονεκτήματα τους, και για τον λόγο αυτό τα πρότυπα IEEE802.16 περιέχουν και τις δύο κατηγορίες ως διαθέσιμες μεθόδους κωδικοποίησης έτσι ώστε να είναι πιο ευέλικτος ο σχεδιασμός ενός συστήματος, ανάλογα με τις ανάγκες του.

4.5 – Άλλες εφαρμογές των turbo κωδικών

Όπως αναφέρθηκε και παραπάνω, οι κώδικες turbo έχουν υλοποιηθεί σε πολλές εφαρμογές. Οι δύο που αναφέρθηκαν στις προηγούμενες παραγράφους ήταν οι σημαντικότερες στα τηλεπικοινωνιακά συστήματα. Όμως, εκτός αυτών, υπάρχουν και άλλες που είναι αρκετά σημαντικές, και για τον λόγο αυτό θα αναφερθούν ονομαστικά. Οι σημαντικότερες αυτών είναι:

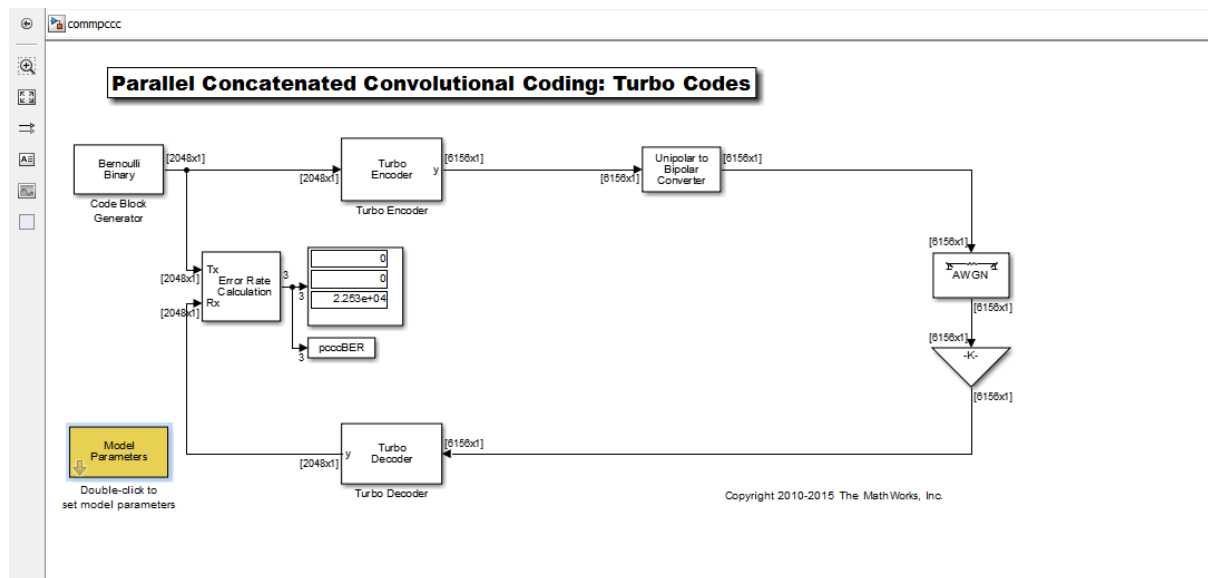
- Χρήση των turbo κωδικών στα μαγνητικά μέσα αποθήκευσης, όπως είναι οι σκληροί δίσκοι, με χρήση των οποίων γίνεται εφικτή η αύξηση της ταχύτητας ανάγνωσης και εγγραφής των δεδομένων, με παράλληλη αύξηση της αξιοπιστίας τους.
- Χρήση στα οπτικά αποθηκευτικά μέσα.
- Χρήση turbo κωδικών, ή κωδικών που μοιάζουν στους turbo, για την κωδικοποίηση διαύλου σε ενσύρματες τεχνολογίες επικοινωνιών, όπως είναι η ADSL.
- Χρήση σε εφαρμογές οπτικών επικοινωνιών, είτε μονού τρόπου είτε πολλαπλών.
- Χρήση των κωδικών turbo στις δορυφορικές επικοινωνίες.

Κεφάλαιο 5

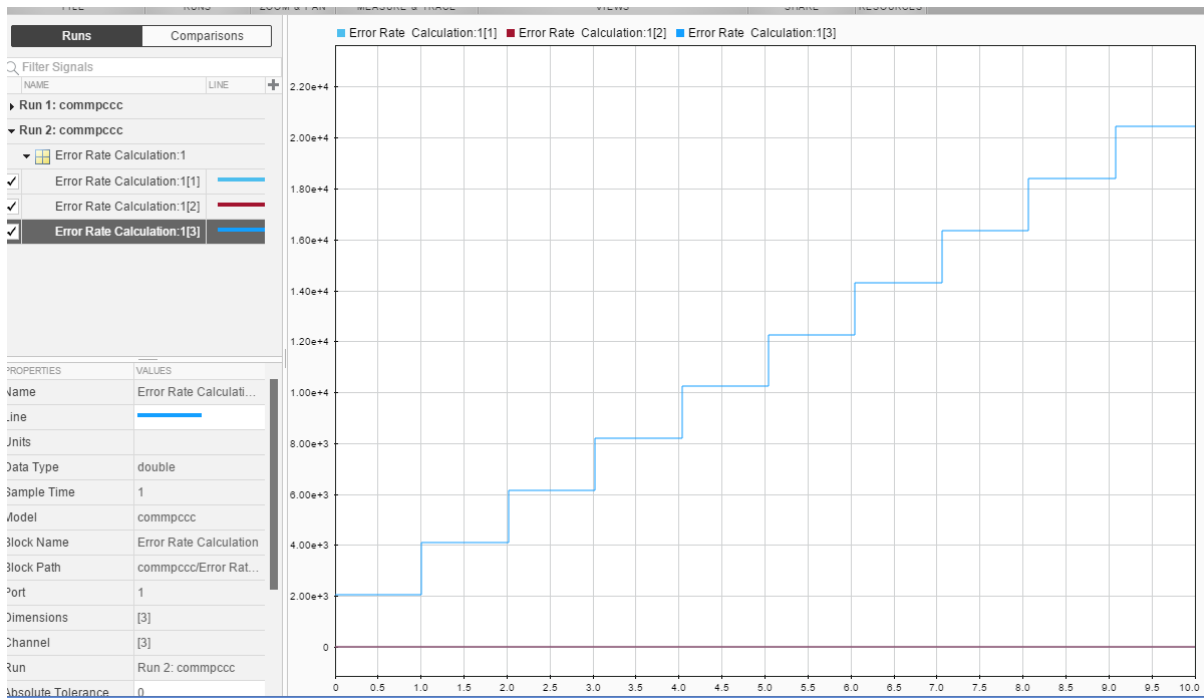
5.1 Κωδικοποιητής turbo

Αυτό το παράδειγμα μας δείχνει την βασική δομή των τούρμπο κωδικών, δύο φορείς και δέκτες, που το χαρακτηριστικό τους είναι η απόδοση πάνω από τον ήχο καναλιού χρησιμοποιώντας στοιχεία από τα επικοινωνιακά συστήματα toolbox. Επιλέξαμε τις προδιαγραφές term (LTE) για τους συστατικούς παραμέτρους.

Η εφεύρεση από τους κώδικες τούρμπο, μαζί με την ανάπτυξη της επαναληπτικής αποκρυπτογράφησης της θεμελιώδους αρχής και μαζί με την απόδοση του ορίου Shannon, οδήγηθηκαν στην απορρόφηση μέσα σ' ένα ευρύ πλήθος από εφαρμογές μερικές από τις οποίες συμπεριλαμβάνουν βαθύ χώρο επικοινωνίας, τρίτης γενιάς ασύρματου πρότυπου και ψηφιακού βίντεο τηλεόρασης.



Σχήμα το οποίο τρέχει στα 10 sec



Αυτό είναι το διάγραμμα της προηγούμενης εικόνας

Ο τούρμπο κωδικοποιητής είναι η παράλληλη σύνδεση με πολλαπλά συστατικά συνελκτικών κωδικοποιητών. Οι πρώτοι κωδικοποιητές λειτουργούν κατευθείαν πάνω στην εισαγωγή ακολουθίας bit ενώ οποιαδήποτε άλλα λειτουργούν με παρεμβαλλόμενη ακολουθία εισόδου, που λαμβάνονται με την παρεμβολή των bits εισόδου σ' ένα μπλοκ μήκους.

Τα block συστήματα βασίζονται στους τούρμπο κωδικοποιητές που χρησιμοποιούν δύο πανομοιότυπα 8-state συστηματικής συνελκτικής κωδικοποίησης. Το convolutional encoder σύστημα χρησιμοποιεί την <<terminated>> ρύθμιση για την ιδιότητα του terminationmethod. Με τον τρόπο αυτό επαναφέρονται οι κωδικοποιητές στο αρχικό στάδιο από κάθε πλαίσιο των δεδομένων block διαδικασίας. Το εσωτερικό block παρεμβάλει χρησιμοποιώντας δείκτες, βασισμένους στις παραμέτρους του block κώδικα που καθορίζεται από το χρήστη. Το bit ξαναρυθμίζει το υποσύστημα αφαιρώντας τα έξτρα σύνολα bit από την δεύτερη έξοδο του κωδικοποιητή.

5.2 Iterative Turbo Decoding (επαναληπτικής αποκωδικοποίησης)

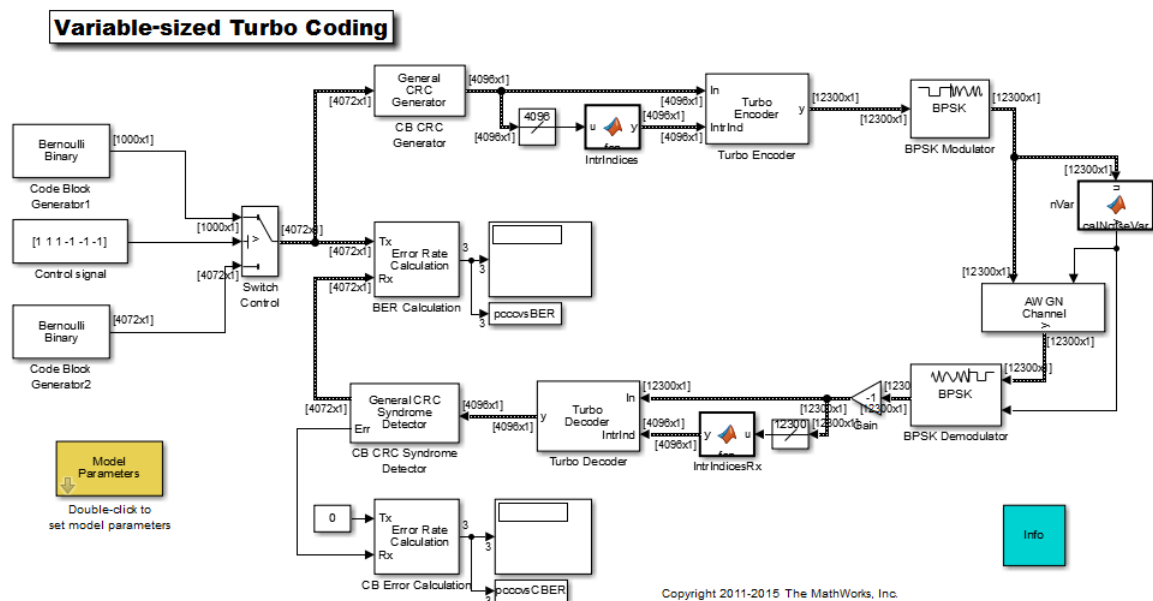
Για επαναληπτικής αποκωδικοποίησης από το παράλληλα συνδεδεμένο σύστημα. Ο turbo αποκωδικοποιητής χρησιμοποιεί την εκ των υστέρων πιθανότητα (APP) ως συστατικό αποκωδικοποίησης.

Κάθε comm APP Decoder αντικείμενο συστήματος αντιστοιχεί σ' ένα συστατικό κωδικοποιητή που παρέχει μια ενημερωμένη ακολουθία τιμών της λογαριθμικής πιθανότητας εκτιμάται για τα κωδικοποιημένα bit κοινώς αποδεκτά από την ακολουθία τιμών της λογαριθμικής πιθανότητας. Για κάθε σύνολο ακολουθιών από τα γενικά κανάλια, ο αποκωδικοποιητής διαδοχικά ενημερώνει την λογαριθμική πιθανότητα για τα ενδεχόμενα bit μέχρι ένα κτήριο να διακοπεί. Το παράδειγμα αυτό χρησιμοποιεί έναν σταθερό αριθμό επαναλήψεων αποκωδικοποιητών, όπως καθορίζεται από την παράμετρο, όπως προβλέπεται από τον αριθμό επαναλήψεων των αποκωδικοποιητών παραμέτρων του μοντέλου block. Ο προεπιλεγμένος αριθμός των επαναλήψεων είναι έξι.

Η Terminationmethod ιδιότητα για τι αντικείμενο του συστήματος εφαρμογής του αποκωδικοποιητή έχει οριστεί ως <<terminated>> ώστε να ταιριάζει με τους κωδικοποιητές. Οι αποκωδικοποιητές δεν προϋποθέτουν στοιχεία από την ουρά bit και ως αποτέλεσμα, αυτές εξαιρούνται από τις πολλές επαναλήψεις.

Η εσωτερική παρεμβολή του αποκωδικοποιητή είναι πανομοιότυπη με την μία που χρησιμοποιεί ο αποκωδικοποιητής. Αναδιοργανώνει τις ακολουθίες έτσι ώστε να ευθυγραμμίζονται σωστά με τους δύο αποκωδικοποιητές.

5.3 Variable-sized turbo coding(Κωδικοποίηση μεταβλητού μεγέθους turbo)



Το μοντέλο αυτό έχει οριστεί να τρέχει δύο συγκεκριμένες χρήσεις code-block lengths, τα οποία διαφέρουν ανάλογα με το σήμα του επιλεγμένου στοιχείου ελέγχου. Οι δείκτες ανά μήκος και η διακύμανση θορύβου υπολογίζονται ανά χρονικό βήμα. Χρησιμοποιώντας τον ανιχνευτή σύνδρομο CRC, το μοντέλο εμφανίζει το ποσοστό σφάλματος εκτός από το ποσοστό λάθους καθώς και η πιο σχετική μέτρηση απόδοσης με μεταβλητό μέγεθος.

Βιβλιογραφία

- Matthew C. Valenti, The Evolution of Error Control Coding
- C. E. Shannon, “A mathematical theory of communication”, Bell Sys. Tech. J. , vol. 27, pp. 379-423, pp. 623-656, 1948.
- John g. Proakis–Masound Salehi, μετάφραση-επιμέλεια: Κ. Καρούμπαλος-Ε. Ζέρβας-Σ. Καραμπογιάς–Ε. Σαγκριώτης (2002) “Συστήματα Τηλεπικοινωνιών”, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
- Herbert Taub – Donald L. Schilling, Αποδοση: Γ.Κ.Τσιρης- Σ.Σ.Κουκουρλης, Μεταφραση: Σ.Σ.Κουκουρλης (2003) “Τηλεπικοινωνιακά Συστήματα”, Εκδόσεις Α. Τζιόλα Ε. Θεσσαλονικη
- Δημήτριος Α. Βάρσος (2005) “Στοιχεία αλγεβρικής θεωρίας κωδίκων”
- D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, J. R. Wall, (2η Έκδοση 2010) “Βασικές Αρχές Θεωρίας Κωδικοποίησης και Κρυπτογραφίας”, Εκδόσεις Κλειδάριθμος
- Β. Ζορκάδη (2002) “Θεωρία Πληροφορίας και Κωδικοποίησης”, Ελληνικό Ανοικτό Πανεπιστήμιο
- R.G. Gallager, (1963) “Low-Density Parity-Check Codes”, MIT Press, Cambridge, MA
- Punya Thitimajshima, “Recursive Systematic Convolutional codes and application to parallel concatenation,” IEEE Globecom’95, Singapore, pp.2267-2272.
- Claude Berrou and Alain Glavieux, “Near optimum error correcting coding and decoding: turbo-codes,” IEEE Transactions on Communications, vol.11, no.10,Οκτώβριος 1996.
- L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate,” IEEE Trans. Inform. Theory, IT-20, pp. 248-287, Μάρτιος 1974.
- G. Battail, “Pondération des symboles d’écodés par l’algorithme de Viterbi” (στα Γαλλικά), Ann. T él’ecommun., Fr., 42, N 1-2, pp. 31-38, Ιανουάριος 1987
- J. Hagenauer and P. Hoeher, “A Viterbi algorithm with soft-decision outputs and its applications”, Proc. of Globecom ’89, Dallas, Texas, pp. 47.11-47.17,Νοέμβριος 1989.
- J. Viterbi, “Convolutional codes and their performance in communication systems,” IEEE Trans. Com. Technology, vol. COM-19, No. 15, pp. 751-772,Οκτώβριος 1971
- G. D. Forney, “The Viterbi algorithm,” Proc. IEEE, vol. 61, N 3, pp. 268-278,Μάρτιος 1973.
- K. Sripmanwat (ed.), Turbo Code Applications: a journey from a paper to realization, 2005 Springer. Printed in the Netherlands
- Διαδίκτυο