



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Πολικοί Κώδικες – Θεωρία, Ανάλυση και Υλοποίηση

**Φοιτητής: Ρούσας Ελευθέριος
ΑΜ: 50346103**

Επιβλέπων Καθηγητής

**Ζέρβας Ευάγγελος
Καθηγητής**

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΜΑΡΤΙΟΣ 2023



UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

Polar Codes – Theory, Analysis and Implementation

Student: Rousas Eleftherios
Registration Number: 50346103

Supervisor

Zervas Evangelos
Professor

ATHENS-EGALEO, MARCH 2023

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

| | | |
|--------------------------------|---------------------------------|--|
| Ζέρβας Ευάγγελος, Καθηγητής | Καλύβας Δημήτριος, Καθηγητής | Καραμπέτσος Σωτήριος, Αναπληρωτής Καθηγητής |
| (Υπογραφή) | (Υπογραφή) | (Υπογραφή) |

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

Ρούσας Ελευθέριος, Μάρτιος 2023

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τους συγγραφείς.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον/την συγγραφέα του και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις θέσεις του επιβλέποντος, της επιτροπής εξέτασης ή τις επίσημες θέσεις του Τμήματος και του Ιδρύματος.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ρούσας Ελευθέριος του Στέφανου, με αριθμό μητρώου 50346103 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.

Ο Δηλών
Ρούσας Ελευθέριος

(Υπογραφή φοιτητή)

Περίληψη

Σε αυτή την εργασία παρουσιάζονται οι βασικές αρχές των πολικών κωδίκων για B-DMC κανάλια. Αναλύεται η διαδικασία της πόλωσης των καναλιών και πως η πολική κωδικοποίηση και αποκωδικοποίηση οδηγεί σε επίτευξη της χωρητικότητας ενός B-DMC καναλιού. Επιπλέον παρουσιάζονται τεχνικές κωδικοποίησης και αποκωδικοποίησης και αποτελέσματα εξομοίωσης για BSC και BEC κανάλια μέσω Matlab. Τέλος, γίνεται μια αναφορά στην πρακτική χρήση των πολικών κωδίκων για το 5G standard.

Λέξεις – κλειδιά

Πολικοί Κώδικες, Επίτευξη Χωρητικότητας, Polarization Martingale, Πολυπλοκότητα Κωδικοποίησης – Αποκωδικοποίησης, SC αποκωδικοποιητής, 5G New Radio

Abstract

In this paper the basic principles of polar codes for B-DMC channels are presented. Moreover, the channel polarization process is analyzed which shows how polar coding and decoding leads to the capacity achieving result for B-DMC channels. In addition, coding and decoding techniques and simulation results via Matlab for BSC and BEC channels are presented. Finally, a reference is made to the practical use of polar codes in the 5G standard.

Keywords

Polar Codes, Capacity Achieving, Polarization Martingale, Encoding – Decoding Complexity, SC decoder, 5G New Radio

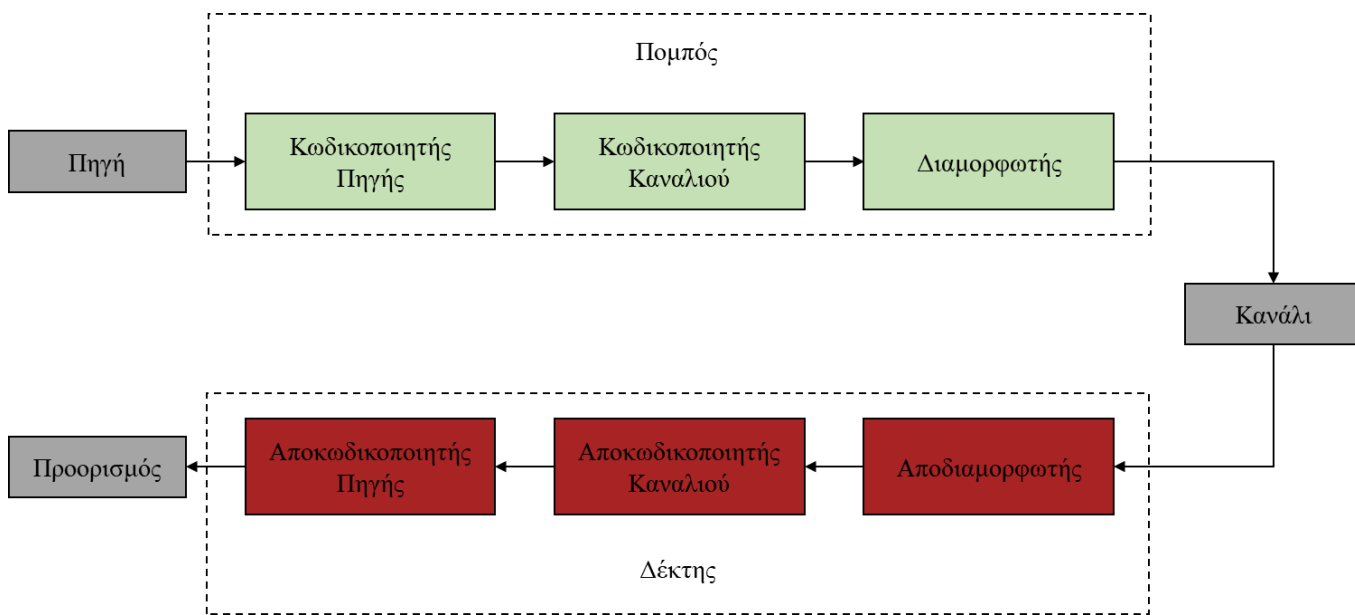
| | |
|---|-----------|
| Κατάλογος Εικόνων..... | 8 |
| 1 ΚΕΦΑΛΑΙΟ 1^ο : Εισαγωγή..... | 9 |
| 1.1 Ταξινόμηση κωδίκων..... | 11 |
| 1.2 Block κώδικες..... | 11 |
| 1.3 Κώδικες δέντρου..... | 11 |
| 1.4 Ιστορική αναδρομή..... | 12 |
| 1.5 Ιστορική αναδρομή κωδικοποίησης καναλιού..... | 13 |
| 1.6 Αλγεβρικοί κώδικες..... | 13 |
| 1.7 Πιθανοκρατικοί κώδικες..... | 13 |
| 2 ΚΕΦΑΛΑΙΟ 2^ο : Εισαγωγή στους πολικούς κώδικες..... | 15 |
| 3 ΚΕΦΑΛΑΙΟ 3^ο : Κωδικοποίηση πολικών κωδίκων..... | 21 |
| 3.1 Βασική αρχή πολικών κωδίκων..... | 21 |
| 3.2 Μοντέλα καναλιών..... | 21 |
| 3.2.1 Το δυαδικό συμμετρικό κανάλι (BSC - Binary Symmetric Channels)..... | 22 |
| 3.2.2 Το διακριτό χωρίς μνήμη κανάλι (DMC - Discrete Memoryless Channels)..... | 23 |
| 3.2.3 Δυαδικό κανάλι διαγραφής (Binary Erasure Channel - BEC)..... | 24 |
| 3.2.4 Το διακριτό-χρόνου AWGN κανάλι..... | 24 |
| 3.3 Συμμετρική χωρητικότητα και παράμετρος Bhattacharyya..... | 25 |
| 3.3.1 Συμμετρική χωρητικότητα (Symmetric Capacity)..... | 25 |
| 3.3.2 Παράμετρος Bhattacharyya (Bhattacharyya Parameter)..... | 25 |
| 3.3.3 Κανόνας αλυσίδας (Chain Rule)..... | 25 |
| 3.4 Συνδυασμός και διαχωρισμός των καναλιών (Channel Combining and Channel Splitting)..... | 26 |
| 3.4.1 Ανάλυση για $N = 2$ | 26 |
| 3.4.2 Ανάλυση για $N = 4$ | 28 |
| 3.4.3 Γενική περίπτωση N | 30 |
| 3.4.4 Προϋποθέσεις για σωστή κωδικοποίηση..... | 35 |
| 3.5 Πίνακας γεννήτορας (G_N)..... | 36 |
| 3.6 Ρυθμός πόλωσης (polarization rate)..... | 41 |
| 3.7 Πολυπλοκότητα κωδικοποίησης (encoding complexity)..... | 44 |
| 4 ΚΕΦΑΛΑΙΟ 4^ο : Αποκωδικοποίηση πολικών κωδίκων..... | 46 |
| 4.1 Αποκωδικοποίηση διαδοχικής ακύρωσης (SCD – successive cancellation decoding)..... | 46 |
| 4.2 Παράδειγμα αποκωδικοποίησης διαδοχικής ακύρωσης..... | 48 |
| 4.3 Error Probability (P_e)..... | 55 |
| 4.4 Ακολουθία αξιοπιστίας (Reliability sequence)..... | 57 |
| 4.5 Πολυπλοκότητα αποκωδικοποίησης διαδοχικής ακύρωσης (successive cancellation decoding complexity)..... | 59 |
| 5 ΚΕΦΑΛΑΙΟ 5^ο : Εφαρμογή πολικών κωδίκων - 5G..... | 61 |
| 5.1 5η γενιά τηλεπικοινωνιακών συστημάτων..... | 61 |
| 5.2 Πολικοί κώδικες στο 5G..... | 62 |
| 5.3 Reliability sequence στο 5G standard..... | 64 |
| 6 ΚΕΦΑΛΑΙΟ 6ο: Εξομοίωση Matlab..... | 66 |
| 7 ΚΕΦΑΛΑΙΟ 7ο :ΣΥΜΠΕΡΑΣΜΑΤΑ..... | 76 |
| Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές..... | 77 |
| Παράρτημα Α..... | 80 |

Κατάλογος Εικόνων

| | |
|--|----|
| Σχήμα 3.12 Διαδικασία μετασχηματισμού του καναλιού όπου $N = 8$ [1] | 38 |
| Σχήμα 4.9 Διαφορετικός τρόπος απεικόνισης της διαδικασίας αποκωδικοποίηση διαδοχικής ακύρωσης για $N = 8$ [1] | 59 |
| Σχήμα 5.2 BLER προς E_s/N_0 για διαφορετικά κανάλια, ρυθμούς και bit πληροφορίας σε πολικούς και LDPC κώδικες [9] | 69 |
| Σχήμα 5.3 Σύγκριση της υπολογιστικής πολυπλοκότητας στους πολικούς και LDPC κώδικες [9] | 69 |

1. Εισαγωγή

Ένα τηλεπικοινωνιακό σύστημα έχει ως αποκλειστικό στόχο την επιτυχή μετάδοση της πληροφορίας από την πηγή έως τον τελικό προορισμό. Η πληροφορία αυτή καθαυτή μπορεί να αλλοιωθεί, σχεδόν εξολοκλήρου, από το κανάλι από το οποίο διέρχεται. Η ανάλυση του κάθε τηλεπικοινωνιακού συστήματος μπορεί να πραγματοποιηθεί μελετώντας τις διεπαφές πηγής-καναλιού και καναλιού-προορισμού. Η απλή μορφή ενός τηλεπικοινωνιακού συστήματος περιγράφεται στο διάγραμμα βαθμίδων του σχήματος 1.1.

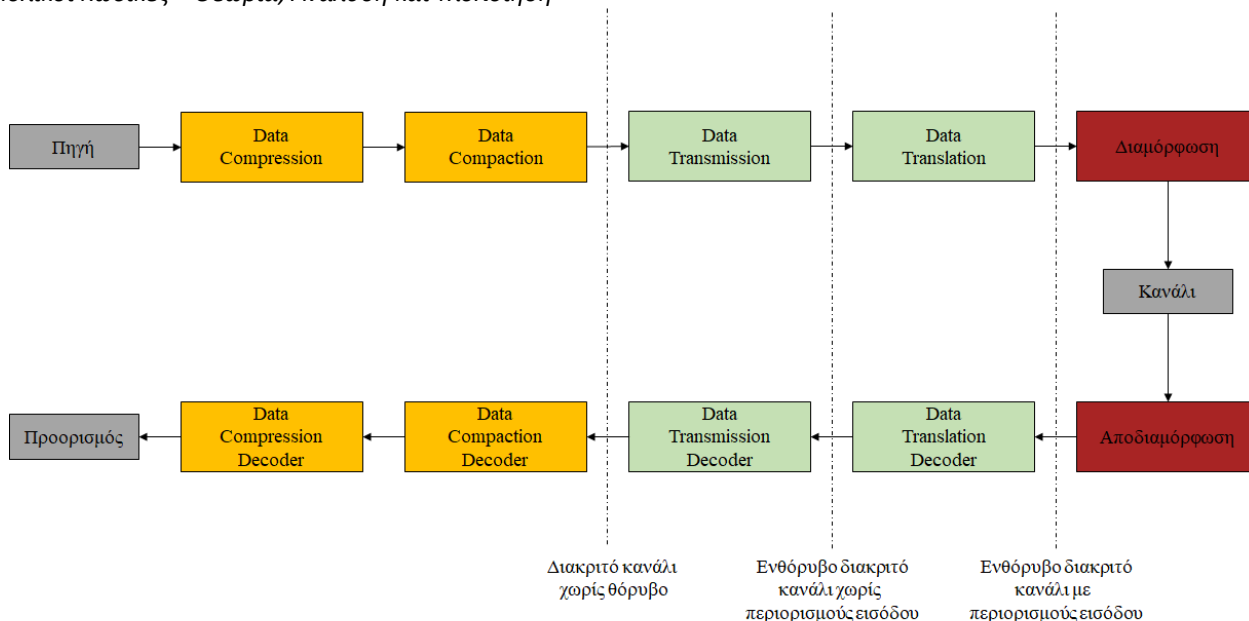


Σχήμα 1.1: Διάγραμμα βαθμίδων ενός τυπικού τηλεπικοινωνιακού συστήματος

Η διεπαφή πηγής-καναλιού αποτελείται από τρεις βασικές βαθμίδες: τον κωδικοποιητή πηγής, τον κωδικοποιητή καναλιού και τον διαμορφωτή. Αντίστοιχα η διεπαφή καναλιού-προορισμού αποτελείται και αυτή από τρεις βαθμίδες: τον αποδιαμορφωτή, τον αποκωδικοποιητή καναλιού και τον αποκωδικοποιητή πηγής.

Η κάθε βαθμίδα έχει διαφορετικό σκοπό και στόχο. Ο κωδικοποιητής πηγής έχει ως στόχο του την αναπαράσταση των δεδομένων της πηγής με όσο το δυνατόν λιγότερα σύμβολα. Πρόκειται για μια συμπίεση του πληροφοριακού περιεχομένου των δεδομένων της πηγής, όπου ένα σύνολο δεδομένων πηγής (**source word**) μετατρέπεται σε μια κωδικολέξη πηγής (**source codeword**). Ο κωδικοποιητής καναλιού έχει ως στόχο την εξασφάλιση της αξιόπιστης μετάδοσης της πληροφορίας. Η έξοδος του καναλιού του κωδικοποιητή καναλιού ονομάζεται κωδικολέξη καναλιού (**channel codeword**). Ο διαμορφωτής αναλαμβάνει το πολύπλευρη διαδικασία της μετατροπής της ψηφιακής πληροφορίας σε αναλογική. Η μετατροπή αυτή είναι απαραίτητη για τη μετάδοσή του ψηφιακού σήματος μέσα από το κανάλι.

Η πιο γενική μορφή ενός τηλεπικοινωνιακού συστήματος φαίνεται στο σχήμα 1.2, όπου οι βαθμίδες της κωδικοποίησης πηγής και κωδικοποίησης καναλιού έχουν αναλυθεί περαιτέρω σε δυο υποσυστήματα κωδικοποίησης η καθεμία.



Σχήμα 1.2: Κωδικοποίηση πηγής και καναλιού

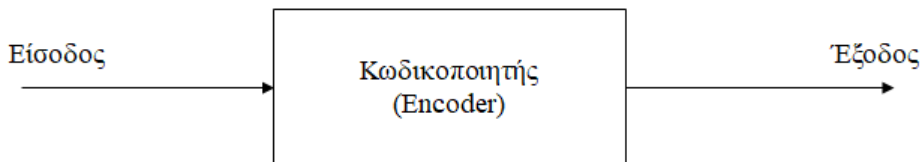
Η κωδικοποίηση πηγής αποτελείται από δύο είδη κώδικων: τους κώδικες συμπίεσης δεδομένων (**data compression codes**) και τους κώδικες σύμπτυξης δεδομένων (**data compaction codes**). Αντίστοιχα, η κωδικοποίηση καναλιού αποτελείται από τους κώδικες μετάδοσης δεδομένων (**data transmission codes**) και τους κώδικες μετάφρασης δεδομένων (**data translation codes**). Όλοι οι παραπάνω κώδικες ικανοποιούν διαφορετικές απαιτήσεις του τηλεπικοινωνιακού συστήματος.

Οι κώδικες συμπίεσης δεδομένων (**data compression codes**) είναι υπεύθυνοι για την μείωση του πληροφοριακού περιεχομένου της πηγής. Πρόκειται για τεχνικές συμπίεσης της πληροφορίας με απώλειες όπως οι PCM, MPEG, JPEG κτλ. Η συμπίεση δεδομένων με απώλειες είναι μια μη αντιστρέψιμη λειτουργία η οποία όμως είναι αναπόφευκτη. Οι κώδικες σύμπτυξης δεδομένων (**data compaction codes**) έχουν ως στόχο την αποτελεσματικότερη αναπαράσταση των δεδομένων εξόδου της πηγής χρησιμοποιώντας όσον το δυνατόν μικρότερο αριθμό από bits. Κατά την σύμπτυξη των δεδομένων δεν υπάρχει απώλεια πληροφορίας. Παραδείγματα τέτοιων τεχνικών είναι οι κώδικες Huffman [54], Shannon-Fano [55], Tunstall [56], Arithmetic coding [57], Lempel-Ziv [58] [59] κτλ. Οι κώδικες μετάδοσης δεδομένων (**data transmission codes**) έχουν ως στόχο τη διόρθωση ή ανίχνευση τυχόν σφαλμάτων που εισάγονται από το κανάλι. Είναι μια διαδικασία όπου εισάγεται ηθελημένα πλεονασμός bits στην ακολουθία εισόδου του κωδικοποιητή. Στην κατηγορία αυτή ανήκουν οι κώδικες Turbo [43], LDPC [42], BCH [60], RS [61] [62] [63], Polar Codes [1] κτλ.

Οι κώδικες μετάφρασης δεδομένων (**data translation codes**) χρησιμοποιούνται σε περιπτώσεις όπου έχουμε περιορισμούς στην είσοδο του καναλιού. Για παράδειγμα, μπορεί να μην επιτρέπονται μεγάλες ακολουθίες από bits ίδιας τιμής. Είναι μια τεχνική η οποία είναι απαραίτητη στα συστήματα αυτοσυγχρονισμού.

1.1 Ταξινόμηση κωδίκων

Η διαδικασία της κωδικοποίησης έγκειται στην αντιστοίχιση μιας ακολουθίας συμβόλων με αλφάβητο $A = \{a_1, a_2 \dots a_J\}$ σε μια διαφορετική ακολουθία συμβόλων με αλφάβητο $B = \{b_1, b_2 \dots b_K\}$ (σχήμα 1.3). Εάν $J = K = 2$ τότε ο κώδικας λέγεται δυαδικός. Οι κώδικες εν γένει ταξινομούνται σε μπλοκ κώδικες (block codes) και σε κώδικες δέντρου (tree codes). Η διαφοροποίηση αυτή εξαρτάται από το εάν η κωδικοποίηση έχει μνήμη ή όχι.



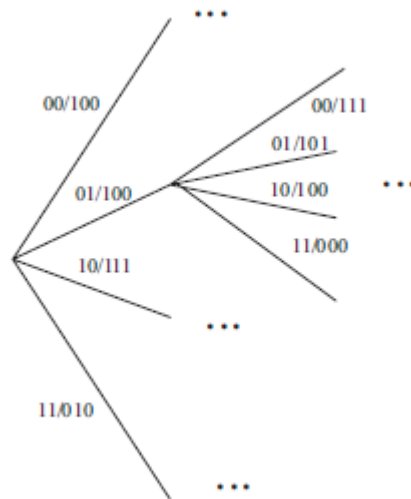
Σχήμα 1.3: Διάγραμμα κωδικοποιητή

1.2 Block κώδικες

Οι μπλοκ κώδικες ανήκουν στην κατηγορία των κωδίκων χωρίς μνήμη. Ονομάζονται μπλόκ κώδικες γιατί τεμαχίζουν την ακολουθία συμβόλων της εισόδου σε μπλοκς (ίδιου ή διαφορετικού μεγέθους). Στην συνέχεια το κάθε μπλοκ κωδικοποιείται σε μια νέα ακολουθία συμβόλων. Η ακολουθία εξόδου που προκύπτει εξαρτάται μόνον από το τρέχον μπλοκ εισόδου και όχι από προηγούμενα μπλοκς. Ανάλογα με το μέγεθος του μπλοκ εισόδου και της ακολουθίας εξόδου οι μπλοκ κώδικες κατηγοριοποιούνται ως: κώδικες σταθερού σε σταθερό μήκος, κώδικες σταθερού σε μεταβλητό μήκος, κώδικες μεταβλητού σε σταθερό μήκος και κώδικες μεταβλητού σε μεταβλητό μήκος. Μια αρκετά συνηθισμένη περίπτωση είναι οι κώδικες σταθερού σε σταθερό μήκος, όπου τα μπλοκς εισόδου και εξόδου έχουν όλα το ίδιο μήκος.

1.3 Κώδικες δέντρου

Οι κώδικες δέντρου ανήκουν στην κατηγορία των κωδίκων με μνήμη. Η διαφορά τους από τους μπλοκ κώδικες είναι ότι τα σύμβολα εξόδου εξαρτώνται όχι μόνο από τα τρέχοντα σύμβολα εισόδου αλλά και από τα προηγούμενα σύμβολα εισόδου. Οι κώδικες δέντρου αντιστοιχούν πλαίσια συμβόλων εισόδου μήκους n σε πλαίσια συμβόλων εξόδου μήκους k με την αντιστοίχιση αυτή να εξαρτάται από προηγούμενα m πλαίσια εισόδου. Αν και το m μπορεί να είναι άπειρο σε πρακτικές εφαρμογές είναι πεπερασμένο, δηλαδή υπάρχει πεπερασμένη μνήμη. Όταν το m είναι πεπερασμένο οι κώδικες δέντρου ονομάζονται κώδικες δικτυώματος (trellis codes). Κατ' αντιστοιχία, υπάρχουν οι κώδικες δέντρου: σταθερού σε σταθερό μήκος, σταθερού σε μεταβλητό μήκος, μεταβλητού σε σταθερό μήκος και μεταβλητού σε μεταβλητό μήκος. Ένα παράδειγμα ενός κώδικα δέντρου φαίνεται στο σχήμα 1.4. Ένας κώδικας δέντρου ονομάζεται κώδικας ολίσθησης (sliding block codes) εάν η διαδικασία κωδικοποίησης είναι χρονικά αμετάβλητη. Ειδικότερα ένας γραμμικός κώδικας ολίσθησης μπλοκ ονομάζεται συνελκτικός ή συγκεραστικός (convolutional codes).



Σχήμα 1.4: Παράδειγμα κώδικα δέντρου

1.4 Ιστορική αναδρομή

Η έννοια της θεωρίας πληροφορίας ξεκίνησε από το έργο του Claude Shannon “The Mathematical Theory of Communication” που δημοσιεύθηκε το 1949 [53]. Σε αυτήν την εργασία θέτονται τα θεμέλια για την κατανόηση και μετάδοση της πληροφορίας μέσω ενός τηλεπικοινωνιακού συστήματος.

Στην εργασία του Shannon δίνεται η γενική ιδέα για την αρχιτεκτονική ενός τηλεπικοινωνιακού συστήματος. Η συνολική διαδικασία διασπάται σε επιμέρους στοιχεία. Πλέον το κάθε στοιχείο μελετάται και σχεδιάζεται ξεχωριστά. Από την ανάλυση αυτή, ο Shannon αντιλήφθηκε ότι το περιεχόμενο ενός μηνύματος δεν σχετίζεται με τη μετάδοσή του και μπορεί να αναπαρασταθεί απλά από μια ακολουθία από bits. Με αυτήν την σκέψη ο Shannon εισάγει την κωδικοποίηση πηγής που πλέον είναι συνώνυμη με τη συμπίεση δεδομένων. Βασική ιδέα της κωδικοποίησης πηγής είναι η αφαίρεση του όποιου πλεονασμού της πληροφορίας έτσι ώστε ο όγκος των δεδομένων προς μετάδοση (ή αποθήκευση) να είναι όσον το δυνατόν μικρότερος. Ταυτόχρονα αποδεικνύει ότι για AWGN (Additive White Gaussian Channel) κανάλια υπάρχει ένα όριο (η χωρητικότητα του καναλιού) πέραν του οποίου δεν υπάρχει αξιόπιστη επικοινωνία. Εάν όμως ο ρυθμός μετάδοσης κρατηθεί μικρότερος της χωρητικότητας του καναλιού τότε υπάρχει τρόπος κωδικοποίησης των δεδομένων ώστε να επιτυγχάνεται αυθαίρετα μικρή πιθανότητα σφάλματος. Η διαδικασία αυτή ονομάζεται κωδικοποίηση διόρθωσης σφαλμάτων ή γενικότερα κωδικοποίηση καναλιού.

Η εργασία του Shannon είναι ιστορική καθώς δημιούργησε το επιστημονικό κλάδο της Θεωρίας Πληροφορίας. Σύντομα το Ινστιτούτο των Ραδιομηχανικών (IRE - Institute of Radio Engineers) ξεκίνησε να δημοσιεύει εργασίες στο αντικείμενο της Θεωρίας Πληροφορίας. Λίγο καιρό αργότερα μία ομάδα καθηγητών διεθνούς εμβέλειας, όπως ο Peter Elias, ο Norbert Wiener, ο Robert Fano κ.ά., ονομαζόμενη PGIT (Professional Group of Information Theory) καθόριζε τα όρια και την ερευνητική κατεύθυνση που έπρεπε να ακολουθήσει η Θεωρία Πληροφορίας.

1.5 Ιστορική αναδρομή κωδικοποίησης καναλιού

Η εργασία του Shannon έθεσε ένα σύνολο νέων ιδεών και απαιτήσεων για ένα τηλεπικοινωνιακό σύστημα. Η κωδικοποίηση καναλιού ξεχάστηκε για ένα αρκετά μεγάλο χρονικό διάστημα. Η έρευνα είχε επικεντρωθεί στην κωδικοποίηση πηγής, ενώ το πρόβλημα της αποτελεσματικής μετάδοσης λυνόταν με απλές μεθόδους όπως αύξηση της ισχύος μετάδοσης. Η σημασία του θεωρήματος του Shannon για τα ενθόρυβα κανάλια αναγνωρίστηκε μετά από μία δεκαετία περίπου. Έπειτα από κάποια χρόνια έρευνας οι επιστήμονες συμπέραναν ότι η καλύτερη μέθοδος για την προσέγγιση της χωρητικότητας του καναλιού δεν ήταν η πολύπλοκη κωδικοποίηση, αλλά η εύρεση αποτελεσματικών μεθόδων αποκωδικοποίησης.

1.6 Αλγεβρικοί κώδικες

Οι αλγεβρικοί κώδικες είναι μπλοκ κώδικες και έχουν βασικό χαρακτηριστικό τους την έλλειψη μνήμης. Οι πρώτοι κώδικες καναλιού που αναπτύχθηκαν ήταν οι αλγεβρικοί. Πιο συγκεκριμένα, αμέσως μετά την εργασία του Shannon ο συνεργάτης του Hamming επινόησε την οικογένεια κωδίκων Hamming με παραμέτρους ($n = 2^m - 1, k = 2^m - 1 - m, d = 3$). Οι κώδικες Hamming χαρακτηρίζονται ως "τέλειοι" (perfect codes) και η χρήση 2^k κωδικολέξεων μήκους n κάνει εφικτή την διόρθωση ενός σφάλματος. Λίγο αργότερα ο μαθηματικός Marcel Golay [52] επινοεί τον τέλειο δυαδικό κώδικα $(23, 12, 7)$ ικανό να διορθώσει 3 σφάλματα με χρήση 2^{12} κωδικολέξεων μήκους $n = 23$.

Λίγα χρόνια αργότερα, το 1954, αναπτύχθηκαν οι Reed-Muller (RM) κώδικες από τους David Muller και Irving Reed [50] [51]. Οι RM κώδικες έχουν μια ιδιαίτερη δομή που τους κάνει πολύ ευέλικτους. Στους RM κώδικες συναντώνται πολλές διαφορετικές κατηγορίες κωδίκων. Για παράδειγμα, οι κώδικες επανάληψης, οι κώδικες ελέγχου απλής ισοτιμίας, οι εκτεταμένοι Hamming κώδικες, οι διορθογώνιοι κώδικες και, οι αυτο-δυικοί (self-dual) κώδικες ανήκουν στους RM κώδικες. Βασικό χαρακτηριστικό των RM κωδίκων είναι ότι η αποκωδικοποίηση βασίζεται στη λογική πλειοψηφίας (majority-logic decoding rule).

Τη δεκαετία του 1960 η έρευνα στην κωδικοποίηση καναλιού επικεντρώθηκε στους κυκλικούς κώδικες. Ωστόσο η ναυαρχίδα των αλγεβρικών μπλοκ κυκλικών κωδίκων είναι οι κώδικες Bose-Chaudhuri-Hocquengham (BCH) και οι κώδικες Reed-Solomon (RS) [47] [48] [49]. Οι RS κώδικες είναι μια ειδική περίπτωση μη δυαδικών BCH κωδίκων. Οι BCH κώδικες συμπεριλαμβάνουν μία μεγάλη κατηγορία κωδίκων που είναι ικανοί να διορθώνουν t σφάλματα (όταν η ελάχιστη απόσταση Hamming είναι $d = 2t + 1$), για μήκος κωδικολέξεων $n = 2^m - 1$ και $k \geq n - mt$. Συγκριτικά με επιβραχυμένους RM κώδικες του ίδιου μήκους $n = 2^m - 1$ υπάρχουν πολύ περισσότεροι BCH κώδικες. Οι BCH κώδικες εφαρμόστηκαν στα κυψελωτά αναλογικά συστήματα επικοινωνίας κινητών 1ης γενιάς.

Την δεκαετία του 1970 έγινε ξεκάθαρο ότι η περαιτέρω έρευνα στους μπλοκ κώδικες ήταν άκαρπη. Λίγες νέες τεχνικές κωδικοποίησης ανακαλύφθηκαν, όπως οι Algebraic Geometry κώδικες το 1977. Την σκυτάλη ανέλαβαν οι πιθανοκρατικοί κώδικες.

1.7 Πιθανοκρατικοί κώδικες

Οι πιθανοκρατικοί κώδικες ονομάζονται και κώδικες γράφων. Ενώ οι αλγεβρικοί κώδικες στοχεύουν στην εύρεση κωδίκων που μεγιστοποιούν την ελάχιστη απόσταση d για δεδομένα (n, k) , οι

πιθανοκρατικοί κώδικες στοχεύουν στη μεγιστοποίηση της μέσης επίδοσης του κώδικα, όσον αφορά στην πολυπλοκότητα κωδικοποίησης και αποκωδικοποίησης. Ο κύριος αντιπρόσωπος των πιθανοκρατικών κωδίκων είναι οι συνελκτικοί κώδικες που αναπτύχθηκαν το 1955 από τον Peter Elias [46]. Στην κατηγορία των πιθανοκρατικών κωδίκων ανήκουν οι συνελκτικοί κώδικες, οι κώδικες γινομένου (product codes), οι αλυσιδωτοί κώδικες (concatenated codes), οι LDPC (Low Density Parity Check), οι Turbo κώδικες και η κατά trellis κωδικοποιημένη διαμόρφωση (TCM - Trellis Coded Modulation).

Ήδη από το 1955, όποτε και ανακαλύφθηκαν οι συνελκτικοί κώδικες, από τον Peter Elias ήταν φανερό ότι οι πιθανοκρατικοί κώδικες πλησιάζουν το όριο της χωρητικότητας που είχε θέσει ο Shannon. Σύντομα μετά την ανακάλυψη των συνελκτικών κωδίκων ακολούθησε η επινόηση μιας σειράς μεθόδων αποκωδικοποίησης. Για παράδειγμα η ακολουθιακή αποκωδικοποίηση, η αποκωδικοποίηση κατωφλίου [45], η αποκωδικοποίηση Viterbi [44], η αποκωδικοποίηση αθροίσματος-γινομένου κ.α.

Γενικά οι συνελκτικοί κώδικες μπορούν να αναπαρασταθούν με τη βοήθεια ενός διαγράμματος μετάπτωσης καταστάσεων (state transition diagram). Με την ανάπτυξη του διαγράμματος μετάπτωσης καταστάσεων στο χρόνο, οδηγούμαστε στο διάγραμμα δικτύωματος (trellis diagram). Το διάγραμμα trellis περιέχει όλη την πληροφορία για τις κωδικολέξεις αφού αυτές είναι ουσιαστικά οι δυνατές διαδρομές μέσα στο διάγραμμα. Παραταύτα, η άφιξη των turbo [43] και LDPC [42] κωδίκων περιθωριοποίησε την χρήση των συνελκτικών κωδίκων.

2. Εισαγωγή στους πολικούς κώδικες

Η κωδικοποίηση καναλιού έχει ως στόχο την αντιστοίχιση της πληροφορίας σε κατάλληλες ακολουθίες συμβόλων (codewords) έτσι ώστε στο δέκτη να είναι δυνατή η ταυτοποίησή τους παρουσία σφαλμάτων μετάδοσης. Η κωδικοποίηση καναλιού εισάγει κάποια μορφή ευφυίας στο σύστημα η οποία έγκειται τόσο στην διαδικασία κωδικοποίησης όσο και στην διαδικασία αποκωδικοποίησης. Εν γένει μία ακολουθία πληροφορίας από k σύμβολα αντιστοιχίζεται σε μία ακολουθία από n σύμβολα με $n > k$. Αν τα σύμβολα λαμβάνονται από το δυαδικό αλφάβητο (bits) τότε ο κώδικας ονομάζεται δυαδικός. Τα επιπρόσθετα $n - k$ bits (bits ισοτιμίας) επιλέγονται με τέτοιο τρόπο ώστε η απόσταση (Hamming απόσταση) μεταξύ των κωδικολέξεων να είναι η μέγιστη δυνατή. Η διορθωτική (ή/και η ανιχνευτική) ικανότητα ενός κώδικα εξαρτάται από την ελάχιστη απόσταση Hamming μεταξύ των κωδικολέξεων. Υπάρχει λοιπόν μία ανταλλαγή ρυθμού $R = k/n$ και ελάχιστης Hamming απόστασης ή αλλιώς της αξιοπιστίας μετάδοσης. Σύμφωνα με το Θεώρημα του Shannon εάν ο ρυθμός μετάδοσης R είναι μικρότερος της χωρητικότητας του καναλιού C υπάρχει τρόπος κωδικοποίησης ώστε να επιτυγχάνεται αυθαίρετα μικρή πιθανότητα σφάλματος στο δέκτη. Η έρευνα λοιπόν στράφηκε στην εύρεση κωδίκων που μας επιτρέπουν να λειτουργούμε στο θεωρητικό όριο του Shannon αλλά ταυτόχρονα η αποκωδικοποίηση αυτών να έχει όσο το δυνατόν μικρότερη πολυπλοκότητα. Θα πρέπει να τονίσουμε ότι το πρόβλημα της κωδικοποίησης καναλιού είναι κατά κάποιον τρόπο το δυϊκό του προβλήματος κωδικοποίησης πηγής. Στην κωδικοποίηση πηγής ο στόχος είναι να μειώσουμε τον πλεονασμό στα δεδομένα, η κωδικοποίηση είναι δύσκολη διαδικασία ενώ η αποκωδικοποίηση είναι η εύκολη διαδικασία. Αντίθετα στην κωδικοποίηση καναλιού, εισάγουμε πλεονασμό στην πληροφορία μας με σκοπό να διευκολύνουμε την ανίχνευση ή και διόρθωση σφαλμάτων κατά την μετάδοση. Η κωδικοποίηση καναλιού είναι η εύκολη διαδικασία ενώ η αποκωδικοποίηση είναι η διαδικασία μεγάλης πολυπλοκότητας.

Με την πρόοδο της τεχνολογίας και την εμφάνιση νέων γενεών (G) οι απαιτήσεις που πρέπει να ικανοποιούν οι νέοι κώδικες είναι όλο και περισσότερες. Δεν αρκεί να βρεθούν νέες τεχνικές κωδικοποίησης καναλιού που είναι απλώς πιο ικανές στο να επιτυγχάνουν πιο αξιόπιστη επικοινωνία (βελτιώνοντας το BER), αλλά η πολυπλοκότητα της αποκωδικοποίησης, η καθυστέρηση της αποκωδικοποίησης καθώς και το μήκος των κωδικολέξεων διαδραματίζουν σημαντικό ρόλο στην επιλογή του κατάλληλου κώδικα. Για παράδειγμα, στις περιπτώσεις όπου ο στόχος είναι η αξιόπιστη επικοινωνία με πολύ μικρή καθυστέρηση (low latency) μεταξύ πομπού και δέκτη, χρειάζεται μια κωδικοποίηση με πολύ αποτελεσματικό αλγόριθμο αποκωδικοποίησης. Επίσης, εκτός από δεδομένα μεταδίδονται και σήματα ελέγχου τα οποία έχουν εν γένει μικρότερο μήκος. Η κωδικοποίηση που θα χρησιμοποιηθεί θα πρέπει να αποτελεσματική για μικρού μήκους κωδικολέξεις. Η πολυπλοκότητα της αποκωδικοποίησης είναι ένα πολύ σημαντικό κριτήριο που καθορίζει εάν ένας κώδικας είναι καλός για πρακτική χρήση ή όχι, αφού από την πολυπλοκότητα εξαρτάται πόση ενέργεια καταναλώνεται από το hardware του συστήματος, πόση μνήμη χρειάζεται το σύστημα και άλλα.

Το 1948 ο Shannon όρισε τη χωρητικότητα ενός καναλιού ως ένα άνω όριο του επιτεύξιμου ρυθμού μετάδοσης για αξιόπιστη επικοινωνία. Μέχρι πρόσφατα, κανένας από τους προταθέντες κώδικες δεν είχε μαθηματικά αποδειχθεί ότι μπορούσε να πετύχει την χωρητικότητα του Shannon. Το 2009 παρουσιάστηκε μια εργασία από τον καθηγητή Erdal Arıkan στην οποία αναλύεται η θεμελιώδης λειτουργία των πολικών κωδίκων. Στην εργασία αυτή αποδεικνύεται και μαθηματικά πως η χωρητικότητα μπορεί να επιτευχθεί καθώς το μήκος των κωδικολέξεων του κώδικα αυξάνεται προς το άπειρο. Επιπλέον οι πολικοί κώδικες έχουν την ιδιότητα χαμηλής πολυπλοκότητας

κωδικοποίησης/αποκωδικοποίησης χωρίς ιδιαίτερα μεγάλη επιβάρυνση. Αυτή η ιδιότητα καθιστά τους πολικούς κώδικες πολύ ελκυστικούς για χρήση σε τεχνολογίες 5G και αμέσως υιοθετήθηκαν στα πρότυπα 5G.

Οι πολικοί κώδικες ανήκουν στην κατηγορία των γραμμικών μπλοκ κωδίκων διόρθωσης σφαλμάτων. Η κατασκευή του πολικού κώδικα βασίζεται σε μια πολλαπλή αναδρομική συνένωση ενός βασικού πίνακα γεννήτορα - kernel table (όπως φαίνεται στο Σχήμα 2.1) με τον εαυτό του, που μετατρέπει ένα σύνολο φυσικών καναλιών σε νέα εικονικά κανάλια, όπως τα αντιλαμβάνεται ο δέκτης που χρησιμοποιεί αποκωδικοποίηση διαδοχικής ακύρωσης. Όταν ο αριθμός των bit εισόδου γίνεται μεγάλος, τα εικονικά κανάλια τείνουν είτε να έχουν υψηλή αξιοπιστία είτε χαμηλή αξιοπιστία (με άλλα λόγια, πολώνονται). Στην συνέχεια τα bits δεδομένων μεταφέρονται στα πιο αξιόπιστα κανάλια. Είναι ο πρώτος κώδικας με κατασκευή που αποδεδειγμένα επιτυγχάνει τη χωρητικότητα καναλιού για B-DMC κανάλια. Οι άλλοι κώδικες που είναι διαθέσιμοι απλώς πλησιάζουν το όριο χωρητικότητας του Shannon, αλλά το κάνουν χωρίς κανέναν μαθηματικά αποδεδειγμένο τρόπο. Η χωρητικότητα αυτών των κωδίκων είναι πολύ κοντά στο όριο χωρητικότητας, αλλά αποδεικνύεται μόνο μέσω προσομοίωσης που δεν αποτελεί επιβεβαιωμένη απόδειξη (LDPC, Turbo, Reed-Solomon). Γενικά οι πολικοί κώδικες μπορούν να χρησιμοποιηθούν σε τηλεπικοινωνιακά συστήματα που είναι ευάλωτα σε σφάλματα λόγω του τυχαίου θορύβου, παρεμβολών κ.λπ.

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Σχήμα 2.1: Πίνακας γεννήτορας G_2 , G_4 για N ίσο με 2 και 4 αντίστοιχα.

Συγκεκριμένα, οι πολικοί κώδικες έχουν πολυπλοκότητα κωδικοποίησης και αποκωδικοποίησης $O(N \cdot \log N)$, γεγονός που τους καθιστά ελκυστικούς για πολλές εφαρμογές. Επιπλέον, η ενεργειακή κατανάλωση κατά την κωδικοποίηση και αποκωδικοποίηση των πολικών κωδίκων μπορεί να φτάσει τα θεμελιώδη κατώτατα όρια κατανάλωσης ενέργειας του κυκλώματος αφού η πολυπλοκότητα του κυκλώματος είναι τάξης $O(N \cdot \text{poly}(\log(N)))$. Παρά ταύτα οι πολικοί κώδικες έχουν ορισμένους περιορισμούς όταν χρησιμοποιούνται σε βιομηχανικές εφαρμογές. Η βασική ιδιότητα των πολικών κωδίκων είναι ότι επιτυγχάνουν την χωρητικότητα όταν τα μεγέθη των μπλοκ από bits είναι ασυμπτωτικά μεγάλα. Ωστόσο, με τα μεγέθη των μπλοκ από bits που χρησιμοποιούνται στην πράξη, και με την τεχνική αποκωδικοποίησης διαδοχικής ακύρωσης, οι πολικοί κώδικες έχουν κακή επίδοση σε σύγκριση με καλά καθορισμένα και εφαρμοσμένα σχήματα κωδικοποίησης, όπως οι LDPC και οι turbo κώδικες. Η επίδοση των πολικών κωδίκων μπορεί να βελτιωθεί με την χρήση αποκωδικοποίησης διαδοχικής ακύρωσης με λίστα, αλλά η χρησιμότητά της σε πραγματικές εφαρμογές εξακολουθεί να είναι αμφισβητήσιμη λόγω της πολύ κακής επίδοσης που προκαλείται από την επαναληπτική προσέγγιση. Τελικά μετά από αρκετή έρευνα, τον Οκτώβριο του 2016, η Huawei ανακοίνωσε ότι είχε επιτύχει 27 Gbit/s σε δοκιμές πεδίου 5G χρησιμοποιώντας πολικούς κώδικες για την κωδικοποίηση καναλιών. Οι βελτιώσεις που έχουν εισαχθεί στο τελικό μοντέλο έχουν ως αποτέλεσμα την αξιοπιστία του καναλιού να έχει σχεδόν κλείσει στο όριο Shannon, το οποίο θέτει τον μέγιστο ρυθμό για ένα δεδομένο εύρος ζώνης και ένα δεδομένο επίπεδο θορύβου. Τον Νοέμβριο του 2016, το 3GPP συμφώνησε να υιοθετήσει τους πολικούς κώδικες για τα κανάλια ελέγχου eMBB (Enhanced Mobile Broadband) για τη διεπαφή 5G NR. Στην ίδια συνάντηση, η 3GPP

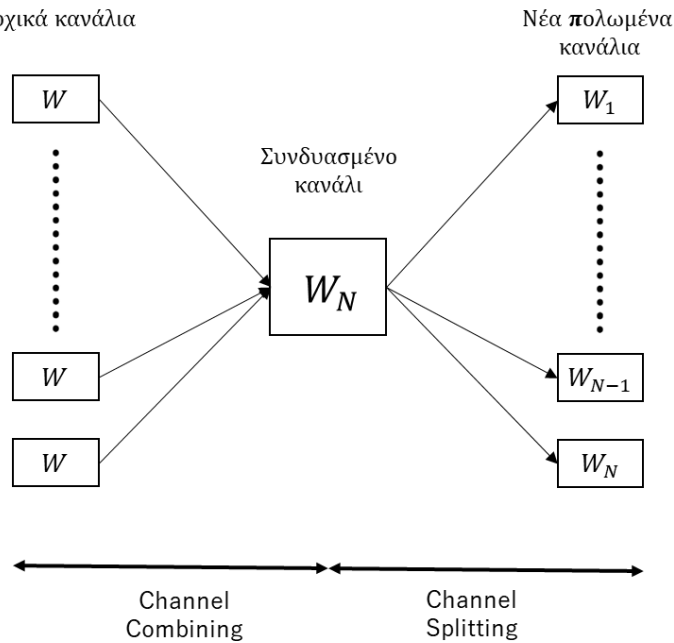
συμφώνησε να χρησιμοποιήσει τους LDPC κώδικες για τα αντίστοιχα κανάλια δεδομένων. Εντούτοις η χρήση των πολικών κωδίκων στα κανάλια ελέγχου δείχνει πόσο σημαντικός είναι ο ρόλος τους, αφού τα κανάλια ελέγχου (control channels) είναι πιο σημαντικά από τα κανάλια δεδομένων (data channels) επειδή τα κανάλια ελέγχου είναι αυτά που είναι υπεύθυνα για την “καθοδήγηση” των δεδομένων και της πληροφορίας που απαιτείται για την επιτυχή ανάκτηση των δεδομένων που στάλθηκαν.

Το θεμελιώδες χαρακτηριστικό των πολικών κωδίκων είναι η πόλωση καναλιών (channel polarization). Η πόλωση των καναλιών οφείλεται στην αύξηση και μείωση της αξιοπιστίας των εικονικών καναλιών που αντιλαμβάνεται ο δέκτης που χρησιμοποιεί αλγόριθμο αποκωδικοποίησης διαδοχικής ακύρωσης. Μέσω της πόλωσης των καναλιών (channel polarization), τα εικονικά κανάλια διαχωρίζονται σε δύο κατηγορίες: τα αξιόπιστα κανάλια σε ποσοστό $I(W)$ (συμμετρική χωρητικότητα φυσικού καναλιού) και τα αναξιόπιστα κανάλια σε ποσοστό $1 - I(W)$. Στη συνέχεια, η ιδέα είναι να αποστέλλονται δεδομένα μόνο στα αξιόπιστα κανάλια. Κάτι παρόμοιο, με τους πολικούς κώδικες, γίνεται στο επίπεδο διαμόρφωσης του σήματος, όπου επιλέγονται προς διαμόρφωση τα καλύτερα κανάλια (subchannels), με βάση το SNR ή και την παρεμβολή. Η βασική διαφορά μεταξύ της πόλωσης των καναλιών και της επιλογής καναλιού (κατά την διαμόρφωση σήματος), είναι ότι στην πολική κωδικοποίηση τα κανάλια με τη χαμηλή αξιοπιστία είναι αυτά εξαιτίας των οποίων τα υπόλοιπα κανάλια γίνονται αξιόπιστα, λόγω της διαδικασίας της περίπλεξης όλων των φυσικών καναλιών W . Τα bits που μεταφέρονται στα αναξιόπιστα κανάλια ονομάζονται “frozen bits” και λαμβάνουν μία προκαθορισμένη τιμή. Κατά την επιλογή των φορέων (subcarriers), στην διαμόρφωση του σήματος, είναι τα ενθόρυβα κανάλια που περιορίζουν την επίδοση της μετάδοσης. Στην πολική κωδικοποίηση τα μη αξιόπιστα κανάλια εξακολουθούν να χρησιμοποιούνται καθώς με τη βοήθεια αυτών και των προκαθορισμένων εισόδων τους τα υπόλοιπα κανάλια καθίστανται αθόρυβα (noiseless).

Πιο απλά, η πόλωση των καναλιών είναι μια διαδικασία από την οποία από N ανεξάρτητα αντίγραφα ενός δεδομένου B-DMC καναλιού W , μπορεί να δημιουργηθεί ένα δεύτερο σύνολο N καναλιών δυαδικής εισόδου, $W_i : \{1 \leq i \leq N\}$. Καθώς το N γίνεται μεγάλο, το κλάσμα των δεικτών i για τους οποίους το $I(W_i)$ είναι κοντά στο 1 προσεγγίζεται από την τιμή $I(W)$ και αντίστοιχα το κλάσμα για το οποίο το $I(W_i)$ είναι κοντά στο 0 προσεγγίζεται από την τιμή $1 - I(W)$. Κατά συνέπεια ο πομπός στέλνει δεδομένα μόνο σε εκείνα τα νέα κανάλια W_i για τα οποία η χωρητικότητα είναι κοντά στο 1. Το αποτέλεσμα είναι τα νέα πολωμένα κανάλια W_i να είναι καλά προετοιμασμένα για την αποκωδικοποίηση καναλιού. Αυτό που απομένει είναι η αποστολή δεδομένων με ρυθμό 1 μέσω των αξιόπιστων καναλιών όπου η χωρητικότητα είναι κοντά στο 1 και αντίστοιχα η αποστολή δεδομένων με ρυθμό 0 στα υπόλοιπα κανάλια. Για αυτό οι κώδικες που κατασκευάζονται με βάση αυτή την ιδέα ονομάζονται πολικοί κώδικες. Δεδομένου οποιουδήποτε B-DMC καναλιού με $I(W) > 0$ και οποιουδήποτε ρυθμού $R < I(W)$ υπάρχει μια ακολουθία πολικών κωδίκων $\{C_n : n \geq 1\}$ έτσι ώστε το C_n να έχει μήκος μπλοκ $N = 2^n$, ρυθμό $\geq R$, και πιθανότητα σφάλματος $P(N, R) \leq O(N^{-1})$ (μέσω της αποκωδικοποίησης διαδοχικής ακύρωσης - SC decoding) ανεξάρτητα από τον ρυθμό R . Η επίδοση αυτή μπορεί να επιτευχθεί με κωδικοποιητές και αποκωδικοποιητές πολυπλοκότητας $O(N \cdot \log N)$.

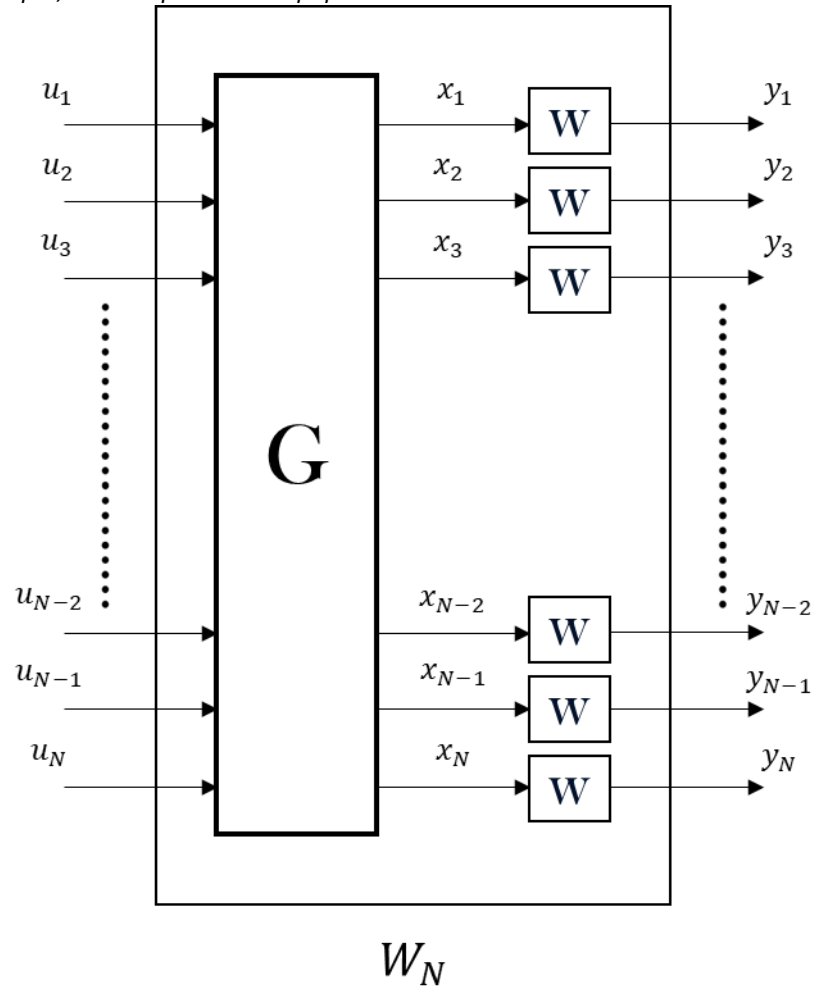
Πιο συγκεκριμένα ο μετασχηματισμός της πολικής κωδικοποίησης περιλαμβάνει δύο βασικές λειτουργίες που ονομάζονται συνδυασμός καναλιών (channel combining) και διαχωρισμός καναλιών (channel splitting) όπως φαίνεται στο σχήμα 2.2.

Αρχικά κανάλια



Σχήμα 2.2: Συνδυασμός καναλιών (channel combining) και διαχωρισμός καναλιών (channel splitting)

Ο συνδυασμός καναλιών καταχωρεί συνδυασμούς από bit σε συγκεκριμένα κανάλια, ενώ ο διαχωρισμός καναλιών που ακολουθεί εκτελεί μια λειτουργία μετασχηματισμού μετατρέποντας αυτούς τους συνδυασμούς bit σε διανύσματα έτοιμα για αποκωδικοποίηση. Η διαδικασία φαίνεται καλύτερα στο σχήμα 2.3, όπου το συνδυασμένο κανάλι ονομάζεται W_N . Ακολουθεί η αποκωδικοποίηση, όπου γίνονται οι εκτιμήσεις των αρχικών bits εισόδου χρησιμοποιώντας την τεχνική αποκωδικοποίησης διαδοχικής ακύρωσης SCD (successive cancellation decoding). Ο συνδυασμός καναλιών, ο διαχωρισμός καναλιών και η αποκωδικοποίηση στην ουσία μετατρέπουν ένα μπλοκ από bits σε μια πολωμένη ροή από bits στον δέκτη. Με αυτόν τον τρόπο, ένα ληφθέν bit και το σχετικό του κανάλι καταλήγουν να είναι είτε "καλό κανάλι" ή "κακό κανάλι".



Σχήμα 2.3: Νέο σύνολο καναλιών $W_{(i)}$ όπου $1 \leq i \leq N$ που προκύπτει από N ανεξάρτητα αντίγραφα του καναλιού W

Τα πλεονεκτήματα και μειονεκτήματα των πολικών κωδίκων συνοψίζονται παρακάτω.

Πλεονεκτήματα:

- I. Σταθερή και ντετερμινιστική πολυπλοκότητα κωδικοποίησης και αποκωδικοποίησης (δεν εξαρτάται από τα κανάλια)
- II. Χαμηλή υπολογιστική πολυπλοκότητα (γνωστά xor και flip flops)
- III. Σαφής κατασκευή (βήμα προς βήμα)
- IV. Εύκολο στην εφαρμογή
- V. Δεν προκαλεί μεγάλο χρόνο καθυστέρησης
- VI. Δεν έχει μεγάλες απαιτήσεις hardware (δεν καταναλώνει υπερβολική ενέργεια κατά τη χρήση του)

VII. Παρουσιάζει εξαιρετική αξιοπιστία κάτω από προηγμένους αποκωδικοποιητές (με εξελιγμένους αποκωδικοποιητές μπορεί να δώσει πολύ καλή αξιοπιστία)

VIII. Δεν έχουν ελάχιστα όρια σφαλμάτων (error floors) κατά την χρήση τους (όταν μια κωδικοποίηση καναλιού έχει ελάχιστα όρια σφαλμάτων τότε αναμένεται η μη βελτίωση του BER καθώς αυξάνεται το SNR, δηλαδή από ένα σημείο και μετά επιτυγχάνεται το ελάχιστο όριο του BER, ωστόσο δεν υπάρχει ανώτατο όριο στους πολικούς κώδικες)

Μειονεκτήματα:

I. Για πεπερασμένο N , η αξιοπιστία που προσφέρουν οι πολικοί κώδικες με χρήση του SCD είναι κατώτερη από την αξιοπιστία που προσφέρουν οι LDPC κώδικες (για να ξεπεραστούν οι LDPC κώδικες απαιτείται ένας πιο εξελιγμένος αποκωδικοποιητής)

II. Η χρήση ενός διαφορετικού αποκωδικοποιητή συνοδεύεται από την μείωση της απόδοσης του συστήματος σε άλλους τομείς (αύξηση της πολυπλοκότητας κατανάλωσης και αποκωδικοποίησης, υψηλότερη καθυστέρηση, ύπαρξη μιας μέγιστης τιμής του BER κ.α.)

3. Κωδικοποίηση πολικών κωδίκων

3.1 Βασική αρχή πολικών κωδίκων

Οι πολικοί κώδικες αρχικά έγιναν γνωστοί λόγω του τίτλου τους ως “κώδικες που αποδεδειγμένα επιτυγχάνουν την χωρητικότητα του καναλιού”, ωστόσο ο τίτλος αυτός δεν περιγράφει την καινοτομία που κρύβεται πίσω από την βασική ιδέα των πολικών κωδίκων. Η βασική ιδέα που διαφοροποίησε τους πολικούς κώδικες από άλλους κώδικες είναι ότι, κατά κάποιο τρόπο, λαμβάνεται υπ’ όψιν η φύση του καναλιού κατά την σχεδίαση του κώδικα.

Η ιδέα είναι ότι ο κώδικας θα είναι πολύ εύκολος σε δυο περιπτώσεις καναλιών:

1. Όταν το κανάλι θα έχει $C(W) = 1$ (τέλειο κανάλι), δηλαδή θα είναι ένα κανάλι χωρίς θόρυβο, όπου στην ουσία δεν χρειάζεται καμία μορφή κωδικοποίησης, αφού τα δεδομένα που στέλνονται περνάνε άθικτα μέσα από το κανάλι,
2. Όταν το κανάλι θα έχει $C(W) = 0$ (ενθόρυβο κανάλι), όπου πάλι δεν χρειάζεται καμία μορφή κωδικοποίησης, αφού είναι δεδομένο ότι η πληροφορία θα αλλοιωθεί πλήρως από το κανάλι.

Και στις δυο παραπάνω περιπτώσεις το κανάλι είναι B-DMC, το οποίο έχει μέγιστη χωρητικότητα $C(W) = 1$ και ελάχιστη χωρητικότητα $C(W) = 0$.

Η ανάγκη της ίδιας της κωδικοποίησης υπάρχει επειδή στην φύση κανένα κανάλι δεν είναι τέλειο ή εντελώς άχρηστο. Με αυτήν την λογική ο στόχος των πολικών κωδίκων είναι να μετατρέψουν ένα σύνολο από N ανεξάρτητα κανάλια W σε ένα σύνολο από N ακραία κανάλια, που θα είναι είτε τέλεια είτε άχρηστα. Η παραπάνω διαδικασία της δημιουργίας των N ακραίων καναλιών ονομάζεται αλλιώς ως πόλωση των καναλιών (channel polarization).

3.2 Μοντέλα καναλιών

Ένα τηλεπικοινωνιακό κανάλι περιγράφεται από το αλφάβητο εισόδου X , που είναι το σύνολο των δυνατών εισόδων του καναλιού, το αλφάβητο εξόδου Y , που είναι το σύνολο των εξόδων, και τις δεσμευμένες πιθανότητες μετάβασης $p(y|x)$, όπου $x = (x_1, x_2 \dots x_n)$ είναι μία ακολουθία εισόδου n συμβόλων και $y = (y_1, y_2 \dots y_n)$ η αντίστοιχη έξοδος του καναλιού. Το κανάλι καλείται χωρίς μνήμη εάν

$$p(y | x) = p(y_1, \dots, y_n | x_1, \dots, x_n) = \prod_{i=1}^n p(y_i | x_i)$$

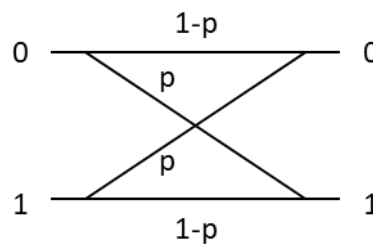
Με άλλα λόγια, το κανάλι είναι χωρίς μνήμη εάν η έξοδος τη χρονική στιγμή i εξαρτάται μόνο από την είσοδο τη χρονική στιγμή i . Εν γένει το μοντέλο ενός καναλιού έχει δύο συνιστώσες, τη στοχαστική και τη νομοτελειακή. Η στοχαστική συνιστώσα μοντελοποιεί φαινόμενα όπως ο θόρυβος, οι διαλείψεις, ενώ η νομοτελειακή συνιστώσα μοντελοποιεί φαινόμενα όπως η ενδοσυμβολική παρεμβολή (ISI - Intersymbol Interference). Η έλλειψη μνήμης ενός καναλιού μεταφράζεται σε έλλειψη ISI μεταξύ συμβόλων.

3.2.1 Το δυαδικό συμμετρικό κανάλι (BSC - Binary Symmetric Channels)

Το απλούστερο μοντέλο καναλιού είναι το δυαδικό συμμετρικό κανάλι, για το οποίο το αλφάβητο εισόδου και εξόδου είναι $X = Y = \{0, 1\}$. Αυτό το μοντέλο καναλιού είναι κατάλληλο για δυαδικές διαμορφώσεις και hard αποφάσεις του φωρατή. Το BSC κανάλι απεικονίζεται παραστατικά στο Σχήμα 3.1. Για το κανάλι αυτό ισχύει ότι:

$$p(y = 0 | x = 0) = p(y = 1 | x = 1) = 1 - p \quad p(y = 1 | x = 0) = p(y = 0 | x = 1) = p$$

όπου p είναι η πιθανότητα σφάλματος και καλείται πιθανότητα διασταύρωσης (crossover probability.)



Σχήμα 3.1: Δυαδικό Συμμετρικό Κανάλι (BSC)

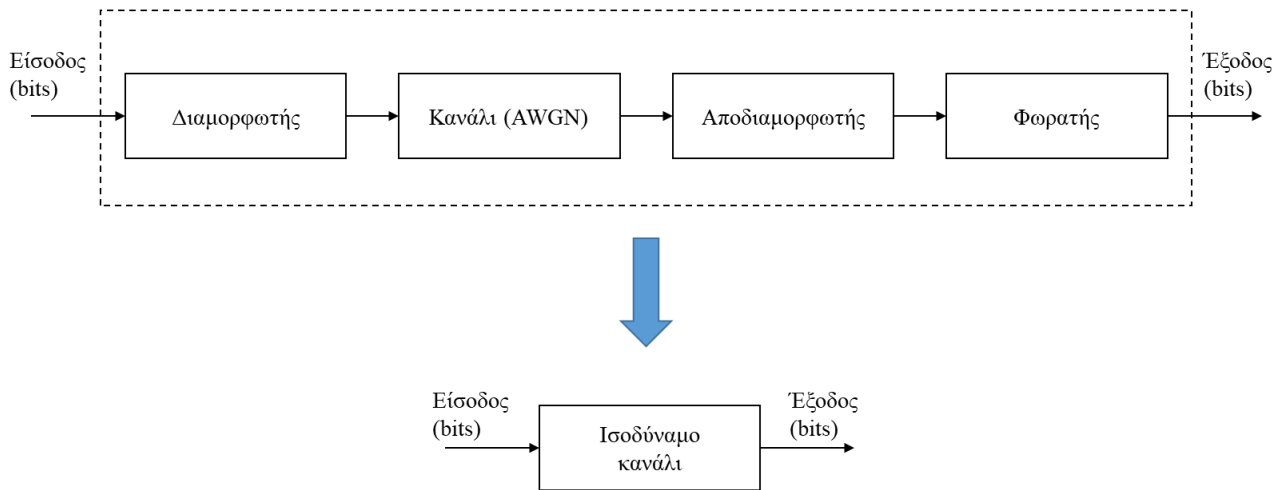
Έστω για παράδειγμα η μετάδοση 2-PAM σημάτων βασικής ζώνης μέσα από AWGN κανάλι με φασματική πυκνότητα ισχύος $N_0/2$. Εάν η ενέργεια των κυματομορφών είναι E_0 , και οι κυματομορφές είναι ισοπίθανες, τότε η πιθανότητα σφάλματος στον δέκτη είναι:

$$p = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

όπου $Q(\cdot)$ η συνάρτηση Marcum που ορίζεται ως:

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$$

Ένα BSC κανάλι θα μπορούσε να είναι η σύνθεση του AWGN καναλιού του διαμορφωτή, του αποδιαμορφωτή και του φωρατή, όπως φαίνεται στο Σχήμα 3.2. Το κανάλι αυτό δέχεται ως είσοδο bits και παράγει στην έξοδο bits. Με πιθανότητα p (που δίνεται ανωτέρω), τα bits της εξόδου του καναλιού διαφέρουν από τα bits της εισόδου.



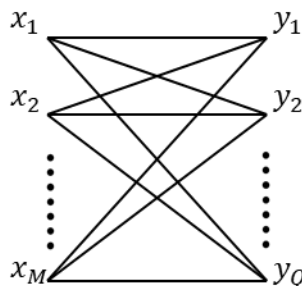
Σχήμα 3.2: Σύνθετο κανάλι διακριτής εισόδου – διακριτής εξόδου και ισοδύναμο κανάλι

3.2.2 Το διακριτό χωρίς μνήμη κανάλι (DMC - Discrete Memoryless Channels)

Το BSC κανάλι είναι ειδική περίπτωση ενός διακριτού και χωρίς μνήμη καναλιού (DMC - Discrete Memoryless Channel). Στο DMC η είσοδος λαμβάνεται από ένα αλφάβητο M συμβόλων, και η έξοδος από ένα αλφάβητο Q συμβόλων, όπως φαίνεται και στο Σχήμα 3.3. Αυτή είναι η περίπτωση ενός M - αδικού συστήματος σηματοδοσίας (χωρίς μνήμη) όπου ο φωρατής κβαντίζει την έξοδο του αποδιαμορφωτή σε Q διαστήματα. Το κανάλι περιγράφεται από $M \times Q$ δεσμευμένες πιθανότητες

$$p(y_j | x_i), \quad x_i \in X, \quad y_j \in Y$$

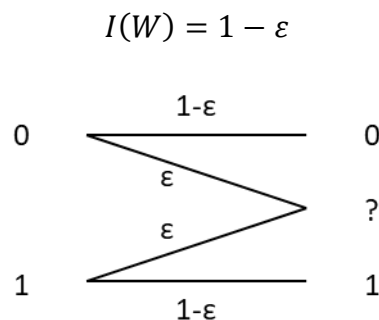
Συνήθως, οι δεσμευμένες πιθανότητες διατάσσονται σε έναν πίνακα P διαστάσεων $M \times Q$. Το $p_{i,j}$ στοιχείο του πίνακα αυτού (i -γραμμή, j -στήλη) είναι η δεσμευμένη πιθανότητα $p(y_j | x_i)$. Επομένως το άθροισμα των στοιχείων μίας γραμμής του πίνακα είναι πάντα ίσο με 1. Ο πίνακας καλείται πίνακας μετάπτωσης πιθανοτήτων (probability transition matrix)



Σχήμα 3.3: Διακριτό χωρίς μνήμη κανάλι (DMC)

3.2.3 Δυαδικό κανάλι διαγραφής (Binary Erasure Channel - BEC)

Το δυαδικό κανάλι διαγραφής (BEC) ανήκει στην κατηγορία των B-DMC καναλιών όπως και το BSC κανάλι. Η διαφορά του με το BSC κανάλι είναι ότι έχει ως είσοδο ένα bit (0 ή 1) και στην έξοδο του δίνει είτε το ίδιο ψηφίο με πιθανότητα $1 - \varepsilon$ είτε ένα μήνυμα ότι το bit δεν ελήφθη με πιθανότητα ε (όπως φαίνεται στο σχήμα 3.4). Στο BEC δεν γίνεται να λάβει λανθασμένη πληροφορία ο δέκτης όπως μπορεί να γίνει στο BSC. Η αμοιβαία πληροφορία του BEC είναι :



Σχήμα 3.4: Δυαδικό κανάλι διαγραφής - BEC

3.2.4 Το διακριτού-χρόνου AWGN κανάλι

Ας υποθέσουμε ότι ο χρόνος είναι διακριτός και ότι την i χρονική στιγμή επιλέγεται μία είσοδος $x_i \in R$ προς μετάδοση. Εάν το κανάλι είναι AWGN το λαμβανόμενο σύμβολο είναι:

$$y_i = x_i + n_i$$

όπου το n_i είναι τυχαία μεταβλητή Gaussian κατανομημένη με μέση τιμή μηδέν και διασπορά σ^2 . Επομένως για το κανάλι αυτό έχουμε $X = Y = R$. Στην πράξη τα προς μετάδοση σύμβολα δεν μπορεί να είναι αυθαίρετα και πρέπει να ικανοποιούν κάποιους περιορισμούς. Ένας τυπικός περιορισμός είναι η πεπερασμένη ισχύς μετάδοσης και αυτό εκφράζεται ως:

$$E[X^2] \leq P$$

Με τον περιορισμό αυτό, μία ακολουθία εισόδου $x = (x_1, x_2 \dots x_n)$, για μεγάλα n , θα πρέπει με πιθανότητα που τείνει στη μονάδα να ικανοποιεί τη σχέση:

$$\frac{1}{n} \sum_{i=1}^n x_i^2 = \frac{1}{n} \|x\|^2 \leq P$$

Το αποτέλεσμα αυτό είναι απόρροια του νόμου των μεγάλων αριθμών. Η τελευταία σχέση ερμηνεύεται γεωμετρικά ως εξής: Η προς μετάδοση ακολουθία x ανήκει σε μία n -διάστατη σφαίρα με κέντρο την αρχή των αξόνων και ακτίνα \sqrt{nP} .

3.3 Συμμετρική χωρητικότητα και παράμετρος Battacharyya

3.3.1 Συμμετρική χωρητικότητα (Symmetric Capacity)

Με δεδομένο ένα δυαδικό διακριτό κανάλι χωρίς μνήμη (B-DMC) W με αλφάβητο εισόδου $X = \{0, 1\}$ και αλφάβητο εξόδου Y , η συμμετρική του χωρητικότητα ορίζεται ως:

$$I(W) = \sum_{y \in Y} \sum_{x \in X} \frac{1}{2} W(y|x) \log_2 \frac{W(y|x)}{\frac{1}{2} W(y|0) + \frac{1}{2} W(y|1)}$$

Η συμμετρική χωρητικότητα είναι η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού, όταν η κατανομή εισόδου είναι ομοιόμορφη ($P(X=0) = P(X=1) = 0,5$). Κατά συνέπεια, όταν το κανάλι είναι συμμετρικό (όπου η βέλτιστη κατανομή εισόδου είναι η ομοιόμορφη), η χωρητικότητά του Shannon είναι ίση με τη συμμετρική του χωρητικότητα.

3.3.2 Παράμετρος Bhattacharyya (Bhattacharyya Parameter)

Η παράμετρος Bhattacharyya χρησιμοποιείται ως μέτρο αξιοπιστίας ενός B-DMC καναλιού, καθώς αποτελεί ένα ανώτερο όριο στην μέγιστη πιθανότητα σφάλματος (maximum-likelihood error) όταν το W χρησιμοποιείται μόνο μία φορά για τη μετάδοση ενός bit.

$$Z(W) = \sum_{y \in Y} \sqrt{W(y|0)W(y|1)}$$

Τα ακόλουθα ισχύουν για οποιοδήποτε κανάλι B-DMC W , και δείχνουν την σχέση μεταξύ της συμμετρικής χωρητικότητας και της παραμέτρου Bhattacharyya.

$$I(W) \geq \log \frac{2}{1 + Z(W)}$$

$$I(W) \leq \sqrt{1 + Z(W)^2}$$

3.3.3 Κανόνας αλυσίδας (Chain Rule)

Ο γενικός κανόνας αλυσίδας που ισχύει για πολλαπλές τυχαίες μεταβλητές είναι:

$$I(Y, X_1, X_2, \dots, X_n) = I(Y, X_1) + I(Y, X_2 | X_1) + \dots + I(Y, X_n | X_1, X_2, \dots, X_{n-1})$$

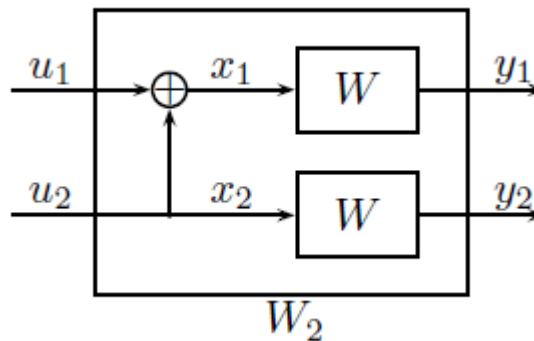
Για παράδειγμα: $I(U; Y, Z) = I(U; Y) + I(U; Z | Y)$

3.4 Συνδυασμός και διαχωρισμός των καναλιών (Channel Combining and Channel Splitting)

Η διαδικασία του συνδυασμού των καναλιών (channel combining) γίνεται μέσω μιας επαναλαμβανόμενης αλγοριθμικής σύνθεσης της πληροφορίας που μεταδίδεται σε δυο ίδια κανάλια τα οποία έχουν διαφορετικές εισόδους u_i και u_{i+1} . Η ίδια διαδικασία γίνεται για κάθε είσοδο u_i και u_{i+1} όπου $1 \leq i \leq N$, με N τα συνολικά αρχικά κανάλια W και για u_i ανεξάρτητα και ομοιόμορφα κατανομημένα (i.i.d.). Το τελικό αποτέλεσμα είναι η συνολική σύνθεση της πληροφορίας των N καναλιών σε ένα κοινό κανάλι W_{vec} (το κανάλι W είναι το ίδιο και απλώς γίνεται επαναλαμβανόμενη χρήση του σε διαφορετικές χρονικές περιόδους).

3.4.1 Ανάλυση για $N = 2$

Στην απλούστερη περίπτωση όπου $N = 2$ η διαδικασία που ακολουθείται για τον μετασχηματισμό των δυο καναλιών W σε ένα νέο συνδυασμένο κανάλι W_2 (σχήμα 3.5) έχει ως εξής:



Σχήμα 3.5: Κανάλι W_2

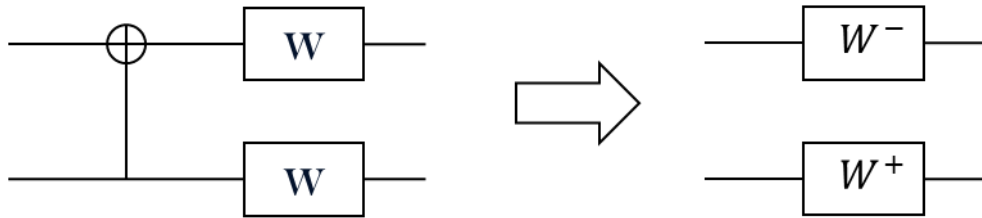
Το κανάλι W_2 δέχεται ως είσοδο τα u_1 και u_2 και δίνει έξοδο τα y_1 και y_2 . Ωστόσο η είσοδος σε καθένα από τα αρχικά κανάλια W είναι διαφορετική. Τα κανάλια W δέχονται ως εισόδους τα x_1 και x_2 αντί για τα u_1 και u_2 που θα δέχονταν αν δεν υπήρχε κωδικοποίηση.

$$x_1 = u_1 \oplus u_2 \text{ και } x_2 = u_2, W(y_1|x_1) = W(y_1|u_1 \oplus u_2) \text{ και } W(y_2|x_2) = W(y_2|u_2)$$

Η συνολική πιθανότητα μετάβασης για το καινούργιο κανάλι $W_2 : X^2 \rightarrow Y^2$ είναι:

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|u_1 \oplus u_2) W(y_2|u_2) \quad (3.1)$$

Το αποτέλεσμα του παραπάνω μετασχηματισμού, σε συνδυασμό με την μέθοδο αποκωδικοποίησης διαδοχικής ακύρωσης, είναι να αλλάξουν τα δυο επιμέρους κανάλια W σε δυο νέα κανάλια W^- και W^+ , ή αλλιώς $W_2^{(1)}$ και $W_2^{(2)}$ (σχήμα 3.6), με την έννοια ότι η αλλαγή που έχει επέλθει στα κανάλια W^- και W^+ είναι στην χωρητικότητά τους. Η διαδικασία αυτή ονομάζεται διαχωρισμός καναλιών (channel splitting). Το αποτέλεσμα αυτού του διαχωρισμού είναι το κανάλι W^+ να έχει μεγαλύτερη χωρητικότητα από το κανάλι W^- . Το φαινόμενο που προκύπτει από τον διαχωρισμό των καναλιών ονομάζεται ακραιοποίηση (extremization).



Σχήμα 3.6: Μετατροπή των δυο καναλιών W σε W^- και W^+

Πλέον ισχύει ότι: $C(W^-) \leq C(W) \leq C(W^+)$, (extremization), (3.2)

$$C(W^+) \geq C(W^-), \quad (3.3)$$

$$C(W^-) + C(W^+) = 2C(W), \quad (3.4)$$

Κατά την αποκωδικοποίηση, το νέο κανάλι W^- ή $W_2^{(1)}$ έχει ως είσοδο το u_1 , ενώ τα y_1 και y_2 είναι η έξοδος του, δηλαδή:

$$W_2^{(1)}: u_1 \rightarrow y_1, y_2$$

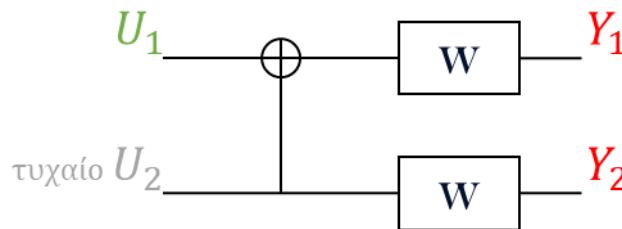
Το νέο κανάλι W^+ ή $W_2^{(2)}$ έχει ως είσοδο το u_2 , αλλά αυτήν την φορά εκτός από το y_1 και y_2 , γνωρίζει και το u_1 από την εκτίμηση που προέκυψε από το κανάλι W^- ή $W_2^{(1)}$, δηλαδή:

$$W_2^{(2)}: u_2 \rightarrow y_1, y_2, u_1$$

Ο μετασχηματισμός των δυο καναλιών W σε W^- και W^+ συμβολίζεται και ως:

$$(W, W) \rightarrow (W^-, W^+) \text{ ή } (W, W) \rightarrow (W_2^{(1)}, W_2^{(2)})$$

1. Μελέτη του καναλιού $W^-: U_1 \rightarrow (Y_1, Y_2)$, (σχήμα 3.7)



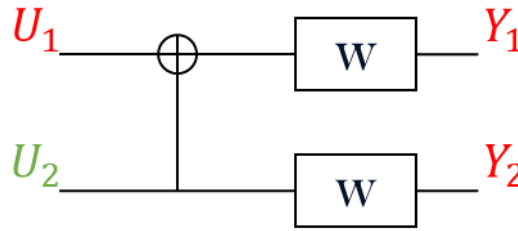
Σχήμα 3.7: Κανάλι W^-

Στην περίπτωση του καναλιού W^- , ο αποκωδικοποιητής εκτιμά την είσοδο το U_1 με την βοήθεια των εξόδων Y_1 και Y_2 . Το U_2 αντιμετωπίζεται ως παρεμβολή που εμποδίζει στην μετάδοση του U_1 .

Αυτό που προκύπτει είναι ότι: $C(W^-) = I(U_1; Y_1, Y_2)$, (3.5)

$$C(W^-) \leq C(W) \quad (3.6)$$

2. Μελέτη του καναλιού $W^+ : U_2 \rightarrow (Y_1, Y_2, U_1)$, (σχήμα 3.8)



Σχήμα 3.8: Κανάλι W^+

Κατά την αποκωδικοποίηση, στην περίπτωση του καναλιού W^+ , το σύστημα λαμβάνει ως είσοδο το U_2 αλλά αυτήν την φορά γνωρίζει το Y_1, Y_2 και το U_1 (η γνώση του U_1 οφείλεται στην εκτίμηση που έγινε κατά την ανάλυση του καναλιού W^-). Με δεδομένο ότι το U_1 είναι γνωστό, το U_2 μπορεί να υπολογιστεί αρκετά εύκολα μέσω μιας πιθανοκρατικής διαδικασίας.

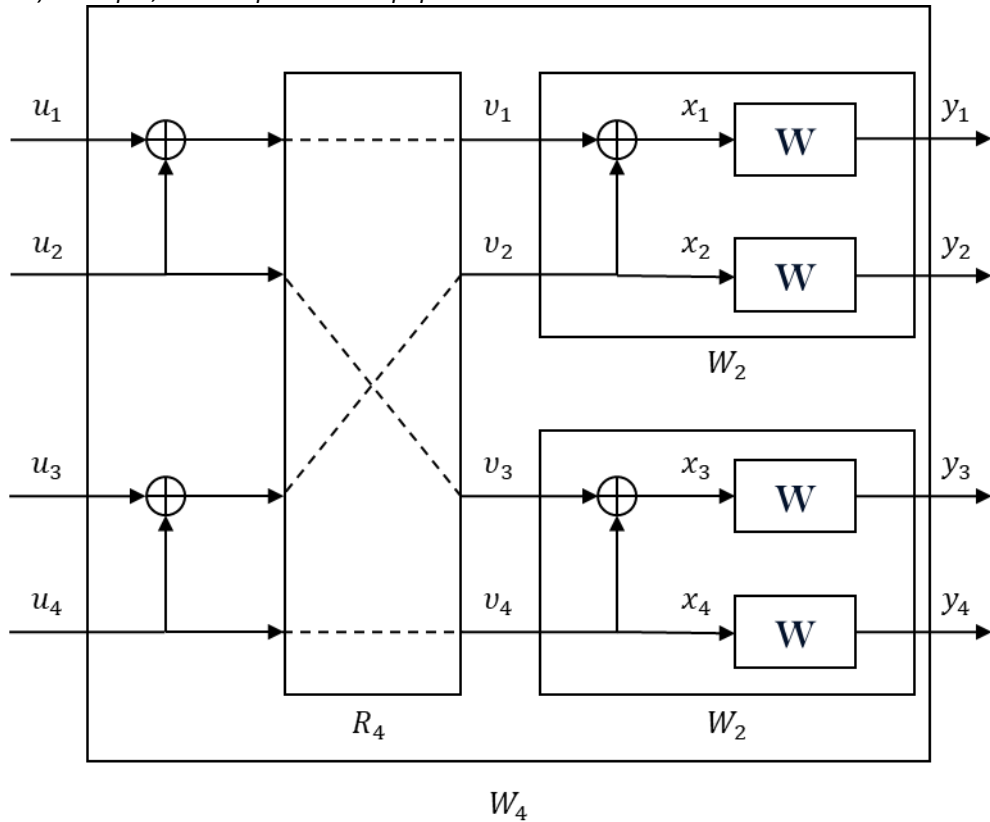
Αυτό που προκύπτει είναι ότι: $C(W^+) = I(U_2 ; Y_1, Y_2, U_1)$, (3.7)

$$C(W^+) \geq C(W) \quad (3.8)$$

Η υπόθεση ότι το U_1 έχει εκτιμηθεί σωστά είναι μια επισφαλής υπόθεση αφού η πιθανότητα της σωστής εκτίμησης με την βοήθεια του W^- είναι μικρότερη από την πιθανότητα της σωστής εκτίμησης του U_1 αν απλώς διερχόταν από το αρχικό κανάλι W . Το πρόβλημα αυτό λύνεται με την χρήση των “frozen” bits στις θέσεις που υπάρχει πολύ χαμηλή πιθανότητα σωστής εκτίμησης του bit εισόδου. Ως frozen bit χαρακτηρίζεται ένα προσυμφωνημένο bit από τον πομπό και τον δέκτη. Στην περίπτωση που χρησιμοποιηθεί frozen bit στην θέση i δεν υπάρχει πιθανότητα λάθους, αφού ο πομπός και ο δέκτης ξέρουν την τιμή του bit στην συγκεκριμένη θέση, όμως ταυτόχρονα αυτή η θέση καθίσταται άχρηστη υπό την έννοια ότι δεν μεταφέρει πληροφορία.

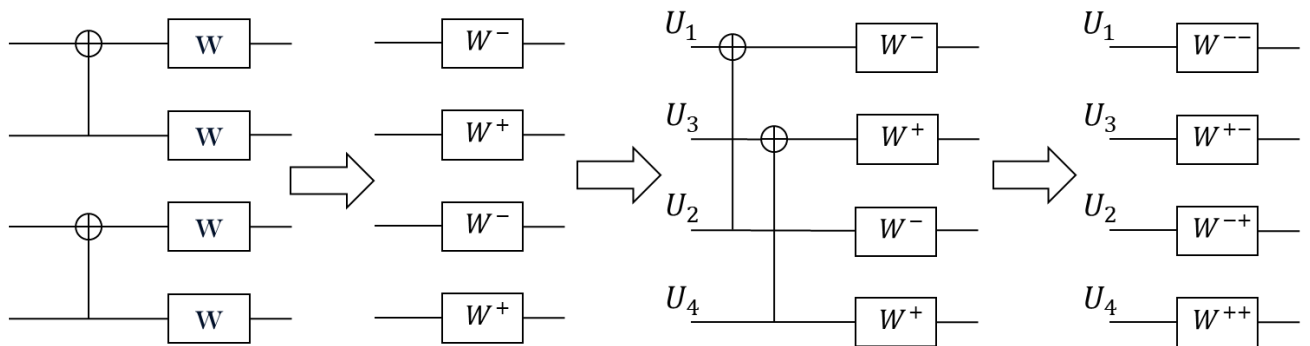
3.4.2 Ανάλυση για $N = 4$

Για την δημιουργία του συνδυασμένου καναλιού W_4 χρειάζεται ο συνδυασμός δυο καναλιών W_2 (σχήμα 3.9). Αυτήν την φορά το καθένα από τα δυο κανάλια W_2 έχει από δυο εξόδους ($W_2^{(1)}$ και $W_2^{(2)}$). Με αντίστοιχη ανάλυση, όπως στην περίπτωση του $N = 2$, τα νέα κανάλια που προκύπτουν μετά τον διαχωρισμό των καναλιών (channel splitting) είναι τα $W^{--}, W^{-+}, W^{+-}, W^{++}$ ή αλλιώς τα κανάλια $W_4^{(1)}, W_4^{(2)}, W_4^{(3)}, W_4^{(4)}$. Ωστόσο για να είναι επιτυχημένος ο συνδυασμός των καναλιών (channel combining) χρειάζεται ένα επιπλέον “ανακάτεμα” των δεδομένων εισόδου. Η περίπλεξη αυτή προσδίδει τον χαρακτήρα της ακραιοποίησης (extremization) των καινούργιων καναλιών που θα δημιουργηθούν.



Σχήμα 3.9: Κανάλι W_4

Ο πίνακας R_4 είναι ένας πίνακας μετάθεσης (permutation matrix) και σε αυτόν οφείλεται η αντιστρέψιμη περίπλεξη των δεδομένων που εισέρχονται στα δυο διαφορετικά κανάλια W_2 . Χωρίς τον πίνακα R_4 δεν μπορεί να επιτευχθεί το κατάλληλο extremization. Η μετατροπή των δυο καναλιών W_2 σε W^{--} , W^{-+} , W^{+-} , W^{++} φαίνεται στο σχήμα 3.10.



Σχήμα 3.10: Μετατροπή των καναλιών $W_2^{(1)}$ και $W_2^{(2)}$ σε W^{--} , W^{-+} , W^{+-} , W^{++}

Τα κανάλια W^{--} , W^{-+} , W^{+-} , W^{++} έχουν υποστεί και αυτά το φαινόμενο του extremization. Η διαφορά στην χωρητικότητα του W^{--} και του W^{++} γίνεται όλο και πιο ορατή. Όσο το N αυξάνεται η χωρητικότητα των νέων καναλιών θα πλησιάζει όλο και πιο πολύ στα άκρα.

Το κανάλι W^{--} συμβολίζεται και ως $W_4^{(1)}$, όπου:

$$W_4^{(1)} : u_1 \rightarrow y_1, y_2, y_3, y_4$$

Το κανάλι W^{-+} συμβολίζεται και ως $W_4^{(2)}$, όπου:

$$W_4^{(2)} : u_2 \rightarrow y_1, y_2, y_3, y_4, u_1$$

Το κανάλι W^{+-} συμβολίζεται και ως $W_4^{(3)}$, όπου:

$$W_4^{(3)} : u_3 \rightarrow y_1, y_2, y_3, y_4, u_1, u_2$$

Το κανάλι W^{++} συμβολίζεται και ως $W_4^{(4)}$, όπου:

$$W_4^{(4)} : u_4 \rightarrow y_1, y_2, y_3, y_4, u_1, u_2, u_3$$

Η συνολική πιθανότητα μετάβασης για το καινούργιο κανάλι $W_4 : X^4 \rightarrow Y^4$ είναι:

$$W_4(y_1^4 | u_1^4) = W_2(y_1^2 | u_1 \oplus u_2, u_3 \oplus u_4) W_2(y_3^2 | u_2, u_4) \quad (3.9)$$

Ως y_1^4 και u_1^4 ορίζεται το διάνυσμα του y_i και u_i για $1 \leq i \leq 4$,

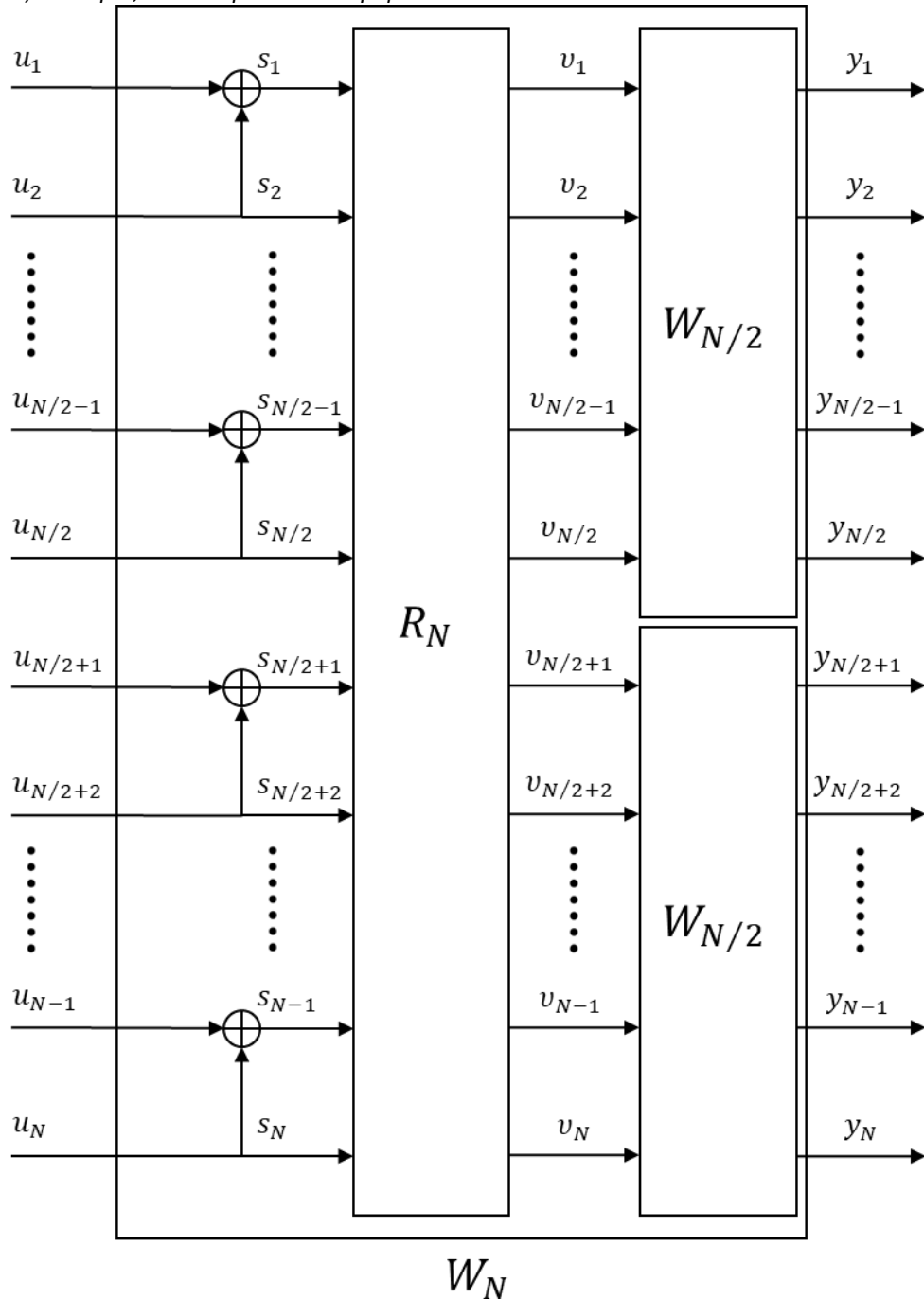
$$y_1^4 = \{y_1, y_2, y_3, y_4\}$$

$$u_1^4 = \{u_1, u_2, u_3, u_4\}$$

Γενικά ο συμβολισμός x_k^j σημαίνει $x_k^j = \{x_k, x_{k+1}, \dots \dots \dots x_{j-1}, x_j\}$

3.4.3 Γενική περίπτωση N

Στην γενική περίπτωση το κανάλι W_N έχει την μορφή που φαίνεται στο σχήμα 3.11:



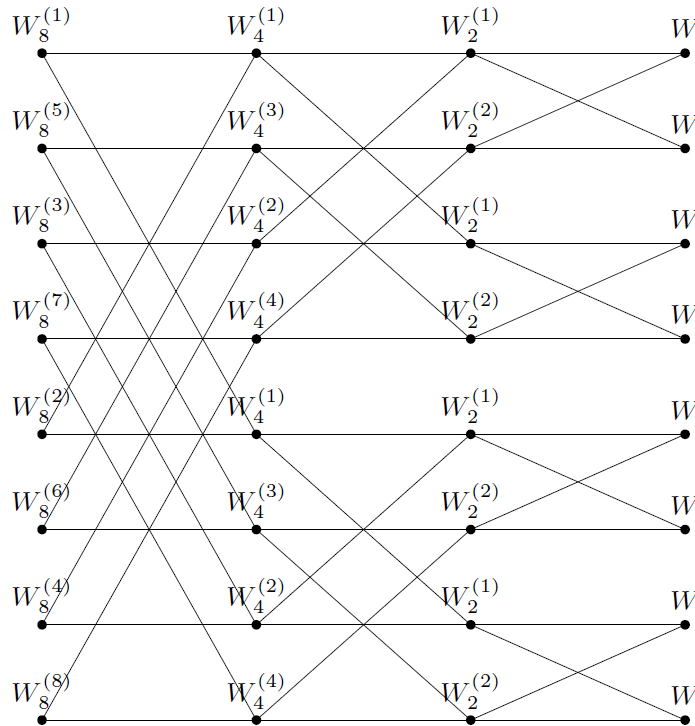
Σχήμα 3.11: Κανάλι W_N

Το κανάλι W_N δημιουργήθηκε από τον συνδυασμό δυο καναλιών $W_{N/2}$ μαζί με τον πίνακα R_N . Η διαδικασία που ακολουθήθηκε είναι η εξής:

Αρχικά το κανάλι W_N δέχεται ως είσοδο το διάνυσμα u_1^N , ενδιάμεσα ο πίνακας R_N δέχεται ως είσοδο το διάνυσμα s_1^N , όπου $s_{2i-1} = u_{2i-1} \oplus u_{2i}$ και $s_{2i} = u_{2i}$ για κάθε $1 \leq i \leq N/2$. Μετά τα δυο κανάλια $W_{N/2}$ δέχονται ως είσοδο το διάνυσμα v_1^N το οποίο στην ουσία πρόκειται για το διάνυσμα s_1^N περιπλεγμένο, όπου $v_1^N = (s_1, s_3, \dots, s_{N-1}, s_2, s_4, \dots, s_N)$. Στην συνέχεια, τα δυο κανάλια διασπώνται σε συνολικά τέσσερα κανάλια $W_{N/4}$ όπου και αυτά με την σειρά τους διασπώνται σε συνολικά οκτώ κανάλια $W_{N/8}$ κλπ. Αυτή η αναδρομική διαδικασία θα τελειώσει όταν, από την

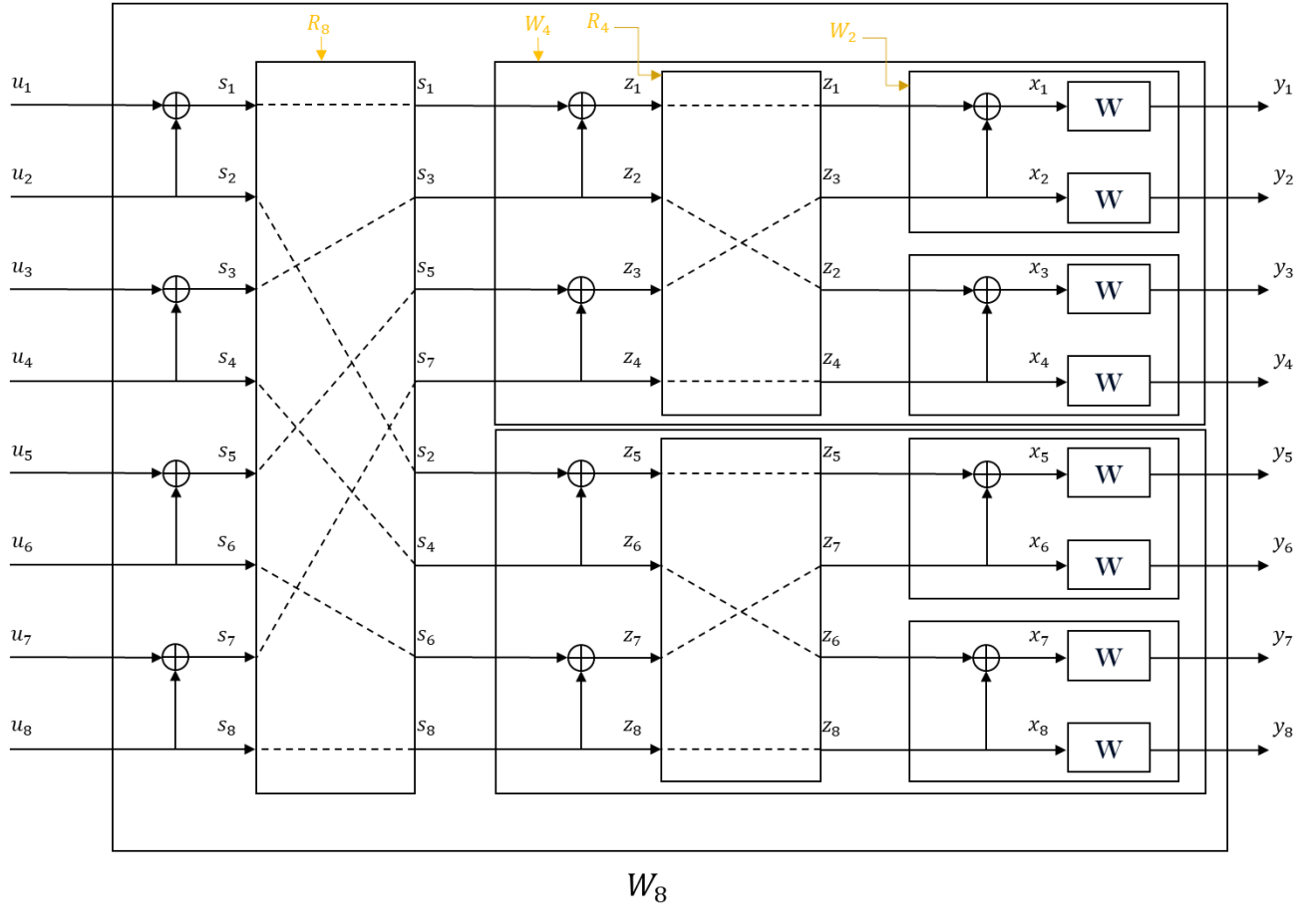
διάσπαση, προκύπτει το κανάλι W_1 το οποίο εξ ορισμού πρόκειται για το αρχικό κανάλι W . Στο τέλος, N ανεξάρτητα κανάλια W θα λάβουν, το καθένα ξεχωριστά, ως είσοδο το τελικό διάνυσμα x_1^N που προέκυψε και η τελική έξοδος του συστήματος θα είναι το διάνυσμα y_1^N .

Στο σχήμα 3.12 φαίνεται ως παράδειγμα η παραπάνω διαδικασία με διαφορετικό τρόπο. Αρχικά 8 κανάλια W συνδυάζονται σε 4 διαφορετικά κανάλια W_2 (όπου το καθένα έχει δυο εξόδους: $W_2^{(1)}$ και $W_2^{(2)}$). Στην συνέχεια, τα 4 κανάλια W_2 συνδυάζονται σε 2 διαφορετικά κανάλια W_4 (όπου το καθένα έχει τέσσερις εξόδους: $W_4^{(1)}$, $W_4^{(2)}$, $W_4^{(3)}$ και $W_4^{(4)}$). Τέλος, τα 2 κανάλια W_4 συνδυάζονται σε ένα κοινό κανάλι W_8 (το οποίο έχει οκτώ εξόδους: $W_8^{(1)}$, $W_8^{(2)}$, $W_8^{(3)}$, $W_8^{(4)}$, $W_8^{(5)}$, $W_8^{(6)}$, $W_8^{(7)}$ και $W_8^{(8)}$).



Σχήμα 3.12: Διαδικασία μετασχηματισμού του καναλιού όπου $N = 8$ [1]

Γενικά, η δημιουργία δυο νέων καναλιών $W_{2N}^{(2i-1)}$ και $W_{2N}^{(2i)}$ γίνεται μέσω του συνδυασμού δυο ίδιων καναλιών $W_N^{(i)}$. Για παράδειγμα, τα κανάλια $W_4^{(3)}$ και $W_4^{(4)}$ προκύπτουν από τον συνδυασμό δυο καναλιών $W_2^{(2)}$, με την ίδια λογική τα κανάλια $W_8^{(7)}$ και $W_8^{(8)}$ προκύπτουν από τον συνδυασμό δυο καναλιών $W_4^{(4)}$ κλπ. Στο σχήμα 3.13 φαίνεται συνολικά το κανάλι W_8 .



Σχήμα 3.13: Κανάλι W_8

Η αναδρομή, κατά γενικό κανόνα, οδηγεί στις μετατροπές των καναλιών:

$$(W_N^{(i)}, W_N^{(i)}) \rightarrow (W_{2N}^{(2i-1)}, W_{2N}^{(2i)})$$

Ο γενικός ορισμός που περιγράφει τις πιθανότητες μετάβασης είναι:

$$\begin{aligned} W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2} | u_{2i-1}) \\ = \sum_{u_{2i}} \frac{1}{2} W_N^{(i)}(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i}) \end{aligned} \quad (3.10)$$

και

$$W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1} | u_{2i}) = \frac{1}{2} W_N^{(i)}(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i}) \quad (3.11)$$

Ως $u_{1,o}^{2i-2}$ ορίζεται το διάνυσμα που περιλαμβάνει τις τιμές του u_i σε όλες τις περιττές θέσεις για το διάστημα $[1, 2i - 2]$, αντίστοιχα ως $u_{1,e}^{2i-2}$ ορίζεται το διάνυσμα που περιλαμβάνει τις τιμές του u_i σε όλες τις άρτιες θέσεις για $[1, 2i - 2]$.

$$u_{1,o}^{2i-2} = \{u_1, u_3, u_5, \dots \dots u_{2i-3}\}$$

$$u_{1,e}^{2i-2} = \{u_2, u_4, u_6, \dots \dots u_{2i-2}\}$$

$$u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} = \{u_1 \oplus u_2, u_3 \oplus u_4, u_5 \oplus u_6, \dots \dots u_{2i-3} \oplus u_{2i-2}\}$$

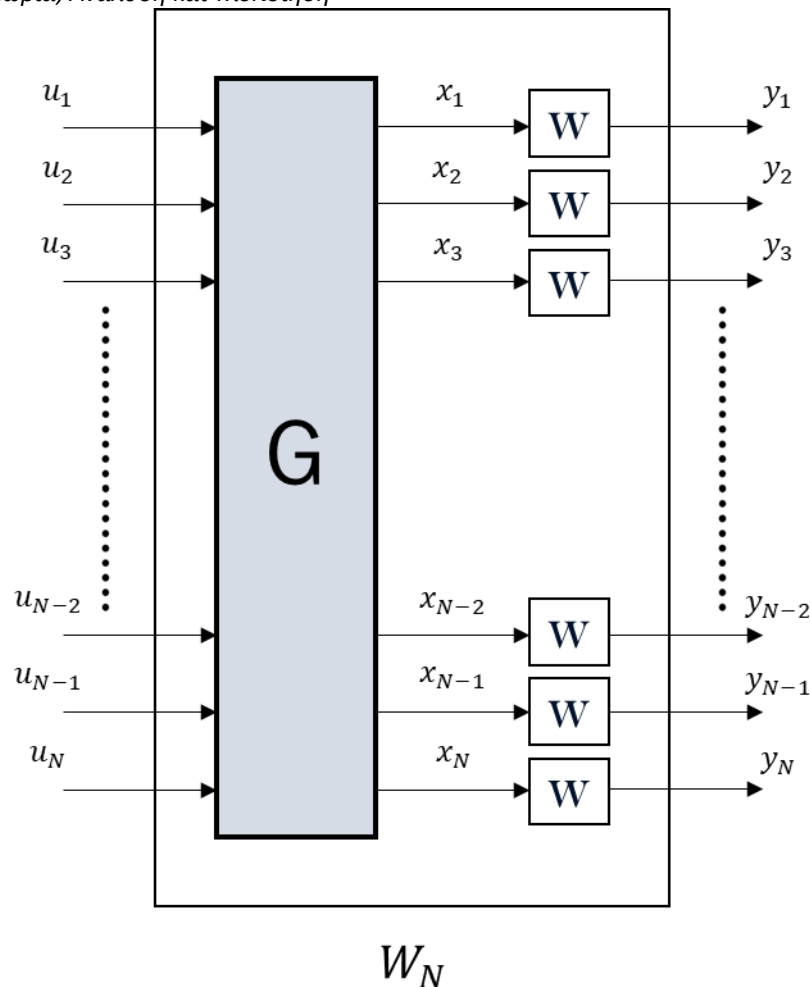
Ενώ τα κανάλια $W_N^{(i)} : X \rightarrow Y^N x X^{i-1}, 1 \leq i \leq N$, έχουν πιθανότητα μετάβασης:

$$W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) \triangleq \sum_{u_{i+1}^N \in X^{N-1}} \frac{1}{2^{N-1}} W_N(y_1^N | u_1^N) \quad (3.12)$$

Το χαρακτηριστικό της γραμμικότητας, των πολικών κωδίκων, οδηγεί σε μια μεγάλη απλοποίηση στην μελέτη του συστήματος. Όπως το u_1^N μπορεί να αντιστοιχηθεί στο s_1^N και κατά συνέπεια και στο v_1^N , το ίδιο μπορεί να γίνει μέχρι και το τελικό διάνυσμα x_1^N . Ο πίνακας που κάνει αυτήν την αντιστοίχιση λέγεται πίνακας γεννήτορας G_N (generator matrix), και ισχύει ότι:

$$x_1^N = u_1^N G_N \quad (3.13)$$

Με αυτόν τον τρόπο, το κανάλι W_N μπορεί να απλοποιηθεί αρκετά όπως φαίνεται στο σχήμα 3.14.



Σχήμα 3.14: Κανάλι W_N

Η πιθανότητα μετάβασης για το καινούργιο κανάλι W_N μπορεί να γραφτεί και ως:

$$W_N(y_1^N | u_1^N) = W^N(y_1^N | u_1^N G_N) \quad (3.14)$$

Όπου το W^N δείχνει την N φορές διαδοχική χρήση του αρχικού καναλιού W .

$$W^N(y_1^N | u_1^N G_N) = W^N(y_1^N | x_1^N) = \prod_{i=1}^N W(y_i | x_i) \quad (3.15)$$

3.4.4 Προϋποθέσεις για σωστή κωδικοποίηση

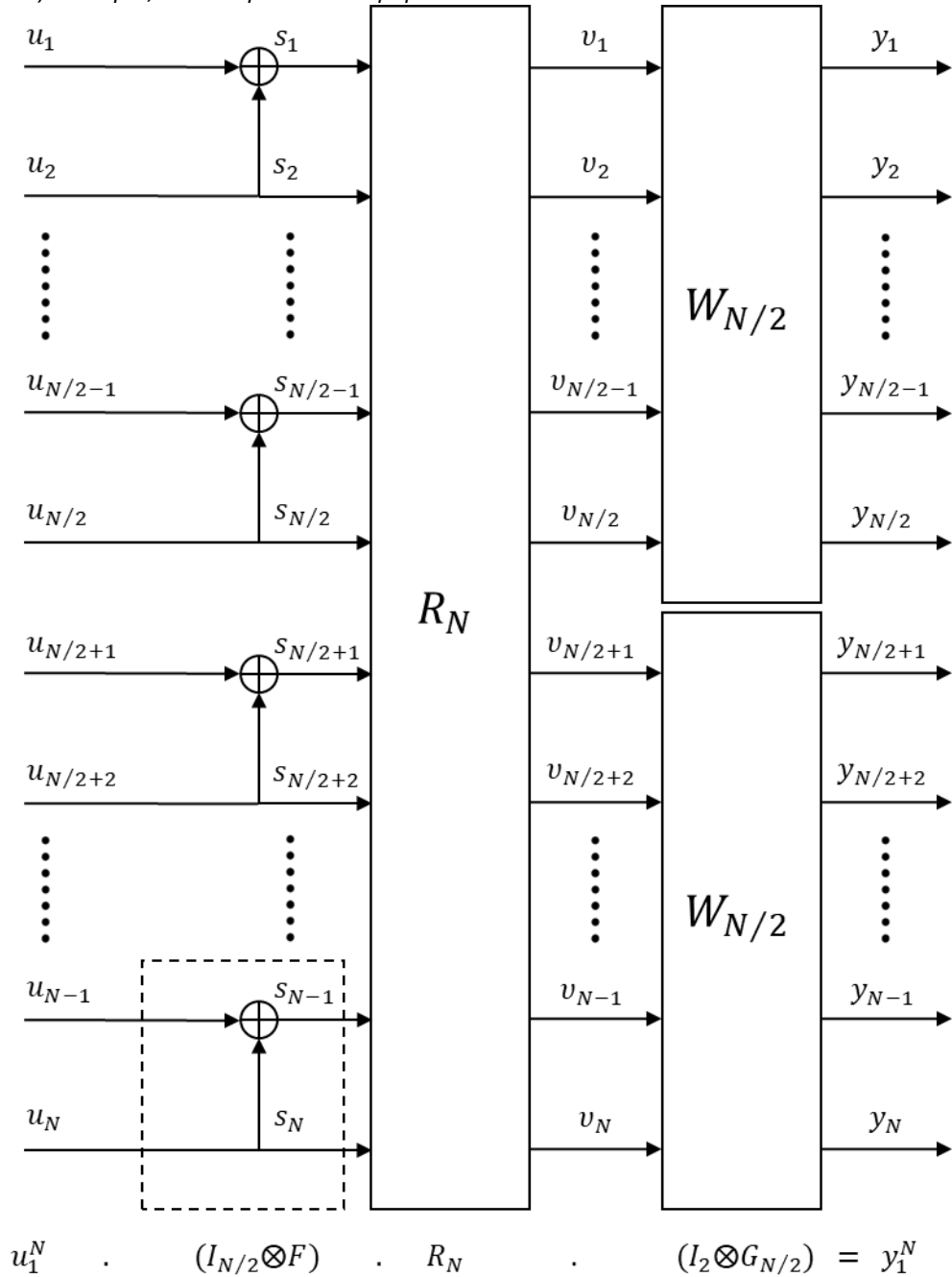
Από την προηγούμενη ανάλυση προκύπτουν ορισμένες προϋποθέσεις που πρέπει να τηρούνται για την σωστή χρήση των πολικών κωδίκων.

- Ο αριθμός των καναλιών πρέπει να είναι δύναμη του 2. Οπότε $N = 2^n$ με $n \geq 0$. Για $n = 0$ η αναδρομή (recursion) βρίσκεται στο επίπεδο 0 όπου το μόνο κανάλι που υπάρχει είναι το αρχικό κανάλι W , εξ ορισμού $W \triangleq W_1$. Για $n = 1$ προκύπτει το κανάλι W_2 , για $n = 2$ το κανάλι W_4 κλπ.

- Είναι απαραίτητη η τεχνική αποκωδικοποίησης διαδοχικής ακύρωσης SCD. Λόγω της συγκεκριμένης τεχνικής αποκωδικοποίησης γίνεται η ένα προς ένα αποτελεσματική αποκωδικοποίηση των bit.
- Πρέπει να υπάρχει μικρή πιθανότητα λάθους γιατί υπάρχει διάδοση σφαλμάτων (error propagation). Ένα λάθος και μόνο προκαλεί μεγάλο πρόβλημα αφού το κάθε u_i αποτελεί είσοδο στους επόμενους κόμβους. Για την αποφυγή αυτού του προβλήματος πρέπει να χρησιμοποιηθούν “frozen bits” στα κανάλια με την μεγαλύτερη πιθανότητα σφάλματος.
- Ο εκάστοτε πολικός κώδικας που εφαρμόζεται, είναι της μορφής Polar Code(N, K), όπου:
 N : αριθμός των bits εισόδου – εξόδου
 K : αριθμός των bits πληροφορίας
 $N - K$: αριθμός των frozen bits (ή αλλιώς είναι ο αριθμός των χειρότερων καναλιών με χωρητικότητα που τείνει στο 0)
Στα $N - K$ channels οι εισοδοί u_i έχουν πάντα την τιμή 0 (frozen positions). Στα υπόλοιπα K κανάλια οι εισοδοί u_i μεταφέρουν την πληροφορία (message positions). Είναι ξεκάθαρο ότι στόχος είναι να βρεθούν τα $N - K$ χειρότερα κανάλια, ώστε να ξεκαθαριστεί ποιες θέσεις θα περιέχουν πληροφορία και ποιες όχι.

3.5 Πίνακας γεννήτορας (G_N)

Ένας από τους κύριους λόγους που οι πολικοί κώδικες έγιναν τόσο δημοφιλείς είναι η χαμηλή πολυπλοκότητα κωδικοποίησης. Αυτό το χαρακτηριστικό οφείλεται στον πίνακα G_N . Η απλούστευση που προσδίδει ο πίνακας G_N είναι ευνοϊκή, αφού η συνολική διαδικασία της κωδικοποίησης μπορεί να περιγραφεί με την χρήση ενός και μόνο πίνακα. Ο πίνακας G_N μπορεί να περιγραφεί με την παρατήρηση της διαδικασίας κωδικοποίησης (όπως φαίνεται στο σχήμα 3.15).



Σχήμα 3.15: Γράφημα των παραγόντων που αποτελούν τον πίνακα G_N

Από το σχήμα φαίνεται ότι: $G_N = (I_{N/2} \otimes F) R_N (I_2 \otimes G_{N/2})$, όπου $G_1 = I_1$

Η πράξη \otimes είναι το γνωστό kronecker product και περιγράφεται στο παρακάτω παράδειγμα.

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes 2} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & 0 \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \\ 1 \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & 1 \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Ο πίνακας F ονομάζεται πυρήνας (kernel) και περιγράφει την βασική διαδικασία της σύνδεσης της πληροφορίας όπως φαίνεται και στην περίπτωση της πολικής κωδικοποίησης όπου $N = 2$.

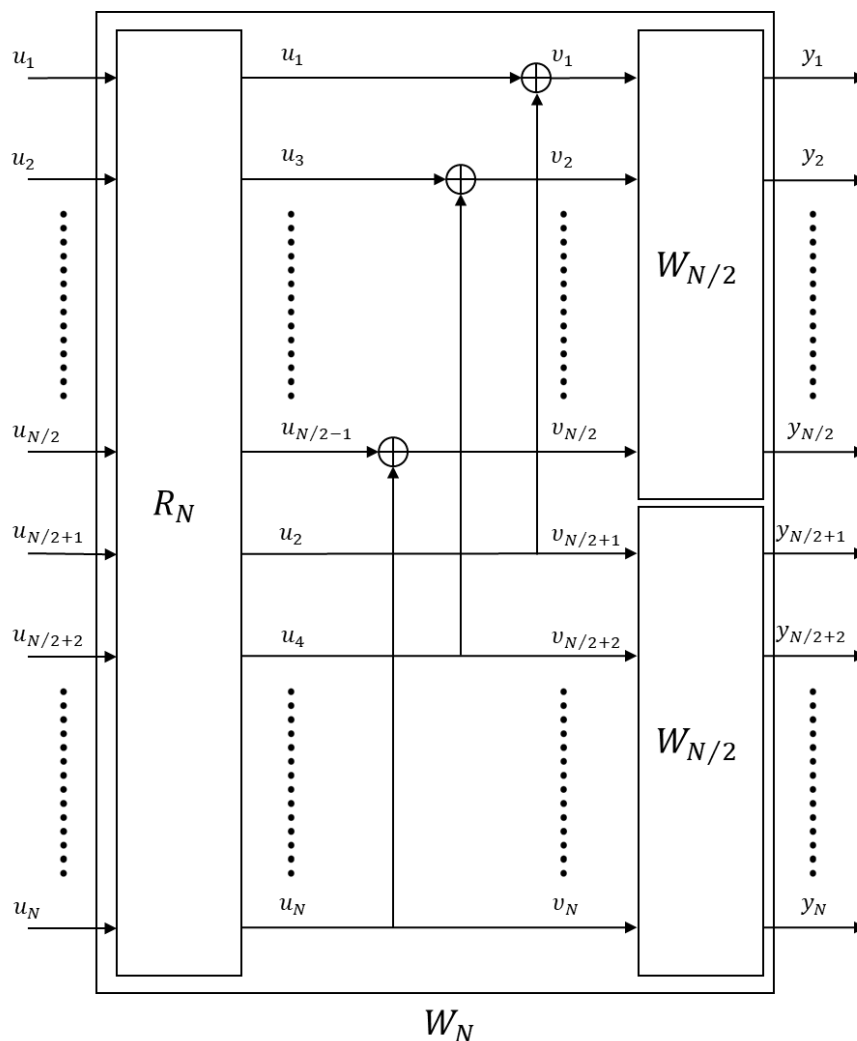
$$F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Για παράδειγμα: $(u_1 \ u_2) \cdot F = (u_1 \ u_2) \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = (u_1 \oplus u_2 \ u_2)$

Λόγω της αλγεβρικής ιδιότητας ότι $(I_{N/2} \otimes F) R_N = R_N (F \otimes I_{N/2})$, ο πίνακας G_N μπορεί να περιγραφεί και από την εξίσωση:

$$G_N = R_N (F \otimes I_{N/2}) (I_2 \otimes G_{N/2})$$

$$\Rightarrow G_N = R_N (F \otimes G_{N/2}), \quad (\text{σχήμα 3.16})$$



Σχήμα 3.16: Διαφορετικός τρόπος προσέγγισης του καναλιού W_N

Εφόσον $G_N = R_N(F \otimes G_{N/2})$, είναι προφανές ότι $G_{N/2} = R_{N/2}(F \otimes G_{N/4})$

Άρα

$$G_N = R_N(F \otimes (R_{N/2}(F \otimes G_{N/4})))$$

Με την χρήση της ιδιότητας $(AC) \otimes (BD) = (A \otimes B)(C \otimes D)$, όπου $A = I_2, B = R_{N/2}, C = F, D = F \otimes G_{N/4}$, ο πίνακας G_N γράφεται και ως:

$$\begin{aligned} G_N &= R_N(I_2 \otimes R_{N/2})(F^{\otimes 2} \otimes G_{N/4}) \\ &\Leftrightarrow G_N = B_N F^{\otimes n}, \end{aligned} \tag{3.16}$$

Όπου:

$$\begin{aligned} B_N &\triangleq R_N(I_2 \otimes R_{N/2})(I_4 \otimes R_{N/4}) \dots \dots (I_{N/2} \otimes R_2) \\ &\Leftrightarrow B_N = R_N(I_2 \otimes B_{N/2}) \end{aligned} \tag{3.17}$$

Ο πίνακας B_N είναι ένας πίνακας μετάθεσης (permutation matrix). Η λειτουργία του πίνακα B_N είναι παρόμοια με αυτήν του πίνακα R_N , και οι δυο τους εκτελούν αντίστροφη περίπλεξη των δεδομένων που εισέρχονται στην είσοδο. Η σχέση τους φαίνεται στο παράδειγμα όπου $N = 8$.

$$u_1^8 B_8 = u_1^8 R_8 (I_2 \otimes B_4)$$

Γενικά ο πολλαπλασιασμός ενός διανύσματος u_1^N με τον πίνακα R_N έχει το εξής αποτέλεσμα:

$$\begin{aligned} u_1^N &\rightarrow u_1^N R_N \\ (u_1, u_2, u_3, u_4, \dots, u_N) &\rightarrow (u_1, u_3, \dots, u_{N-1}, u_2, u_4, \dots, u_N) \end{aligned}$$

Τα στοιχεία του διανύσματος u_1^N μπορούν να έχουν και δυαδικούς δείκτες αντί για δεκαδικούς, δηλαδή:

$$(u_{0..000}, u_{0..001}, u_{0..010}, \dots, u_{1..110}, u_{1..111})$$

Οπότε στην περίπτωση όπου $N = 8$, τότε:

$$u_1^8 \rightarrow u_1^8 R_8$$

$$(u_{000}, u_{001}, u_{010}, u_{011}, u_{100}, u_{101}, u_{110}, u_{111}) \rightarrow (u_{000}, u_{010}, u_{100}, u_{110}, u_{001}, u_{011}, u_{101}, u_{111})$$

Η διαφορά που προκύπτει από την προσθήκη του όρου $(I_2 \otimes B_4)$ είναι ότι περιπλέκονται και τα ενδιάμεσα στοιχεία των δυο τετράδων που έχουν δημιουργηθεί.

Αν $u_1^8 R_8 = (c_1^4, d_1^4) = (c_{00}, c_{01}, c_{10}, c_{11}, d_{00}, d_{01}, d_{10}, d_{11})$ τότε $u_1^8 R_8(I_2 \otimes B_4) = (c_{00}, c_{10}, c_{01}, c_{11}, d_{00}, d_{10}, d_{01}, d_{11})$, δηλαδή :

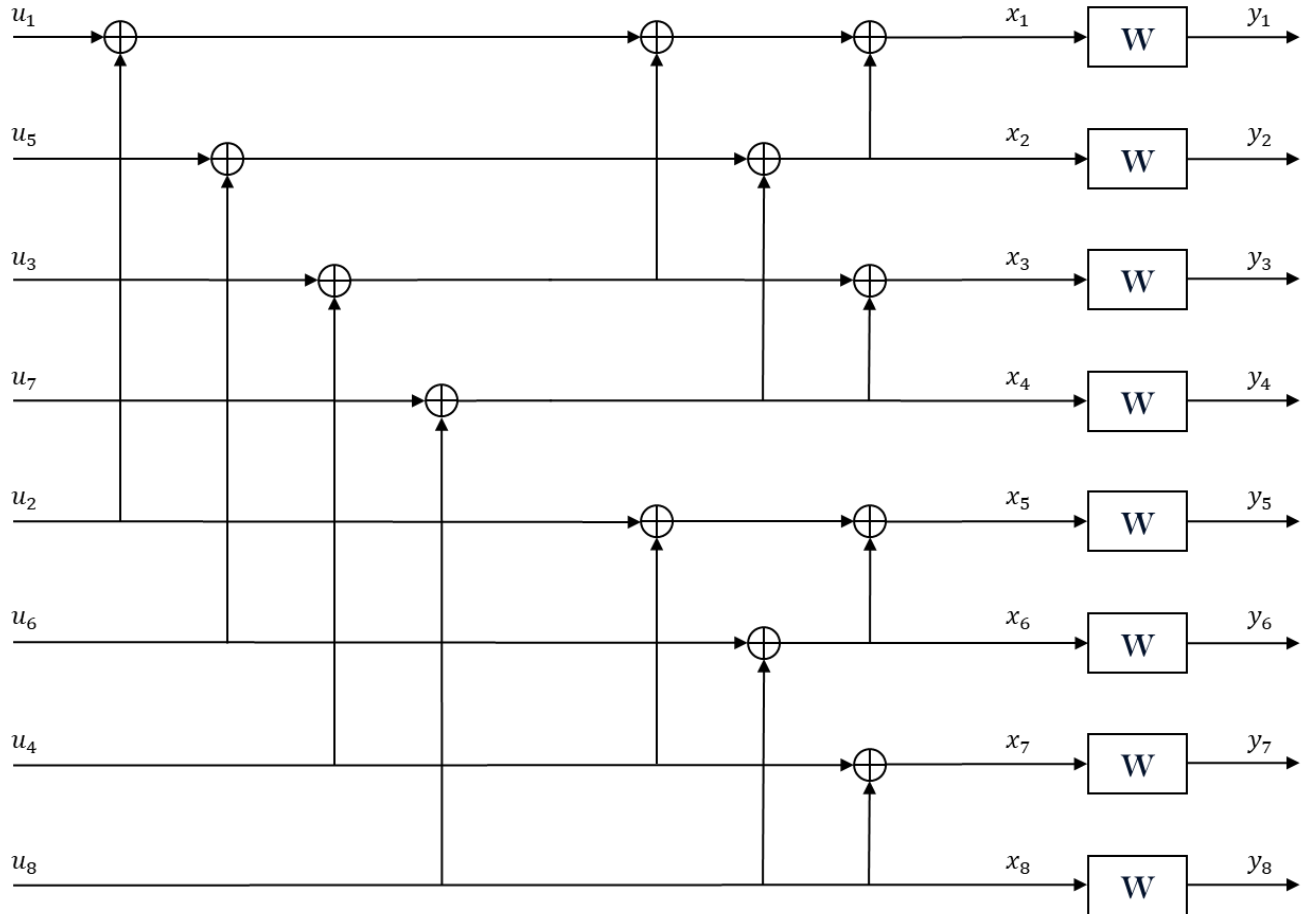
$$u_1^8 R_8 \rightarrow u_1^8 R_8(I_2 \otimes B_4)$$

$$(u_{000}, u_{010}, u_{100}, u_{110}, u_{001}, u_{011}, u_{101}, u_{111}) \rightarrow (u_{000}, u_{010}, u_{100}, u_{110}, u_{001}, u_{011}, u_{101}, u_{111})$$

Τελικά, όπως φαίνεται και από τον ορισμό του, ο πίνακας G_N εξαρτάται από τον παράγοντα N και μόνο. Για $N = 2$, $N = 4$ και $N = 8$ οι πίνακες G_2 , G_4 και G_8 αντίστοιχα, είναι:

$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad G_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Η συνολική λειτουργία του πίνακα G_N φαίνεται καλύτερα στο σχήμα 3.17, όπου αποτυπώνεται το παράδειγμα του καναλιού W_8 .



Σχήμα 3.17: Κανάλι W_8

3.6 Ρυθμός πόλωσης (polarization rate)

Με την βοήθεια διαδικασιών martingale μπορούμε να αποδείξουμε πως όταν το N τείνει στο άπειρο η ποιότητα του κάθε νέου καναλιού $W_N^{(i)}$ γίνεται πάρα πολύ καλή ή πάρα πολύ κακή, ενώ η πιθανότητα ενδιάμεσων τιμών είναι μηδενική. Κανάλι με πολύ καλή ποιότητα θεωρείται αυτό που έχει $C(W_N^{(i)}) \approx 1$, ενώ κανάλι με πολύ κακή ποιότητα θεωρείται αυτό που έχει $C(W_N^{(i)}) \approx 0$. Το σύνολο των καναλιών $W_N^{(i)}$, που έχουν χωρητικότητα ίση με 1, είναι $C(W) \cdot N$ (όπου W είναι το αρχικό κανάλι). Αντίστοιχα, το σύνολο των καναλιών $W_N^{(i)}$, που έχουν χωρητικότητα ίση με 0, είναι $(1 - C(W)) \cdot N$.

Για $N \rightarrow \infty$ και $1 \leq i \leq N$ ισχύει ότι:

$$\sum (C(W_N^{(i)}) = 1) = C(W) \cdot N \quad (3.18)$$

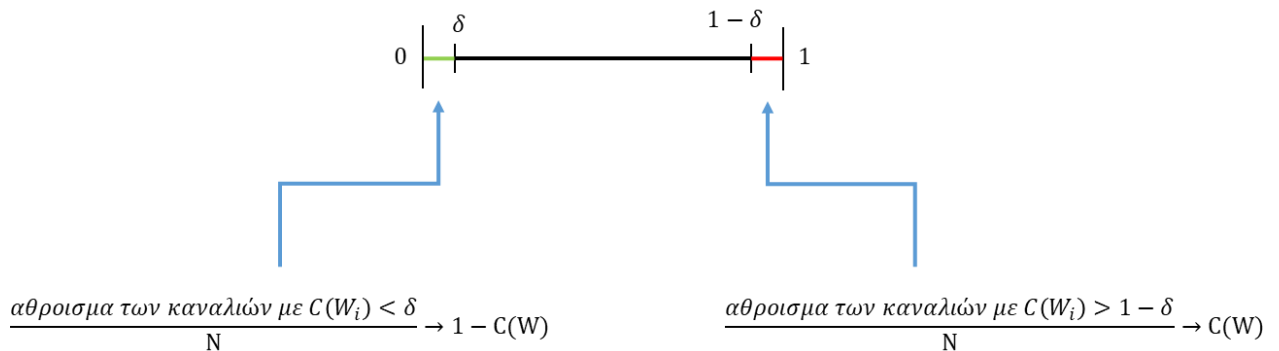
$$\sum (C(W_N^{(i)}) = 0) = (1 - C(W)) \cdot N \quad (3.19)$$

Από την τιμή του $C(W)$ καθορίζεται και ο ρυθμός μετάδοσης. Για παράδειγμα αν $C(W) = 0,7$ τότε το 70% των καναλιών θα μεταφέρουν πληροφορία και το υπόλοιπο 30% θα είναι frozen bits.

Στην πράξη το N δεν επιτρέπεται να λαμβάνει πολύ μεγάλες τιμές λόγω της απαίτησης των υπηρεσιών, να υπάρχει μικρή καθυστέρηση (low latency) στην αποστολή των δεδομένων. Όταν το N δεν είναι άπειρο ένας μικρός αριθμός καναλιών $W_N^{(i)}$ θα έχει χωρητικότητα που δεν είναι απαραίτητα κοντά στο 0 ή 1.

Ως δ ορίζεται ο όρος που περιγράφει τον ρυθμό πόλωσης. Το δ δείχνει την μέγιστη απόσταση που υπάρχει από την χωρητικότητα 0 και 1 από τα κανάλια $W_N^{(i)}$ (σχήμα 3.18), και ορίζεται ως:

$$\delta \cong 2^{-\sqrt{N}} \quad (3.20)$$



Σχήμα 3.18: Σχέση χωρητικότητας και ρυθμού πόλωσης

Το αποτέλεσμα της πόλωσης των καναλιών είναι $N \cdot C(W)$ κανάλια έχουν χωρητικότητα από $1 - \delta$ έως 1. Αντίστοιχα $N \cdot (1 - C(W))$ κανάλια έχουν χωρητικότητα από 0 έως δ . Ο αριθμός των καναλιών που βρίσκονται μεταξύ $(\delta, 1 - \delta)$ είναι ελάχιστος και όσο το N τείνει στο άπειρο μηδενίζονται Αυτό μπορεί να περιγραφεί από την σχέση:

$$\lim_{N \rightarrow \infty} \frac{(\{\delta < I(U_i; Y_1^N, U_1^{i-1}) < 1 - \delta\})}{N} = 0 \quad (3.21)$$

Η παραπάνω σχέση ισχύει επειδή οι εισοδοι $U_i \forall 1 \leq i \leq N$ είναι ανεξάρτητες και ομοιόμορφα κατανομημένες (i.i.d.).

Στις θέσεις i , για τις οποίες ισχύει ότι $I(U_i; Y_1^N, U_1^{i-1}) \approx 1$, στέλνονται τα δεδομένα χωρίς καμία απολύτως κωδικοποίηση. Ενώ στις θέσεις i , για τις οποίες ισχύει ότι $I(U_i; Y_1^N, U_1^{i-1}) \approx 0$, δεν στέλνονται δεδομένα, είναι οι θέσεις στις οποίες μπαίνουν τα frozen bits. Τα frozen bits δεν έχει

σημασία αν θα έχουν τιμή 0 ή 1. Η πρακτική που ακολουθείται διεθνώς είναι τα frozen bits να παίρνουν την τιμή 0.

Ένα σημαντικό χαρακτηριστικό, κατά την πόλωση του καναλιού, είναι ότι η εντροπία του συστήματος δεν μεταβάλλεται. Δηλαδή υπάρχει διατήρηση της εντροπίας και κατά συνέπεια της αμοιβαίας πληροφορίας. Επιπλέον, υπάρχει και βελτίωση της αξιοπιστίας. Από την σκοπιά της αμοιβαίας πληροφορίας – χωρητικότητας ισχύει ότι:

$$\begin{aligned} C(W_N) &= I(U_1^N; Y_1^N) \\ &= I(X_1^N; Y_1^N) \\ &= N \cdot C(W) \end{aligned} \quad (3.22)$$

Πιο γενικά, ο μετασχηματισμός $(W, W) \rightarrow (W', W'')$ έχει σαν αποτέλεσμα την διατήρηση της πληροφορίας (rate-preserving) και την βελτίωση της αξιοπιστίας (reliability-improving), με την έννοια ότι:

$$I(W') \leq I(W) \leq I(W''), \quad (3.23)$$

$$I(W') + I(W'') = 2I(W) \quad (3.24)$$

Και αντίστοιχα για την παράμετρο Bhattacharyya:

$$Z(W'') = Z(W)^2, \quad (3.25)$$

$$Z(W') \leq 2Z(W) - Z(W)^2, \quad (3.26)$$

$$Z(W') \geq Z(W) \geq Z(W''), \quad (3.27)$$

$$Z(W') + Z(W'') \leq 2Z(W) \quad (3.28)$$

Ενώ, στην πιο γενική του περίπτωση, για τον μετασχηματισμό $(W_N^{(i)}, W_N^{(i)}) \rightarrow (W_{2N}^{(2i-1)}, W_{2N}^{(2i)})$, ισχύουν οι σχέσεις:

$$I(W_{2N}^{(2i-1)}) + I(W_{2N}^{(2i)}) = 2I(W_N^{(i)}), \quad (3.29)$$

$$Z(W_{2N}^{(2i-1)}) + Z(W_{2N}^{(2i)}) \leq 2Z(W_N^{(i)}), \quad (3.30)$$

$$I(W_{2N}^{(2i-1)}) \leq I(W_N^{(i)}) \leq I(W_{2N}^{(2i)}), \quad (3.31)$$

$$Z(W_{2N}^{(2i-1)}) \geq Z(W_N^{(i)}) \geq Z(W_{2N}^{(2i)}), \quad (3.32)$$

$$Z(W_{2N}^{(2i-1)}) \leq 2Z(W_N^{(i)}) - Z(W_N^{(i)})^2, \quad (3.33)$$

$$Z(W_{2N}^{(2i)}) = Z(W_N^{(i)})^2, \quad (3.34)$$

$$\sum_{i=1}^N I(W_N^{(i)}) = N \cdot I(W) \quad (3.35)$$

$$\sum_{i=1}^N Z(W_N^{(i)}) \leq N \cdot Z(W) \quad (3.36)$$

Ειδικά στην περίπτωση του BEC καναλιού οι γενικές σχέσεις (3.30), (3.33) και (3.36) από ανισότητες γίνονται ισότητες, δηλαδή:

$$Z(W_{2N}^{(2i-1)}) + Z(W_{2N}^{(2i)}) = 2Z(W_N^{(i)}), \quad (3.37)$$

$$Z(W_{2N}^{(2i-1)}) = 2Z(W_N^{(i)}) - Z(W_N^{(i)})^2, \quad (3.38)$$

$$\sum_{i=1}^N Z(W_N^{(i)}) = N \cdot Z(W) \quad (3.39)$$

και επειδή $Z(W_1^1) = Z(W) = \varepsilon$, ισχύει ότι:

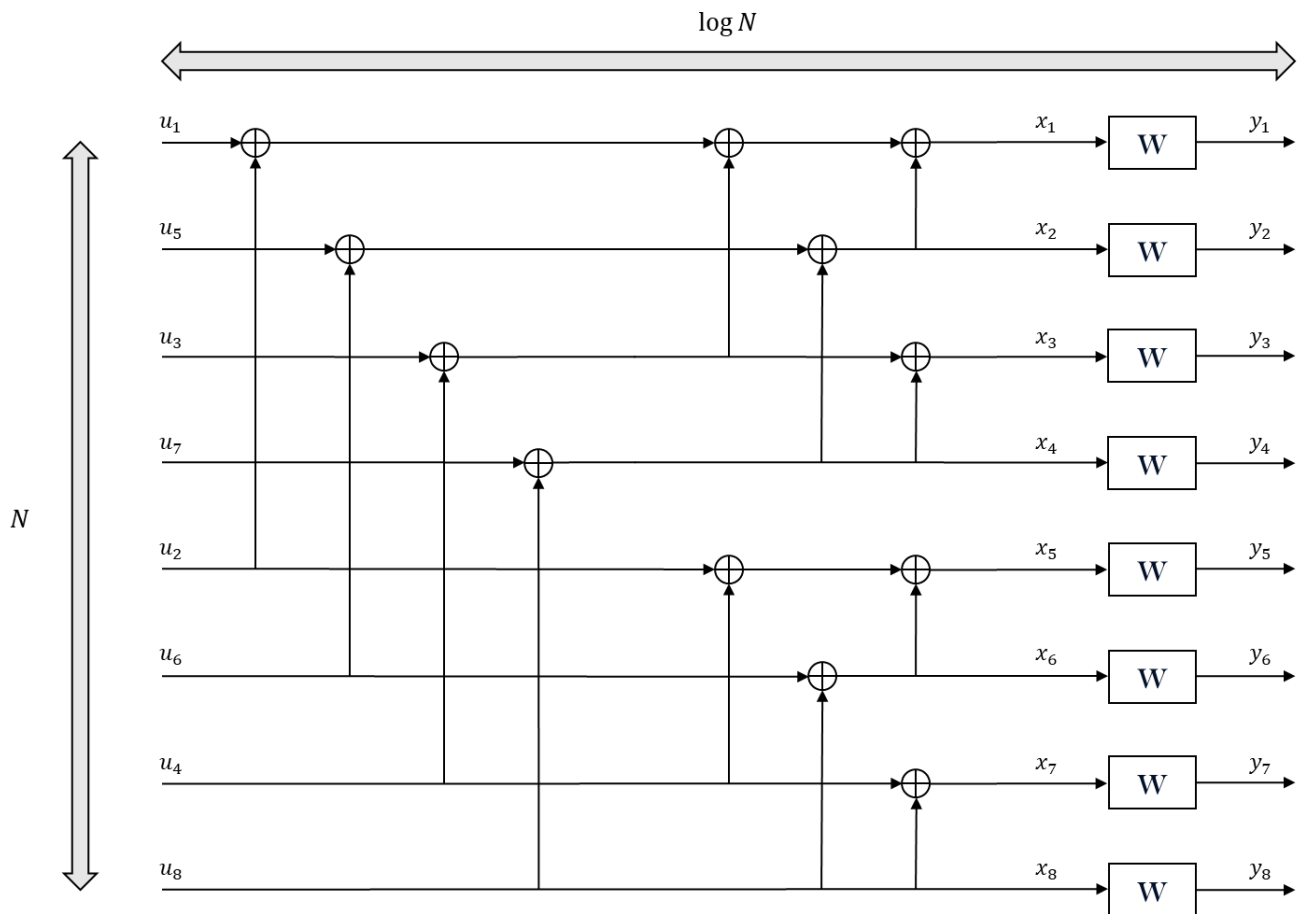
$$I(W_N^{(i)}) = 1 - Z(W_N^{(i)}) \quad (3.40)$$

3.7 Πολυπλοκότητα κωδικοποίησης (encoding complexity)

Ένα βασικό χαρακτηριστικό των πολικών κωδίκων είναι η πολύ μικρή πολυπλοκότητα κωδικοποίησης τους. Η πολυπλοκότητα κωδικοποίησης ορίζεται από τον αριθμό των πράξεων που πρέπει να γίνουν για να ολοκληρωθεί η κωδικοποίηση. Η μοναδική πράξη που γίνεται κατά την κωδικοποίηση είναι η πράξη χορ. Ο ρυθμός με τον οποίο γίνονται οι πράξεις είναι:

$$O(N \log N)$$

Όπου ο ρυθμός O είναι το big O notation. Ο όρος N δείχνει τον γραμμικό ρυθμό πράξεων που υπάρχει στις γραμμές, ενώ ο όρος $\log N$ δείχνει τον λογαριθμικό ρυθμό πράξεων που υπάρχει στις στήλες. Όπως φαίνεται στο παράδειγμα του $N = 8$, σχήμα 3.19.



Σχήμα 3.19: Γραφική απεικόνιση για τον υπολογισμό του ρυθμού πολυπλοκότητας

4. Αποκωδικοποίηση πολικών κωδίκων

4.1 Αποκωδικοποίηση διαδοχικής ακύρωσης (SCD – successive cancellation decoding)

Για την αποκωδικοποίηση των πολικών κωδίκων χρησιμοποιείται η μέθοδος της αποκωδικοποίησης διαδοχικής ακύρωσης (SCD). Η επιλογή αυτού του τύπου αποκωδικοποίησης δεν γίνεται απλώς γιατί πρόκειται για μια βολική μέθοδο αποκωδικοποίησης. Η αποκωδικοποίηση διαδοχικής ακύρωσης είναι ένα αναπόσπαστο κομμάτι της συνολικής διαδικασίας των πολικών κωδίκων, καθώς η συγκεκριμένη αποκωδικοποίηση καθιστά ικανή την πόλωση των καναλιών $W_N^{(i)}$.

Ο SCD αποκωδικοποιητής πετυχαίνει να αποκωδικοποιήσει ένα προς ένα τα bit εισόδου (u_i), μέσω μιας επαναλαμβανόμενης πιθανοκρατικής εκτίμησης του κάθε bit εισόδου ξεχωριστά. Ωστόσο, η κάθε εκτίμηση που κάνει ο SCD αποκωδικοποιητής δεν είναι ανεξάρτητη από τις προηγούμενες εκτιμήσεις. Κάθε bit που αποκωδικοποιείται στην συνέχεια χρησιμοποιείται ως δεδομένο για την επόμενη εκτίμηση \hat{u}_i . Με αυτήν την λογική οι επερχόμενες εκτιμήσεις γίνονται όλο και πιο αξιόπιστες, αφού ο SCD αποκωδικοποιητής διαθέτει περισσότερη πληροφορία για τις μελλοντικές εκτιμήσεις. Η σειρά με την οποία υπολογίζονται τα \hat{u}_i δεν μπορεί να παραβιαστεί, διαφορετικά δεν λειτουργεί ο κώδικας. Γενικά για κάθε μια εκτίμηση \hat{u}_i ο αποκωδικοποιητής χρειάζεται απαραίτητα ολόκληρο το διάνυμα y_1^N και επιπλέον τις εκτιμήσεις \hat{u}_1^{i-1} . Το τελικό αποτέλεσμα αυτού του τρόπου αποκωδικοποίησης είναι η πόλωση των καναλιών $W_N^{(i)}$.

Ωστόσο, αυτό σημαίνει ότι το όλο εγχείρημα της αποκωδικοποίησης διαδοχικής ακύρωσης οφείλεται στις αρχικές εκτιμήσεις των \hat{u}_i , για μικρότερους δείκτες i . Αν οι αρχικές εκτιμήσεις που θα γίνουν είναι σωστές, τότε θα επιτευχθεί η πόλωση των καναλιών. Αν οι αρχικές εκτιμήσεις είναι λάθος τότε το πρόβλημα αυξάνεται δραματικά, καθώς η κάθε λάθος εκτίμηση θα χρησιμοποιείται ως δεδομένο για τις επόμενες εκτιμήσεις, δηλαδή θα υπάρχει διάδοση του σφάλματος (error propagation). Όσο πιο νωρίς γίνει λάθος στην εκτίμηση \hat{u}_i , τόσο πιο σημαντικό είναι το πρόβλημα που θα δημιουργεί. Οι πιο πιθανές θέσεις i , όπου μπορεί να γίνει λάθος εκτίμηση, είναι αυτές στις οποίες το κανάλι $W_N^{(i)}$ έχει χωρητικότητα που βρίσκεται κοντά στο 0.

Το πρόβλημα που δημιουργείται από τις θέσεις i , όπου $W_N^{(i)} \approx 0$, λύνεται με την χρήση των frozen bits. Με την χρήση των frozen bits, στις κατάλληλες θέσεις i , η πιθανότητα λάθους μηδενίζεται. Από την άλλη δεν μεταφέρεται πληροφορία σε αυτά τα κανάλια, αλλά αυτό δεν είναι απαραίτητα κάτι αρνητικό, αφού η χωρητικότητα αυτών των καναλιών ήταν ήδη κοντά στο 0.

Η μέθοδος εκτίμησης στην αποκωδικοποίηση διαδοχικής ακύρωσης πραγματοποιείται από την σχέση:

$$\hat{u}_i \triangleq \begin{cases} u_i, & \text{αν } i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}), & \text{αν } i \in A \end{cases} \quad (4.1)$$

$$h_i(\mathbf{y}_1^N, \hat{u}_i^{i-1}) \triangleq \begin{cases} 0, & \frac{W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 0)}{W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 1)} \geq 1 \\ 1, & \text{διαφορετικά} \end{cases} \quad (4.2)$$

Όπου ο πίνακας A^C περιέχει τις θέσεις i στις οποίες υπάρχουν frozen bits, ενώ ο πίνακας A περιέχει τις θέσεις i στις οποίες υπάρχουν τα δεδομένα.

Ο λόγος των πιθανοτήτων $W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 0)$ και $W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 1)$ ονομάζεται λόγος πιθανοφάνειας (likelihood ratio - LR), δηλαδή:

$$L_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1}) \triangleq \frac{W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 0)}{W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 1)} \quad (4.3)$$

Η σχέση του \hat{u}_i , για όλα τα $i \in A$, μπορεί να γραφτεί και ως:

$$\hat{u}_i \triangleq \begin{cases} 0, & \text{αν } L_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1}) \geq 1 \\ 1, & \text{διαφορετικά} \end{cases} \quad (4.4)$$

Εφόσον το likelihood ratio προκύπτει από τις πιθανότητες $W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 0)$ και $W_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1} | 1)$, τότε το $L_N^{(i)}(\mathbf{y}_1^N, \hat{u}_1^{i-1})$ μπορεί να υπολογιστεί και αναδρομικά για κάθε κανάλι (όπως ακριβώς και με τον υπολογισμό των πιθανοτήτων μετάβασης $W_N^{(2i)}$, $W_{N/2}^{(i)}$ κλπ.). Με παρόμοια λογική ισχύει η εξής μετάβαση:

$$(L_N^{(2i-1)}(\mathbf{y}_1^N, \hat{u}_1^{2i-2}), L_N^{(2i)}(\mathbf{y}_1^N, \hat{u}_1^{2i-1})) \rightarrow (L_{N/2}^{(i)}(\mathbf{y}_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2}), L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N, \hat{u}_{1,e}^{2i-2}))$$

Η γενική σχέση που περιγράφει τα αντίστοιχα likelihood ratios προκύπτει από τις σχέσεις (3.10) και (3.11), δηλαδή:

$$L_N^{(2i-1)}(\mathbf{y}_1^N, \hat{u}_1^{2i-2}) = \frac{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2}) \cdot L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N, \hat{u}_{1,e}^{2i-2}) + 1}{L_{N/2}^{(i)}(\mathbf{y}_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2}) + L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N, \hat{u}_{1,e}^{2i-2})} \quad (4.5)$$

$$L_N^{(2i)}(\mathbf{y}_1^N, \hat{u}_1^{2i-1}) = [L_{N/2}^{(i)}(\mathbf{y}_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2})]^{1-2\hat{u}_{2i-1}} \cdot L_{N/2}^{(i)}(\mathbf{y}_{N/2+1}^N, \hat{u}_{1,e}^{2i-2}) \quad (4.6)$$

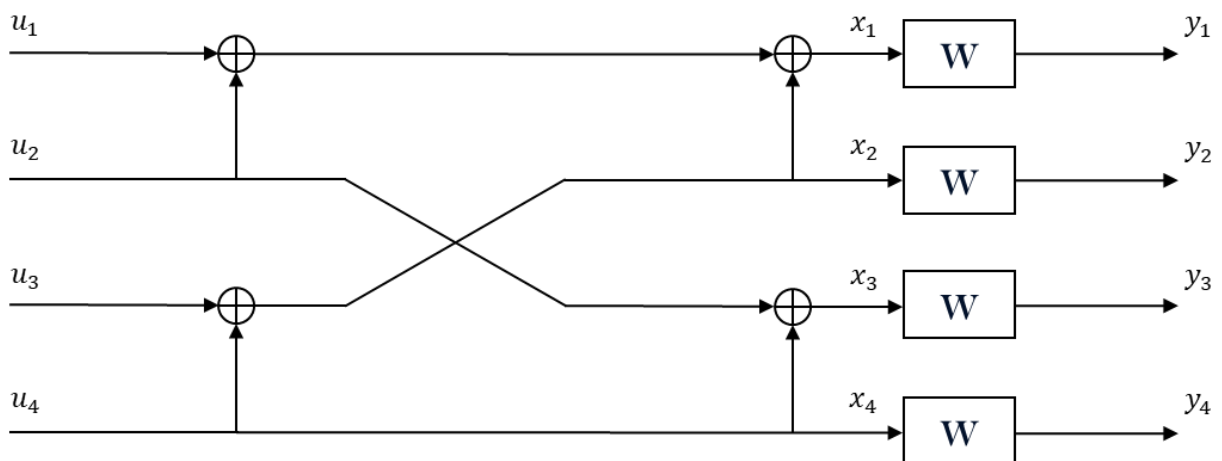
Μέσω των likelihood ratios $L_N^{(2i-1)}(y_1^N, \hat{u}_1^{2i-2})$ και $L_N^{(2i)}(y_1^N, \hat{u}_1^{2i-1})$, προκύπτουν δυο νέα likelihood ratios. Από το κάθε likelihood ratio δεν προκύπτουν αναγκαστικά οι εκτιμήσεις των u_i . Αρκετά συχνά, από τα likelihood ratios, προκύπτουν τα ενδιαμέσα bit που βοηθούν στην εύρεση των \hat{u}_i .

Ιδιαίτερη σημασία έχει ότι τα likelihood ratios $L_N^{(2i-1)}(y_1^N, \hat{u}_1^{2i-2})$ και $L_N^{(2i)}(y_1^N, \hat{u}_1^{2i-1})$ έχουν διαφορετικό επίπεδο δυσκολίας κατά τον υπολογισμό τους. Ο όρος $L_{N/2}^{(i)}(y_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2})$ κάνει εκτίμηση του δυσκολότερου bit από τα δυο. Ενώ ο όρος $L_{N/2}^{(i)}(y_{N/2+1}^N, \hat{u}_{1,e}^{2i-2})$ κάνει μια πιο εύκολη εκτίμηση, αφού εξαρτάται από το bit που προέκυψε από τον όρο $L_{N/2}^{(i)}(y_1^{N/2}, \hat{u}_{1,o}^{2i-2} \oplus \hat{u}_{1,e}^{2i-2})$.

4.2 Παράδειγμα αποκωδικοποίησης διαδοχικής ακύρωσης

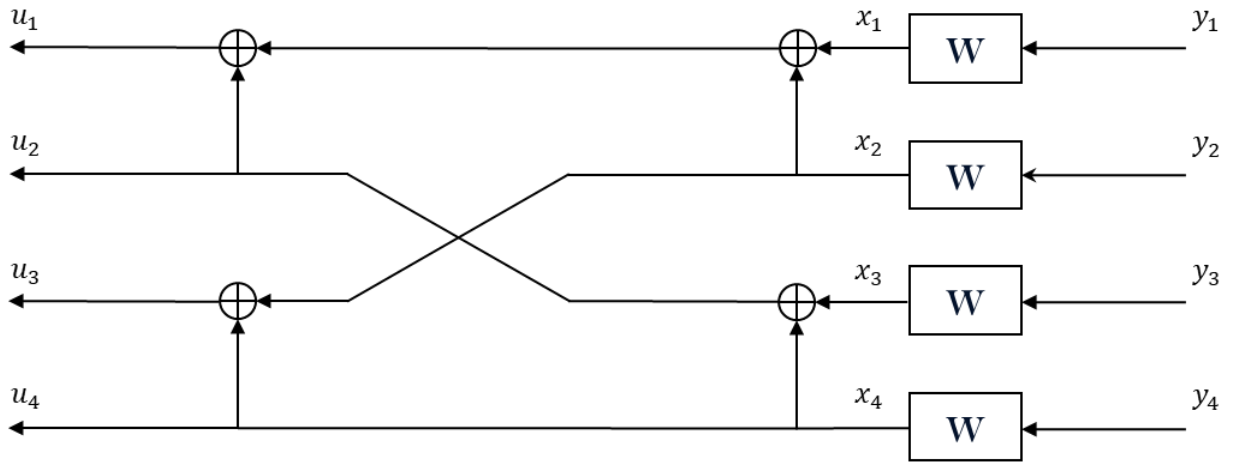
Η διαδικασία της αποκωδικοποίησης διαδοχικής ακύρωσης φαίνεται καλύτερα στο παράδειγμα όπου $N = 4$ [4].

Το αναλυτικό σχηματικό της πολικής κωδικοποίησης για $N = 4$, χωρίς την χρήση του ισοδύναμου πίνακα G_4 , φαίνεται στο σχήμα 4.1.



Σχήμα 4.1: Πολική κωδικοποίηση για $N = 4$

Η διαδικασία της αποκωδικοποίησης διαδοχικής ακύρωσης είναι η αντίστροφη της κωδικοποίησης. Για $N = 4$ η αποκωδικοποίηση διαδοχικής ακύρωσης φαίνεται στο σχήμα 4.2.

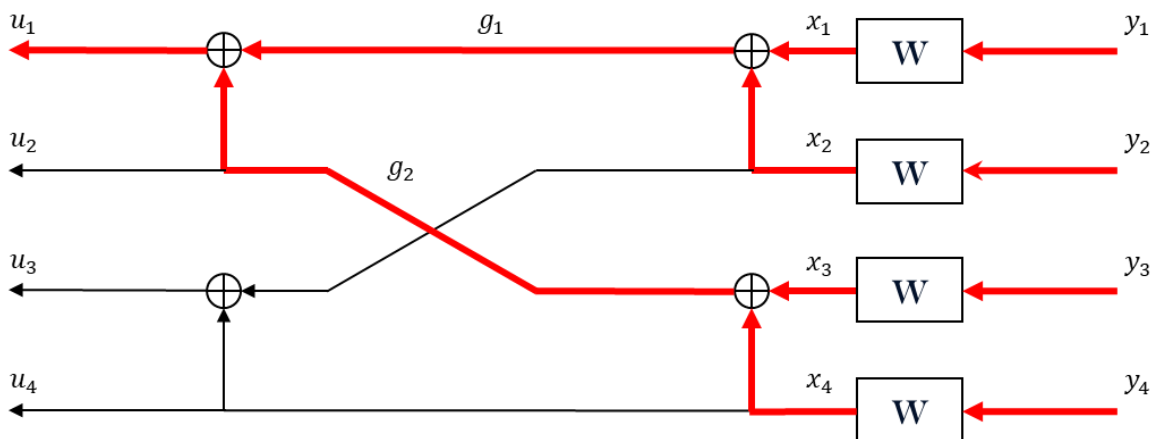


Σχήμα 4.2: Αποκωδικοποίηση διαδοχικής ακύρωσης για $N = 4$

Για να γίνουν οι εκτιμήσεις $\hat{u}_1, \hat{u}_2, \hat{u}_3$ και \hat{u}_4 είναι απαραίτητο να υπολογιστούν πρώτα τα likelihood ratios των ενδιάμεσων καταστάσεων. Για ευκολία των ονομασιών και των σχημάτων, τα likelihood ratios έχουν διαφορετική ονομασία από ότι στον γενικό ορισμό τους.

1. Υπολογισμός \hat{u}_1

Για τον υπολογισμό των εκτιμήσεων \hat{u}_1, \hat{u}_2 πρέπει να υπολογιστούν τα likelihood ratios g_1 και g_2 (όπως φαίνονται στο σχήμα 4.3). Ενώ για τον αποκλειστικό υπολογισμό του \hat{u}_1 είναι απαραίτητος ο υπολογισμός όλων των κόκκινων βελών (τα οποία συμβολίζουν likelihood ratios).



Σχήμα 4.3: Αποκωδικοποίηση του \hat{u}_1

Οι σχέσεις που χρειάζονται για τον υπολογισμό του \hat{u}_1 είναι οι εξής:

$$L(g_1) = \frac{1 + L(x_1)L(x_2)}{L(x_1) + L(x_2)}$$

$$L(g_2) = \frac{1 + L(x_3)L(x_4)}{L(x_3) + L(x_4)}$$

$$L(\hat{u}_1) = \frac{1 + L(g_1)L(g_2)}{L(g_1) + L(g_2)}$$

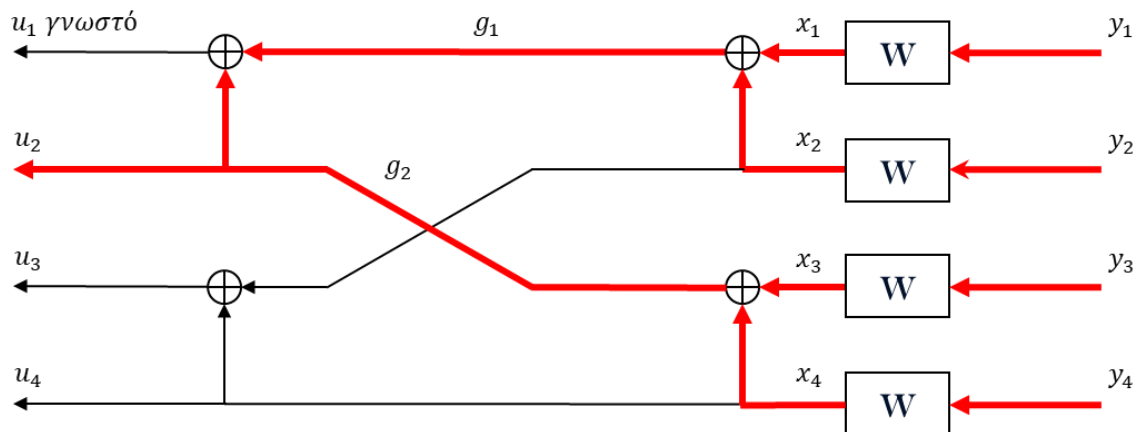
Όπου τα likelihood των x_i ορίζονται ως:

$$L(x_i) = \frac{P(x_i = 0 | y_i = 0)}{P(x_i = 0 | y_i = 1)}$$

Σε όλους τους υπολογισμούς χρησιμοποιήθηκε ο γενικός τύπος $L_N^{(2i-1)}(y_1^N, \hat{u}_1^{2i-2})$.

2. Υπολογισμός \hat{u}_2

Ο υπολογισμός του \hat{u}_2 γίνεται όπως φαίνεται στο σχήμα 4.4.



Σχήμα 4.4: Αποκωδικοποίηση του \hat{u}_2

Οι σχέσεις που χρειάζονται για τον υπολογισμό του \hat{u}_2 είναι οι εξής:

$$L(g_1) = \frac{1 + L(x_1)L(x_2)}{L(x_1) + L(x_2)}$$

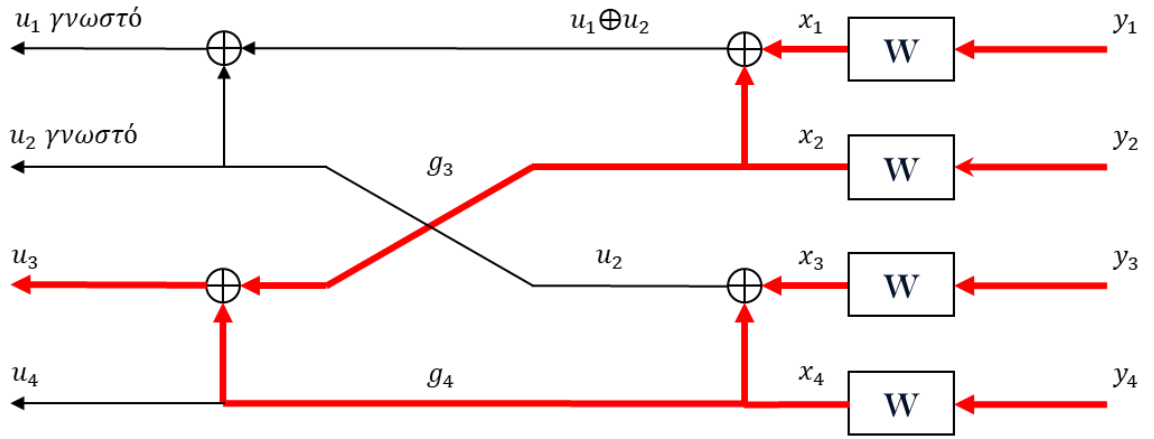
$$L(g_2) = \frac{1 + L(x_3)L(x_4)}{L(x_3) + L(x_4)}$$

$$L(\hat{u}_2) = [L(g_1)]^{1-2\hat{u}_1} \cdot L(g_2)$$

Για τον υπολογισμό του \hat{u}_2 χρησιμοποιήθηκε ο τύπος $L_N^{(2i)}(y_1^N, \hat{u}_1^{2i-1})$. Ο λόγος είναι ότι το \hat{u}_2 βασίζεται στην υπάρχουσα γνώση για το \hat{u}_1 .

3. Υπολογισμός \hat{u}_3

Με αντίστοιχη λογική προκύπτει ο υπολογισμός του \hat{u}_3 (σχήμα 4.5).



Σχήμα 4.5: Αποκωδικοποίηση του \hat{u}_3

Οι σχέσεις που χρειάζονται για τον υπολογισμό του \hat{u}_3 είναι οι εξής:

$$L(g_3) = [L(x_1)]^{1-2(\hat{u}_1 \oplus \hat{u}_2)} \cdot L(x_2)$$

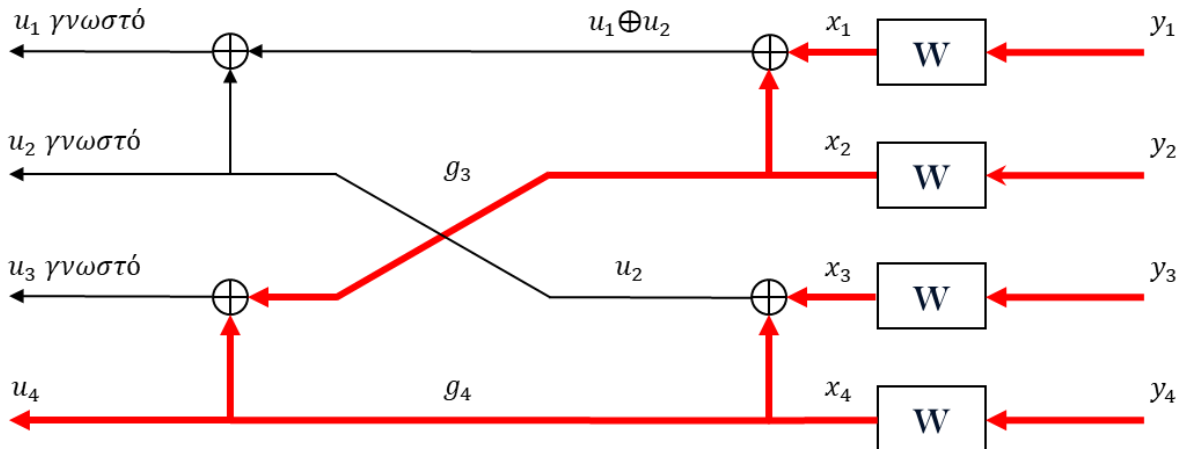
$$L(g_4) = [L(x_3)]^{1-2\hat{u}_2} \cdot L(x_4)$$

$$L(\hat{u}_3) = \frac{1 + L(g_3)L(g_4)}{L(g_3) + L(g_4)}$$

Τα likelihood g_3 και g_4 χρησιμοποιήθηκαν για τον υπολογισμό των \hat{u}_1 και \hat{u}_2 (σχήματα 4.3 και 4.4). Τα likelihood g_3 και g_4 βασίζονται στην γνώση των \hat{u}_1 και \hat{u}_2 . Για τον υπολογισμό του \hat{u}_3 χρησιμοποιείται ο γενικός τύπος $L_N^{(2^i-1)}(y_1^N, \hat{u}_1^{2^i-2})$.

4. Υπολογισμός \hat{u}_4

Ο υπολογισμός του \hat{u}_2 γίνεται όπως φαίνεται στο σχήμα 4.6.



Σχήμα 4.6: Αποκωδικοποίηση του \hat{u}_4

Οι σχέσεις που χρειάζονται για τον υπολογισμό του \hat{u}_4 είναι οι εξής:

$$L(g_3) = [L(x_1)]^{1-2\hat{u}_1} \oplus [L(x_2)]^{1-2\hat{u}_2} \cdot L(x_2)$$

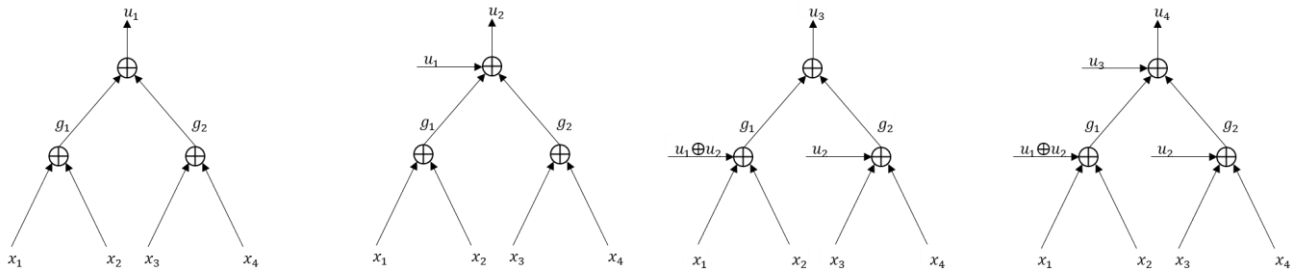
$$L(g_4) = [L(x_3)]^{1-2\hat{u}_2} \cdot L(x_4)$$

$$L(\hat{u}_4) = [L(g_3)]^{1-2\hat{u}_3} \cdot L(g_4)$$

Η περίπτωση, του υπολογισμού του \hat{u}_4 , είναι η ευκολότερη, καθώς για τον υπολογισμό του πρέπει τα \hat{u}_1 , \hat{u}_2 και \hat{u}_3 να είναι γνωστά.

Τα \hat{u}_1 και \hat{u}_2 χρειάζονται για τον υπολογισμό των g_3 και g_4 , ενώ το \hat{u}_3 είναι απαραίτητο για τον υπολογισμό του \hat{u}_4 .

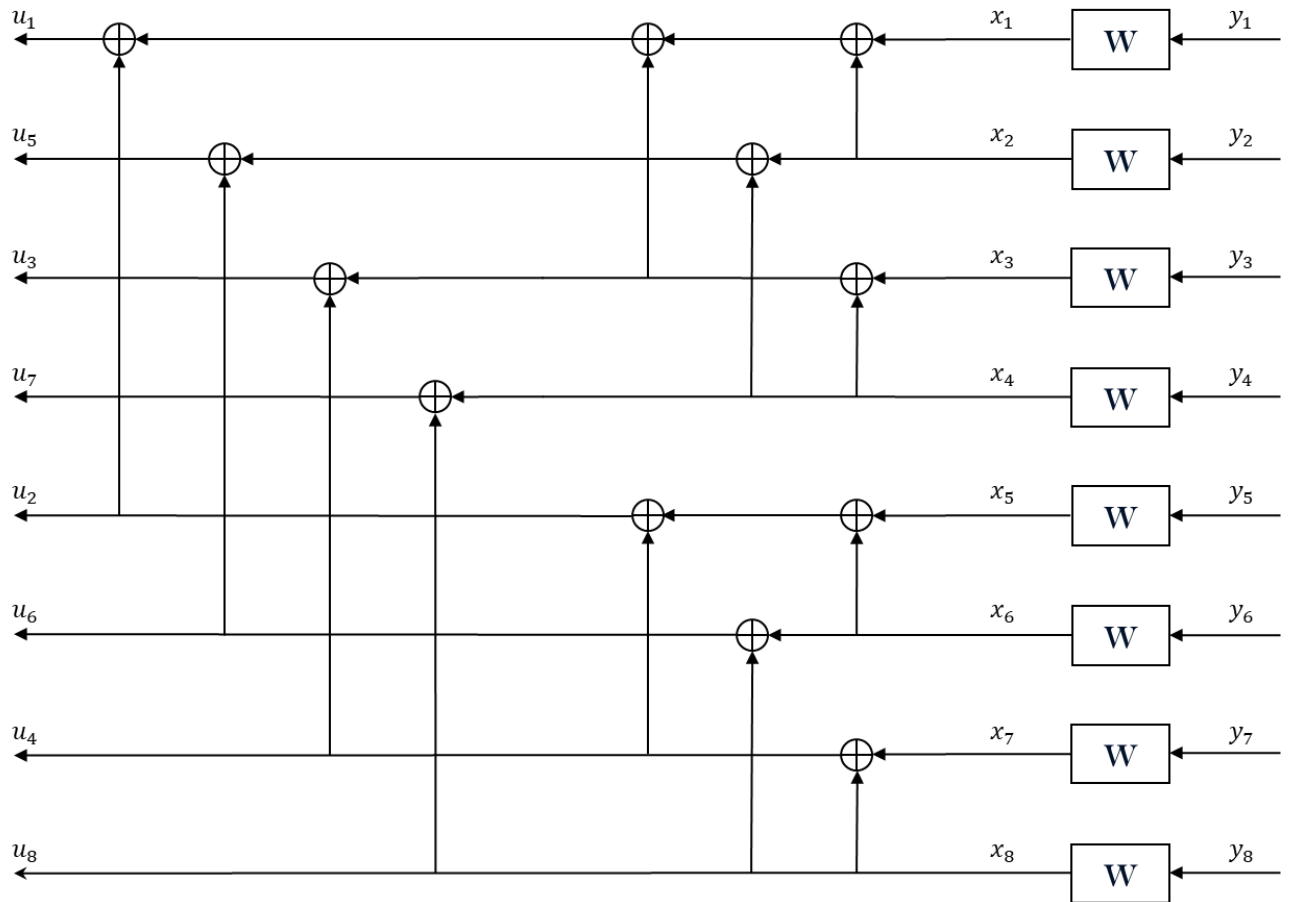
Ένας διαφορετικός τρόπος απεικόνισης της διαδικασίας της αποκωδικοποίησης διαδοχικής ακύρωσης είναι με το δέντρο αποκωδικοποίησης (decoding tree). Η απεικόνιση του δέντρου αποκωδικοποίησης δεν είναι αρκετά αναλυτική, αλλά έχει το πλεονέκτημα του απλού σχεδιασμού της. Στην περίπτωση όπου $N = 4$ τα δέντρα αποκωδικοποίησης για καθεμιά από τις εκτιμήσεις \hat{u}_1 , \hat{u}_2 , \hat{u}_3 και \hat{u}_4 φαίνονται στο σχήμα 4.7.



Σχήμα 4.7: Δέντρα αποκωδικοποίησης για καθεμιά από τις εκτιμήσεις \hat{u}_1 , \hat{u}_2 , \hat{u}_3 και \hat{u}_4 αντίστοιχα

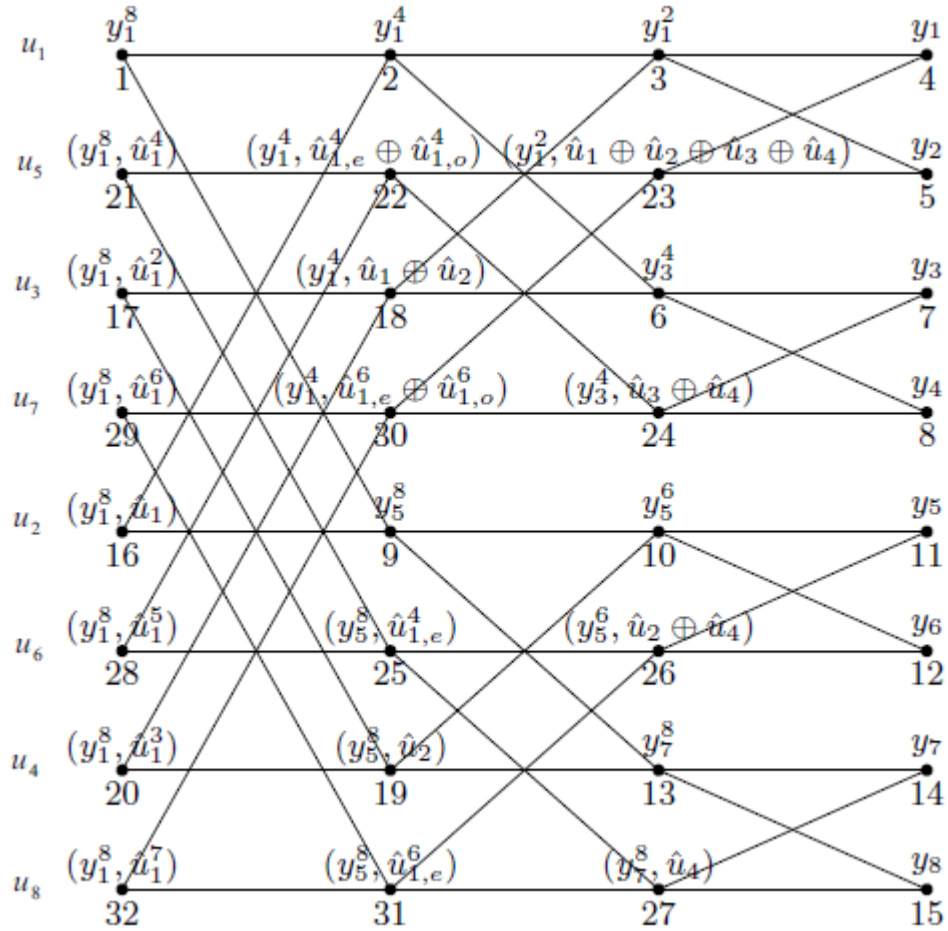
Ήδη από το $N = 4$ φαίνεται ότι για να γίνει η εκτίμηση του \hat{u}_1 γίνεται χρήση της πληροφορίας των x_1, x_2, x_3, x_4 , ενώ δεν υπάρχει κάποια άλλη βοήθεια στην αποκωδικοποίηση του \hat{u}_1 . Αυτό σημαίνει ότι το κανάλι W_1 έχει αρκετά χαμηλή χωρητικότητα ή αλλιώς αρκετά μεγάλη πιθανότητα λάθους εκτίμησης, οπότε θα ήταν καλύτερο αν για αυτή τη θέση χρησιμοποιούταν ένα frozen bit. Όσο το N αυξάνεται είναι φανερό η όλο και μεγαλύτερη ανάγκη για την χρήση των frozen bits. Αντιθέτως για την εκτίμηση του \hat{u}_4 εκτός από τα x_1, x_2, x_3, x_4 χρησιμοποιείται και η γνώση των \hat{u}_1, \hat{u}_2 και \hat{u}_3 . Αυτό έχει σαν αποτέλεσμα την μεγάλη αύξηση στην χωρητικότητα του καναλιού W_4 . Τελικά, μετά και την τελευταία εκτίμηση θα ισχύει ότι $C(W_1) \ll C(W) \ll C(W_4)$.

Για $N = 8$ η διαδικασία αποκωδικοποίησης διαδοχικής ακύρωσης είναι η ίδια. Η μόνη διαφορά, σε σχέση με την αποκωδικοποίηση όταν $N = 4$, είναι ότι για την αποκωδικοποίηση του κάθε \hat{u}_i χρειάζεται ο υπολογισμός επιπλέον likelihood ratios. Για $N = 8$ η αποκωδικοποίηση διαδοχικής ακύρωσης φαίνεται στο σχήμα 4.8.



Σχήμα 4.8: Αποκωδικοποίηση διαδοχικής ακύρωσης για $N = 8$

Ένας πιο γενικός τρόπος απεικόνισης της διαδικασίας αποκωδικοποίησης διαδοχικής ακύρωσης για $N = 8$ φαίνεται στο σχήμα 4.9. Σε αυτόν τον τρόπο απεικόνισης κάθε κόμβος αντιπροσωπεύεται από ένα bit το οποίο έχει υπολογιστεί από κάποιο likelihood ratio. Στον κάθε κόμβο υπάρχει από πάνω μια ή πολλές μεταβλητές που δείχνουν τις απαραίτητες γνώσεις που πρέπει να υπάρχουν για τον υπολογισμό αυτού του κόμβου. Ενώ, κάτω από τον κόμβο υπάρχει ένας αριθμός που δείχνει την σειρά με την οποία ζητείται ο υπολογισμός του.



Σχήμα 4.9: Διαφορετικός τρόπος απεικόνισης της διαδικασίας αποκωδικοποίησης διαδοχικής ακύρωσης για $N = 8$ [1]

Για παράδειγμα, η περίπτωση του κόμβου που έχει από κάτω του τον αριθμό 1 και από πάνω του το διάνυσμα y_1^8 αφορά στο likelihood ratio που υπολογίζει το \hat{u}_1 , δηλαδή το $L_8^{(1)}(y_1^8)$. Για τον υπολογισμό του $L_8^{(1)}(y_1^8)$ χρειάζεται γνώση του διανύσματος y_1^8 και είναι το πρώτο likelihood ratio που θα ζητηθεί να υπολογιστεί, αφού η γνώση του \hat{u}_1 είναι αναγκαία για τον υπολογισμό του \hat{u}_2 . Ωστόσο, το $L_8^{(1)}(y_1^8)$ δεν μπορεί να υπολογιστεί χωρίς την γνώση των $L_4^{(1)}(y_1^4)$ και $L_4^{(1)}(y_5^4)$. Οπότε ο δεύτερος κόμβος που ζητείται να αποκωδικοποιηθεί είναι ο κόμβος με αριθμό 2, ο οποίος χρειάζεται την γνώση του διανύσματος y_1^4 , πρόκειται για το likelihood ratio $L_4^{(1)}(y_1^4)$. Ωστόσο, ούτε αυτός ο κόμβος μπορεί να υπολογιστεί, οπότε η διαδικασία συνεχίζεται με τον κόμβο 3, που αφορά το likelihood ratio $L_2^{(1)}(y_1^2)$ κλπ. Η διαδικασία της αποκωδικοποίησης θα σταματήσει όταν υπολογιστεί και ο τελευταίως 32^{ος} κόμβος, που αφορά το likelihood ratio $L_8^{(8)}(y_1^8, \hat{u}_1^7)$.

Η επίτευξη της πόλωσης γίνεται πιο φανερή στην περίπτωση όπου $N = 8$. Καθώς το N αυξάνεται η χωρητικότητα των καναλιών W_i σιγά σιγά προσεγγίζει τα άκρα. Ειδικότερα στην περίπτωση των $C(W_1)$ και $C(W_8)$, η χωρητικότητα βρίσκεται κοντά στο 0 και στο 1 αντίστοιχα. Γίνεται φανερό ότι από το κανάλι W_1 δεν θα πρέπει να περάσει πληροφορία. Άρα στην θέση $i = 1$ θα πρέπει να τοποθετηθεί frozen bit (δηλαδή bit ίσο με 0). Αυτό έχει ως αποτέλεσμα να μην χρειάζεται να γίνει

προσπάθεια αποκωδικοποίησης για το \hat{u}_1 , οπότε ένα έμμεσο αποτέλεσμα είναι να υπάρχει μικρότερη πολυπλοκότητα αποκωδικοποίησης.

4.3 Error Probability (Pe)

Η πιθανότητα σφάλματος είναι από τα σημαντικότερα χαρακτηριστικά οποιουδήποτε κώδικα, ειδικότερα στην κωδικοποίηση καναλιού. Στους πολικούς κώδικες η πιθανότητα σφάλματος είναι ιδιαίτερος μικρή λόγω της χρήσης των frozen bits. Πάρα ταύτα, ένα και μόνο σφάλμα μπορεί να δημιουργήσει ένα τεράστιο πρόβλημα αφού θα διαδοθεί ως δεδομένο για τις επόμενες εκτιμήσεις που θα γίνουν από τον SCD αποκωδικοποιητή.

Η αιτία της μικρής πιθανότητας σφάλματος είναι ότι οι πιο επικίνδυνες θέσεις είναι αυτές που έχουν χωρητικότητα που τείνει στο 0. Ωστόσο, σε αυτές τις θέσεις δεν μεταφέρεται πληροφορία, οπότε δεν υπάρχει πιθανότητα σφάλματος. Το σφάλμα υποχρεωτικά θα γίνει σε μια από τις θέσεις υψηλής χωρητικότητας, όπου $C(W_N^{(i)}) \approx 1$. Ένα σφάλμα στις θέσεις $C(W_N^{(i)}) \approx 1$ είναι από μόνο του αρκετά δύσκολο, αλλά όχι αδύνατο.

Ο κυριότερος λόγος που θα γίνει ένα σφάλμα είναι η κακή πόλωση του καναλιού, δηλαδή όταν το N δεν είναι αρκετά μεγάλο. Ενώ ένας άλλος βασικός λόγος που θα γίνει ένα σφάλμα είναι η όχι και τόσο εκλεπτυσμένη πιθανοκρατική μέθοδος εκτίμησης, της εισόδου, που ακολουθεί ο SCD αποκωδικοποιητής.

Κάθε σφάλμα που θα συμβεί οφείλεται στην κακή εκτίμηση που θα γίνει κατά την αποκωδικοποίηση. Λόγω της πιθανοκρατικής διαδικασίας απόφασης, σφάλμα στην θέση i σημαίνει ότι:

$$W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i \oplus 1) \geq W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i) \quad (4.7)$$

Αν για ευκολία θεωρηθεί ότι η πιθανότητα $W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i \oplus 1)$ είναι ίση με $p(y | x \oplus 1)$ και η πιθανότητα $W_N^{(i-1)}(y_1^N, u_1^{i-1} | u_i)$ είναι ίση με $p(y | x)$, τότε σε αντιστοιχία θα ισχύει ότι:

$$\begin{aligned} p(y | x \oplus 1) &\geq p(y | x) \\ \Leftrightarrow \frac{p(y | x \oplus 1)}{p(y | x)} &\geq 1 \end{aligned}$$

Γενικά ισχύει ότι: $p(y, x) = p(y | x) \cdot p(x)$, και επειδή η μετατροπή από u σε x είναι ένα προς ένα (one to one) και τα u είναι ανεξάρτητα και ομοιόμορφα κατανεμημένα, $p(x) = 1/2$.

Οπότε το γεγονός του σφάλματος στην θέση i μπορεί να εκφραστεί και ως:

$$\begin{aligned} E_i &= \{(x, y) \in X \times Y: \frac{p(y | x \oplus 1)}{p(y | x)} \geq 1\} \\ \Leftrightarrow E_i &= \{(x, y) \in X \times Y: \frac{W(y | x \oplus 1)}{W(y | x)} \geq 1\} \end{aligned}$$

Η πιθανότητα σφάλματος στην θέση i ονομάζεται γεγονός E_i , και γενικά υπολογίζεται ως:

$$P(E_i) = \sum_y \sum_x p(x, y) I_{E_i}(x, y)$$

Ο δείκτης $I_{E_i}(x, y)$ δείχνει για το εάν έγινε το σφάλμα, και εκφράζεται ως:

$$I_{E_i}(x, y) = \begin{cases} 1 & \text{αν } (x, y) \in E_i \\ 0 & \text{διαφορετικά} \end{cases} \quad (4.8)$$

Δεδομένου ότι:

$$\sqrt{\frac{p(y | x \oplus 1)}{p(y | x)}} \geq 1$$

από τα παραπάνω φαίνεται ότι η σχέση του δείκτη $I_{E_i}(x, y)$ και του $\sqrt{\frac{p(y | x \oplus 1)}{p(y | x)}}$ είναι:

$$I_{E_i}(x, y) \leq \sqrt{\frac{p(y | x \oplus 1)}{p(y | x)}}$$

Άρα, η πιθανότητα του γεγονότος E_i μπορεί να γραφεί και ως:

$$\begin{aligned} P(E_i) &\leq \sum_y \sum_x \frac{1}{2} p(y | x) \sqrt{\frac{p(y | x \oplus 1)}{p(y | x)}} \\ \Leftrightarrow P(E_i) &\leq \sum_y \sum_x \frac{1}{2} \sqrt{p(y | x) p(y | x \oplus 1)} \end{aligned}$$

Για όλα τα ενδεχόμενα του x , δηλαδή για $x = 0$ και $x = 1$, η πιθανότητα του γεγονότος E_i γίνεται:

$$\begin{aligned} P(E_i) &\leq \sum_y \frac{1}{2} \sqrt{p(y | 0) p(y | 1)} + \sum_y \frac{1}{2} \sqrt{p(y | 1) p(y | 0)} \\ \Leftrightarrow P(E_i) &\leq \sum_y \sqrt{p(y | 0) p(y | 1)} \end{aligned}$$

Ή αλλιώς:

$$P(E_i) \leq \sum_y \sqrt{W(y | 0) W(y | 1)}$$

$$\Leftrightarrow P(E_i) \leq Z(W_N^{(i)}), \text{ δηλαδή η παράμετρος Bhattacharyya}$$

Άρα το εκάστοτε κανάλι $W_N^{(i)}$ έχει ανώτατη πιθανότητα σφάλματος ίση με $Z(W_N^{(i)})$.

Το γεγονός που περιγράφει την συνολική μέγιστη πιθανότητα σφάλματος είναι:

$$E \subset \bigcup_i E_i$$

Τελικά το άνω όριο της πιθανότητας σφάλματος, με χρήση αποκωδικοποίησης SCD, δίνεται από την σχέση:

$$\begin{aligned} P(E) &\leq \sum_i P(E_i) \\ \Leftrightarrow P(E) &\leq \sum_i Z(W_N^{(i)}) \end{aligned} \tag{4.9}$$

4.4 Ακολουθία αξιοπιστίας (Reliability sequence)

Το βασικό χαρακτηριστικό της πολικής κωδικοποίησης είναι η πόλωση των καναλιών W_i . Όσο το N τείνει στο άπειρο τόσο καλύτερη γίνεται η πόλωση. Ένα πολύ σημαντικό πρόβλημα που προκύπτει λόγω των πρακτικών περιορισμών είναι ότι το N δεν μπορεί να έχει ανεξέλεγκτα μεγάλες τιμές. Ωστόσο, το βασικό πρόβλημα των πολικών κωδίκων είναι ο διαχωρισμός των καναλιών σε αξιόπιστα και μη αξιόπιστα κανάλια. Η ποιότητα του κάθε καναλιού W_i οφείλεται κυρίως:

- a) στην γνώση των προηγούμενων εκτιμήσεων \hat{u}_i^{i-1}
- b) στο πόσο δύσκολη είναι η απόκτηση του \hat{u}_i
- c) στο είδος του καναλιού

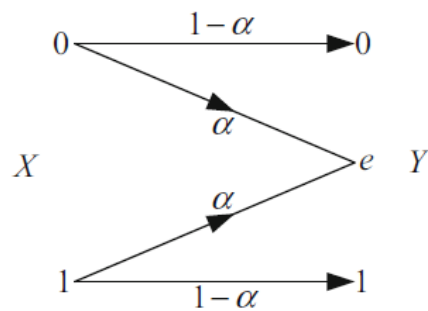
Αν για παράδειγμα το σύστημα, στο οποίο θα γίνει πολική κωδικοποίηση, έχει $N = 1024$ και $I(W) = 0.5$, δεν σημαίνει ότι για i από 0 έως 511 θα υπάρχουν frozen bits και στα υπόλοιπα i θα υπάρχει πληροφορία.

Το πρόβλημα της εύρεσης των πιο ποιοτικών καναλιών λύνεται με τον υπολογισμό της παραμέτρου Bhattacharyya για κάθε κανάλι W_i , δηλαδή τον υπολογισμό των $Z(W_N^{(i)})$. Τα πιο μικρά $Z(W_N^{(i)})$ δείχνουν τα πιο αξιόπιστα κανάλια W_i .

Όταν για παράδειγμα ένα κανάλι B-DMC έχει ρυθμό $I(W) = 0.7$, τότε το πρώτο που πρέπει να γίνει είναι ο υπολογισμός των $Z(W_N^{(i)})$. Στην συνέχεια η τοποθέτηση των $Z(W_N^{(i)})$, σε μια σειρά, από το μεγαλύτερο στο μικρότερο. Αλλά το κάθε $Z(W_N^{(i)})$ αντιστοιχίζεται σε ένα κανάλι W_i και κατά συνέπεια σε μια θέση i , οπότε δημιουργείται μια σειρά από θέσεις i , που δείχνει τις λιγότερο ποιοτικές θέσεις προς τις πιο ποιοτικές. Στις πρώτες $0.3N$ θέσεις i , της σειράς που δημιουργήθηκε, θα τοποθετηθούν frozen bits, οι θέσεις που απομένουν θα περιέχουν τα δεδομένα.

Η ταξινομημένη σειρά των i , από τις λιγότερο ποιοτικές θέσεις στις πιο ποιοτικές, ονομάζεται reliability sequence. Η εύρεση του reliability sequence είναι το πραγματικά δύσκολο πρόβλημα που πρέπει να αντιμετωπίσει ο κατασκευαστής του εκάστοτε πολικού κώδικα.

Ωστόσο, ειδικά για την περίπτωση του BEC καναλιού, η εύρεση του reliability sequence είναι μια εύκολη διαδικασία. Αυτό οφείλεται στην θεμελιώδη τρόπο λειτουργίας του BEC καναλιού (σχήμα 4.10).



Σχήμα 4.10: Κανάλι BEC

Με πιθανότητες μετάβασης:

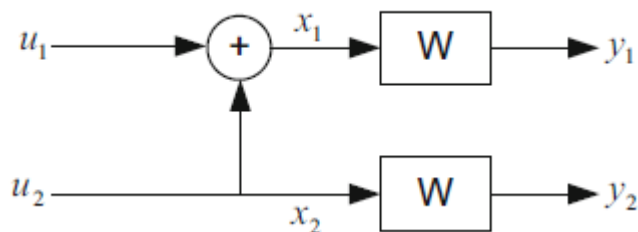
$$P(Y = 0 | X = 0) = P(Y = 1 | X = 1) = 1 - \alpha$$

$$P(Y = e | X = 0) = P(Y = e | X = 1) = \alpha$$

Η χωρητικότητα του BEC καναλιού είναι ίση με:

$$C = 1 - \alpha$$

- Για $N = 2$ το σχήμα της πολικής κωδικοποίησης είναι:



Όπου:

$$x_1 = u_1 \oplus u_2 \text{ και } x_2 = u_2 ,$$

$$W_2^1: u_1 \rightarrow y_1, y_2 ,$$

$$W_2^2: u_2 \rightarrow y_1, y_2, \hat{u}_1$$

Το αρχικό κανάλι W είναι BEC και στις δυο περιπτώσεις.

1. Για την περίπτωση όπου $W_2^1: u_1 \rightarrow y_1, y_2$

Το u_1 υπάρχει πιθανότητα να χαθεί μόνο εάν το x_1 ή το x_2 χαθούν, άρα:

$$P_{erasure}(u_1) = P(x_1 \text{ να χαθεί}) + P(x_2 \text{ να χαθεί}) + P(x_1 \text{ και } x_2 \text{ να χαθούν})$$

$$P_{erasure}(u_1) = \alpha(1 - \alpha) + (1 - \alpha)\alpha + \alpha^2$$

$$P_{erasure}(u_1) = 2\alpha - \alpha^2$$

2. Για την περίπτωση όπου $W_2^2: u_2 \rightarrow y_1, y_2, \hat{u}_1$

Η πιθανότητα να χαθεί το u_2 είναι ίση με το να χαθεί το x_2 αλλά και το x_1 ταυτόχρονα. Αυτό ισχύει λόγω της γνώσης του \hat{u}_1 , αφού $u_2 = x_1 \oplus u_1$, άρα:

$$P_{erasure}(u_2) = P(x_1 \text{ και } x_2 \text{ να χαθούν})$$

$$P_{erasure}(u_2) = \alpha^2$$

Από τον ορισμό του BEC καναλιού και την μελέτη των W_2^1 και W_2^2 ξεχωριστά, προκύπτει ότι:

$$C(W_2^1) = 1 - P_{erasure}(u_1) = 1 - 2\alpha + \alpha^2$$

$$C(W_2^2) = 1 - P_{erasure}(u_2) = 1 - \alpha^2$$

Ο υπολογισμός της χωρητικότητας των καναλιών W_1 και W_2 δίνει και τον υπολογισμό των $Z(W_1)$ και $Z(W_2)$ αντίστοιχα, αφού:

$$C(W) = I(W) = \sqrt{1 + Z(W)^2} \quad (4.10)$$

Με αντίστοιχη λογική, όταν το κανάλι είναι BEC, προκύπτουν και τα reliability sequences για μεγαλύτερα N . Για παράδειγμα, σε μια περίπτωση όπου $N = 8$, σε ένα BEC με $I(W) = 0.5$, και το reliability sequence είναι : $[1, 2, 3, 5, 4, 6, 7, 8]$, τα τέσσερα πιο ποιοτικά κανάλια είναι τα W_4, W_6, W_7 και W_8 . Σε αυτά τα κανάλια θα πρέπει να τοποθετηθεί πληροφορία, τα υπόλοιπα θα περιέχουν frozen bits.

4.5 Πολυπλοκότητα αποκωδικοποίησης διαδοχικής ακύρωσης (successive cancellation decoding complexity)

Η πολυπλοκότητα αποκωδικοποίησης διαδοχικής ακύρωσης είναι επίσης πολύ μικρή, όπως και η πολυπλοκότητα αποκωδικοποίησης. Ορίζεται αντίστοιχα από τον αριθμό των likelihood ratios που πρέπει να υπολογιστούν για να ολοκληρωθεί η αποκωδικοποίηση. Λόγω της αναδρομικής διαδικασίας αποκωδικοποίησης, πρέπει να υπολογιστεί ο αντίστοιχος αριθμός των πράξεων που απαιτούνται. Με παρόμοια λογική με την πολυπλοκότητα κωδικοποίησης, η πολυπλοκότητα αποκωδικοποίησης διαδοχικής ακύρωσης είναι τάξης:

$$O(N \log N)$$

Ωστόσο, λόγω της ύπαρξης των frozen bits, δεν χρειάζεται να υπολογιστούν όλα τα likelihoods. Ο περιορισμός των απαραίτητων πράξεων, για την ολοκλήρωση της αποκωδικοποίησης, ήταν αυτό που έκανε τους πολικούς κώδικες πρακτικά εφαρμόσιμους στο 5G standard.

5. Εφαρμογή πολικών κωδίκων - 5G

5.1 5^η γενιά τηλεπικοινωνιακών συστημάτων

Ήδη από τα τέλη του 20^{ου} αιώνα, η ασύρματη μεταφοράς πληροφορίας είχε γίνει μια θεμελιώδης ανάγκη των ανεπτυγμένων κοινωνιών. Ωστόσο, σύντομα έγινε φανερός ένας γενικός κανόνας, καθώς η τεχνολογία θα βελτιώνεται, η ολοένα αυξανόμενη ανάγκη κατανάλωσης πληροφορίας θα κάνει επιτακτική την ύπαρξη μιας νέας γενιάς τηλεπικοινωνιακών συστημάτων, η οποία θα συμπληρώνει τις αδυναμίες της προηγούμενης γενιάς. Πλέον βρισκόμαστε στην εποχή όπου το 5G (5^η γενιά) αντικαθιστά το 4G (4^η γενιά). Η νέα γενιά τηλεπικοινωνιακών συστημάτων 5G δεν επικεντρώνεται μόνο στη χωρητικότητα του συστήματος, αλλά και στις ενεργειακές προδιαγραφές (computational complexity), την αξιοπιστία (reliability), την πυκνότητα σύνδεσης (connection density) και την καθυστέρηση (latency). Τον Σεπτέμβριο του 2015 η ITU-R περιέγραψε τρεις κύριες περιπτώσεις χρήσης του 5G, δηλαδή για:

- (i) Enhanced Mobile Broadband - eMBB,
- (ii) Ultra-Reliable and Low-Latency Communication (URLLC),
- (iii) Massive Machine Type Communication (mMTC).

Οι νέες τεχνολογίες του 5G δημιουργήθηκαν για να καλύψουν συγκεκριμένες ανάγκες, και να ικανοποιήσουν όλες τις παραπάνω διαφορετικές εφαρμογές. Στο 5G New Radio (5G-NR) βελτιώνεται η ταχύτητα μετάδοσης, σε σχέση με το 4G Radio Access Technologies (4G-RAT), και εισάγονται νέες τεχνολογίες. Ειδικότερα, η νέα τεχνολογία πρόσβασης ραδιοφώνου 5G-NRAT περιλαμβάνει νέα ετερογενή κυψελοειδή αρχιτεκτονική, νέες ζώνες συχνοτήτων GHz με τεράστια διαθέσιμα εύρη ζώνης, MIMO, mMTC, IoT κ.λπ. Το 5G-eMBB έγινε πραγματικότητα το έτος 2020 και επιτυγχάνει πρακτικά ταχύτητες έως 1Gbps.

Μια από τις απαραίτητες αλλαγές, για την μετάβαση στο 5G, έγινε στην μέθοδο κωδικοποίησης καναλιού. Οι κώδικες turbo και LDPC, που είναι βασικοί κώδικες που χρησιμοποιούνται στα υπάρχοντα συστήματα κινητής τηλεφωνίας 3G και 4G (UMTS και Long Term Evolution - LTE), δεν έχουν τα επιθυμητά αποτελέσματα για πολλές νέες εφαρμογές στο 5G. Επομένως, μια αλλαγή στις τεχνικές κωδικοποίησης καναλιών ήταν αναγκαία. Οι πολικοί κώδικες αναδεικνύονται ως μια σημαντική πρόοδος στην περιοχή κωδικοποίησης καναλιού για το 5G, καθώς πληρούν τις απαιτήσεις σχεδόν όλων των διαφορετικών εφαρμογών του 5G.

Οι πολικοί κώδικες θεωρούνται ισχυροί υποψήφιοι στον αγώνα επιλογής των καλύτερων τεχνικών κωδικοποίησης καναλιών για το 5G. Το 2016, το 3GPP, συμφώνησε να υιοθετήσει τους πολικούς κώδικες για τα κανάλια ελέγχου eMBB (Enhanced Mobile Broadband), όπου αντικατέστησαν τον συνελκτικό κώδικα ουράς (που χρησιμοποιούνταν ως κώδικας καναλιού για τα κανάλια ελέγχου στο 4G). Στην συνέχεια αποφασίστηκε ότι οι κώδικες LDPC θα χρησιμοποιηθούν για κανάλια δεδομένων. Για τις περιπτώσεις των URLLC και mMTC δεν έχει ληφθεί ακόμη απόφαση, πρόκειται για ένα ανοιχτό θέμα για έρευνα.

Στην γενική τους περίπτωση, τα πιο βασικά χαρακτηριστικά που πρέπει να παρουσιάζουν οι κώδικες που χρησιμοποιούνται για την κωδικοποίηση καναλιού είναι:

- (i) Εξαιρετικά υψηλή αξιοπιστία (reliability),
- (ii) Χαμηλός χρόνος καθυστέρηση (low latency)

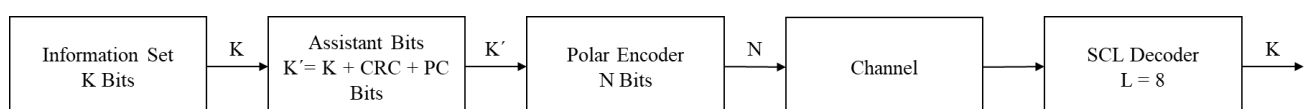
Για την μείωση του χρόνου καθυστέρησης χρειάζονται μικρά μπλοκ πληροφορίας, που έχουν ως αποτέλεσμα χαμηλότερα κέρδη από την κωδικοποίηση και μείωση της αξιοπιστίας. Από την άλλη πλευρά, η αύξηση της αξιοπιστίας απαιτεί περισσότερα bits ισοτιμίας/πλεονασμού που προστίθενται στις πληροφορίες και ορισμένες φορές ακόμα και επαναμετάδοση της πληροφορίας που οδηγεί σε αύξηση του χρόνου καθυστέρησης. Επομένως, η επιλογή της μεθόδου κωδικοποίησης καναλιού πρέπει να γίνεται με σύνεση. Μετά την υιοθέτηση των προτύπων για την περίπτωση του eMBB, το 3GPP άρχισε να αναζητά κριτήρια για το 5G-URLLC. Με την λογική αυτή, όρισε τα βασικά όρια επίδοσης του 5G-URLLC ως:

- (i) Καθυστέρηση (Latency): Ο συνολικός χρόνος καθυστέρησης από άκρο σε άκρο πρέπει να είναι μικρότερος ή ίσος του 1 ms (0,5 ms για μετάδοση και 0,5 ms για λήψη) για ένα πακέτο,
- (ii) Reliability (Αξιοπιστία): Το σύστημα θεωρείται αξιόπιστο όταν έχει τιμές BLER (Block Error Rate) 10^{-5} ανά μπλοκ. Η επιθυμητή αξιοπιστία είναι της τάξης του 99,999% και άνω.

5.2 Πολικοί κώδικες στο 5G

Οι πολικοί κώδικες, που ανακαλύφθηκαν το 2009, ήταν μια τεράστια καινοτομία στον χώρο των τηλεπικοινωνιών και της κωδικοποίησης καναλιού, αλλά απείχαν πολύ από το να γίνουν πρακτικά χρήσιμοι. Χρειάστηκε αρκετή έρευνα μετά την αρχική δημοσίευση του καθηγητή Arikan για να τελειοποιηθεί η αναβαθμισμένη μορφή τους. Οι βελτιώσεις, στην πολική κωδικοποίηση, λαμβάνουν χώρα τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Πλέον στην κωδικοποίηση απαιτούνται επιπλέον bits κυκλικού προθέματος (CRC) και ελέγχου ισοτιμίας (Parity Check - PC). Τα CRC bits κατανέμονται μέσα στην κωδικολέξη και χρησιμοποιούνται για την ανίχνευση πιθανών σφαλμάτων κατά την αποκωδικοποίηση και ενδεχομένως για πρόωρο τερματισμό της αποκωδικοποίησης του εκάστοτε bit. Τα PC bits βοηθούν στη διόρθωση σφαλμάτων και επίσης στον πρόωρο τερματισμό της αποκωδικοποίησης. Επιπλέον, η αποκωδικοποίηση γίνεται με τον αποκωδικοποιητή διαδοχικής ακύρωσης με λίστα (SCL decoder), κατά τον οποίο χρησιμοποιούνται L ταυτόχρονες διαδρομές για την εύρεση του βέλτιστου τρόπου αποκωδικοποίησης. Παρόλο που ο χρόνος καθυστέρησης στον απλό αποκωδικοποιητή διαδοχικής ακύρωσης (SC) είναι μικρότερος από αυτόν του αποκωδικοποιητή διαδοχικής ακύρωσης με λίστα (SCL), ο SC αποκωδικοποιητής παρουσιάζει χαμηλότερη αξιοπιστία σε σύγκριση με αυτόν του SCL αποκωδικοποιητή. Η καθυστέρηση αποκωδικοποίησης του αποκωδικοποιητή SCL μπορεί να ελαχιστοποιηθεί όταν η τιμή L είναι μικρή, αλλά η μείωση του L θα επιφέρει υποβάθμιση της αξιοπιστίας του συστήματος. Έτσι, υπάρχει μια αντιστάθμιση μεταξύ της καθυστέρησης και της αξιοπιστίας, η οποία εξαρτάται από την πολυπλοκότητα του SCL αποκωδικοποιητή.

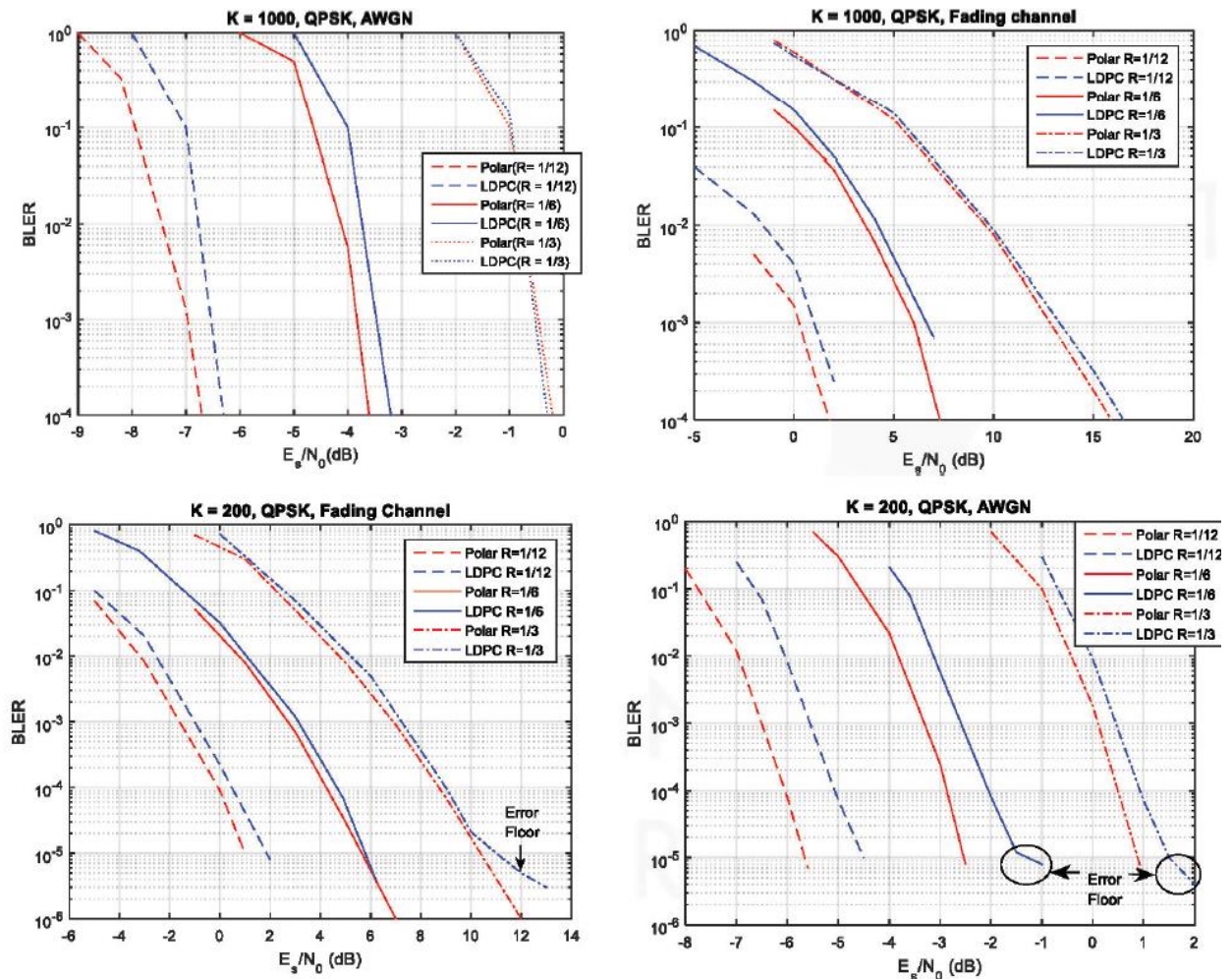
Συνολικά, τα CRC και PC bits σε συνδυασμό με τον SCL αποκωδικοποιητή βοηθούν στη βελτίωση της επίδοσης των πολικών κωδίκων (σχήμα 5.1). Τον Οκτώβριο του 2016 επιτεύχθηκε η ταχύτητα των 27 Gbps downlink με την χρήση των πολικών κωδίκων.



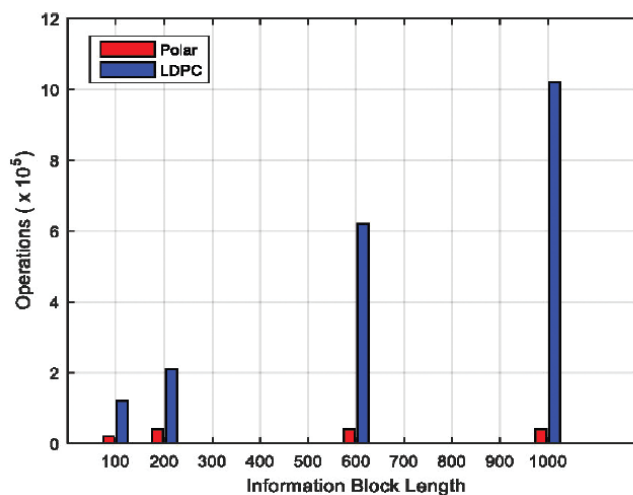
Με τις παραπάνω μετατροπές, οι πολικοί κώδικες μπορούν να επιτύχουν εξαιρετική επίδοση όσον αφορά την πιθανότητα σφάλματος, με αξιοπιστία 99,999% και πολύ χαμηλή καθυστέρηση της τάξης του 1 ms. Επιπλέον, το υψηλό κέρδος κωδικοποίησης, χωρίς κατώτατο όριο σφάλματος (error floor), και οι μέθοδοι αποκωδικοποίησης χαμηλής πολυπλοκότητας καθιστούν την πολική κωδικοποίηση πιο ελκυστική στην περίπτωση του URLLC. Ωστόσο, η συνολική επίδοση των πολικών κωδίκων εξαρτάται και από άλλους παράγοντες όπως: η ικανότητα διόρθωσης σφαλμάτων (Block Error Rate - BLER), η μη ύπαρξη ελάχιστων ορίων σφαλμάτων, η πολύ μικρή υπολογιστική πολυπλοκότητα και η μικρή καθυστέρηση αποκωδικοποίησης.

Γενικά, οι πολικοί κώδικες έχουν χαμηλότερες απαιτήσεις SNR σε σύγκριση με άλλους κώδικες με παρόμοιο ποσοστό σφάλματος, ως εκ τούτου, επιτυγχάνουν υψηλότερο κέρδος κωδικοποίησης και βελτιωμένη φασματική απόδοση. Το BLER τους είναι κάτω από 10^{-5} , σε αντίθεση με τους Turbo και LDPC κώδικες που αποδίδουν βέλτιστη τιμή BLER κοντά στο 10^{-5} για μικρά μπλοκ κωδικολέξεων. Επιπλέον, η αποκωδικοποίηση, των πολικών κωδίκων, καταναλώνει λιγότερη ενέργεια λόγω της χρήσης αποκωδικοποιητών βασισμένων στην λογική διαδοχικής ακύρωσης (όπως SC και SCL decoders). Συγκριτικά, ένα τηλεπικοινωνιακό σύστημα που χρησιμοποιεί πολική κωδικοποίηση έχει ακόμη και 20 φορές μικρότερη κατανάλωση από ένα σύστημα με ισοδύναμη πολυπλοκότητα, που χρησιμοποιεί turbo κώδικες, ενώ ταυτόχρονα ικανοποιεί τις απαιτήσεις των εφαρμογών σε ότι αφορά τον χαμηλό χρόνο καθυστέρησης.

Στο σχήμα 5.2 φαίνεται η αξιοπιστία των πολικών κωδίκων σε όρους BLER προς E_s/N_0 , όπου συγκρίνεται με την αξιοπιστία των LDPC κωδίκων, σε AWGN και fading κανάλια (πάντα για μικρά μπλοκ κωδικολέξεων), ενώ στο σχήμα 5.3 γίνεται μια σύγκριση της υπολογιστικής πολυπλοκότητας των πολικών και LDPC κωδίκων.



Σχήμα 5.2: BLER προς E_s/N_0 για διαφορετικά κανάλια, ρυθμούς και bit πληροφορίας σε πολικούς και LDPC κώδικες [9]



Σχήμα 5.3: Σύγκριση της υπολογιστικής πολυπλοκότητας στους πολικούς και LDPC κώδικες [9]

5.3 Reliability sequence στο 5G standard

Ένα ακόμα βασικό θέμα που βρίσκεται υπό διαρκή μελέτη είναι η εύρεση του reliability sequence στο εκάστοτε σύστημα που χρησιμοποιεί πολικούς κώδικες. Γενικά, το reliability sequence των καναλιών $W_N^{(i)}$ εξαρτάται από το κανάλι, και επομένως δεν είναι καθολικό. Αυτή η μη καθολικότητα ΠΑΔΑ, Τμήμα Η&ΗΜ, Διπλωματική Εργασία, Ρούσας Ελευθέριος

θέτει τεράστια πρακτικά προβλήματα στην κατασκευή πολικών κωδίκων όταν προβλέπεται ένα μεγάλο εύρος κωδικολέξεων και ρυθμών στο ίδιο τηλεπικοινωνιακό σύστημα. Η μέθοδος density evolution (DE) μπορεί να παρέχει θεωρητικές εγγυήσεις για την ακρίβεια της σωστής εκτίμησης των παραμέτρων Z_i , αλλά αυτό επιτυγχάνεται με υψηλό υπολογιστικό κόστος. Μια μέθοδος εκτίμησης αξιοπιστίας των καναλιών $W_N^{(i)}$ για AWGN κανάλια με βάση την προσέγγιση Gaussian (GA) του density evolution δίνει ακριβή αποτελέσματα με περιορισμένη πολυπλοκότητα. Ωστόσο, η σχεδίαση του αυξάνει τον χρόνο καθυστέρησης κωδικοποίησης πάρα πολύ για να καλύψει τις απαιτήσεις του 5G. Μελέτες που έγιναν, λαμβάνοντας υπόψη το είδος του καναλιού, τις ιδιότητες των πολικών κωδίκων που έχουν μικρά μήκη κωδικολέξεων, τη χρήση αποκωδικοποιητών διαδοχικής ακύρωσης λίστας και την παρουσία βοηθητικών bit στον κώδικα (CRC και PC bits), έδωσαν την δυνατότητα δημιουργίας ενός καθολικού reliability sequence που θα χρησιμοποιείται για το 5G, “ανεξάρτητα” από το κανάλι. Αυτές οι μελέτες και οι συνεχείς προσομοιώσεις οδήγησαν στην τυποποίηση ενός γενικού reliability sequence, στο 5G, που χρησιμοποιείται ως βάση για την εξαγωγή του εκάστοτε reliability sequence για κάθε πολικό κώδικα ξεχωριστά. Αυτό το reliability sequence αποτελείται $N = 1024$ ταξινομημένες θέσεις με σειρά αξιοπιστίας, ενώ ταυτόχρονα μπορεί να χρησιμοποιηθεί για την εξαγωγή οποιουδήποτε reliability sequence ενός πολικού κώδικα με N μικρότερο από 1024. Πρόκειται για μια πραγματικά ριζοσπαστική ανακάλυψη στον σχεδιασμό των πολικών κωδίκων.

6. Εξομοίωση Matlab

Στο παράδειγμα που ακολουθεί γίνεται η προσομοίωση της απλής κωδικοποίησης και SC αποκωδικοποίησης του BSC και BEC καναλιού σε κώδικα matlab. Ο κώδικας δεν περιέχει καμία από τις βελτιώσεις που προστέθηκαν στο 5G standard. Επιπλέον, ο υπολογισμός των likelihood (δηλαδή των πιθανοτήτων $W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 0)$ και $W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 1)$) γίνεται με τρεις διαφορετικές μεθόδους, με τον απλό υπολογισμό των LR (LR domain), με τον υπολογισμό των LLR (LLR domain) και τον υπολογισμό στο P1 domain. Ο κώδικας έχει βασιστεί στο [5].

Ο υπολογισμός της εκάστοτε πιθανότητας στο επίπεδο καναλιού του LR domain, όταν $N = 1$ (σχήμα 6.1), δίνεται από την σχέση:

$$y_i = \frac{P(Y_i = y_i | X_i = 0)}{P(Y_i = y_i | X_i = 1)} \quad (6.1)$$

Αντίστοιχα, ο υπολογισμός της εκάστοτε πιθανότητας στο επίπεδο καναλιού του LLR domain, όταν $N = 1$, δίνεται από την σχέση:

$$y_i = \ln \frac{P(Y_i = y_i | X_i = 0)}{P(Y_i = y_i | X_i = 1)} \quad (6.2)$$

Τέλος, ο υπολογισμός της εκάστοτε πιθανότητας στο επίπεδο καναλιού του P1 domain όταν $N = 1$, δίνεται από την σχέση:

$$y_i = P(X_i = 1 | Y_i = y_i) = \frac{P(Y_i = y_i | X_i = 1)}{P(Y_i = y_i | X_i = 0) + P(Y_i = y_i | X_i = 1)} \quad (6.3)$$



Σχήμα 6.1: Υπολογισμός του likelihood σε επίπεδο καναλιού

Πιο συγκεκριμένα, για την περίπτωση του BSC καναλιού, με πιθανότητα μετάβασης p , η σχέση 6.1 (LLR domain) γίνεται:

$$y_i = \frac{P(Y_i = y_i | X_i = 0)}{P(Y_i = y_i | X_i = 1)} = \frac{P(y_i = 0)}{P(y_i = 1)} = \frac{P(y_i = 0)}{P(y_i = 1)} = \frac{1 - p}{p} \quad (6.4)$$

Στην περίπτωση του BEC καναλιού, με πιθανότητα διαγραφής e , η σχέση 6.1 (LLR domain) γίνεται:

$$y_i = \frac{P(Y_i = y_i | X_i = 0)}{P(Y_i = y_i | X_i = 1)} = \frac{+\infty}{0} = +\infty \quad (6.5)$$

Οπότε, για το LLR domain, οι αρχικές τιμές των likelihoods (y_i) μπορούν να πάρουν τιμές από 0 έως άπειρο. Όμοια, από τις σχέσεις 6.2 και 6.3 προκύπτει ότι οι πιθανές τιμές του y_i είναι:

$$\begin{cases} y_i \in [0, +\infty) & LR \text{ domain} \\ y_i \in (-\infty, +\infty) & LLR \text{ domain} \\ y_i \in [0,1] & P1 \text{ domain} \end{cases} \quad (6.6)$$

Ενώ η οριακή απόφαση, δηλαδή όταν $W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 0) = W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | 1)$, είναι:

$$\begin{cases} y_i = 1 & LR \text{ domain} \\ y_i = 0 & LLR \text{ domain} \\ y_i = 0,5 & P1 \text{ domain} \end{cases} \quad (6.7)$$

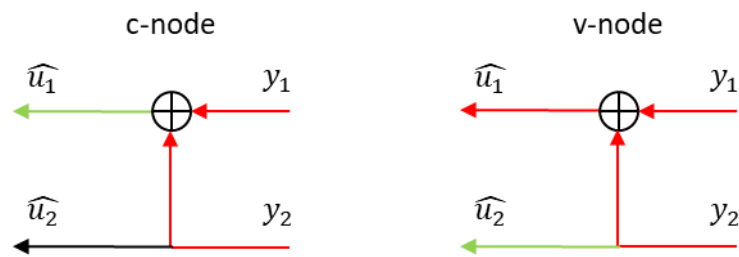
Όταν συνδυάζονται τα δυο likelihood (σχήμα 6.2), ο υπολογισμός του άνω και κάτω likelihood στο LR, LLR και P1 domain γίνεται με τον υπολογισμό του c-node και v-node:

Στην περίπτωση του (c-node) γίνεται ο υπολογισμός του \hat{u}_1 , δηλαδή:

$$y_1 \boxdot y_2 = \begin{cases} \frac{1+y_1y_2}{y_1y_2} & LR \text{ domain} \\ 2 \tanh^{-1}(\tanh(y_1/2) \tanh(y_2/2)) & LLR \text{ domain} \\ y_1(1-y_2) + y_2(1-y_1) & P1 \text{ domain} \end{cases} \quad (6.8)$$

Στην περίπτωση του (v-node) γίνεται ο υπολογισμός του \hat{u}_2 , δηλαδή:

$$y_1 \odot y_2 = \begin{cases} y_1y_2 & LR \text{ domain} \\ y_1 + y_2 & LLR \text{ domain} \\ \frac{y_1y_2}{y_1y_2 + (1-y_1)(1-y_2)} & P1 \text{ domain} \end{cases} \quad (6.9)$$



Σχήμα 6.2: Υπολογισμός $L_N^{(i)}(y_1^N, \hat{u}_i^{i-1})$

Ο τελικός υπολογισμός των likelihood για τις εκτιμήσεις των \hat{u}_1 και \hat{u}_2 γίνεται από τις σχέσεις:

$$\hat{u}_1 = y_1 \boxminus y_2 \quad (6.10)$$

$$\hat{u}_2 = y_1 \odot y_2 \quad (6.11)$$

Ειδικά για την περίπτωση του P1 domain ισχύει ότι $\hat{u}_2 = (y_1 \boxminus y_2) \odot y_2$.

Στο παράδειγμα που ακολουθεί έχει επιλεχθεί, για την περίπτωση του BSC καναλιού, η πιθανότητα μετάβασης να είναι $p = 0,11$ και η πιθανότητα διαγραφής να είναι $e = 0,5$, για την περίπτωση του BEC καναλιού. Η επιλογή αυτών των δυο πιθανοτήτων δεν είναι τυχαία. Με τις συγκεκριμένες τιμές το υπό μελέτη σύστημα μπορεί να έχει μέγιστο ρυθμό μετάδοσης $R = 0,5$. Το παραπάνω ισχύει επειδή για την περίπτωση του BSC καναλιού η χωρητικότητα είναι $C = 1 - H(p) = 0,5$, ενώ για την περίπτωση του BEC καναλιού η χωρητικότητα είναι $C = 1 - \varepsilon = 0,5$.

- Κύριο πρόγραμμα

```

clc
clear all

n=8;
N=2^n; % number of bits
p=0.11; % transition probability
bec=0; % 1 if bec
e=0.5; % erasure probability

point=1;
for rate=0.25:0.02:0.45 % rate
k=round(rate*N); % number of data bits

if (bec)
[biterrd] = polar_bec(n,e); % computation of effective-channel erasure rates on
BEC
else
[biterrd] = polar_bsc(n,p,1000); % probabilistic evaluation of the error
probability for every channel (Monte Carlo Evaluation)
end

% Design polar code
f=polar_design(biterrd,k); %vector of frozen and data channels
A=(f==1/2); % 1 for data channel, 0 for frozen channel

M=500 ; %number of blocks
biterr=zeros(1,M); % bit error rate of each block
for i=1:M
% Set frozen bits, add random data and encode
u=f;
u(A)=rand(1,k)<0.5; % iid choosing of the data bits
x=polar_transform(u); % polar transformation

% Transmit

```

```

% LR domain
if (bec)
y(x==0)=999999;
y(x==1)=0.000001;
y(rand(1,N)<e)=1;
else
err=rand(1,N)<p;
y=zeros(1,N)+(1-p)/p;
y(x==1)=y(x==1).^(-1);
y(err)=y(err).^(-1);
end

%LLR domain
if (bec)
y(x==0)=Inf;
y(x==1)=-Inf;
y(rand(1,N)<e)=0;
else
err=rand(1,N)<p;
y=zeros(1,N)+log((1-p)/p);
y(x==1)=-y(x==1);
y(err)=-y(err);
end

%P1 domain
if (bec)
y = x;
y(rand(1,N)<e)=1/2;
else
err=rand(1,N)<p;
y=zeros(1,N)+p;
y(x==1)=1-y(x==1);
y(err)=1-y(err);
end

% Decode and compute error rate for info bits
[uhat,xhat]=polar_decode(y,f);
biterr(i)=mean(uhat(A)~=u(A));
end

bit_error_rate(point)=mean(biterr); %BER
block_error_rate(point)=mean(biterr>0); %BLER
point=point+1;

end

figure(1)
subplot(121)
plot([0.25:0.02:0.45],bit_error_rate,'g');
xlabel('rate');
ylabel('BER');
axis([0.25,0.45,0,1]);
title('BSC , n=8 , LR domain');
subplot(122)
plot([0.25:0.02:0.45],block_error_rate,'r')
xlabel('rate');
ylabel('BLER');
axis([0.25,0.45,0,1]);
title('BSC , n=8 , LR domain');

```

- Συναρτήσεις

1. Εύρεση των πιο αξιόπιστων θέσεων στην περίπτωση του BEC καναλιού

```
function E = polar_bec(n,e)

E = e;
for i=1:n
    E = reshape([1-(1-E).*(1-E); E.*E],1,[]);
end

end
```

2. Εύρεση των πιο αξιόπιστων θέσεων στην περίπτωση του BSC καναλιού

```
function [biterrd]=polar_bsc(n,p,M)

N=2^n;
f=zeros(1,N);
biterrd=zeros(1,N);

% Monte Carlo Evaluation of error probability
for i=1:M

    %LR domain
    y=zeros(1,N)+(1-p)/p;
    y(rand(1,N)<p)=p/(1-p);

    %LLR domain
    y=zeros(1,N)+log((1-p)/p);
    y(rand(1,N)<p)=-log((1-p)/p);

    %P1 domain
    y=zeros(1,N)+p;
    y(rand(1,N)<p)=1-p;

    % Decode received vector using all-zero frozen vector
    [uhat,xhat]=polar_decode(y,f);
    biterrd=biterrd+uhat;
end
biterrd=biterrd/M;

end
```

3. Τοποθέτηση των δεδομένων στις κατάλληλες θέσεις

```
function f=polar_design(biterrd,k)

[SE, order]=sort(biterrd); % sort into increasing order

f=zeros(1,length(biterrd)); % channels with frozen bits
f(order(1:k))=1/2; % channels with data bits

end
```

4. Κωδικοποίηση

```
function x=polar_transform(u)

if (length(u)==1)
    x=u;
else
    u1u2=mod(u(1:2:end)+u(2:2:end),2);
    u2=u(2:2:end);

    x=[polar_transform(u1u2) polar_transform(u2)];
end
return

end
```

5. Αποκωδικοποίηση διαδοχικής ακύρωσης

```
function [u,x]=polar_decode(y,f)
% x= output hard decision in output order
% u= input hard decisions in input order

N=length(y);
if (N==1)
    if (f==1/2) % ff data bit

        % LR domain
        x=1-(y>1); u=x;

        % LLR domain
        x=1-(y>0); u=x;

        %P1 domain
        x=round(y); u=x;

    else % if frozen bit

        % LR domain
        x=f; u=1-(y>1);

        % LLR domain
        x=f; u=1-(y>0);

        %P1 domain
        x=f; u=round(y);

    end
else

    %LR domain

    % Compute soft mapping back one stage
    ulest=cnop(y(1:2:end),y(2:2:end));
    % R_N^T maps ulest to top polar code
    [uhat1, ulhardprev]=polar_decode(ulest,f(1:(N/2)));
    % Using ulest and x1hard, we can estimate u2
    u2est=vnop(y(1:2:end).^(1-2*ulhardprev),y(2:2:end));
    % R_N^T maps u2est to bottom polar code
    [uhat2, u2hardprev]=polar_decode(u2est,f((N/2+1):end));
```

```

%LLR domain

% Compute soft mapping back one stage
ulest=cnop(y(1:2:end),y(2:2:end));
% R_N^T maps ulest to top polar code
[uhat1, ulhardprev]=polar_decode(ulest,f(1:(N/2)));
% Using ulest and xlhard, we can estimate u2
u2est=vnop((-1).^ulhardprev).*y(1:2:end),y(2:2:end));
% R_N^T maps u2est to bottom polar code
[uhat2, u2hardprev]=polar_decode(u2est,f((N/2+1):end));

%P1 domain

% Compute soft mapping back one stage
ulest=cnop(y(1:2:end),y(2:2:end));
% R_N^T maps ulest to top polar code
[uhat1, ulhardprev]=polar_decode(ulest,f(1:(N/2)));
% Using ulest and xlhard, we can estimate u2
u2est=vnop(cnop(ulhardprev,y(1:2:end)),y(2:2:end));
% R_N^T maps u2est to bottom polar code
[uhat2, u2hardprev]=polar_decode(u2est,f((N/2+1):end));

% decisions
u=[uhat1 uhat2];
x=reshape([ ulhardprev.*(1-u2hardprev)+(1-ulhardprev).*u2hardprev ;
u2hardprev],1,[]);
end

return

end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% LR domain

function z=cnop(w1,w2)
    z=(w1.*w2+1)./(w1+w2);
return
end

% LLR domain

function z=cnop(w1,w2)
    z=2*atanh(tanh(w1/2).*tanh(w2/2));
return
end

% P1 domain

function z=cnop(w1,w2)
    z=w1.*(1-w2) + w2.*(1-w1);
return
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% LR domain

```



```
function z=vnop(w1,w2)
    z=w1.*w2;
return
end

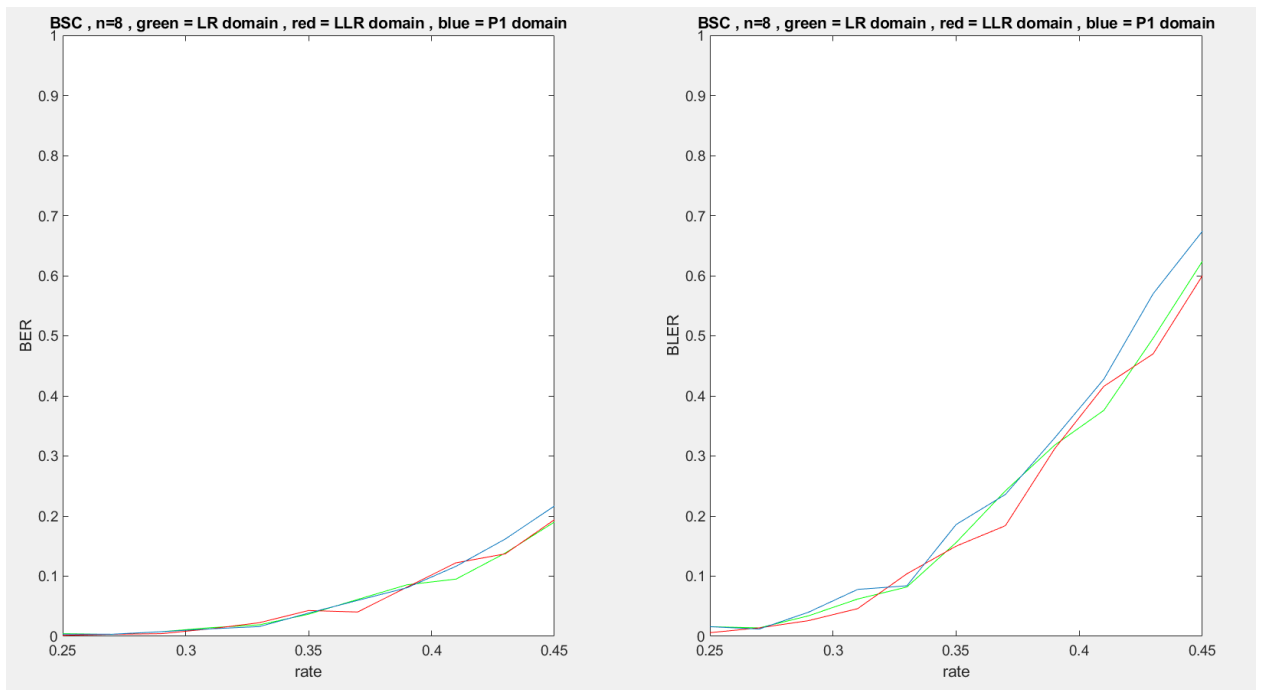
% LLR domain

function z=vnop(w1,w2)
    z=w1+w2;
return
end

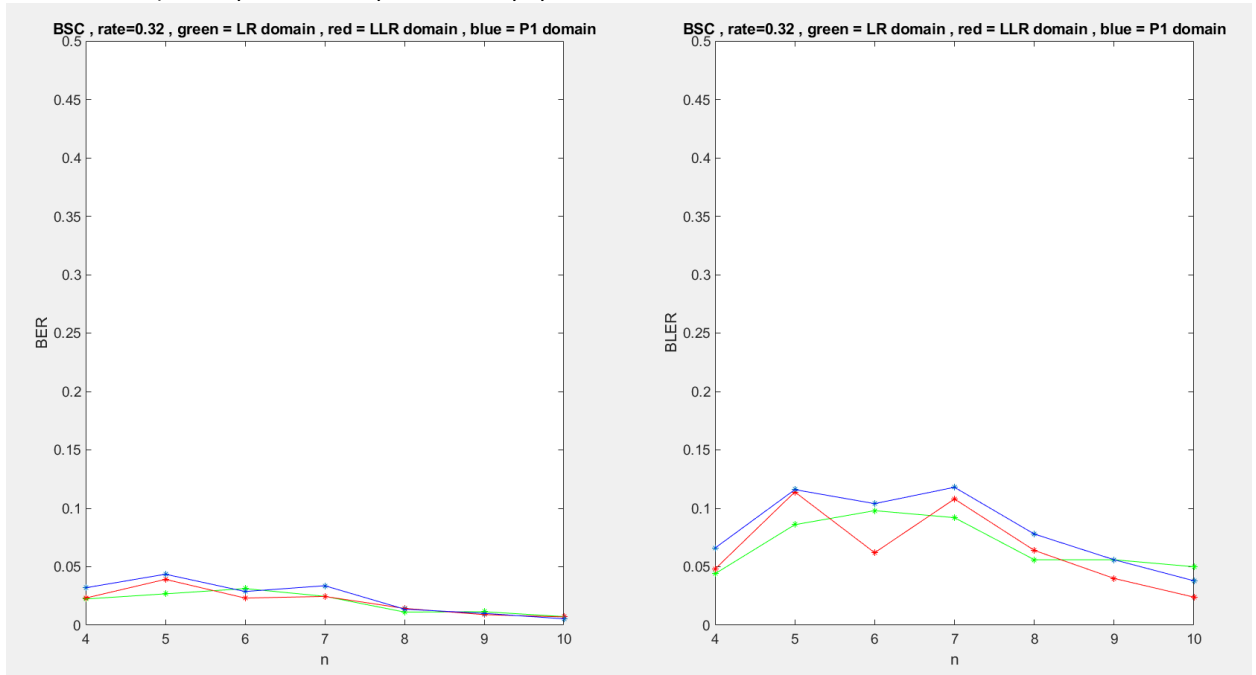
% P1 domain

function z=vnop(w1,w2)
    z=w1.*w2 ./ (w1.*w2 + (1-w1).*(1-w2));
return
end
```

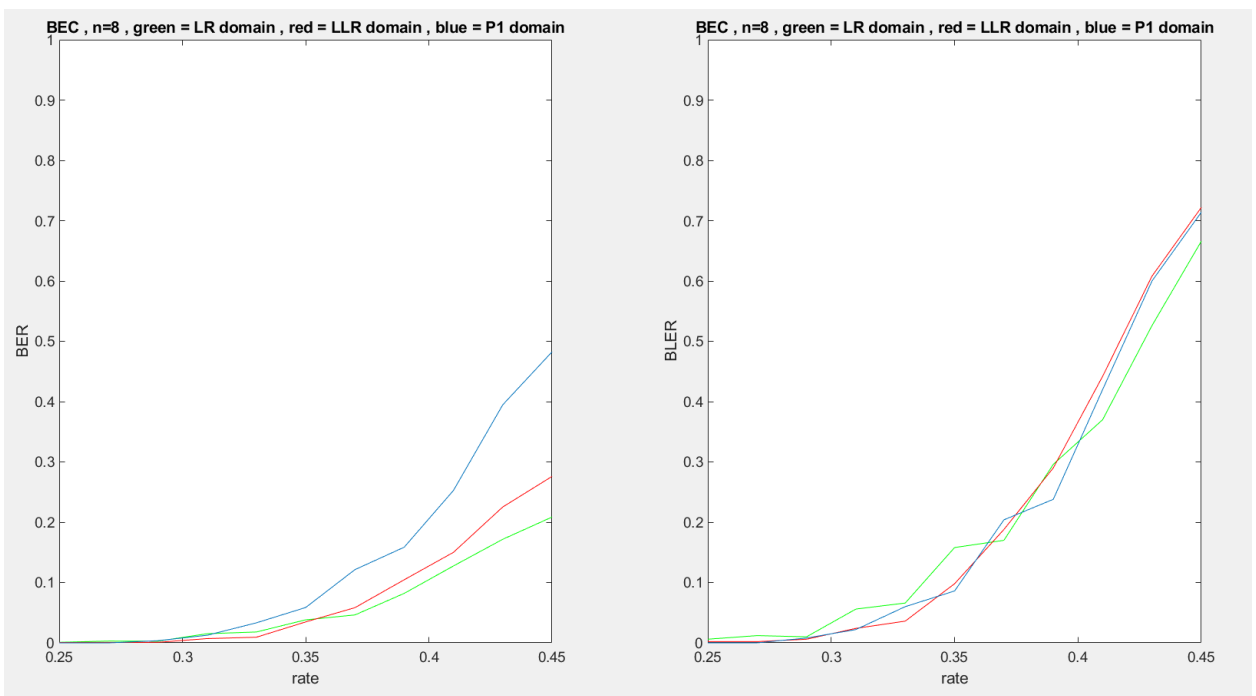
Από τον παραπάνω κώδικα προκύπτουν τα εξής σχήματα:



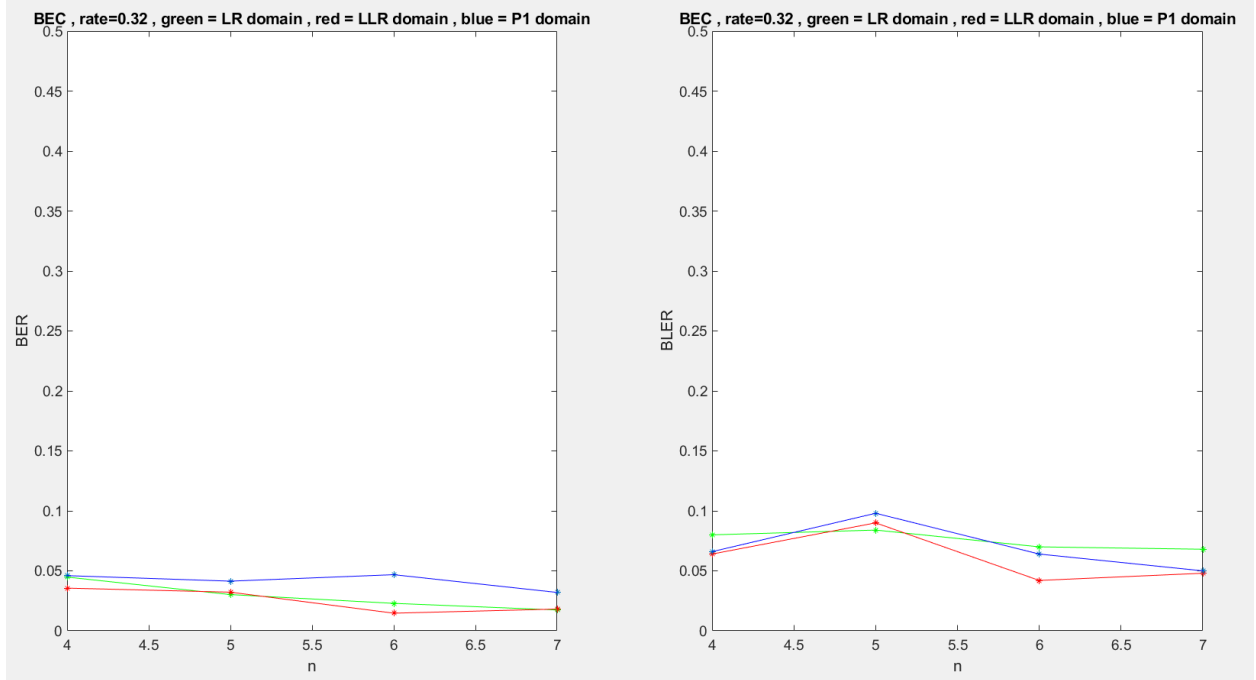
Σχήμα 6.3: Σύγκριση των BER και BLER, σε BSC κανάλι, για ρυθμούς μετάδοσης από 0.25 έως 0.45 και σταθερό $n = 8$ στα LR, LLR και P1 domain



Σχήμα 6.4: Σύγκριση των BER και BLER, σε BSC κανάλι, για σταθερό rate= 0.32 και μεταβλητό n από 4 έως 10 στα LR, LLR και P1 domain



Σχήμα 6.5: Σύγκριση των BER και BLER, σε BEC κανάλι, για ρυθμούς μετάδοσης από 0.25 έως 0.45 και σταθερό $n = 8$ στα LR, LLR και P1 domain



Σχήμα 6.6: Σύγκριση των BER και BLER, σε BEC κανάλι, για σταθερό rate= 0.32 και μεταβλητό n από 4 έως 7 στα LR, LLR και P1 domain

Από το παράδειγμα υλοποίησης φαίνεται ότι κατά την αποκωδικοποίηση του BER καναλιού, στην περίπτωση του LR domain, συναντάται πρόβλημα όταν το n γίνεται μεγαλύτερο του επτά. Αυτό οφείλεται στο error propagation που συμβαίνει λόγω του μεγέθους του μπλοκ και των πολλών λαθών στις αρχικές εκτιμήσεις των \hat{u}_i . Ωστόσο και στις τρεις περιπτώσεις τα αποτελέσματα είναι αρκετά όμοια.

7. Συμπεράσματα

Στα πλαίσια της διπλωματικής εργασίας έγινε λεπτομερής ανάλυση - διερεύνηση των βασικών αρχών των πολικών κωδίκων και των δυνατοτήτων τους. Ιδιαίτερη έμφαση δόθηκε στην θεωρητική και πρακτική περιγραφή τους, ενώ η προσομοίωση στο matlab προσφέρει περαιτέρω βοήθεια στην κατανόησή τους. Η σύγχρονη μορφή των πολικών κωδίκων κατάφερε να ανταποκριθεί σε πολλές απαιτήσεις τηλεπικοινωνιακών υπηρεσιών, όπως: χαμηλή πολυπλοκότητα κωδικοποίησης-αποκωδικοποίησης και υλοποίησης ενώ για ένα ευρύ φάσμα κωδικολέξεων και ρυθμών προσφέρει μεγάλη αξιοπιστία και μικρό χρόνο καθυστέρησης. Ωστόσο, νέες τεχνικές αποκωδικοποίησης αναζητούνται για την βελτιστοποίηση της πολυπλοκότητας της αποκωδικοποίησης και την βελτίωση της επίδοσης σε ρυθμό σφαλμάτων. Παρόλο που η επινόηση των πολικών κωδίκων έγινε το 2009, η πρώτη χρήση των κωδίκων αυτών έγινε μόλις 10 χρόνια μετά στο 5G-eMBB πρότυπο. Η δημοφιλία τους έχει πυροδοτήσει την περαιτέρω ακαδημαϊκή και βιομηχανική έρευνα και με ασφάλεια μπορεί να προβλεφθεί η υιοθέτησή τους σε μελλοντικά πρότυπα και συστήματα, δεδομένης της ευελιξίας στον σχεδιασμό τους και της ικανοποιητικής επίδοσής τους.

- [1] E. Arıkan, *Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels*. *IEEE Trans. Inf. Theory* 55(7), 3051–3073 (2009).
- [2] A. Andi, O. Gazi, *Fast decoding of polar codes*, *IET Communications*, submitted, (2017).
- [3] E. Arıkan, *A performance comparison of polar codes and Reed-Muller codes*. *IEEE Comm. Lett.* 12(6), June (2008).
- [4] Orhan Gazi, *Polar Codes: A Non-Trivial Approach to Channel Coding* (2019).
- [5] Henry D. Pfister, *A Brief Introduction to Polar Codes: Notes for Introduction to Error-Correcting Codes* (2017).
- [6] Erdal Arıkan, *Polar Coding Tutorial*, Simons Institute, US Berkeley, Jan. 15 2015
- [7] E. Arıkan and E. Telatar, “On the rate of channel polarization,” 2008. [Online]. Available: <http://arxiv.org/abs/0807.3806v3>.
- [8] E. Sasoglu, E. Telatar, and E. Arıkan, “Polarization for arbitrary discrete memoryless channels,” in *Proc. 2009 IEEE Information Theory Workshop, Taormina, Italy, 11–16 Oct. 2009*, pp. 144–148S.
- [9] A. Sharma, M. Salim, *Polar Code Appropriateness for Ultra-Reliable and Low-Latency Use Cases of 5G Systems*, Electronics & Communication Department, Malaviya National Institute of Technology, Jaipur, Rajasthan, India (2019).
- [10] Valerio Bioglio, Carlo Condo, Ingmar Land, Senior Member, *Design of Polar Codes in 5G New Radio*, arXiv:1804.04389v3 [cs.IT] 6 Jan 2020.
- [11] E. Ankan, N. ul Hassan, M. Lentmaier, G. Montorsi, J. Sayir, *Challenges and some new directions in channel coding*, *Journal of Communications and Networks*, IEEE, 2015, pp. 328–338.
- [12] 3GPP TR 38.913, *Study on scenarios and requirements for next generation access technologies*, 2016.
- [13] K. Niu and K. Chen, “CRC-aided decoding of polar codes,” *IEEE Communications Letters*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012.
- [14] T. Wang, D. Qu, and T. Jiang, “Parity-check-concatenated polar codes,” *IEEE Communications Letters*, vol. 20, no. 12, pp. 2342–2345, Dec. 2016.
- [15] J. Park and H. Y. Kim, I. and Song, “Construction of parity-check- concatenated polar codes based on minimum Hamming weight code- words,” *Electronics Letters*, vol. 53, no. 14, pp. 924–926, July 2017.
- [16] R. U. N. Hussami, S. B. Korada, “Performance of polar codes for channel and source coding,” *Proc. IEEE International Symposium on Information Theory, Seoul, Jul 2009*.
- [17] M. Seidl, A. Schenk, C. Stierstorfer, and J. B. Huber, “Polar-coded modulation,” *IEEE Transactions on Communications*, vol. 61, no. 10, pp. 4108–4119, Oct. 2013.
- [18] H. Afser, N. Tirpan, H. Delic, and M. Koca, “Bit-interleaved polar- coded modulation,” in *IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, Apr. 2014*.
- [19] K. Tian, R. Liu, and R. Wang, “Joint successive cancellation decoding for bit-interleaved polar coded modulation,” *IEEE Communications Letters*, vol. 20, no. 2, pp. 224–227, Feb. 2016.
- [20] H. Ji, S. Park, J. Yeo, Y. Kim, J. Lee, B. Shim, *Introduction to ultra-reliable and low latency communications in 5G*, arXiv: 1704.05565v1, 2017.

- [21] 3GPP TSG RAN WG1, R1-1706965, *polar coding design*, Huawei, HiSilicon, 2017.
- [22] C. Leroux, A.J. Raymond, G. Sarkis, and W.J. Gross, “A semi-parallel successive-cancellation decoder for polar codes,” *IEEE Transactions on Signal Processing*, vol. 61, no. 2, pp. 289–299, Jan. 2013.
- [23] O. Afisiadis, A. Balatsoukas-Stimming, and A. Burg, “A low-complexity improved successive cancellation decoder for polar codes,” in *IEEE Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, Nov. 2014.
- [24] K. Niu and K. Chen, “Stack decoding of polar codes,” *Electronics Letters*, vol. 48, no. 12, pp. 695–697, June 2012.
- [25] H. Imai and S. Hiraoka, “A new multilevel coding method using error-correcting codes,” *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 371–377, May 1977.
- [26] Mayank Bakshi, Sidharth Jaggi, Michelle Effros, *Concatenated Polar Codes*, California Institute of Technology, Chinese University of Hong Kong, arXiv:1001.2545v1 [cs.IT] 14 Jan 2010.
- [27] G. D. Forney, “Low-density parity-check codes,” Cambridge, Massachusetts, The M.I.T. Press, 1966.
- [28] O. Iscan, D. Lentner, W. Xu, *A comparison of channel coding schemes for 5G short message transmission*, 2016 *IEEE Globecom Workshops (GC Wkshps)*, IEEE, Washington, DC, USA, 2016, pp. 1–6.
- [29] M. Mondelli, S.H. Hassani, R.L. Urbanke, *Unified scaling of polar codes: error exponent, scaling exponent, moderate deviations, and error floors*, *IEEE Transactions on Information Theory*, IEEE, 2016, pp. 6698–6712.
- [30] H. Hassani, K. Alishahi, and R. Urbanke, “Finite-length scaling for polar codes,” *IEEE Trans. Inform. Theory*, vol. 60, no. 10, pp. 5875–5898, 2014.
- [31] M. Alsan and E. Telatar, “A simple proof of polarization and polarization for non-stationary memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 62, no. 9, pp. 4873–4878, 2016.
- [32] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley Series in Telecommunications, Wiley, 2nd. ed., 2006.
- [33] I. Tal and A. Vardy, “List decoding of polar codes,” *IEEE Trans. Inform. Theory*, vol. 61, no. 5, pp. 2213–2226, 2015.
- [34] C. Leroux, A. J. Raymond, G. Sarkis, I. Tal, A. Vardy, and W. J. Gross. *Hardware implementation of successive-cancellation decoders for polar codes*. *Journal of Signal Processing Systems*, 69(3):305–315, 2012.
- [35] H. Mahdaviifar and A. Vardy. *Achieving the secrecy capacity of wiretap channels using polar codes*. *IEEE Transactions on Information Theory*, 57(10):6428–6443, 2011.
- [36] Y. Fountzoulas, A. Kosta, and G. N. Karystinos. *Polar-code-based security on the bsc modeled harq in fading*. In *Telecommunications (ICT), 2016 23rd International Conference on*, 1–5, IEEE, 2016.
- [37] R. A. Chou and M. R. Bloch. *Polar coding for the broadcast channel with confidential messages: A random binning analogy*. *IEEE Transactions on Information Theory*, 62(5):2410–2429, 2016.
- [38] Eleni Antoniou, *Polar Coding for the Binary Erasure Channel* (2018)
- [39] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.
- [40] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [41] C. E. Shannon. *Communication theory of secrecy systems*. *Bell Labs Technical Journal*, 28(4):656–715, 1949.
- [42] R. G. Gallager, “Low Density Parity Check Codes,” Cambridge, MA, MIT Press, 1963.

- [43]C. Berrou, A. Glavieux and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo Codes,” in *Proc. 1993 Int. Conf. Commun.*, Geneva, Switzerland, May 1993.
- [44]A. J. Viterbi, “Error bounds for convolutional codes and an asymptotically optimum decoding algorithm,” *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260-269, Apr. 1967.
- [45]J. Wozencraft and B. Reiffen, “*Sequential Decoding*,” Cambridge, MA, MIT Press, 1961.
- [46]P. Elias, “Coding for noisy channels,” *IRE Conv. Rec.*, pt. 4, pp. 37-46, March 1955.
- [47]A. Hocquengham, “Codes correcteurs d’erreurs,” *Chiffres*, Vol. 2, pp. 147-156, 1959.
- [48]R. C. Bose and D. K. Chaudhuri, “On the class of error-correcting binary group codes,” *Inform. Contr.*, Vol. 3, pp. 68-79, March 1960.
- [49]I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. SIAM*, Vol. 8, pp. 300-304, June 1960.
- [50]D. E. Muller, “Application of Boolean Algebra to switching circuits design and to error detection,” *IRE Trans. Electron. Comput.*, Vol. EC-3, pp. 6-12, Sept. 1954.
- [51]I. S. Reed, “A class of multiple-error correcting codes and the decoding scheme,” *IRE Trans. Inform. Theory*, Vol. IT-4, pp. 38-49, Sept. 1954.
- [52]M. J. Golay, “Notes on Digital Coding,” *Proc. IRE*, Vol. 37, pp. 657, June 1949.
- [53]C. E. Shannon, W. Weaver “*The Mathematical Theory of Communication*,” Urbana Illinois, University of Illinois Press, 1949.
- [54]D. Huffman, “A method for the construction of minimum redundancy codes,” *Proc. IRE*, Vol. 40, pp. 1098-1101, Sept. 1952.
- [55]R. M. Fano, “A heuristic discussion of probability decoding,” *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 64-74, Jan. 1963.
- [56]B. P. Tunstall, “*Synthesis of noiseless compression codes*,” Ph.D. dissertation, Georgia Inst. Technol., Atlanta, GA, Sept. 1967.
- [57]J. Rissanen, “Generalized Kraft inequality and arithmetic coding,” *IBM J. Res. Devel.*, Vol. 20, pp. 198-203, 1976.
- [58]A. Lempel and J. Ziv, “On the complexity of an individual sequence,” *IEEE Trans. on Inform. Theory*, Vol. IT-22, pp. 75-81, Jan. 1976.
- [59]J. Ziv and A. Lempel, “A universal algorithm for sequential data compression,” *IEEE Trans. on Inform. Theory*, Vol. IT-24, pp. 337-343, May 1977.
- [60]J. L. Massey, “Shift register synthesis and BCH decoding,” *IEEE, Trans. Inform. Theory*, Vol. IT-15, no. 1, pp. 122-127, Jan. 1969.
- [61]A. Hocquengham, “Codes correcteurs d’erreurs,” *Chiffres*, Vol. 2, pp. 147-156, 1959.
- [62]R. C. Bose and D. K. Chaudhuri, “On the class of error-correcting binary group codes,” *Inform. Contr.*, Vol. 3, pp. 68-79, March 1960.
- [63]S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. SIAM*, Vol. 8, pp. 300-304, June 1960.

Παράρτημα Α

- Απόδειξη σχέσης (3.12):

$$P(y_1^N, u_1^{i-1} | u_i) = \frac{P(y_1^N, u_1^{i-1}, u_i)}{P(u_i)}$$

$$P(y_1^N, u_1^{i-1} | u_i) = \frac{\sum_{u_{i+1}^N} P(u_1^N, y_1^N)}{P(u_i)}$$

(Λόγω της ιδιότητας: $p(w, x) = \sum_{y, z} p(w, x, y, z)$)

$$P(y_1^N, u_1^{i-1} | u_i) = \frac{\sum_{u_{i+1}^N} P(u_1^N | y_1^N) \cdot P(u_1^N)}{P(u_i)}$$

Αλλά

$$P(u_i) = \frac{1}{2}$$

$$P(u_1^N) = \frac{1}{2^N}$$

Οπότε

$$P(y_1^N, u_1^{i-1} | u_i) = \frac{\sum_{u_{i+1}^N} P(u_1^N | y_1^N) \cdot \frac{1}{2^N}}{\frac{1}{2}}$$

$$P(y_1^N, u_1^{i-1} | u_i) = \frac{1}{2^{N-1}} \sum_{u_{i+1}^N} P(u_1^N | y_1^N)$$

Άρα όταν περιγράφεται το κανάλι $W_N^{(i)}$, ισχύει ότι:

$$W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) \triangleq \sum_{u_{i+1}^N \in X^{N-1}} \frac{1}{2^{N-1}} W_N(y_1^N | u_1^N)$$

- Απόδειξη σχέσης (3.10):

Για $i = 2i - 1$, η σχέση 3.12 γίνεται:

$$W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2} | u_{2i-1}) = \sum_{u_{2i}^{2N}} \frac{1}{2^{2N-1}} W_{2N}(y_1^{2N} | u_1^{2N})$$

$$W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2} | u_{2i-1}) = \sum_{u_{2i,o}^{2N}, u_{2i,e}^{2N}} \frac{1}{2^{2N-1}} W_N(y_1^N | u_{1,o}^{2N} \oplus u_{1,e}^{2N}) W_N(y_{N+1}^{2N} | u_{1,e}^{2N})$$

$$W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2} | u_{2i-1}) = \sum_{u_{2i}} \frac{1}{2} \sum_{u_{2i+1,e}^{2N}} \frac{1}{2^{N-1}} W_N(y_{N+1}^{2N} | u_{1,e}^{2N}) \sum_{u_{2i+1,o}^{2N}} \frac{1}{2^{N-1}} W_N(y_1^N | u_{1,o}^{2N} \oplus u_{1,e}^{2N})$$

Όπου, εξ' ορισμού από την σχέση 3.12, το άθροισμα των $u_{2i+1,o}^{2N}$ είναι ίσο με:

$$W_N^{(i)}(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i})$$

Ενώ το άθροισμα των $u_{2i+1,e}^{2N}$ είναι ίσο με:

$$W_N^{(i)}(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i})$$

Άρα

$$W_{2N}^{(2i-1)}(y_1^{2N}, u_1^{2i-2} | u_{2i-1}) = \sum_{u_{2i}} \frac{1}{2} W_N^{(i)}(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i})$$

- **Απόδειξη σχέσης (3.11):**

Για $i = 2i$, η σχέση 3.12 γίνεται:

$$W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1} | u_{2i}) = \sum_{u_{2i+1}^{2N}} \frac{1}{2^{2N-1}} W_{2N}(y_1^{2N} | u_1^{2N})$$

$$W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1} | u_{2i}) = \frac{1}{2} \sum_{u_{2i+1,e}^{2N}} \frac{1}{2^{N-1}} W_N(y_{N+1}^{2N} | u_{1,e}^{2N}) \sum_{u_{2i+1,o}^{2N}} \frac{1}{2^{N-1}} W_N(y_1^N | u_{1,o}^{2N} \oplus u_{1,e}^{2N})$$

Άρα

$$W_{2N}^{(2i)}(y_1^{2N}, u_1^{2i-1} | u_{2i}) = \frac{1}{2} W_N^{(i)}(y_1^N, u_{1,o}^{2i-2} \oplus u_{1,e}^{2i-2} | u_{2i-1} \oplus u_{2i}) \cdot W_N^{(i)}(y_{N+1}^{2N}, u_{1,e}^{2i-2} | u_{2i})$$

- **Απόδειξη σχέσης (3.23):**

Κατά την μετατροπή $(W, W) \rightarrow (W', W'')$ ισχύει ότι:

$$I(W') = I(U_1; Y_1 Y_2),$$

$$I(W'') = I(U_2; Y_1 Y_2 | U_1) = I(U_2; Y_1 Y_2 U_1)$$

$(I(U_2; Y_1 Y_2 | U_1) = I(U_2; Y_1 Y_2 U_1))$ γιατί U_1 και U_2 είναι ανεξάρτητα

Αλλά επειδή τα (U_1, U_2) έχουν one to one σχέση με τα (X_1, X_2)

$$I(W') + I(W'') = I(U_1 U_2 ; Y_1 Y_2) = I(X_1 X_2 ; Y_1 Y_2) = I(X_1 ; Y_1) + I(X_2 ; Y_2) = 2I(W)$$

$$I(W'') = I(U_2 ; Y_1 Y_2 U_1)$$

$$I(W'') = I(U_2 ; Y_2) + I(U_2 ; Y_1 U_1 | Y_2)$$

$$I(W'') = I(W) + I(U_2 ; Y_1 U_1 | Y_2)$$

Οπότε

$$I(W'') \geq I(W)$$

Άρα

$$I(W') \leq I(W) \leq I(W'')$$

Η πιο γενικά:

$$I(W_{2N}^{(2i-1)}) \leq I(W_N^{(i)}) \leq I(W_{2N}^{(2i)})$$

- **Απόδειξη σχέσης (3.28):**

Για το $Z(W'')$ ισχύει ότι:

$$Z(W'') = \sum_{y_1^2, u_1} \sqrt{W''(f(y_1, y_2), u_1 | 0)} \cdot \sqrt{W''(f(y_1, y_2), u_1 | 1)}$$

$$Z(W'') = \sum_{y_1^2, u_1} \frac{1}{2} \sqrt{W(y_1 | u_1) W(y_2 | 0)} \cdot \sqrt{W(y_1 | u_1 \oplus 1) W(y_2 | 1)}$$

$$Z(W'') = \sum_{y_2} \sqrt{W(y_2 | 0) W(y_2 | 1)} \cdot \sum_{u_1} \frac{1}{2} \sum_{y_1} \sqrt{W(y_1 | u_1) W(y_1 | u_1 \oplus 1)}$$

$$Z(W'') = Z(W)^2$$

Για το $Z(W')$ ισχύει ότι:

$$Z(W') = \sum_{y_1^2} \sqrt{W'(f(y_1, y_2) | 0)} \cdot \sqrt{W'(f(y_1, y_2) | 1)}$$

Αν $\alpha(y_1) = W(y_1 | 0)$, $\delta(y_1) = W(y_1 | 1)$, $\beta(y_2) = W(y_2 | 0)$ και $\gamma(y_2) = W(y_2 | 1)$, τότε:

$$Z(W') = \sum_{y_1^2} \frac{1}{2} \sqrt{\alpha(y_1) \beta(y_2) + \delta(y_1) \gamma(y_2)} \cdot \sqrt{\alpha(y_1) \gamma(y_2) + \delta(y_1) \beta(y_2)}$$

$$Z(W') \leq \sum_{y_1^2} \frac{1}{2} \left[\sqrt{\alpha(y_1)\beta(y_2)} + \sqrt{\delta(y_1)\gamma(y_2)} \right] \cdot \left[\sqrt{\alpha(y_1)\gamma(y_2)} + \sqrt{\delta(y_1)\beta(y_2)} \right] \\ - \sum_{y_1^2} \sqrt{\alpha(y_1)\beta(y_2)\delta(y_1)\gamma(y_2)}$$

$$\left(\text{από την σχέση } \left[\sqrt{(\alpha\beta + \delta\gamma)(\alpha\gamma + \delta\beta)} \right]^2 + 2\sqrt{\alpha\beta\delta\gamma} \cdot (\sqrt{\alpha} - \sqrt{\delta})^2 (\sqrt{\beta} - \sqrt{\gamma})^2 = \right. \\ \left. [(\sqrt{\alpha\beta} + \sqrt{\delta\gamma})(\sqrt{\alpha\gamma} + \sqrt{\delta\beta}) - 2\sqrt{\alpha\beta\delta\gamma}]^2 \right)$$

Όπου

$$\left[\sqrt{\alpha(y_1)\beta(y_2)} + \sqrt{\delta(y_1)\gamma(y_2)} \right] \left[\sqrt{\alpha(y_1)\gamma(y_2)} + \sqrt{\delta(y_1)\beta(y_2)} \right] = Z(W), \\ \sqrt{\alpha(y_1)\beta(y_2)\delta(y_1)\gamma(y_2)} = Z(W)^2$$

Συνεπώς

$$Z(W') \leq 2Z(W) - Z(W)^2$$

Άρα

$$Z(W') + Z(W'') \leq 2Z(W)$$

Ή πιο γενικά:

$$Z(W_{2N}^{(2i-1)}) + Z(W_{2N}^{(2i)}) \leq 2Z(W_N^{(i)})$$

- **Απόδειξη polarization:**

Το βασικό αποτέλεσμα της διαδικασίας του recursion είναι ότι από το αρχικό κανάλι W προκύπτουν δυο νέα κανάλια, το $W_2^{(1)}$ και το $W_2^{(2)}$. Η μετατροπή που προκύπτει από το αρχικό κανάλι W είναι το πρώτο βήμα της διαδικασίας του recursion, δηλαδή:

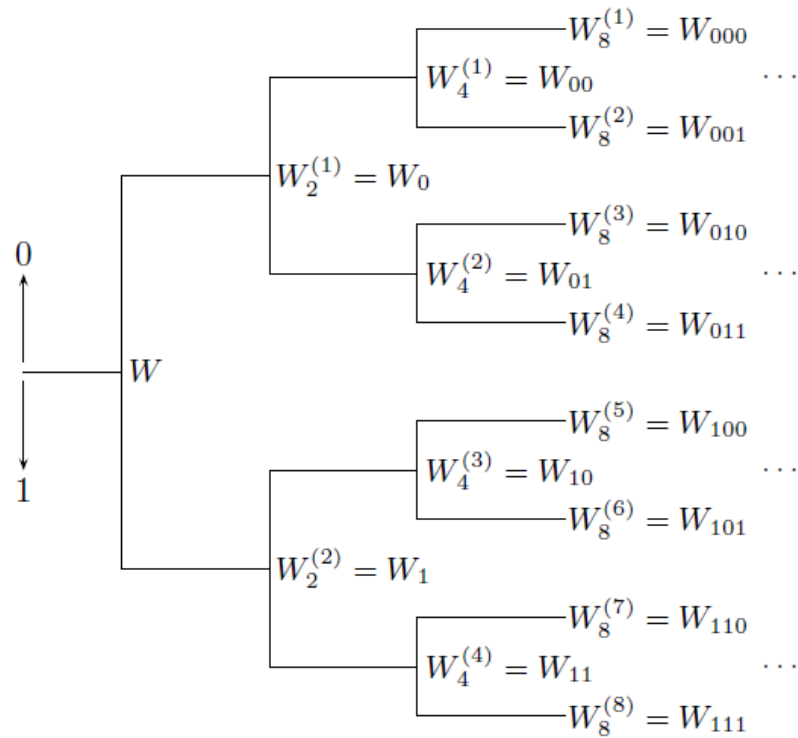
$$(W, W) \rightarrow (W_2^{(1)}, W_2^{(2)}) \text{ ή } (W, W) \rightarrow (W^-, W^+)$$

Με την ίδια λογική, το δεύτερο βήμα του recursion γίνεται στα κανάλια $W_2^{(1)}$ και $W_2^{(2)}$, από τα οποία προκύπτουν τέσσερα νέα κανάλια, δηλαδή:

$$(W_2^{(1)}, W_2^{(1)}) \rightarrow (W_4^{(1)}, W_4^{(2)})$$

$$(W_2^{(1)}, W_2^{(2)}) \rightarrow (W_4^{(3)}, W_4^{(4)})$$

Αν το γενικό κανάλι οριστεί ως $W_{2^n}^{(i)}$, τότε πρέπει να γίνουν n βήματα για να προκύψουν τα κανάλια $W_N^{(i)}$, η διαδικασία φαίνεται καλύτερα στο σχήμα 9.1.



Σχήμα 9.1: Αναδρομική κατασκευή καναλιών

Το κάθε κανάλι $W_{2^n}^{(i)}$ μπορεί να αναπαρασταθεί και στην δυαδική μορφή του, δηλαδή:

$$W_{b_1 b_2 \dots b_n}$$

Όπου τα $b_1 b_2 \dots b_n$ δείχνουν τον δυαδικό αριθμό του εκάστοτε καναλιού και ταυτόχρονα περιγράφουν από ποιους κόμβους προήλθε το κανάλι $W_{b_1 b_2 \dots b_n}$. Για b ίσο με 1 τότε ακολουθείται ο κάτω κόμβος, ενώ για b ίσο με 0 τότε ακολουθείται ο άνω κόμβος (σχήμα 9.1). Για παράδειγμα, $W_8^{(3)} = W_{010}$. Το επόμενο βήμα, από n , θα έχει αριθμό $b_1 b_2 \dots b_n 0$ ή $b_1 b_2 \dots b_n 1$, αν πρόκειται για τον άνω ή κάτω κόμβο αντίστοιχα.

Τα κανάλια $W_{b_1 b_2 \dots b_n}$ μπορούν να οριστούν ισοδύναμα και ως K_n , για $n \geq 0$, και ισχύει ότι:

$$K_0 = W$$

$$K_n = W_{b_1 b_2 \dots b_n}$$

Το K_{n+1} είναι ίσο με $W_{b_1 b_2 \dots b_n 0}$ ή $W_{b_1 b_2 \dots b_n 1}$, όπου και τα δυο ενδεχόμενα έχουν πιθανότητα $\frac{1}{2}$.

Η χωρητικότητα και η παράμετρος Bhattacharyya, του κάθε καναλιού K_n , δίνεται από τους τύπους:

$$I_n = I(K_n), Z_n = Z(K_n)$$

Από τα παραπάνω, με την χρήση της σ -Algebra προκύπτει το probability space (Ω, F, P) . Όπου:

1. το Ω δείχνει τον χώρο όλων των δυαδικών σειρών $(b_1, b_2, \dots) \in \{0, 1\}^\infty$,
2. το F είναι το Borel field που δημιουργείται από τα κυλινδρικά sets $S(b_1 b_2 \dots b_n) \triangleq \{\omega \in \Omega : \omega_1 = b_1, \dots, \omega_n = b_n\}, n \geq 1, b_1 \dots b_n \in \{0, 1\}$
3. το P είναι η πιθανότητα που υπολογίζεται στο εκάστοτε πεδίο F , όπου $P(S(b_1 b_2 \dots b_n)) = 1/2^n$

Λόγω του είδους το προβλήματος, προκύπτει ότι:

$$F_0 \subset F_1 \subset \dots \subset F, \text{ για } 1 \leq i \leq n$$

- Αν το πρόβλημα μελετηθεί υπό όρους χωρητικότητας I_n , τότε:

$$F_n \subset F_{n+1},$$

$$E[|I_n|] < \infty,$$

Για $0 \leq I_n \leq 1$, ισχύει ότι:

$$E[I_{n+1} | S(b_1 b_2 \dots b_n)] = \frac{1}{2}I(W_{b_1 b_2 \dots b_n 0}) + \frac{1}{2}I(W_{b_1 b_2 \dots b_n 1}) = I(W_{b_1 b_2 \dots b_n})$$

Οπότε το σύστημα μπορεί να χαρακτηριστεί ως martingale, που σημαίνει ότι η χωρητικότητα συγκλίνει σε μια τιμή I_∞ , όπου γενικά ισχύει:

$$E[I_\infty] = I_0$$

- Αν το πρόβλημα μελετηθεί υπό όρους της παραμέτρου Bhattacharyya Z_n , τότε:

$$F_n \subset F_{n+1},$$

$$E[|Z_n|] < \infty,$$

Για $0 \leq Z_n \leq 1$, ισχύει ότι:

$$E[Z_{n+1} | S(b_1 b_2 \dots b_n)] = \frac{1}{2}Z(W_{b_1 b_2 \dots b_n 0}) + \frac{1}{2}Z(W_{b_1 b_2 \dots b_n 1}) \leq Z(W_{b_1 b_2 \dots b_n})$$

Αυτήν την φορά, λόγω της ανισότητας, το σύστημα χαρακτηρίζεται ως super-martingale, που σημαίνει ότι η παράμετρος Bhattacharyya συγκλίνει σε μια τιμή Z_∞ .

Από το Doob's Martingale θεώρημα σύγκλισης, για Bounded Martingales, το σύστημα συγκλίνει όταν:

$$E[|Z_n - Z_\infty|] \rightarrow 0,$$

$$E[|Z_{n+1} - Z_n|] \rightarrow 0$$

Αλλά

$$Z_{n+1} = Z_n^2 \text{ με πιθανότητα } 1/2$$

Οπότε

$$E[|Z_{n+1} - Z_n|] \geq (1/2)E[Z_n(1 - Z_n)] \geq 0$$

Άρα

$$E[Z_n(1 - Z_n)] \rightarrow 0$$

$$E[Z_\infty(1 - Z_\infty)] = 0$$

$$Z_\infty = 0 \text{ ή } Z_\infty = 1$$

Και επειδή

$$I_\infty = 1 - Z_\infty$$

$$I_\infty = 0 \text{ ή } I_\infty = 1$$