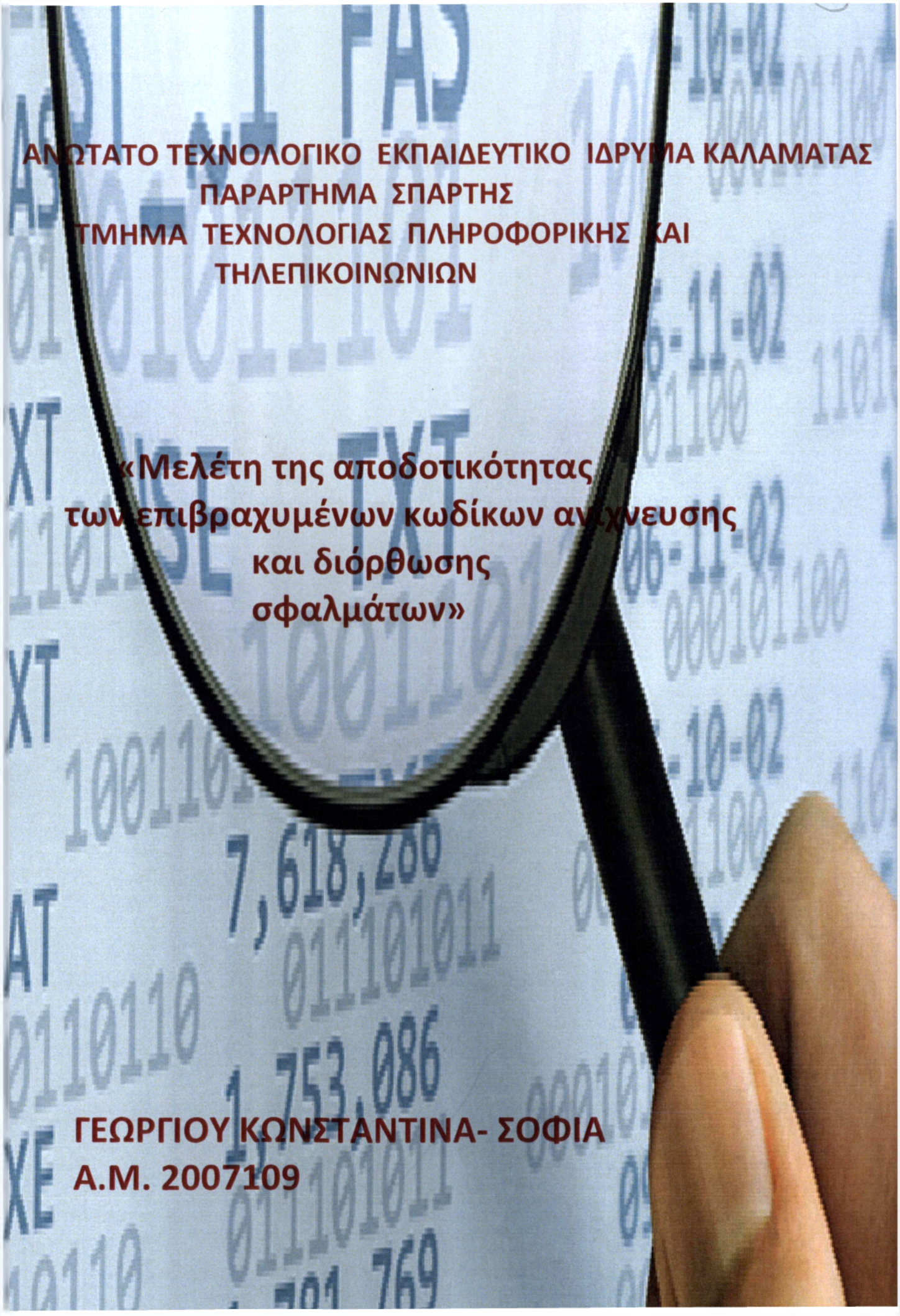
ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ
ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

«Μελέτη της αποδοτικότητας των επιβραχυμένων κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων»



ΓΕΩΡΓΙΟΥ ΚΩΝΣΤΑΝΤΙΝΑ- ΣΟΦΙΑ
Α.Μ. 2007109

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΛΑΜΑΤΑΣ
ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

«Μελέτη της αποδοτικότητας των επιβραχυμένων κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΓΕΩΡΓΙΟΥ ΚΩΝΣΤΑΝΤΙΝΑ- ΣΟΦΙΑ
Α.Μ. 2007109

Επιβλέπων καθηγητής: Γιάννης Λιαπέρδος

ΣΠΑΡΤΗ 2012

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 3^{Ο}

ΚΩΔΙΚΕΣ ΜΠΛΟΚ

ΚΕΦΑΛΑΙΟ 4^{Ο}

ΕΦΑΡΜΟΓΕΣ - ΠΡΑΚΤΙΚΗ ΑΞΙΑ

Ευχαριστίες

Για την εκπόνηση αυτής της πτυχιακής εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Ιωάννη Λιαπέρδο για τη θερμή υποστήριξή του και τη βοήθειά του, αλλά κυρίως για την υπομονή και το ενδιαφέρον που έδειξε όλο αυτό το διάστημα. Επίσης, ευχαριστώ ιδιαίτερα τους γονείς μου και την αδερφή μου για την αμέριστη συμπαράσταση και υποστήριξη, υλική και ηθική, που μου παρείχαν όλα αυτά τα χρόνια.

Πρόλογος

Αντικείμενο της πτυχιακής μου εργασίας είναι η μελέτη της αποδοτικότητας των επιβραχυμένων κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων. Το γεγονός ότι το θέμα επιβάλλει ευρεία ανάπτυξη, με οδήγησε στο να διαιρέσω την εργασία σε τέσσερα (4) επιμέρους κεφάλαια.

Το 1° κεφάλαιο παρουσιάζει μια γενική εισαγωγή του θέματος, δίνοντας εννοιολογικές αρχές και χρήσεις των κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων.

Οι διάφορες κατηγορίες κωδίκων ελέγχου σφάλματος αναφέρονται στο 2° κεφάλαιο.

Στο 3° κεφάλαιο, περιγράφονται αναλυτικά οι υποκατηγορίες στις οποίες διαχωρίζονται οι «κώδικες μπλοκ».

Στο 4° και τελευταίο κεφάλαιο, παρουσιάζονται οι εφαρμογές των κωδίκων ελέγχου σφάλματος (ψηφιακή μετάδοση και αποθήκευση-αναπαραγωγή).

Η μελέτη ολοκληρώνεται με έναν συνοπτικό επίλογο και αξιόπιστη βιβλιογραφία.

Εισαγωγή

Η τεχνολογία έκανε αισθητή την παρουσία της στην καθημερινότητα του ανθρώπου διευκολύνοντας, ως επί το πλείστον , την ποιότητα της ζωής του και την κάλυψη των αναγκών του. Ο κυριότερος τομέας της καθημερινότητας είναι οι επικοινωνία, η οποία έχει παρουσιάσει σημαντική εξέλιξη τα τελευταία χρόνια. Καθημερινά, δίνουν το παρόν ολοένα και περισσότερες υπηρεσίες στον τομέα της επικοινωνίας, με συνεχώς αυξανόμενες απαιτήσεις σε ταχύτητα, ποιότητα και αξιόπιστη μετάδοση σε πραγματικό χρόνο. Η θεαματική αυτή πρόοδος στον τομέα της επικοινωνίας οφείλεται σε μεγάλο βαθμό στην απόδοση αλλά και στο χαμηλό κόστος των συσκευών και κυκλωμάτων γενικά που χρησιμοποιούνται. [1]

Η παρουσία λαθών στα ψηφιακά συστήματα επεξεργασίας πληροφοριών είναι κάτι που παρατηρήθηκε από τα πρώτα χρόνια εμφάνισής τους. Τα λάθη συμβαίνουν λόγω γήρανσης των μεταλλικών αγωγών, επηρεασμού από το περιβάλλον, ατελειών στην κατασκευή κλπ. Όπως θα μάθετε στα Ψηφιακά Ηλεκτρονικά στην ουσία το λάθος είναι απόρροια της ανικανότητας χειρισμού αλλαγών στις στάθμες δυναμικού πέρα από συγκεκριμένα όρια.

[1] Γεώργιος Κων. Κοκκινάκης, (2004), "Εισαγωγή στις Επικοινωνίες"

Για να γίνει πιο κατανοητό αυτό, ας δώσουμε ένα πραγματικό παράδειγμα έχοντας κατά νου την παραδοσιακή τεχνολογία TTL. Ένα ψηφιακό κύκλωμα της τεχνολογίας αυτής θεωρεί ως λογικό 0 οτιδήποτε βρίσκεται σε στάθμες δυναμικού 0 – 0,7 V και ως λογικό 1 οτιδήποτε βρίσκεται σε στάθμες δυναμικού 2,7 – 5 V. Υπάρχει συνεπώς μια περιοχή απαγορευμένων δυναμικών μεταξύ 0,7 και 2,7 V. Υπό κανονικές συνθήκες δεν περιμένουμε τα σήματα εισόδου του ψηφιακού μας κυκλώματος να βρεθούν εντός αυτής της περιοχής, διότι δεν ξέρουμε κατά πόσο οι αντιπροσωπευόμενες πληροφορίες θα ερμηνευτούν σωστά. Ας υποθέσουμε ωστόσο ότι μία εκ των εξόδων του ψηφιακού μας συστήματος διέρχεται μέσα από ένα πεδίο μέχρι να αποτελέσει είσοδο της επόμενης βαθμίδας επεξεργασίας. Υποθέστε ότι αυτή βρίσκεται στο λογικό 0 με δυναμικό 0,3 V. Ας υποθέσουμε ότι στιγμιαία το πεδίο μας λόγω παρεμβολών μετατρέπεται σε μαγνητικό. Η ψηφιακή γραμμή μας αυτόματα μετατρέπεται σε αγωγό εντός μαγνητικού πεδίου και συνεπώς επάγεται πάνω της κάποιο ρεύμα με αποτέλεσμα να αποκτήσει κάποιο νέο δυναμικό.

Αν το επαγόμενο ρεύμα έχει αντίθετη φορά με το αρχικό τότε το δυναμικό θα μειωθεί περαιτέρω από τα 0,3 V και συνεπώς το ψηφιακό μας σύστημα θα λειτουργήσει m σωστά.

Στην αντίθετη περίπτωση μπορεί είτε η επήρεια του επαγόμενου ρεύματος να είναι μικρή και το δυναμικό να μη ξεπεράσει τα 0,7 V είτε να συμβεί το αντίθετο.

Στη δεύτερη περίπτωση αν το δυναμικό υπερβεί τα 2,7 V τότε το επόμενο ψηφιακό μας σύστημα θα ερμηνεύσει εντελώς ανάποδα την αρχική πληροφορία και ένα λάθος θα έχει συμβεί.

Στην παραπάνω απλουστευμένη περιγραφή θεωρήσαμε ότι ένα λάθος ισοδυναμεί με την αντιστροφή της τιμής ενός δυαδικού ψηφίου (single bit error). Αν και αυτή η θεώρηση θα μας διευκολύνει παρακάτω να διατυπώσουμε βασικές αρχές, δε συμβαδίζει πάντοτε με την πραγματικότητα. Μπορεί δηλαδή περισσότερα του ενός δυαδικά ψηφία να αλλοιωθούν (multiple bit error). Και οι δύο παραπάνω περιπτώσεις όμως απαιτούν την ανάπτυξη αποτελεσματικών μέτρων προστασίας. Το πλέον ευρύτερα διαδεδομένο όπλο κατά της δημιουργίας λαθών στα ψηφιακά συστήματα αποτελούν οι κώδικες ανίχνευσης ή / και διόρθωσης λαθών (errormdetection / correction codes).

Για να υπάρχει δυνατότητα ανίχνευσης / διόρθωσης λαθών, πρέπει ο αποστολέας και ο παραλήπτης να συνεννοηθούν εξ αρχής, έτσι ώστε ένα μόνο υποσύνολο των δυνατών συνδυασμών να θεωρείται έγκυρο (σύνολο κωδικών λέξεων – set of codewords) και οι λοιποί συνδυασμοί να

θεωρούνται άκυροι (non-codewords). Η ιδέα πίσω από αυτή τη συμφωνία είναι ότι ο αποστολέας παράγει μόνο κωδικές λέξεις που απουσία λαθών φτάνουν και γίνονται αποδεκτές από τον παραλήπτη, ενώ παρουσία λαθών μετατρέπονται σε μη κωδικές λέξεις που απαιτούν ειδικές ενέργειες από τον παραλήπτη. Η υλοποίηση της παραπάνω σύμβασης μπορεί να πραγματοποιηθεί επισυνάπτοντας k επιπλέον δυαδικά ψηφία στην αρχική πληροφορία (ψηφία ελέγχου – check bits) και χαρακτηρίζοντας ορισμένους μόνο από τους 2n+k συνδυασμούς ως έγκυρους. Στην ουσία αυτό οδηγεί σε μια κωδικοποίηση της αρχικής πληροφορίας αφού κάθε αρχική λέξη των n δυαδικών ψηφίων αντιστοιχίζεται σε μια νέα λέξη των n+k δυαδικών ψηφίων. Η ανάλυση αυτή καθιστά προφανές ότι η ανάγκη για ανίχνευση / διόρθωση λαθών οδηγεί το αρχικό μας σύστημα σε διάφορες επιβαρύνσεις. Ο ρυθμός μεταφοράς δεδομένων είναι πλέον χαμηλότερος ενώ χρειάζεται χρόνος στον αποστολέα για την κωδικοποίηση της πληροφορίας και στον παραλήπτη για τον έλεγχο της ορθότητας.

Υποθέστε ότι το αρχικό μας σύστημα έχει n=8 και ρυθμό μεταφοράς δεδομένων 2 Mbit/s. Αν θέσουμε k=3, τότε σε 1 sec μεταφέρονται πάλι 2Mbit, με τη διαφορά όμως ότι μόνο τα 8/11 είναι χρήσιμη πληροφορία και τα 3/11 πληροφορία ελέγχου. Συνεπώς ο ωφέλιμος ρυθμός μεταφοράς

δεδομένων είναι πλέον (8/11) * 2 Mbit = 1,45 Mbit και η επιβάρυνση του συστήματός μας είναι 27%.

Τα μεγάλα ερωτήματα που καλείται η επιστήμη μας να απαντήσει είναι :

α) Πόσα είναι τα ελάχιστα ψηφία ελέγχου που απαιτούνται για την επίτευξη διαφορετικών στόχων ανίχνευσης / διόρθωσης λαθών ;

β) Μεταξύ των διαφορετικών κωδικοποιήσεων που μπορώ να πάρω με k δυαδικά ψηφία ελέγχου, ποια προσφέρει τις περισσότερες δυνατότητες ανίχνευσης /διόρθωσης λαθών, ποια οδηγεί στα πιο γρήγορα κυκλώματα κωδικοποίησης /αποκωδικοποίησης κλπ. ;

Απαντήσεις σε πολλά από αυτά τα ερωτήματα βρίσκουμε από τις εργασίες του μαθηματικού Richard Wesley Hamming (1915 – 1998), ο οποίος θεωρείται ο θεμελιωτής αυτού του κομματιού της επιστήμης μας μιας και ήταν ο πρώτος που εισήγαγε τυπικούς τρόπους κατασκευής ορισμένων κωδίκων. Στη συνέχεια αναπτύσσουμε ορισμένες από τις έννοιες που εισήγαγε ο Hamming. Πρωταρχική είναι η έννοια της *απόστασης μεταξύ δύο ψηφιολέξεων (Hamming distance)*, ο αριθμός δηλαδή των αντίστοιχων δυαδικών ψηφίων στις οποίες αυτές διαφέρουν. Για παράδειγμα οι ψηφιολέξεις 01001 και 11101 έχουν απόσταση κατά Hamming 2, αφού διαφέρουν στο 1ο και το 3ο από αριστερά ψηφία.

Όμοια οι ψηφιολέξεις 111 και 011 έχουν απόσταση 1. Ας υποθέσουμε τώρα ότι κατασκευάζουμε ένα κώδικα του οποίου οι κωδικές λέξεις έχουν όλες μήκος 2n+k δυαδικά ψηφία. Ο Hamming ονόμασε απόσταση του κώδικα (code distance) τον ελάχιστο αριθμό των ψηφίων στα οποία διαφέρει κάθε δυνατό ζεύγος κωδικών λέξεων. Για παράδειγμα ας υποθέσουμε τον κώδικα που έχει τις εξής κωδικές λέξεις : 1111, 0011, 0000, 1101. Η κατά Hamming απόσταση μεταξύ 2 κωδικών λέξεων φαίνεται στον πιο κάτω πίνακα. Ο κώδικάς συνεπώς έχει απόσταση την ελάχιστη τιμή που εμφανίζεται στη δεξιά στήλη, δηλαδή 1.

Ας εξετάσουμε τώρα τη φυσική έννοια αυτών των μεγεθών και ας μαθηματικοποιήσουμε ορισμένες παρατηρήσεις. Παρατηρείστε ότι *ένας κώδικας με απόσταση 1 δε μας προσφέρει καμία δυνατότητα για ανίχνευση και διόρθωση λαθών.* Ο λόγος είναι προφανής, αφού ακόμη και ένα λάθος μπορεί να οδηγήσει σε άλλη κωδική λέξη. Στον παραπάνω κώδικα εάν ο αποστολέας έστελνε την κωδική λέξη 1111 και αυτή αλλοιωνόταν στο 1ο δυαδικό ψηφίο, τότε ο παραλήπτης θα έπαιρνε την λέξη 0111, η οποία δεν είναι λέξη του κώδικα και συνεπώς θα αντιλαμβανόταν ότι κάτι πήγε λάθος. Ωστόσο αν αλλοιωνόταν το 3° δυαδικό ψηφίο, ο παραλήπτης θα λάμβανε λανθασμένα την λέξη 1101, που καθόσον είναι κωδική θα γινόταν αποδεκτή. Αν περιορίζαμε τον κώδικά μας στις λέξεις 1111, 0011, 0000,

τότε αυτός θα αποκτούσε απόσταση 2. Είναι πλέον προφανές ότι ο νέος κώδικας έχει την ικανότητα ανίχνευσης απλού λάθους. Ένα απλό λάθος εφαρμοζόμενο σε οποιαδήποτε κωδική λέξη δε μπορεί να οδηγήσει σε κάποια άλλη αφού κάθε άλλη διαφέρει σε τουλάχιστον 2 δυαδικά ψηφία. Γενικεύοντας αυτή τη λογική μπορούμε να πούμε ότι ένας κώδικας με απόσταση d+1 προσφέρει ικανότητα ανίχνευσης έως και d λαθών.

Υποθέστε τώρα ότι μεταξύ του αποστολέα και του παραλήπτη ανταλλάσσονται πλέον κωδικές λέξεις από κάποιον κώδικα με απόσταση 2. Όταν λοιπόν συμβεί ένα απλό λάθος ο παραλήπτης αγνοεί αυτή τη πληροφορία και ζητάει από τον αποστολέα να επαναλάβει την αποστολή της ίδιας πληροφορίας.

Προφανώς όταν ο ρυθμός των λαθών είναι αυξημένος χάνεται πολύτιμος χρόνος για επαναμετάδοση πληροφοριών. Επίσης ο μέγιστος χρόνος για μια ορθή μετάδοση δεν είναι φραγμένος άνω. Σε αυτές τις περιπτώσεις είναι ίσως καλύτερο να δώσουμε στον παραλήπτη την ικανότητα να διορθώνει τυχόν λάθη. Δεδομένου του δυαδικού συστήματος, η διόρθωση των λαθών στην πραγματικότητα έγκειται στον εντοπισμό των δυαδικών ψηφίων που έχουν υποστεί αλλοίωση και στην αντιστροφή της αλλοιωμένης τιμής τους. Πως όμως μπορεί να γίνει ο εντοπισμός αυτός;

Υποθέστε και πάλι το περιορισμένο κώδικα με απόσταση 2 που χρησιμοποιήσαμε πιο πάνω. Ας υποθέσουμε ότι ο αποστολέας στέλνει την κωδική λέξη 1111 και ένα απλό λάθος την αλλοιώνει στην μη κωδική λέξη 1011. Ο παραλήπτης προφανώς αντιλαμβάνεται ότι συνέβη λάθος όμως δε μπορεί να το διορθώσει γιατί η λέξη 1011 που έφτασε σε αυτόν "μοιάζει" με δύο κωδικές λέξεις την 1111 και την 0011. Αν περιορίζαμε ακόμα περισσότερο τον κώδικά μας σε δύο μόνο κωδικές λέξεις 1111 και 0000 τότε είναι προφανές ότι το πιο πάνω λάθος σε καθεστώς απλών λαθών είναι σαφέστατα διαχωρίσιμο και συνεπώς ο παραλήπτης μπορεί πλέον να το διορθώσει. Οι παραπάνω δύο κωδικές λέξεις έχουν απόσταση 4 αλλά το ίδιο θα συνέβαινε και αν είχαν απόσταση 3. Κάθε απλό λάθος σε έναν κώδικα με απόσταση 3 οδηγεί σε μία μη κωδική λέξη που έχει απόσταση 1 από μία μόνο κωδική λέξη και 2 από κάθε άλλη. Συνεπώς ο παραλήπτης μπορεί να αναγνωρίζει αυτή τη μη κωδική λέξη σαν την κωδική λέξη εκ της οποίας απέχει το λιγότερο. Γενικεύοντας αυτή τη λογική μπορούμε να πούμε ότι ένας κώδικας με απόσταση 2c+1 προσφέρει ικανότητα διόρθωσης έως και c λαθών.

Για την εφαρμογή των παραπάνω στην πράξη, κάποιος χρειάζεται να ορίσει τον αριθμό των ψηφίων ελέγχου καθώς και τις λογικές συναρτήσεις που θα πρέπει να υλοποιηθούν για την αύξηση της απόστασης μεταξύ των πληροφοριών που θα κωδικοποιηθούν. Προφανώς ένας κώδικας είναι εφαρμόσιμος αν οδηγεί σε απλά κυκλώματα κωδικοποίησης / αποκωδικοποίησης.

Στην πλέον συνήθη περίπτωση της ανίχνευσης απλού λάθους έχει δειχθεί ότι απαιτείται μόνο ένα επιπλέον δυαδικό ψηφίο ισοτιμίας για την επίτευξη κώδικα απόστασης 2. Το ψηφίο αυτό ονομάζεται ψηφίο ισοτιμίας (parity bit) και υπολογίζεται έτσι ώστε ο τελικός αριθμός των άσσων στην κωδική λέξη να είναι άρτιος ή περιττός ανάλογα με την επιλογή άρτιας ή περιττής ισοτιμίας. Αν η αρχική μας πληροφορία είναι η 100111011 και θελήσουμε να κατασκευάσουμε την κωδική λέξη για αυτή την πληροφορία σε έναν κώδικα άρτιας ισοτιμίας θα πρέπει να προσθέσουμε ένα δυαδικό ψηφίο ώστε η τελική λέξη να έχει άρτιο αριθμό από άσους. Άρα στο παράδειγμά μας η προκύπτουσα κωδική λέξη θα είναι : 0 1 100111011.

Οι Lin και Costello έδειξαν ότι μπορούν να πετύχουν ανίχνευση πολλαπλών λαθών αν επισυνάψουν στην αρχική πληροφορία το υπόλοιπο της διαίρεσής της θεωρούμενης ως πολυώνυμο με ένα άλλο πολυώνυμο το οποίο ονομάζεται γεννήτορας πολυώνυμο.

Οι ικανότητες ανίχνευσης που παρέχονται από αυτούς τους κώδικες περιορίζονται μόνο από το βαθμό και την "ποιότητα" του γεννήτορα πολυωνύμου. Πολλά από αυτά τα πολυώνυμα προστατεύονται από πατέντες και αποτελούν πλέον στάνταρτ τα οποία υποχρεωτικά πρέπει να υλοποιούν όλες οι συσκευές ενός δικτύου. Τους κυκλικούς κώδικες θα έχετε την ευκαιρία να γνωρίσετε αναλυτικότερα στα μαθήματα των Δικτύων Υπολογιστών και Σχεδιασμού Συστημάτων Ειδικού Σκοπού.[2]

Αξιόλογη ήταν η επίδραση της θεωρίας του C. Shannon, ο οποίος έθεσε τις βάσεις στη θεωρία της Πληροφορίας, στην εξέλιξη των επικοινωνιακών συστημάτων. Το θεώρημα του Shannon[3] ασχολείται με την εύρεση του κατάλληλου κώδικα λαθών με στόχο την αξιόπιστη μετάδοση σήματος μέσω ενός καναλιού με θόρυβο υποβάθρου.[4]

Στην συνέχεια θα αναφερθούμε στους κώδικες ανίχνευσης και διόρθωσης σφαλμάτων, στις κατηγορίες αυτών και στους τομείς που βρίσκουν εφαρμογή.

[2] Lin Shu, Costello D.J.(1983) Error Control Coding Fundamentals and Applications

[3] Το 1948 ο Shannon απέδειξε ότι για κάθε κανάλι με θόρυβο υπάρχει ένας οριακός ρυθμός εκπομπής (Shannon limit), κάτω από τον οποίο η αξιοπιστία της λήψης γίνεται αυθαίρετα υψηλή, αν τα μηνύματα κωδικοποιηθούν κατάλληλα. Ο οριακός αυτός ρυθμός ονομάζεται «χωρητικότητα πληροφορίας του καναλιού» (channel capacity) και έχει μονάδες bits/second.

[4] C. E. Shannon, "A Mathematical Theory of Communication", Bell System

ΚΕΦΑΛΑΙΟ 1^{Ο}

ΜΙΑ ΓΕΝΙΚΗ ΘΕΩΡΗΣΗ ΤΩΝ «ΚΩΔΙΚΩΝ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΔΙΟΡΘΩΣΗΣ ΤΩΝ ΣΦΑΛΜΑΤΩΝ»

1.1 Η ανάγκη για «κωδικοποίηση ελέγχου σφάλματος»

Από την εποχή της αναλογικής μετάδοσης της πληροφορίας, εχθρός των αξιόπιστων τηλεπικοινωνιών υπήρξε ο θόρυβος. Ένα συχνό φαινόμενο είναι ο «θερμικός θόρυβος». Τα ηλεκτρόνια στα χάλκινα σύρματα περιστρέφονται με μεγάλη ταχύτητα προς όλες τις κατευθύνσεις, παράγοντας ένα θόρυβο υποβάθρου, που χαρακτηρίζεται από ένα ευρύ φάσμα συχνοτήτων, «λευκός θόρυβος».[5]

Υπάρχουν και άλλες πηγές θορύβου, ένα παράδειγμα είναι ο κρουστικός θόρυβος. Προκαλείται από διακόπτες ισχυρών ρευμάτων (π.χ. ηλεκτρονόμους της ΔΕΗ, κεραυνούς, διακόπτες, αναφλέξεις, ηλεκτρικά τόξα κτλ.). Στις τηλεπικοινωνίες, αυτός ο θόρυβος γίνεται αντιληπτός ως μικρά κλικ[6]. Κατά τη μετάδοση δεδομένων, όμως, καταστρέφεται μια σειρά από διαδοχικά bits. [7]

[5] Γεώργιος Κων. Κοκκινάκης, (2004), "Εισαγωγή στις Επικοινωνίες"
[6] Γεώργιος Κων. Κοκκινάκης, (2004), "Εισαγωγή στις Επικοινωνίες"
[7] Ζορκάδης Β., (2002), "Θεωρία Πληροφορίας και Κωδικοπίησης", Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο

Μια άλλη πηγή σφαλμάτων είναι η διαφορετική «συμπεριφορά» των καναλιών στις διάφορες συχνότητες, δηλαδή η εξασθένιση του πλάτους, η ταχύτητα διάδοσης και η στροφή της φάσης των σημάτων έχουν διαφορετικές τιμές στην κάθε συχνότητα στην οποία αναλύεται ένα σήμα.[8]

Το ψηφιακό σήμα καταπολέμησε σε ένα βαθμό το πρόβλημα του θορύβου. Αυτό επιτυγχάνεται με την αναπαράσταση του αναλογικού σήματος με το δυαδικό σύστημα, δηλαδή με 0 ή 1, τα οποία εκπέμπονται με χαρακτηριστικά που διαφέρουν σημαντικά (υψηλή/χαμηλή τάση, συχνότητα εκπομπής), ώστε να γίνονται ευδιάκριτα ακόμα και με την επίδραση του θορύβου. [9]

Επειδή, όμως, ο θόρυβος δεν είναι δυνατόν να εξουδετερωθεί πλήρως, και σε περίπτωση που είναι αρκετά ισχυρός στη ψηφιακή μετάδοση μπορεί να προκαλέσει καταστροφή των δυαδικών ψηφίων και αλλαγή της τιμής του ενός ψηφίου από 0 σε 1 και αντίστροφα, τη λύση δίνει η «κωδικοποίηση ελέγχου σφάλματος», μειώνοντας τον κίνδυνο σφάλματος ακόμη και σε σοβαρές περιπτώσεις όπως, ο συγχρονισμός των τηλεπικοινωνιακών συστημάτων. [10]

[8] Γεώργιος Κων. Κοκκινάκης, (2004), "Εισαγωγή στις Επικοινωνίες"
[9] John G. Proakis, "Digital Communications", Fourth Edition
[10] John G. Proakis, "Digital Communications", Fourth Edition

1.2 Μηχανισμοί αντιμετώπισης σφαλμάτων

Η αντιμετώπιση των σφαλμάτων γίνεται στην πράξη με τους παρακάτω τρεις μηχανισμούς:

i. ***Αγνόηση των σφαλμάτων:*** η λύση αυτή γίνεται αποδεκτή όταν τα σφάλματα δε δημιουργούν στην πράξη σοβαρά προβλήματα. Ένα παράδειγμα είναι η μετάδοση τηλεγραφικού κειμένου. Με ένα λάθος, όπως είναι η παράλειψη ενός άρθρου δε δυσκολεύεται η ανάγνωση του κειμένου.

ii. ***Ανίχνευση των σφαλμάτων:*** η λύση αυτή είναι δυνατόν να εφαρμοσθεί μόνο όταν τα σφάλματα εντοπίζονται μέσα στο σταθμό προορισμού. Τότε, γίνεται αναφορά στο σταθμό αποστολής ότι η πληροφορία που έφτασε είναι λαθεμένη, με σκοπό να αναμεταδοθεί. [11]

iii. ***Ανίχνευση και διόρθωση των σφαλμάτων:*** όπως και παραπάνω, σε αυτή την περίπτωση η λύση μπορεί να εφαρμοσθεί μόνο εάν το σφάλμα εντοπισθεί στο σταθμό προορισμού, και επιχειρείται διόρθωσή του, χωρίς να απαιτείται αναμετάδοση. [12]

[11] Ζορκάδης Β., (2002), "Θεωρία Πληροφορίας και Κωδικοποίησης", Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο
[12] R.W. Hamming, (1950), "Error detection and error correcting codes", Bell Syst. Technology Journal

1.3 Ορισμός των «κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων»

Η μεταβίβαση μια πληροφορίας σε ένα σύστημα επικοινωνίας επιβάλλει, σχεδόν πάντα, τον έλεγχο της μεταδιδόμενης πληροφορίας, δηλαδή εάν ο αποδέκτης έλαβε πραγματικά αυτό που έστειλε ο αποστολέας. Από την πληθώρα των κωδίκων ελέγχου σφάλματος, οι περισσότεροι απαιτούν αυξημένη εμπειρία στις τεχνικές εφαρμογής και ειδικές γνώσεις που στηρίζονται σε προηγμένες μαθηματικές τεχνικές. [13]

Η λύση της «ανίχνευσης και διόρθωσης σφαλμάτων», όπως προαναφέρθηκε, προτείνεται όταν τα σφάλματα εντοπίζονται στο σταθμό προορισμού. Σε αυτή την περίπτωση γίνεται ανίχνευση των σφαλμάτων και προσπάθεια διόρθωσή τους, χωρίς να απαιτείται αναμετάδοση. Έπειτα, μεταβιβάζονται τόσο οι απαιτούμενοι κώδικες της πληροφορίας, όσο και οι πρόσθετες ή πλεοναστικές πληροφορίες, που χρησιμοποιούνται στην ανίχνευση και διόρθωση σφαλμάτων, και ονομάζονται «δυαδικά ψηφία ελέγχου».[14] Η ακολουθία των n δυαδικών ψηφίων που μεταβιβάζονται αποτελείται από δύο τμήματα.

[13] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

[14] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

Το πρώτο είναι το πληροφοριακό τμήμα, που αποτελείται από m δυαδικά ψηφία, στο οποίο περιέχεται η πληροφορία που μεταβιβάζεται, ενώ το δεύτερο είναι το τμήμα ελέγχου, που αποτελείται από c δυαδικά ψηφία, έτσι ώστε n = m + c. Συνήθως το τμήμα ελέγχου αποτελεί και το τέλος της ακολουθίας των δυαδικών ψηφίων που μεταβιβάζονται. Το τμήμα ελέγχου των διορθωτικών κωδίκων είναι πάντα πολύ μεγαλύτερο από το τμήμα ελέγχου των ανιχνευτικών κωδίκων. Επομένως η διόρθωση σφαλμάτων απαιτεί πολύ περισσότερα δυαδικά ψηφία ελέγχου από ότι η ανίχνευση σφαλμάτων. [15]

[15] R.W. Hamming, (1950), "Error detection and error correcting codes", Bell Syst. Technology Journal

ΚΕΦΑΛΑΙΟ 2°

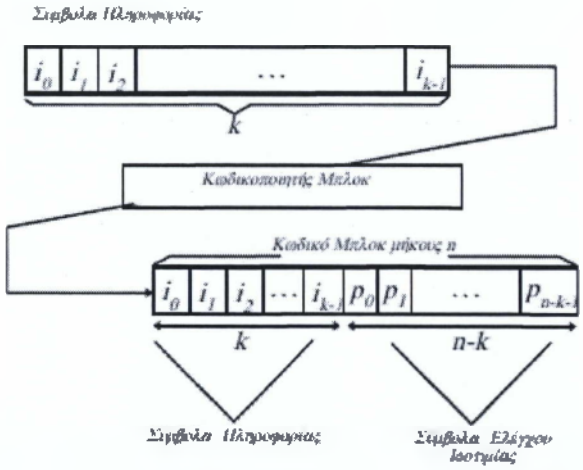
ΚΑΤΗΓΟΡΙΕΣ ΚΩΔΙΚΩΝ ΕΛΕΓΧΟΥ ΣΦΑΛΜΑΤΟΣ

Ο κώδικας που χρησιμοποιείται και οι διαδικασίες που ακολουθούνται κατά την κωδικοποίηση και αποκωδικοποίηση καθορίζουν σε σημαντικό βαθμό την αποδοτικότητα του συστήματος. Υπάρχουν δύο διαφορετικές θεωρήσεις σχετικά με την κωδικοποίηση ελέγχου σφάλματος: η κωδικοποίηση κατά μπλοκ και η συγκεραστική κωδικοποίηση.

2.1 Κωδικοποίηση κατά μπλοκ

Η κεντρική ιδέα της φιλοσοφίας αυτής στηρίζεται στην εξής βάση: μια ομάδα ψηφίων (bits) - ή γενικότερα σύμβολα, δηλαδή bytes- , η οποία ονομάζεται μπλοκ, προστίθενται επιπλέον ψηφία ή σύμβολα που προκύπτουν από κατάλληλη επεξεργασία των ψηφίων / συμβόλων πληροφορίας, και εκπέμπονται. Στο δέκτη ο αποκωδικοποιητής ελέγχει εάν τα ψηφία ή σύμβολα της πληροφορίας που λαμβάνει δίνουν τα προστιθέμενα ψηφία/ σύμβολα σύμφωνα με την ίδια επεξεργασία.

Με τον τρόπο αυτό παρέχεται η δυνατότητα εντοπισμού του σφάλματος και διόρθωσής του με τον κατάλληλο αλγόριθμο.[16]



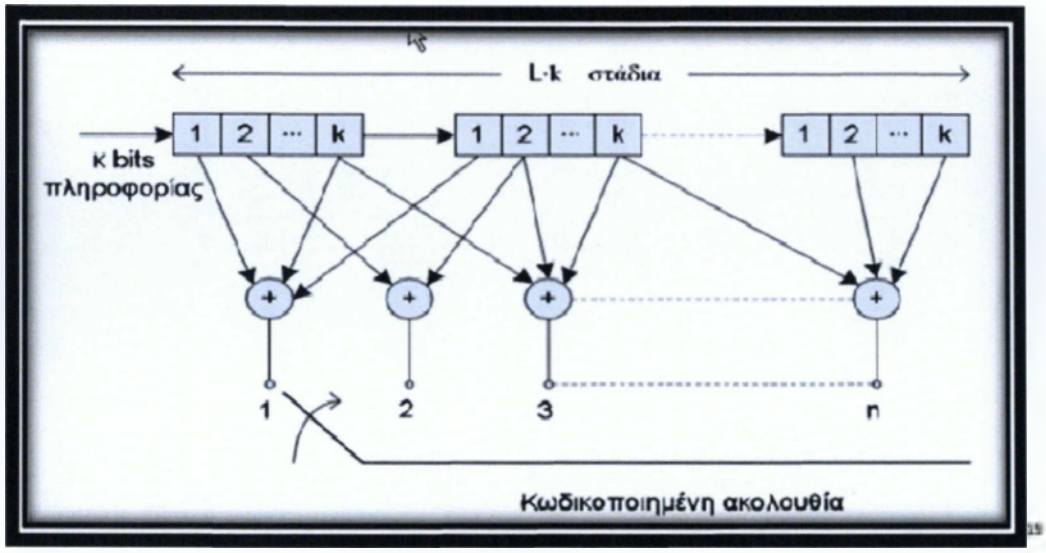
παράδειγμα κωδικοποίησης κατά μπλοκ[17] *Σχήμα 1*

[16] Lin Shu, Daniel J. Costello Jr, "Error Control Coding, Fundamentals and Applications", Prentice Hall 1983

[17] Διπλωματική Εργασία του Φοιτητή Γεώργιου Αγγελόπουλου του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών με Θέμα "Ανάλυση, σχεδιασμός και υλοποίηση κωδίκων διόρθωσης λαθών για τηλεπικοινωνιακές εφαρμογές υψηλών ταχυτήτων", 2009

2.2 Συγκεραστική (Convolutional) κωδικοποίηση

Εδώ η ροή του Κωδικοποιητή προκύπτει μέσω ενός μηχανισμού μνήμης στον οποίο εμπλέκονται όλα τα ψηφία πληροφορίας εκπομπής. Ο αποκωδικοποιητής ανιχνεύει κάθε παραβίαση του μηχανισμού αυτού στο δέκτη (ανίχνευση σφάλματος) και αποκαθιστά τη λειτουργία του μηχανισμού (διόρθωση σφάλματος).[18]



Παράδειγμα συγκεραστικής κωδικοποίησης, σχήμα 2

[18] Lin Shu, Daniel J. Costello Jr, "Error Control Coding, Fundamentals and Applications", Prentice Hall 1983

[19] Διπλωματική Εργασία του Φοιτητή Γεώργιου Αγγελόπουλου του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών με Θέμα "Ανάλυση, σχεδιασμός και υλοποίηση κωδίκων διόρθωσης λαθών για τηλεπικοινωνιακές εφαρμογές υψηλών ταχυτήτων", 2009

Κωδικοποιημένη Διαμόρφωση TCM

Ο πρώτος διαμορφωτής/αποδιαμορφωτής MODEM για τηλεφωνικά κανάλια έγινε εμπορικά διαθέσιμος το έτος 1962 και επιτύγχανε ρυθμό μετάδοσης ίσο με 2400 bits/s. Στο διάστημα των επομένων 10 με 15 ετών, οι ρυθμοί μετάδοσης βελτιώθηκαν, φθάνοντας έως και τα 9600 bits/s, ρυθμός που μάλιστα θεωρήθηκε ως ο μέγιστος δυνατός. Ο δρόμος για τους υψηλότερους ρυθμούς άνοιξε αναπάντεχα στα τέλη της δεκαετίας του 1970, όταν εφευρέθηκε η κωδικοποιημένη κατά «trellis» διαμόρφωση (trellis-coded modulation – TCM) από τον Gottfried Ungerboeck. Χρησιμοποιώντας την κωδικοποιημένη διαμόρφωση TCM, οι ρυθμοί των MODEM αυξήθηκαν άμεσα στα 14400 bits/s και με τη σύνθετη κωδικοποιημένη διαμόρφωση, σύντομα έφθασαν στα 19200 bits/s. Εντούτοις, στους υψηλούς αυτούς ρυθμούς, τα MODEM λειτουργούν με επιτυχία σε ένα μικρό μόνο ποσοστό των τηλεφωνικών συνδέσεων, επειδή η χωρητικότητα των καναλιών φωνής κυμαίνεται κοντά στα 30000 bits/s. Η εφαρμογή της TCM είναι μνημείο ταχύτατης μεταφοράς από το πρωτότυπο εργαστηριακό σύστημα σε μία διεθνή σύσταση : αυτό που αρχικά θεωρείτο αδύνατο, δηλαδή η προσέγγιση της χωρητικότητας σε

κανάλια φωνής, έγινε γεγονός εντός μίας δεκαετίας και μισής από την αρχική εφεύρεση της TCM.[20]

Τα τηλεφωνικά κανάλια απετέλεσαν από νωρίς το ιδεώδες πεδίο πειραματισμού για μεθόδους ελέγχου σφαλμάτων υψηλής πολυπλοκότητας. Δεν πρέπει επομένως να μας εκπλήσσει ότι η κωδικοποίηση τηλεφωνικών καναλιών ήταν η ιστορικά πρώτη επιτυχημένη εφαρμογή ελέγχου σφαλμάτων με κίνητρο την απόδοση φάσματος. Σήμερα, τόσο η κωδικοποιημένη διαμόρφωση κατά «trellis» (TCM) όσο και οι πιο συμβατικοί συνελικτικοί κώδικες, έχουν πληθώρα εφαρμογών. Μεταξύ άλλων, εφαρμόζονται στις δορυφορικές επικοινωνίες (GEO/LEO SATCOM), τις επίγειες και δορυφορικές κινητές επικοινωνίες, τις προσωπικές υπηρεσίες επικοινωνίας (PCS) και τις υψίσυχνες (HF) τροποσφαιρικές επικοινωνίες μεγάλων αποστάσεων.

[20] Ζορκάδης Β., "Θεωρία Πληροφορίας και Κωδικοποίησης", Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο, 2002

Κώδικες Turbo

Εφαρμόζοντας την επαναληπτική αποκωδικοποίηση, οι κώδικες «turbo» κατόρθωσαν πρόσφατα να καλύψουν σχεδόν πλήρως το κενό, που χωρίζει την αιχμή της τεχνολογίας από τη χωρητικότητα του καναλιού, επιτυγχάνοντας ρυθμό σφαλμάτων $P_b = 10^{-5}$ για τη θεαματικά χαμηλή τιμή $E_b/N_o = 0.70$ dB με $R_d = 0.5$ bits/σύμβολο. Μάλιστα, οι παραπάνω κώδικες προσεγγίζουν ακόμα περισσότερο τη χωρητικότητα του καναλιού, όταν το μήκος τους αυξάνεται. Οι κώδικες «turbo» εφευρέθηκαν το έτος 1993 από τους Γάλλους ερευνητές Claude Berrou και Alain Glavieux. Οι κώδικες αυτοί εμπεριέχουν εύκολη άλγεβρα, χρησιμοποιούν επαναληπτικούς και κατανεμημένους αλγόριθμους, εισάγουν την έννοια της τυχαιότητας στη διαδικασία της αποκωδικοποίησης και παρουσιάζουν εξαίρετες αποδόσεις που φτάνουν πολύ κοντά στο όριο του Shannon. Προσπαθώντας να εξηγήσουν την υπερβολικά καλή απόδοση των Turbo Codes, οι ερευνητές παρατήρησαν ότι υπήρχαν κοινά χαρακτηριστικά με τους LDPC κώδικες, και η ομοιότητα αυτή επανέφερε το ενδιαφέρον των ερευνητών για τους LDPC κώδικες. Πριν από την εφεύρεση των Turbo Codes, ουδείς γνώριζε πρακτικό τρόπο για την προσέγγιση της θεωρητικής επίδοσης, που προδιέγραψε ο Shannon.

Χωρίς υπερβολή, η ιστορία της κωδικοποίησης ελέγχου σφαλμάτων μπορεί να χωριστεί στην εποχή πριν από τους κώδικες «turbo» και μετά από αυτούς.[21]

2.3 Σύγκριση των μεθόδων ECC

Η κύρια διαφορά μεταξύ των δύο κατηγοριών κωδικών είναι η ύπαρξη μνήμης στους συγκεραστικούς κώδικες. Λόγω της πολυπλοκότητας του μηχανισμού μνήμης της συγκεραστικής κωδικοποίησης, οι αντίστοιχοι Κωδικοποιητές – Αποκωδικοποιητές επιβαρύνονται ως προς την υλοποίηση και την ταχύτητα της επεξεργασίας. Για το λόγο αυτό οι Κωδικοποιητές – Αποκωδικοποιητές Μπλοκ βρίσκουν ευρύτερη εφαρμογή.

[21]http://de.wikipedia.org/wiki/Turbo-Code

ΚΕΦΑΛΑΙΟ 3^{Ο}

ΚΩΔΙΚΕΣ ΜΠΛΟΚ

3.1 Κώδικες μπλοκ

Ένας κώδικας μπλοκ παίρνει μια ομάδα k συμβόλων πληροφορίας και την επεκτείνει με την προσθήκη n-k πρόσθετων συμβόλων, τα οποία προκύπτουν από την επεξεργασία, βάσει κατάλληλου αλγορίθμου των συμβόλων πληροφορίας. Τα πρόσθετα αυτά σύμβολα ονομάζονται σύμβολα ελέγχου ισοτιμίας (parity check symbols). Ακολουθείται, δηλαδή, η διαδικασία του παρακάτω σχήματος, και συμβολίζουμε έναν τέτοιο κώδικα με (n,k) : βλέπε εικ. Ενότητας 2.1

3.1.1 Γραμμικοί μπλοκ κώδικες

Ένας κώδικας είναι μία διαδικασία μονοσήμαντης απεικόνισης στοιχείων από ένα σύνολο Α σε ένα σύνολο Β. Στην περίπτωση της κωδικοποίησης καναλιού και των κωδικών που χρησιμοποιούνται για αυτήν, τα στοιχεία του συνόλου Α ονομάζονται λέξεις πληροφορίας u_i (i= 1,2,…,M), ενώ εκείνα του συνόλου Β, στα οποία και αντιστοιχίζονται, ονομάζονται κωδικές λέξεις, ή codewords, c_i .

Το M ισούται με τους δυνατούς συνδυασμούς των ακολουθιών k δυαδικών ψηφίων, δηλαδή $M=2^k$. Δυαδικός ονομάζεται ένας κώδικας όταν τα στοιχεία και των δύο συνόλων είναι ακολουθίες δυαδικών ψηφίων (0 ή 1). Εφόσον μιλάμε για μονοσήμαντη απεικόνιση δεν μπορεί το πλήθος των στοιχείων των δύο συνόλων να διαφέρει.

Μια από τις κατηγορίες κωδικών καναλιού είναι οι γραμμικοί κώδικες μπλοκ. Ένας κώδικας μπλοκ είναι γραμμικός αν κάθε γραμμικός συνδυασμός δύο κωδικών του λέξεων είναι επίσης κωδική του λέξη. Στην περίπτωση δυαδικού κώδικα αυτό σημαίνει πως το αποτέλεσμα της συνιστώσας-προς-συνιστώσα XOR λογικής πράξης μεταξύ δύο κωδικών του λέξεων, είναι επίσης κωδική λέξη.

Η μετατροπή της ακολουθίας των k bits (λέξη πληροφορίας) σε ακολουθία των n bits (codeword) πραγματοποιείται με την βοήθεια ενός $k \times n$ δυαδικού πίνακα G, ο οποίος ονομάζεται γεννήτορας πίνακας του κώδικα. Η κωδική λέξη παράγεται με τον πολλαπλασιασμό της λέξης πληροφορίας με τον γεννήτορα πίνακα :

$$c_I = u_I \otimes G$$

Προκύπτει έτσι η κωδική λέξη c_i . Τα n δυαδικά ψηφία που συνιστούν την κωδική λέξη ορίζουν έναν χώρο n διαστάσεων. Κάθε δυαδικό σύμβολο της κωδικής λέξης είναι και μία συνιστώσα του χώρου αυτού.

Ο n-διάστατος χώρος περιλαμβάνει 2^n στοιχεία, μόνο τα 2^k εκ των οποίων αποτελούν έγκυρες κωδικές λέξεις. Οι 2^k έγκυρες κωδικές λέξεις συνιστούν έναν k-διαστατό υποχώρο του n-διαστατού χώρου. Ονομάζουμε C αυτόν τον υποχώρο. Οι γραμμές του γεννήτορα πίνακα G δεν είναι τίποτα περισσότερο από τα k διανύσματα που αποτελούν τη βάση του υποχώρου C.

Έστω όλες οι δυαδικές ακολουθίες μήκους n οι οποίες είναι ορθογώνιες προς όλα τα διανύσματα του k-διάστατου υποχώρου C. Κάθε μία από αυτές τις ακολουθίες έχει την εξής ιδιότητα :

$$h \otimes c_I^T = 0 ,$$

{όπου i= 1,2,…, 2^k , *h* είναι μία από τις ορθογώνιες ακολουθίες μήκους n, c_I^T είναι η ανάστροφη εκδοχή της έγκυρης κωδικής λέξης c_I , ενώ ο τελεστής ⊗ δηλώνει την συνιστώσα-προς-συνιστώσα XOR λογική πράξη ή, ισοδύναμα, την modulo-2 άθροιση.}

Αποδεικνύεται ότι το πλήθος των μήκους n ακολουθιών που έχουν την παραπάνω ιδιότητα είναι 2^{n-k}. Οι 2^{n-k} ορθογώνιες ακολουθίες h_i μπορεί να θεωρηθεί ότι είναι οι έγκυρες κωδικές λέξεις ενός (n,n-k) γραμμικού κώδικα μπλοκ, ο οποίος συμβολίζεται με C^T και καλείται δυϊκός του αρχικού (n,k)

κώδικα C. Οι κωδικές λέξεις του κώδικα C^T είναι σύμφωνα με τη σχέση (4.1) ορθογώνιες ως προς τις κωδικές λέξεις c_i του κώδικα C. Έστω H ο γεννήτορας πίνακας του κώδικα C^T . Ο πίνακας H αποτελείται από (n-k) γραμμές n στοιχείων οι οποίες είναι τα διανύσματα βάσης του (n-k)-διάστατου χώρου. Κάθε μία εξ' αυτών είναι μία έγκυρη κωδική λέξη του κώδικα C^T . Επομένως, κάθε γραμμή του πίνακα H είναι ορθογώνια ως προς κάθε έγκυρη κωδική λέξη του κώδικα C. Κατά συνέπεια, ο πίνακας H μας παρέχει n-k σχέσεις, τις οποίες θα πρέπει να επαληθεύει μία κωδική λέξη για να είναι έγκυρη, και οι οποίες συνοψίζονται στην ακόλουθη σχέση:

$$c_i \otimes H^T = 0$$

Πρακτικά, στην περίπτωση του δυαδικού κώδικα, λόγω της modulo-2 άθροισης, κάθε μία γραμμή ελέγχει αν μεταξύ συγκεκριμένων ψηφίων της κωδικής λέξης υπάρχει άρτιο πλήθος άσων. Επομένως, ο πίνακας H ελέγχει την ισοτιμία των άσων της κωδικής λέξης. Για τον λόγο αυτό, ονομάζεται Πίνακας Ελέγχου Ισοτιμίας του αρχικού κώδικα C και είναι, όπως και ο γεννήτορας πίνακας G, χαρακτηριστικός του κώδικα. [22]

[22] http://www.e-yliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf

3.1.2 Κώδικας ανίχνευσης απλού σφάλματος

Έστω κώδικας (9,8) με το σύμβολο ελέγχου ισοτιμίας να ορίζεται ως το modulo-2 άθροισμα των συμβόλων πληροφορίας, να είναι δηλαδή 1 αν το πλήθος των μη μηδενικών συμβόλων πληροφορίας είναι περιττός αριθμός, και 0 αν είναι άρτιος.

Έτσι το μπλοκ πληροφορίας (0, 1, 1, 0, 1, 0, 1, 0) κωδικοποιείται στο (0, 1, 1, 0, 1, 0, 1, 0 / 0).

Έστω ότι στη λήψη παίρνουμε (¨1¨, 1, 1, 0, 1, 0, 1, 0 / 0). Εφαρμογή του αλγορίθμου εξαγωγής του συμβόλου ισοτιμίας δίνει γι αυτό τιμή **1**, που διαφέρει από την τιμή 0 στη λήψη. Άρα έχει συμβεί σφάλμα, που ανιχνεύεται από τον αποκωδικοποιητή.

Διόρθωση του σφάλματος αυτού δεν είναι δυνατή αφού στο ίδιο αποτέλεσμα (ανίχνευση λάθους) θα οδηγούσε, για παράδειγμα, και το μπλοκ (0, ¨0¨, 1, 0, 1, 0, 1, 0 / 0). Θα πρέπει να σημειωθεί, επίσης, η αδυναμία του κώδικα να ανιχνεύσει δύο ή περισσότερα λάθη. Μια τέτοια περίπτωση θα είχαμε αν στη λήψη έφτανε το μπλοκ (¨1¨, 1, 1, 0, 1, 0, 1, ¨1¨ / 0), το οποίο

δεν παραβιάζει τον κανόνα ισοτιμίας οπότε εκλαμβάνεται από τον αποκωδικοποιητή ως λέξη χωρίς λάθος.[23]

3.1.3 Κώδικας διόρθωσης απλού σφάλματος

Έστω κώδικας Hamming(8,4) με τα σύμβολα ελέγχου ισοτιμίας να προκύπτουν από την ακόλουθη διαδικασία: [24]

Έστω το μπλοκ πληροφορίας (i_0, i_1, i_2, i_3).

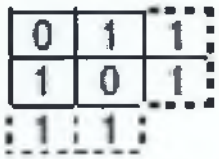
i_0	i_1	I_2
i_2	i_3	I_2
r_1	r_2	

Όπου I_1 σύμβολο ισοτιμίας των στοιχείων της 1ης γραμμής, I_2 το σύμβολο ισοτιμίας των στοιχείων της 2ης γραμμής και όμοια r_1 και r_2 για την πρώτη και δεύτερη στήλη του πίνακα, αντίστοιχα.

Το κωδικοποιημένο μπλοκ είναι (i_0, i_1, i_2, i_3 / I_1, I_2, r_1, r_2).

[23] http://www.e-yliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf
[24] http://www.e-yliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf

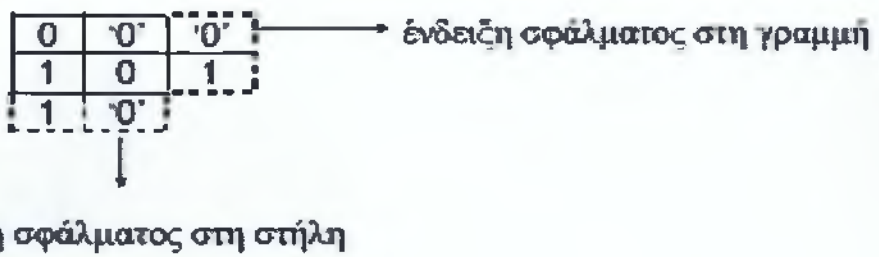
Σύμφωνα με τον πιο πάνω ορισμό το μπλοκ πληροφορίας (0, 1, 1, 0)



κωδικοποιείται ως εξής :

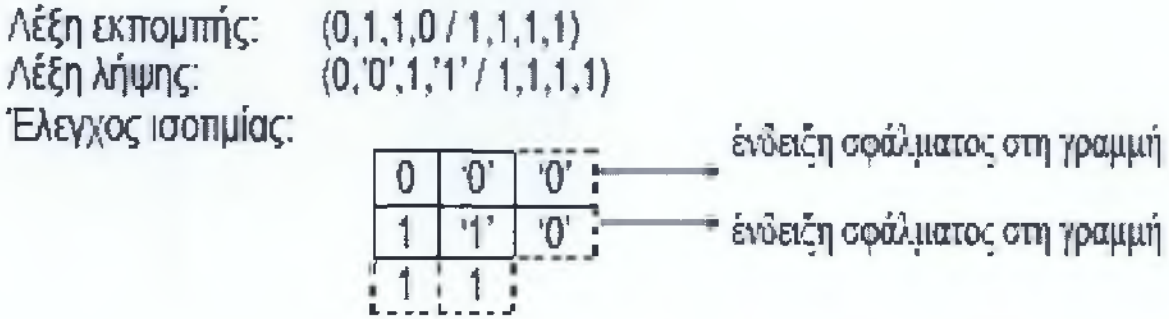
δηλαδή (0, 1, 1, 0 / 1, 1, 1, 1).

Αν στη λήψη πάρουμε (0, ¨0¨, 1, 0 / 1, 1, 1, 1) τότε έλεγχος ισοτιμίας θα δώσει:



Το εσφαλμένο σύμβολο εντοπίζεται ως η τομή της γραμμής και της στήλης για τα οποία προέκυψε παραβίαση ισοτιμίας, και επομένως η διόρθωση είναι δυνατή.

Στις δυνατότητες του κώδικα συγκαταλέγεται η ικανότητα εντοπισμού δύο σφαλμάτων, τα οποία αδυνατεί να διορθώσει, όπως φαίνεται στο παράδειγμα:



3.1.4 Κώδικας Hamming

Το ενδιαφέρον του Richard Hamming στην κωδικοποίηση ελέγχου σφαλμάτων γεννήθηκε κατά την ανάπτυξη ενός πρωτόγονου υπολογιστή. Ο υπολογιστής παρουσίαζε κάθε τόσο πρόβλημα στη λειτουργία του, με συνέπεια να απαιτείται η παρέμβαση ενός ειδικού. Στην πράξη, η παρουσία του ειδικού θα έπρεπε να είναι συνεχής, χωρίς να εξαιρούνται οι αργίες (π.χ. τα Σαββατοκύριακα), γεγονός που περιόριζε την πρακτική του αξία. Ο Hamming αναζήτησε ένα τρόπο, ώστε ο υπολογιστής να διορθώνει τα σφάλματα αυτόματα, δηλαδή χωρίς την ανθρώπινη παρέμβαση. Τελικά εφηύρε έναν κώδικα, ο οποίος προσθέτει 3 bits «ελέγχου» σε 4 bits «πληροφορίας». Τα bits «ελέγχου» επιλέγονται με βάση τα bits «πληροφορίας», ώστε η προκύπτουσα κωδική λέξη να υπακούει σε ένα σύνολο από γραμμικές δυαδικές εξισώσεις.

Αν ένα και μοναδικό bit ληφθεί εσφαλμένα (δηλαδή έχει αντίθετη τιμή), η κωδική λέξη παύει να ικανοποιεί τις εξισώσεις και επιπλέον, είναι δυνατό να υπολογιστεί η θέση του σφάλματος. Οι κώδικες Hamming και οι μειωμένου μήκους εκδοχές τους, χρησιμοποιήθηκαν ευρέως για έλεγχο λαθών στις ψηφιακές επικοινωνίες και στα συστήματα αποθήκευσης δεδομένων, μιας και διαθέτουν υψηλό ρυθμό μετάδοσης και απλή διαδικασία αποκωδικοποίησής τους.

Οι κώδικες Hamming ορίζονται ως εξής:

Μήκος κώδικα: $n = 2m-1$,

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

Πλήθος συμβόλων ελέγχου ισοτιμίας: n - k = m

Ικανότητα διόρθωσης σφαλμάτων: t = 1 (dmin = 3) .

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

$H = [I_m \; Q]$, όπου I_m είναι η m x m μοναδιαία μήτρα και η υπό-μήτρα Q αποτελείται από 2m - m – 1 στήλες, οι οποίες είναι m-διαστατά διανύσματα με βάρος μεγαλύτερο ή ίσο από 2.

Για παράδειγμα, για m = 3, η μήτρα ισοτιμίας του κώδικα Hamming με μήκος 7 μπορεί να αναπαρασταθεί με τη μορφή

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

Οι στήλες της μήτρας Q μπορούν να διαταχθούν με οποιαδήποτε σειρά, χωρίς αυτό να επηρεάζει την ιδιότητα της απόστασης και την κατανομή του βάρους του κώδικα. Η μήτρα γεννήτορας G μπορεί να εκφραστεί σε συστηματική μορφή ως

$$G = [\, Q^T\ I_2{}^m{}_{-m-1} \,],$$

όπου Q^T είναι η αντιμεταθετική μήτρα του Q και $I_2{}^m{}_{-m-1}$ είναι ένας $(2^m - m - 1) \times (2^m - m - 1)$ μοναδιαία μήτρα. Εφόσον οι στήλες της μήτρας H είναι μη-μηδενικές και διακριτές, το άθροισμα δύο στηλών της H δεν μπορεί να είναι μηδενικό. Με βάση τις ιδιότητες της ελάχιστης απόστασης κώδικα μπλοκ προκύπτει ότι η ελάχιστη απόσταση ενός κώδικα Hamming είναι 3.

Επομένως ο κώδικας έχει την ικανότητα να διορθώσει όλα τα πρότυπα λάθους με ένα σφάλμα και να ανιχνεύσει όλα τα πρότυπα λάθους με δύο σφάλματα.[25]

Παρακάτω δίνουμε το παράδειγμα για απλό λάθος το οποίο εύκολα μπορεί να επαυξηθεί για τα περισσότερα λάθη. Η πληροφορία που φτάνει στον αποδέκτη έχει μήκος n+k δυαδικά ψηφία. Κάθε κωδική λέξη παρουσία απλών λαθών μπορεί να μετασχηματιστεί :

α) Στην αρχική κωδική λέξη αν δε συμβεί κανένα λάθος.

β) Σε n διαφορετικές λέξεις αν το λάθος συμβεί σε κάποιο δυαδικό ψηφίο της πληροφορίας

γ) Σε k διαφορετικές λέξεις αν το λάθος συμβεί σε κάποιο δυαδικό ψηφίο των ψηφίων ελέγχου.

Έστω για παράδειγμα ότι η αρχική πληροφορία είναι η b3 b2 b1 b0 και σε αυτήν επισυνάπτονται τα ψηφία ελέγχου ck-1 … c0. Η κωδική λέξη συνεπώς που σχηματίζεται είναι η b3 b2 b1 b0 ck-1 … c0. Παρουσία απλών λαθών η λέξη αυτή μπορεί να αλλοιωθεί ή να μην αλλοιωθεί ως εξής :

[25] http://courses.softlab.ntua.gr/softdev/#lesson2811

b3 b2 b1 b0 ck-1 … c0 Να μην αλλοιωθεί διόλου.

b3 b2 b1 b0 ck-1 … c0

Να αλλοιωθεί κατά 4 τρόπους, όσους δηλαδή και τα ψηφία πληροφορίας.

b3 b2 b1 b0 ck-1 … c0

b3 b2 b1 b0 ck-1 … c0

b3 b2 b1 b0 ck-1 … c0

b3 b2 b1 b0 ck-1 … c0 Να αλλοιωθεί κατά κ τρόπους, όσους

b3 b2 b1 b0 ck-1 … c0 δηλαδή και τα ψηφία ελέγχου.

Σύμφωνα με τα παραπάνω, η αρχική μορφή όσο και οι πιθανές αλλοιώσεις μιας πληροφορίας συνιστούν μια ***ομάδα*** με πληθάριθμο (1+n+k). Ο παραλήπτης της πληροφορίας για να έχει ικανότητα διόρθωσης του απλού λάθους θα πρέπει κάθε στοιχείο μιας τέτοιας ομάδας να μπορεί να το αντιστοιχεί στην αρχική πληροφορία, π.χ. η πληροφορία b3b2b1b0ck-1…c0 θα πρέπει να αντιστοιχεί μοναδικά στην μη αλλοιωμένη πληροφορία b3b2b1b0ck-1…c0. Αυτό σημαίνει ότι κάθε ομάδα θα πρέπει να είναι ένα υποσύνολο ξένο ως προς κάθε άλλη πιθανή ομάδα.

Εφόσον ο αριθμός των ομάδων είναι 2n, τα διαφορετικά στοιχεία που πρέπει να παρασταθούν είναι 2n * (1+n+k). Όμως με n+k δυαδικά ψηφία μπορώ να έχω το πολύ 2n+k διαφορετικές παραστάσεις. Συνεπώς,

$$2n * (1+n+k) \leq 2^{n+k} \Leftrightarrow (1+n+k) \leq 2k.$$

Η παραπάνω σχέση δίνει τον ελάχιστο αριθμό δυαδικών ψηφίων ελέγχου που πρέπει να προστεθούν σε n δυαδικά ψηφία πληροφορίας ώστε να υπάρχει η δυνατότητα διόρθωσης απλού λάθους. Έστω για παράδειγμα ότι n=12. Τότε η παραπάνω ανισότητα ισχύει για $\kappa \geq 5$. Προφανώς επιλέγεται κ=5 ώστε η επιβάρυνση να είναι η μικρότερη δυνατή. Μπορείτε να συγκρίνετε τον ελάχιστο αυτό αριθμό δυαδικών ψηφίων με τα 7 (ή 8) ψηφία ελέγχου που απαιτεί η ισοτιμία στήλης γραμμής και να διαπιστώσετε πόσο αποτελεσματικός είναι ο κώδικας Hamming.

Για να γίνει όμως αποδεκτός ο παραπάνω κώδικας, απαιτείται και η εφαρμογή του να είναι εύκολη. Η εφαρμογή βασίζεται στην ιδέα των επικαλυπτόμενων ομάδων ισοτιμίας. Δηλαδή, τα ψηφία της πληροφορίας χωρίζονται σε ομάδες, που όμως δεν είναι ξένες μεταξύ τους. Κάθε ομάδα έχει ένα ψηφίο ισοτιμίας και προφανώς ένα ψηφίο πληροφορίας που ανήκει σε περισσότερες από μία ομάδες ελέγχεται από περισσότερα του ενός ψηφία ελέγχου. Ο αριθμός και η θέση των ψηφίων ελέγχου που παρουσιάζουν λάθος ισοτιμία μας εντοπίζουν το ψηφίο που είναι λανθασμένο.

Ας δούμε ένα παράδειγμα. Έστω ότι έχω 4 δυαδικά ψηφία πληροφορίας b3b2b1b0 και συνεπώς και 3 ψηφία ελέγχου c3c2c1. Σχηματίζω τις εξής ομάδες : (b3, b1, b0, c1), (b3, b2, b0, c2) και (b3, b2, b1, c3). Κάθε ψηφίο ελέγχου ορίζεται σαν το ψηφίο ισοτιμίας για την ομάδα που ανήκει. Έστω λοιπόν τώρα ότι αλλοιώνεται η τιμή του b0. Ο παραλήπτης θα διαπιστώσει λάθος ισοτιμία τόσο στο ψηφίο ελέγχου c1 όσο και στο c2. Οι δύο ομάδες ισοτιμίας που ελέγχονται από τα ψηφία ελέγχου c1 και c2 έχουν κοινά στοιχεία τα b0 και b3. Το b3 όμως δε μπορεί να είναι λάθος, γιατί τότε θα υπήρχε λάθος ισοτιμίας και στην ομάδα του c3, κάτι που δεν ισχύει. Συνεπώς το λάθος εντοπίζεται στο b0 και μπορεί να διορθωθεί.

3.1.5 Κώδικας BCH

Το έτος 1967 εφευρέθηκε μία γενική μέθοδος αποκωδικοποίησης για τους κώδικες Bose-Chaudhuri-Hocquenghem (BCH). Πρόκειται για κυκλικούς κώδικες και παρέχουν στο σχεδιαστή ευρεία γκάμα επιλογών για το μέγεθος της λέξης κωδικοποίησης, τον ρυθμό του κώδικα και τη διορθωτική ικανότητα. Έχουν την καλύτερη δυνατή επίδοση, από όλες τις υπόλοιπες κλάσεις συμπαγών κωδίκων του ίδιου μεγέθους λέξης και ρυθμού κώδικα, όταν το μήκος λέξης τους είναι της τάξης των 100 ψηφίων. Η μέθοδος είναι αλγεβρική και οριστικής απόφασης. Χρησιμοποιώντας την αλγεβρική μέθοδο αποκωδικοποίησης, ο κώδικας BCH επιτυγχάνει $P_b = 10^{-5}$ για $E_b/N_o = 5.70$ dB με $R_d \approx 0.5$ bits/σύμβολο. Το μέγεθος της επιτυχίας απορρέει αφενός από την ευκολία υλοποίησης του αποκωδικοποιητή και αφετέρου από τη μεγάλη ευρύτητα της τάξης των κωδίκων BCH. Πράγματι, η ίδια μέθοδος αποκωδικοποιεί εξίσου τόσο τους κώδικες Hamming όσο και τους κώδικες Reed-Solomon, οι οποίοι υπάγονται στους BCH.[26]

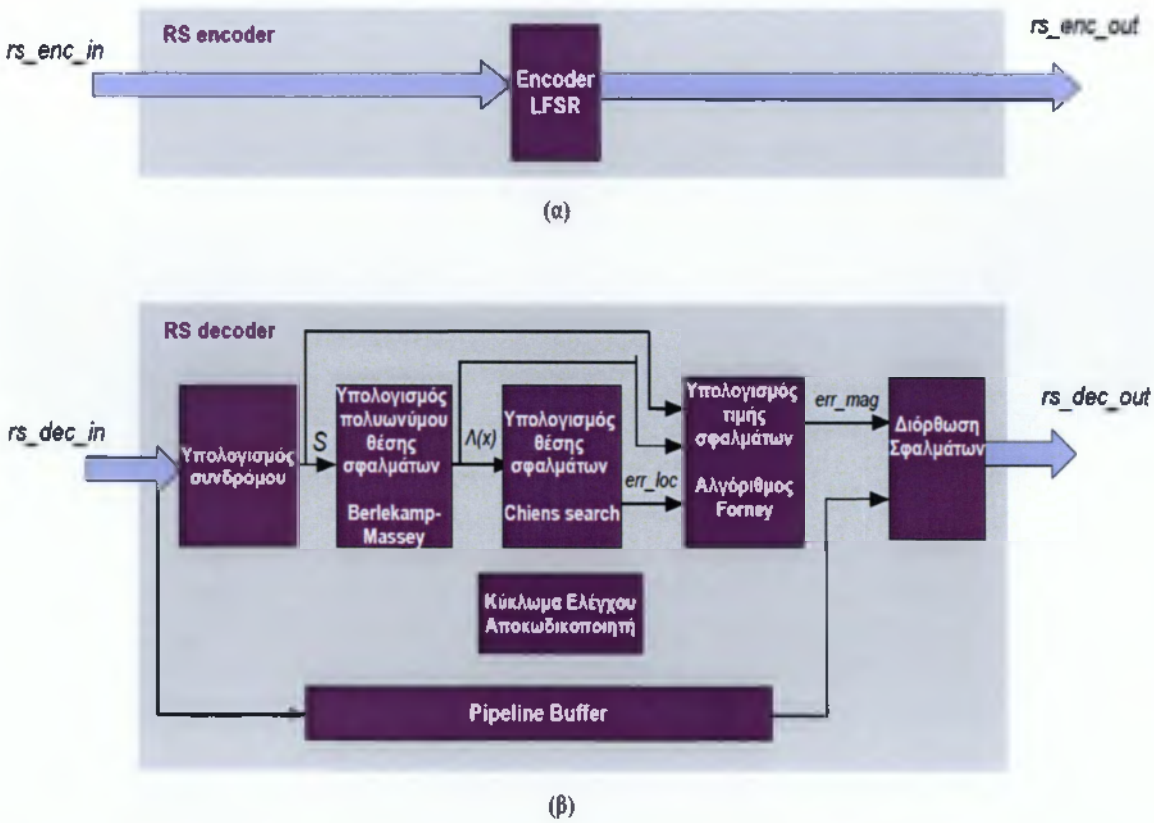
[26] http://courses.softlab.ntua.gr/softdev/#lesson2811

3.1.6 Κώδικας Reed-Solomon

Ο Reed-Solomon, όπως και όλοι οι κώδικες-μπλοκ επεξεργάζονται τα δεδομένα ως μονάδες πεπερασμένου μεγέθους (blocks). Στις τεχνικές των κωδίκων RS συμπεριλαμβάνονται πολλά στοιχεία ψηφιακής επεξεργασίας σήματος (signal processing), όπως ο γρήγορος μετασχηματισμός Fourier (FFT), επαναληπτικοί αλγόριθμοι, ο καταχωρητής ολίσθησης με γραμμική ανάδραση (LFSR) κ.α. Ο γενικός τους συμβολισμός είναι ο RS(n,k,b), όπου n το πλήθος των συμβόλων (μήκος) της κωδικής λέξης που προκύπτει από την προσθήκη πλεονασμού στο αρχικό μήνυμα, k το πλήθος των συμβόλων του μηνύματος (καθαρή πληροφορία φορτίου) και b ο αριθμός των bits που συνθέτουν κάθε σύμβολο του κώδικα. Επιπλέον, με το πηλίκο $r = k / n \leq 1$, ορίζεται ο ρυθμός του κώδικα. Το μέγεθος αυτό αυξάνει το ρυθμό των δεδομένων στο κανάλι κατά 1 / r, οπότε όσο μικρότερη είναι η τιμή του r, τόσο μεγαλύτερη είναι η επιβάρυνση στο εύρος ζώνης του καναλιού μετάδοσης (εισάγονται περισσότερα σύμβολα κωδικοποίησης).[27] Η αρχιτεκτονική του Reed-Solomon κωδικοποιητή / αποκωδικοποιητή RS(n,k) φαίνεται στο δομικό διάγραμμα του σχήματος 3. Ο κωδικοποιητής φαίνεται στο σχήμα 3(α) και αντιστοιχεί σε μία υλοποίηση με LFSR.

[27] http://eclass.teilam.gr/claroline/document/document.php

Ο αποκωδικοποιητής φαίνεται στο σχήμα 3(β) και αποτελείται από δομικά στοιχεία που αντιστοιχούν στα στάδια της αποκωδικοποίησης κωδίκων Reed-Solomon και είναι i) υπολογισμός συνδρόμου, ii) υπολογισμός πολυωνύμου θέσης σφαλμάτων, iii) υπολογισμός θέσης σφαλμάτων, iv) υπολογισμός τιμής σφαλμάτων, v) διόρθωση σφαλμάτων.[28]



Διάγραμμα (α) Κωδικοποιητή και (β) Αποκωδικοποιητή Reed-Solomon, σχήμα 3

[28] http://courses.softlab.ntua.gr/softdev/#lesson2811

Τόσο ο κωδικοποιητής, όσο και ο αποκωδικοποιητής λειτουργούν σειριακά σε επίπεδο συμβόλου. Στον κωδικοποιητή εισάγεται μια ακολουθία k συμβόλων δεδομένων και μεταδίδεται μία ακολουθία n συμβόλων (k σύμβολα δεδομένων + n-k σύμβολα ελέγχου ισοτιμίας). Ο αποκωδικοποιητής δέχεται μπλοκ των n συμβόλων, εντοπίζει και διορθώνει πιθανά σφάλματα και εξάγει τα k σύμβολα δεδομένων του αρχικού μηνύματος.[29]

[29] http://eclass.teilam.gr/claroline/document/document.php

3.1.7 CRC (Κυκλικοί μπλοκ κώδικες)[30]

Ένας από τους πιο κοινούς, και ένας από τους πιο ισχυρούς κώδικες ανίχνευσης σφαλμάτων, είναι ο Κυκλικός Έλεγχος Πλεονασμού (Cyclic Redundancy Check, CRC). Για ένα block ή μήνυμα, που αποτελείται από k bit, ο πομπός δημιουργεί μια ακολουθία bit μήκους (n-k), η οποία λέγεται ακολουθία πλαισίου (Frame check sequence,FCS), έτσι ώστε το πλαίσιο που προκύπτει, το οποίο αποτελείται από n bit, να διαιρείται ακριβώς με κάποιο προκαθορισμένο αριθμό, ο οποίος είναι γνωστός στον αποστολέα καθώς και στο δέκτη. Ο δέκτης διαιρεί το εισερχόμενο πλαίσιο με τον αριθμό αυτό και αν δεν υπάρξει υπόλοιπο, θεωρεί ότι δεν υπάρχει κανένα σφάλμα.

Η τεχνική αυτή είναι πιο αποτελεσματική στην ανίχνευση σφαλμάτων. Βασίζεται στη δυαδική διαίρεση. Ο πομπός προσαρμόζει μια ακολουθία από n-1 '0' στο τέλος των δεδομένων και διαιρεί το σύνολο με ένα διαιρέτη (CRC Generator των n bits). Το υπόλοιπο (δηλαδή, το CRC των n-1 bits) αντικαθιστά την ακολουθία των '0' στο τέλος των δεδομένων, ώστε η διαίρεση να είναι τέλεια. Ο δέκτης επαναλαμβάνει τη δυαδική διαίρεση και αν είναι τέλεια, δέχεται τα δεδομένα, αλλιώς απορρίπτει το frame. Ο γεννήτορας CRC μπορεί να αναπαρασταθεί και με μορφή πολυωνύμων, για συντομία και για τη μαθηματική τεκμηρίωση της τεχνικής.

[30] Lin Shu, Daniel J. Costello Jr, "Error Control Coding, Fundamentals and Applications", Prentice Hall 1983

Με βάση τα πολυώνυμα, ο γεννήτορας CRC επιλέγεται έτσι ώστε να μην διαιρείται από το x και να διαιρείται από το (x + 1). Η μέθοδος αυτή μπορεί να ανιχνεύει σε περιττού αριθμού bits, τα λάθη μήκους μικρότερου ή ίσου του βαθμού του πολυωνύμου, και με μεγάλη πιθανότητα τα λάθη καταιγισμού, μήκους μεγαλύτερου του βαθμού του πολυωνύμου. Τα πιο γνωστά πρωτόκολλα είναι τα: CRC –12, CRC – 16, CRC – 32 και CRC – ITU – T.[31]

Η διαδικασία CRC μπορεί να αναπαρασταθεί και να υλοποιηθεί, ως ένα κύκλωμα διαίρεσης αποτελούμενο μόνο από πύλες XOR και από έναν καταχωρητή ολίσθησης. Ο καταχωρητής ολίσθησης αποτελείται από μια σειρά στοιχείων αποθήκευσης του ενός bit. Κάθε στοιχείο έχει μια γραμμή εξόδου, η οποία δείχνει την τρέχουσα αποθηκευμένη τιμή, και μια γραμμή εισόδου. Σε διακριτές χρονικές στιγμές, που λέγονται χρόνοι ρολογιού, η τιμή στο στοιχείο αποθήκευσης αντικαθιστάται από την τιμή που υποδεικνύεται από την γραμμή εισόδου της. Τα στοιχεία αποθήκευσης του καταχωρητή χρονίζονται ταυτόχρονα, προκαλώντας ολίσθηση ενός bit, κατά μήκος ολόκληρου του καταχωρητή.

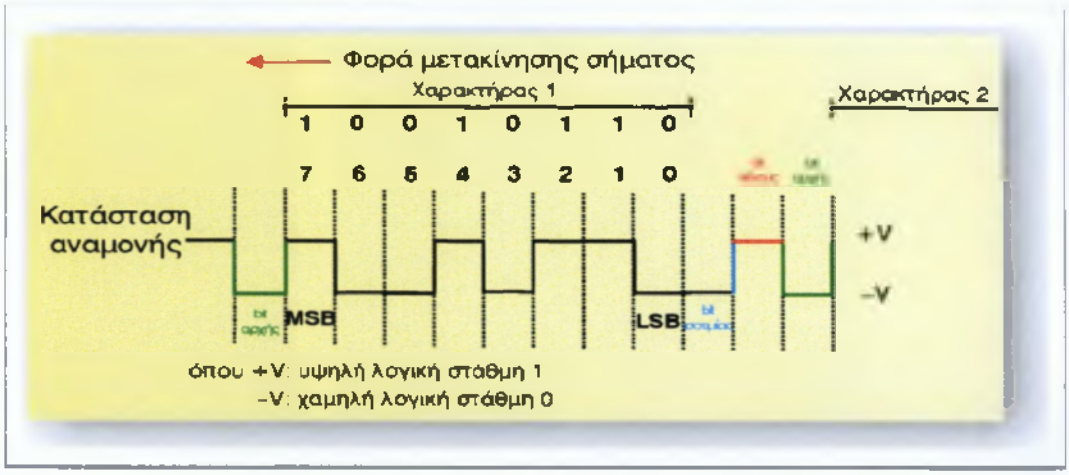
[31] http://www.e-yliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf

Για παράδειγμα το πλαίσιο 1 1 0 0 0 1 των 6 bit παριστάνει ένα πολυώνυμο 5ου βαθμού με 6 όρους, που έχουν συντελεστές τα δυαδικά ψηφία 1, 1, 0, 0, 0 και 1. Επομένως το πολυώνυμο θα είναι το : $x^6 + x^4 x^0$. Οι πράξεις στα πολυώνυμα γίνονται modulo 2, σύμφωνα με τους κανόνες της άλγεβρας, που σημαίνει ότι δεν υπάρχουν κρατούμενα στην πρόσθεση και δανεικά στην αφαίρεση. Αυτό φαίνεται και στις τέσσερις πράξεις που ακολουθούν.

1001101	00110011	11110000	01010101
+11001010	+11001101	-10100110	-10101111
01010001	11111110	01010110	11111010

Όταν χρησιμοποιείται η μέθοδος του πολυωνυμικού κώδικα, ο πομπός και ο δέκτης πρέπει να συμφωνήσουν εκ των προτέρων στη μορφή του πολυωνύμου-γεννήτορα, δηλαδή του G(x). Τόσο το πιο σημαντικό όσο και το λιγότερο σημαντικό δυαδικό ψηφίο του πολυωνύμου-γεννήτορα πρέπει να είναι το δυαδικό ψηφίο 1. Το πιο σημαντικό ψηφίο (MSB, Most Significant Bit) είναι το ψηφίο εκκίνησης της πληροφορίας στην γραμμή μετάδοσης, δηλαδή το 7ο ή το 8ο δυαδικό ψηφίο.

Ακολούθως εμφανίζονται όλα τα άλλα δυαδικά ψηφία και τελευταίο το λιγότερο σημαντικό ψηφίο (LSB, Least Significant Bit), που είναι το 0 ή το 1ο δυαδικό ψηφίο.

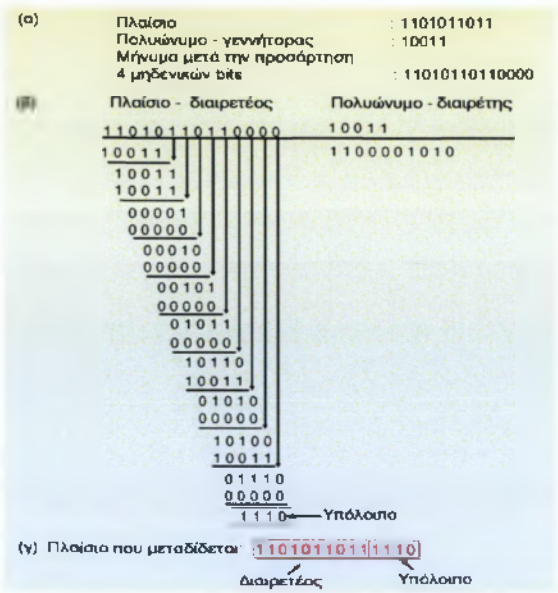


Μετάδοση των δυαδικών ψηφίων στη γραμμή επικοινωνίας, σχήμα 4

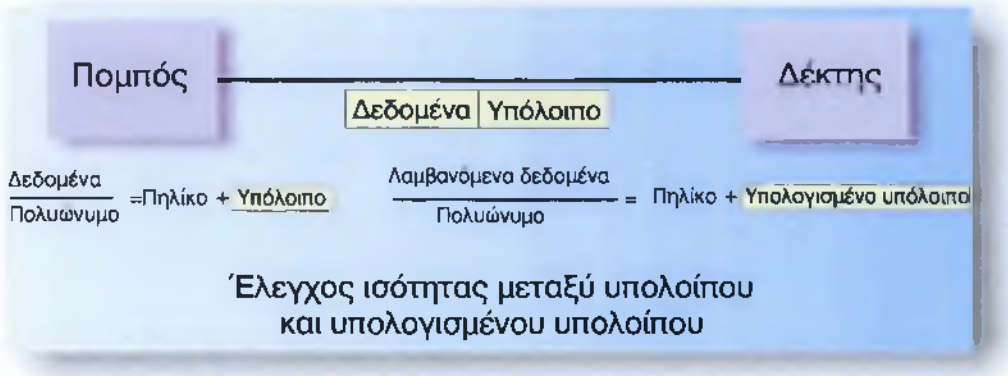
Για να υπολογιστεί το άθροισμα ελέγχου μερικών πλαισίων των m bits, τα οποία αντιστοιχούν στο πολυώνυμο M(x), πρέπει κάθε πλαίσιο να είναι μεγαλύτερο από το πολυώνυμο-γεννήτορα. Η βασική ιδέα είναι να προσαρτηθεί ένα άθροισμα στο τέλος του πλαισίου, έτσι ώστε το πολυώνυμο που παριστάνεται από το πλαίσιο μαζί με το άθροισμα ελέγχου να διαιρείται ακριβώς με το G(x). Όταν ο δέκτης πάρει το πλαίσιο μαζί με το άθροισμα ελέγχου, το διαιρεί με το G(x) και αν υπάρχει υπόλοιπο, σημαίνει ότι υπήρξε σφάλμα μετάδοσης.

Άρα αντί για πράξεις επάνω σε κώδικες-λέξεις είναι δυνατόν να γίνονται πράξεις στα αντίστοιχα πολυώνυμα που αυτές αντιπροσωπεύουν.

Πριν από τη μετάδοση η πληροφορία χωρίζεται σε πλαίσια, κάθε πλαίσιο διαιρείται με ένα προκαθορισμένο πολυώνυμο, τόσο το πλαίσιο της πληροφορίας όσο και το υπόλοιπο της διαίρεσης αποστέλλονται στον αποδέκτη, ο αποδέκτης διαιρεί το πλαίσιο της πληροφορίας με το ίδιο προκαθορισμένο πολυώνυμο και εξετάζει αν το υπόλοιπο της διαίρεσης που υπολόγισε συμπίπτει με το υπόλοιπο που του έστειλε ο πομπός. Η όλη διαδικασία φαίνεται στο σχήμα 5.



Σχήμα 5



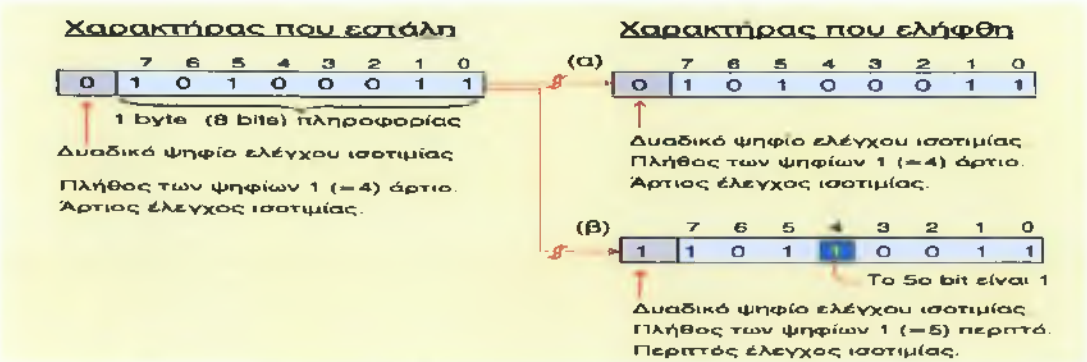
Σχήμα 6

3.1.8 Κώδικας ισοτιμίας

Μερικά συστήματα μετάδοσης δεδομένων χρησιμοποιούν τον κατακόρυφο έλεγχο πλεονασμού (VRC, Vertical Redundancy Checking), μια τεχνική σύμφωνα με την οποία κάθε χαρακτήρας που μεταδίδεται συνοδεύεται από ένα δυαδικό ψηφίο ισοτιμίας (Parity Bit). Ο έλεγχος αυτός λέγεται και έλεγχος ισοτιμίας (Parity Check). Κατά την αποστολή ο πομπός θέτει στο δυαδικό ψηφίο ισοτιμίας την τιμή 0 ή 1. Η θέση του δυαδικού ψηφίου ισοτιμίας καθορίζεται από το εκάστοτε πρωτόκολλο που χρησιμοποιείται για την μετάδοση της πληροφορίας. Υπάρχουν δύο κλασικοί έλεγχοι ισοτιμίας, ο έλεγχος περιττής ισοτιμίας (Odd Parity Check) και ο έλεγχος άρτιας ισοτιμίας (Even Parity Check). Ο έλεγχος είναι απλός.

Στο μεταφερόμενο χαρακτήρα μετράμε τα ψηφία που έχουν τιμή 1 και εάν ο συνολικός αριθμός των δυαδικών ψηφίων που έχουν την τιμή 1 είναι περιττός, λέμε ότι έχουμε περιττό έλεγχο ισοτιμίας. Εάν ο συνολικός αριθμός των δυαδικών ψηφίων που έχουν την τιμή 1 είναι άρτιος, λέμε ότι έχουμε άρτιο έλεγχο ισοτιμίας. Όταν ο δέκτης ανιχνεύσει σφάλμα στο ψηφίο ισοτιμίας, γνωρίζει ότι έχει συμβεί σφάλμα μετάδοσης.

Στο σχήμα περιγράφονται δύο σενάρια μεταφοράς ενός χαρακτήρα πληροφορίας. Στην πρώτη περίπτωση έχουμε μεταφορά χωρίς σφάλμα, επειδή το άρτιο ψηφίο ισοτιμίας της αποστολής είναι σύμφωνο με το άρτιο ψηφίο ισοτιμίας της λήψης. Επομένως στην περίπτωση αυτή υπάρχει άρτιος έλεγχος ισοτιμίας, σχήμα 4.7α. Στη δεύτερη περίπτωση έχουμε εσφαλμένη μεταφορά, επειδή το άρτιο ψηφίο ισοτιμίας της αποστολής δε συμφωνεί με το περιττό ψηφίο ισοτιμίας της λήψης, σχήμα 4.7β. Αυτό συνέβη, γιατί κατά την μεταφορά της πληροφορίας υπήρξε σφάλμα στο 5ο ψηφίο.



Ανίχνευση Σφάλματος με την τεχνική του Δυαδικού Ψηφίου Ισοτιμίας, σχήμα 7

Ο έλεγχος ισοτιμίας είναι η παλαιότερη από τις τεχνικές ανίχνευσης σφαλμάτων. Τα πλεονεκτήματά της είναι η απλότητα του αλγορίθμου και η εύκολη υλοποίησή της. Έτσι, αντίθετα με τις επιδόσεις της, που δεν θεωρούνται υψηλές, ειδικά όταν ο ρυθμός μετάδοσης είναι υψηλός, η μέθοδος, εφαρμόζεται ευρύτατα. Αυτό συμβαίνει επειδή ο ρυθμός αναγνώρισης των σφαλμάτων είναι χαμηλός, με αποτέλεσμα όταν δημιουργηθεί κάποιο σφάλμα, να αλλοιώνονται πολλά γειτονικά ψηφία. Ο έλεγχος ισοτιμίας σε αυτήν την περίπτωση μπορεί να δώσει θετικό αποτέλεσμα, ωστόσο πρέπει να έχουμε υπόψη μας το ενδεχόμενο να υπάρχουν και σφάλματα που δεν ανιχνεύτηκαν. Ένα πρόσθετο μειονέκτημα της τεχνικής αυτής είναι η μη αναγνώριση άρτιου αριθμού σφαλμάτων. Είναι αυτονόητο ότι κάθε περιττός αριθμός σφαλμάτων που θα δημιουργηθεί στη μετάδοση θα προκαλέσει την αύξηση ή τη μείωση των ψηφίων 1 στην ακολουθία των δυαδικών ψηφίων και επομένως θα αλλάξει την τιμή του δυαδικού ψηφίου ισοτιμίας (από άρτια σε περιττή ή αντίστροφα). Αν όμως δημιουργηθεί άρτιος αριθμός σφαλμάτων, τότε δεν θα αλλάξει η τιμή του δυαδικού ψηφίου ισοτιμίας και επομένως δεν θα ανιχνευτούν αυτά τα σφάλματα.

Ακολουθία των 7+1 bits που στάλθηκε								Ακολουθία των 7+1 bits που έφτασε							
1	0	1	1	0	0	1	0	1	0	0	1	0	0	1	1
1	1	1	0	1	0	1	1	1	0	1	1	1	0	1	1 *
1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0	0	1	0	1	0	0	0
1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1 *

Αδυναμία Ανίχνευσης Σφάλματος με την τεχνική του Δυαδικού Ψηφίου Ισοτιμίας, σχήμα 8

Στο παραπάνω σχήμα ο χαρακτήρας αποτελείται από 7 bits πληροφορίας και από 1 bit που παριστάνει το δυαδικό ψηφίο ισοτιμίας. Με τα υπογραμμισμένα δυαδικά ψηφία (_) δηλώνονται οι σειρές στις οποίες ανιχνεύτηκε το σφάλμα. Με τον αστερίσκο (*) σημειώνονται οι εσφαλμένες σειρές που δεν ανιχνεύονται με την μέθοδο της ισοτιμίας. Όπως φαίνεται, η μέθοδος της ισοτιμίας δεν ανιχνεύει όλα τα σφάλματα. Δηλαδή δεν μπορεί να ανιχνεύσει άρτιο αριθμό σφαλμάτων, αφού το δυαδικό ψηφίο ισοτιμίας που στάλθηκε είναι ίδιο με το δυαδικό ψηφίο ισοτιμίας που έφτασε στον παραλήπτη.

Η μέθοδος που περιγράφτηκε εφαρμόζεται ευρύτατα στην πράξη, επειδή χρησιμοποιεί απλούς αλγορίθμους δημιουργίας και ελέγχου ισοτιμίας και επομένως μη δαπανηρά κυκλώματα.

3.1.9 Κώδικας LDPC

Οι LDPC είναι κώδικες διόρθωσης λαθών και ανήκουν στους μπλοκ κώδικες. Δε μπορούν να εξασφαλίσουν την τέλεια μετάδοση, μπορούν όμως, να εξαλείψουν κατά πολύ την πιθανότητα λάθους. Οι LDPC ήταν οι πρώτοι κώδικες διόρθωσης λαθών, οι οποίοι μπορούσαν να προσεγγίσουν ρυθμούς μετάδοσης δεδομένων, πολύ κοντά στο θεωρητικό μέγιστο, το όριο Shannon.

Το Μάρτιο του 2005, οι LDPC κώδικες έγιναν standard για το DVB-S2 (Digital Video Broadcasting). Συγκεκριμένα, το DVB-S2 χρησιμοποιεί σύστημα διόρθωσης λαθών, το οποίο βασίζεται στην αλληλουχία ενός Bose-Chaudhuri-Hochquenghem κώδικα με ένα LDPC κώδικα. Η απόδοση του συστήματος θα πρέπει να απέχει μέχρι 0.7 dB από το όριο Shannon. Επίσης, από το Δεκέμβριο του 2005, το πρότυπο επικοινωνίας WiMAX[32] που ενσαρκώνεται μέσω του "Mobile WiMAX" βασίζεται στα πρότυπο IEEE 802.16e-2005-WirelessMAN που αποτελεί αναβάθμιση του παλαιοτέρου IEEE 802.16-2004. Σύμφωνα με αυτό το Mobile WiMAX χρησιμοποιεί κωδικοποίηση με κώδικες υψηλής απόδοσης όπως οι LDPC και οι turbo, ενισχύοντας έτσι την ασφάλεια και την απόδοση NLOS.

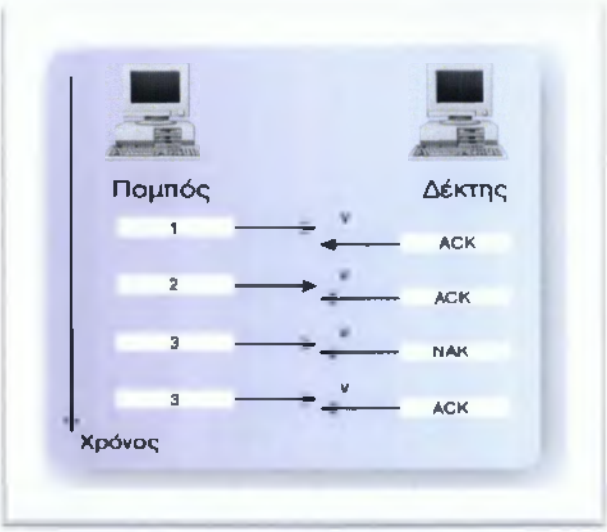
[32] http://el.wikipedia.org/wiki/WiMAX

Το WiMAX-Worldwide Interoperability for Microwave Access είναι μια τεχνολογία τηλεπικοινωνιών, που παρέχει ασύρματα δεδομένα με ποικίλους τρόπους, από συνδέσεις «σημείο-προς-σημείο», μέχρι την πλήρη πρόσβαση για κινητή τηλεφωνία.[33]

[33] Bernard M. J. Leiner, "LDPC Codes – a brief Tutorial", April 8 2005

3.2 Τεχνικές ελέγχου και διόρθωσης των σφαλμάτων

Αυτόματη Αίτηση Επανεκπομπής (Automatic Repeat Request, ARQ)



σχήμα 9

Στο σύστημα αυτό ο δέκτης εκτελεί ανίχνευση των σφαλμάτων και απλά ζητά από τον πομπό, επανεκπομπή των εσφαλμένων πακέτων δεδομένων. Η συγκεκριμένη τεχνική συμβάλλει στην αξιοπιστία της λαμβανόμενης πληροφορίας, αν και έχει αυξημένη πολυπλοκότητα, αφού απαιτεί την ύπαρξη ενός καναλιού ανάδρασης, το οποίο όμως δεν είναι πάντα διαθέσιμο, καθιστώντας την έτσι μη πρακτική για αρκετές εφαρμογές. Στην περίπτωση της διόρθωσης των σφαλμάτων με επαναμετάδοση, ο παραλήπτης αποστέλλει στον αποστολέα ένα ειδικό πλαίσιο ελέγχου, το οποίο περιέχει μία θετική επιβεβαίωση (ACK), εφόσον η μετάδοση υπήρξε επιτυχής, ή μια αρνητική επιβεβαίωση (NAK), εφόσον εντοπίστηκαν

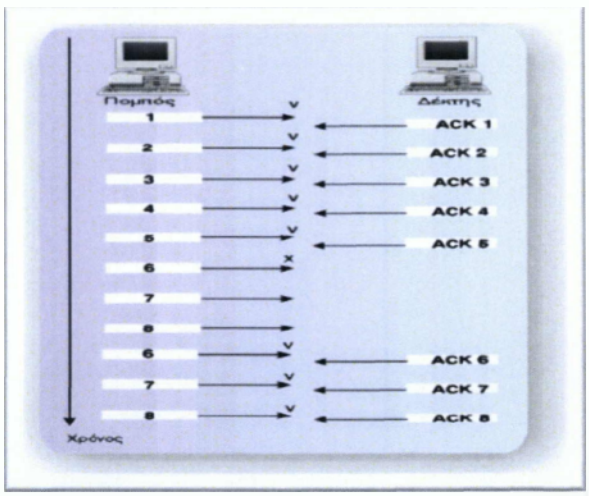
σφάλματα στα διακινούμενα δεδομένα. Η μέθοδος αυτή εμφανίζεται σε τρεις παραλλαγές οι οποίες χρησιμοποιούνται ανάλογα με τις περιστάσεις. Στην πρώτη περίπτωση, **ARQ Παύσης και Αναμονής (ARQ Stop And Wait)**, για κάθε μεταδιδόμενο πακέτο, αποστέλλεται ένα πλαίσιο επιβεβαίωσης στον αποστολέα. Εάν η επιβεβαίωση αυτή είναι θετική, ο αποστολέας στέλνει το επόμενο πακέτο, ενώ στην αντίθετη περίπτωση, αναμεταδίδει αυτό που έφτασε εσφαλμένο.[34]

σχήμα 10

Στην δεύτερη περίπτωση **ARQ Οπισθοδρόμησης Κατά N (ARQ Go-Back-N)**, ο αποστολέας δεν περιμένει την επιβεβαίωση για το κάθε πακέτο, αλλά αποστέλλει όλα τα πακέτα της πληροφορίας, το ένα μετά το άλλο.

[34] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

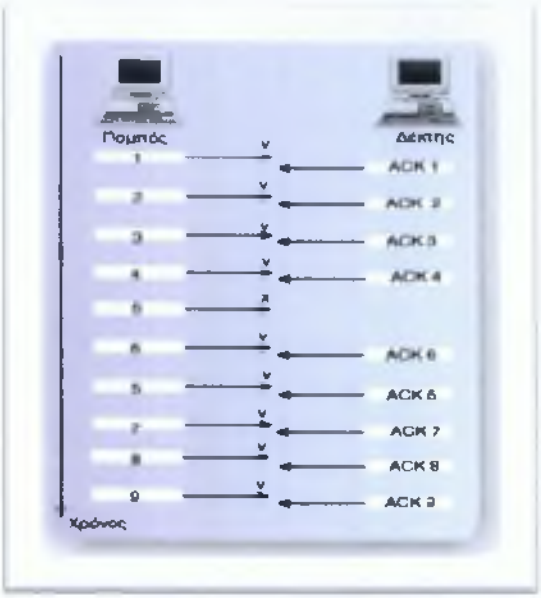
Εάν όμως λάβει αρνητική επιβεβαίωση για κάποιο από τα προηγούμενα πακέτα, τότε αναμεταδίδει αυτό το πακέτο, και μαζί με αυτό, όλα τα πακέτα από εκεί και κάτω, ακόμα και αν αυτά έχουν μεταδοθεί σωστά. [35]



σχήμα 11

Τέλος, ο αποστολέας αποστέλλει όλα τα πακέτα της πληροφορίας και αν λάβει αρνητική επιβεβαίωση για κάποιο από τα προηγούμενα πακέτα, ξαναστέλνει μόνο το εσφαλμένο πακέτο και όχι όλα τα υπόλοιπα. Αυτή είναι η τρίτη μέθοδος **ARQ Επιλεκτικής Απόρριψης (ARQ Selective Reject)** , όπου είναι μία παραλλαγή της δεύτερης περίπτωσης.

[35] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley



σχήμα 12 [36]

Τεχνική Επιλεκτικής Απόρριψης

Προωθημένη ή Πρόσθια Διόρθωση Λαθών (Forward Error Correction, FEC)

Εδώ ο δέκτης, σε περίπτωση ανίχνευσης σφάλματος, προβαίνει και στην διόρθωσή του σύμφωνα με τους κανόνες κωδικοποίησης. Η κωδικοποίηση FEC χρησιμοποιείται στις τηλεπικοινωνίες και στην θεωρία πληροφορίας, ως ένα σύστημα ελέγχου λαθών (error correction code).

[36] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

Ο αποστολέας συμπεριλαμβάνει πλεονάζουσα πληροφορία στο μήνυμά του, που επιτρέπει στο δέκτη να ανιχνεύσει και να διορθώσει λάθη, χωρίς να ζητήσει αναμετάδοση πακέτων.

Η αυτόματη διόρθωση σφαλμάτων μπορεί να πάρει διάφορες μορφές. Ο πλέον γνωστός κώδικας αυτόματης διόρθωσης σφαλμάτων είναι ο κώδικας Hamming, που διορθώνει απλά σφάλματα με την προσθήκη δυαδικών ψηφίων ελέγχου. Παράδειγμα χρησιμοποίησης της μεθόδου αυτόματης διόρθωσης σφαλμάτων αποτελεί το σχήμα κωδικοποίησης που χρησιμοποιείται στους δίσκους CD-ROM, στους οποίους το φυσικό μέσο αποθήκευσης είναι πολύ ευαίσθητο σε σφάλματα. Το σύστημα αυτό σχεδιάστηκε με την προοπτική να διορθώνεται αυτόματα ένας μεγάλος αριθμός σφαλμάτων, ώστε το σύστημα αποθήκευσης να έχει τον απαιτούμενο βαθμό αξιοπιστίας.

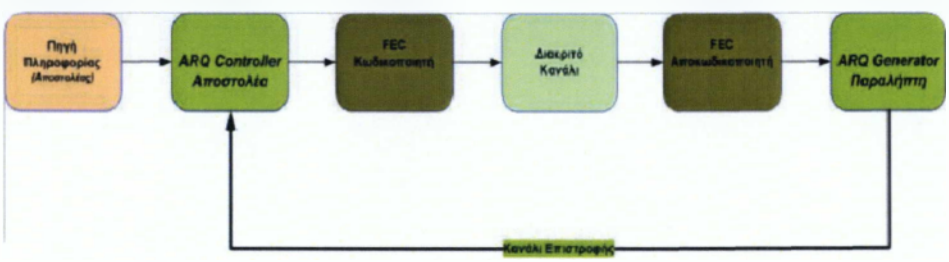
Η τεχνική αυτή, αν και δυσκολότερη στην εφαρμογή από την ARQ, το πλεονέκτημά της έγκειται στο ότι δεν απαιτείται αμφίδρομο κανάλι για την επικοινωνία προορισμού – πηγής και συνεπώς αποφεύγεται η αναμετάδοση πακέτων και η αντίστοιχη σπατάλη εύρους ζώνης.

Βασική διαφορά των δύο τεχνικών αποτελεί η διόρθωση σφαλμάτων, διαδικασία που συμβαίνει μόνο στη FEC.[37]

[37] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

Υβριδική FEC / ARQ Μέθοδος

Η κάθε μία από τις παραπάνω μεθόδους FEC και ARQ, κατέχει τα δικά της πλεονεκτήματα και μειονεκτήματα. Ιδανικό σενάριο θα ήταν τα πλεονεκτήματα των παραπάνω τεχνικών, επικερδώς να τα ενσωματώσουμε σε μια νέα μέθοδο, έτσι ώστε όταν έχουμε να κάνουμε με μεσαίες προς καλές συνθήκες καναλιού, να φροντίζει ο FEC κώδικας για τη χωρίς σφάλματα μετάδοση, ξεπερνώντας το μειονέκτημα που παρουσιάζει ο ARQ. Στην περίπτωση που οι συνθήκες που επικρατούν στο κανάλι δεν είναι ιδανικές, οπότε θα υπάρχουν σφάλματα κατά την μετάδοση, θα φροντίζει η ARQ μέθοδος για τη συγκεκριμένη επαναμετάδοση.[38]



Απεικόνιση ενός Υβριδικού FEC-ARQ Συστήματος. σχήμα 13

[38] G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley

3.3 Πρακτικά συστήματα ανίχνευσης και διόρθωσης σφαλμάτων

Τεχνολογία Οπτικής Μετάδοσης

Η τεχνολογία οπτικής πολυπλεξίας με διαίρεση στο μήκος κύματος (WDM) απετέλεσε σταθμό στην εξέλιξη της οπτικής μετάδοσης, επειδή άνοιξε το δρόμο για την καλύτερη εκμετάλλευση του πρακτικά απεριόριστου εύρους ζώνης μίας οπτικής ίνας. Η επιτυχία της οφείλεται στην καθαρά οπτική ενίσχυση των οπτικών παλμών, η οποία διεξάγεται χωρίς οπτικοηλεκτρονική μετατροπή και από κοινού για όλα τα μήκη κύματος. Αν δεν υπήρχε η παραπάνω δυνατότητα, τότε η αναγέννηση θα έπρεπε αφενός να διεξάγεται ανεξάρτητα για κάθε μήκος κύματος και αφετέρου να είναι πλήρης. Όμως, η πλήρης αναγέννηση ενός οπτικού σήματος είναι μία ιδιαίτερα δαπανηρή λειτουργία. Επομένως, χωρίς την καθαρά οπτική ενίσχυση των οπτικών παλμών, το συνολικό κόστος ενός δικτύου WDM θα εκτινασσόταν κυριολεκτικά, αφού το ήδη υψηλό κόστος της πλήρους αναγέννησης θα πολλαπλασιαζόταν με το πλήθος των πολυπλεγμένων μηκών κύματος για κάθε κόμβο του δικτύου. [39]

[39] http://www.ipet.gr/digitech2/index.php

Γενεές Συστημάτων FEC

- **1η Γενεά**

Τα παραπάνω φανερώνουν την καθοριστική σημασία της καθαρά οπτικής ενίσχυσης για την εμπορική επιτυχία των δικτύων WDM. Εντούτοις, η καθαρά οπτική ενίσχυση έχει το μειονέκτημα ότι μαζί με το ωφέλιμο σήμα ενισχύεται και ο εσωτερικός θόρυβος του ενισχυτή (ASE), ο οποίος προκαλεί σφάλματα τυχαίου χαρακτήρα. Αυτά τα σφάλματα ήταν η κυρίαρχη ατέλεια της οπτικής μετάδοσης στα πρώτα εμπορικά δίκτυα WDM (ρυθμοί μετάδοσης μέχρι 2.5 Gb/s) και για την αντιμετώπιση τους έγινε για πρώτη φορά συστηματική χρήση της κωδικοποίησης FEC. Το γεγονός αυτό οδήγησε σύντομα στην πρώτη διεθνή τυποποίηση σε σχέση με την εφαρμογή της κωδικοποίησης FEC σε οπτικά δίκτυα. Τα συστήματα, που σχεδιάστηκαν για την αντιμετώπιση του θορύβου των οπτικών ενισχυτών στα πρώτα δίκτυα WDM, αποτελούν την 1η γενεά συστημάτων FEC (1993-1996) και διακρίνονται από ένα κέρδος κωδικοποίησης της τάξεως των 6 dB.[40]

[40] Μπάρδης Γ., Νικολόπουλος Β., Μπράττος Ι., "Μελέτες – Εφαρμογές Και Υλοποίηση Δικτύων Η/Υ", 1η Έκδοση, 2007, Β. Γκιούρδας Εκδοτική

- **2η Γενεά**

Καθώς όμως οι ρυθμοί μετάδοσης συνέχισαν να αυξάνονται, πρώτα στα 10 Gb/s και έπειτα στα 40 Gb/s, άλλες ατέλειες της οπτικής μετάδοσης κέρδισαν σε βαρύτητα, όπως τα μη-γραμμικά φαινόμενα (NL), η χρωματική διασπορά (CD) και η διασπορά τρόπου πόλωσης (PMD). Τα συστήματα κωδικοποίησης FEC 1ης γενεάς αποδείχτηκαν ανεπαρκή στην αντιμετώπιση αυτών των ατελειών. Κατά συνέπεια, σχεδιάστηκαν συστήματα με ισχυρότερη και πιο περίπλοκη κωδικοποίηση FEC, που αποτελούν τη 2η γενεά συστημάτων FEC (2000-2004) και διακρίνονται από ένα κέρδος κωδικοποίησης της τάξεως των 8dB. Από την άλλη όμως πλευρά, τα συστήματα FEC 2ης γενεάς συνέβαλαν στη σοβαρή κλιμάκωση του κόστους των οπτικών δικτύων, που επισκίασε την ώριμη πλέον τεχνολογία οπτικής μετάδοσης ρυθμού 10 Gb/s. Η κλιμάκωση του κόστους, που αναμένεται με το πέρασμα στην τεχνολογία οπτικής μετάδοσης ρυθμού 40 Gb/s, είναι ακόμα μεγαλύτερη. Άρα, η οικονομική βιωσιμότητα των νέων τεχνολογιών της οπτικής μετάδοσης τίθεται σε κίνδυνο, ιδιαίτερα κατά την ευαίσθητη φάση της διείσδυσης στη σύγχρονη αγορά τηλεπικοινωνιών.[41]

[41] Μπάρδης Γ., Νικολόπουλος Β., Μπράττος Ι., "Μελέτες – Εφαρμογές Και Υλοποίηση Δικτύων Η/Υ", 1η Έκδοση, 2007, Β. Γκιούρδας Εκδοτική

- **3η Γενεά**

Η επίλυση του διαφαινόμενου οικονομικού αδιεξόδου επιτάσσει την κατά το δυνατό μείωση ή ακόμα και εξάλειψη των πλήρων αναγεννητών 3R, καθώς αυτοί εκπροσωπούν ένα σημαντικό μέρος του κόστους των οπτικών δικτύων. Όμως, η αντικατάσταση των πλήρων αναγεννητών 3R από κατά πολύ οικονομικότερους, καθαρά οπτικούς αναγεννητές 1R οδηγεί σε ένα νέο αδιέξοδο: οι αλλοιώσεις των οπτικών παλμών εξαιτίας των ατελειών της οπτικής μετάδοσης συσσωρεύονται σε μεγαλύτερα διαστήματα με αποτέλεσμα να αστοχούν ακόμα και τα συστήματα FEC 2ης γενεάς. Για αυτό το λόγο, συστήματα FEC 3ης γενεάς έχουν ήδη αρχίσει να διαδέχονται τους προκατόχους τους 2ης γενεάς (2004). Τα συστήματα FEC 3ης γενεάς διακρίνονται από κέρδη κωδικοποίησης άνω των 10 dB και καθιστούν οικονομικά προσιτή την εγκατάσταση οπτικών ζεύξεων υψηλής ταχύτητας (10Gb/s και άνω), τοποθετούμενα μόνο στα άκρα των ζεύξεων.[42]

Μία μεγάλη ποικιλία συστημάτων FEC έχουν σήμερα μερίδιο στην αγορά των οπτικών τηλεπικοινωνιών. Διαφέρουν σε αρκετές απόψεις, όπως το ποσοστό του πλεονασμού, η πολυπλοκότητα υλοποίησης, το

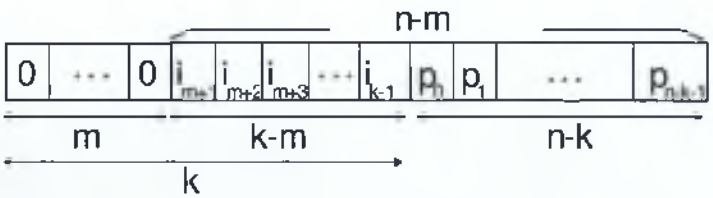
[42] Μπάρδης Γ., Νικολόπουλος Β., Μπράττος Ι., "Μελέτες – Εφαρμογές Και Υλοποίηση Δικτύων Η/Υ", 1η Έκδοση, 2007, Β. Γκιούρδας Εκδοτική

κέρδος-κωδικοποίησης, η καμπύλη βελτίωσης του ρυθμού σφαλμάτων, η ικανότητα διόρθωσης σφαλμάτων που εμφανίζονται σε ομοβροντίες, κ.λπ. Σημαντικό μέρος της σύγχρονης έρευνας εστιάζεται σε υβριδικά σχήματα, που συνδυάζουν την άμεση διόρθωση σφαλμάτων με προηγμένες κωδικοποιήσεις γραμμής και μεθόδους ισοστάθμισης σήματος.[43]

[43] http://www.ipet.gr/digitech2/index.php

3.4 Επιβράχυνση κωδίκων μπλοκ

Επαύξηση των δυνατοτήτων ενός κώδικα μπλοκ επιτυγχάνεται με τη μέθοδο της επιβράχυνσης. Η βασική ιδέα της μεθόδου αυτής έγκειται στο εξής: Τα πρώτα m σύμβολα πληροφορίας από τα k που κωδικοποιούνται σύμφωνα με κώδικα μπλοκ (n,k) διορθωτικής ικανότητας t τίθενται μηδενικά (δεν μεταφέρουν δηλαδή πληροφορία), κατά τον παρακάτω πίνακα:



Τα μηδενικά αυτά σύμβολα δεν εκπέμπονται, παρά μόνο συμπληρώνονται από το δέκτη προκειμένου να γίνει σωστή αποκωδικοποίηση. Με τον τρόπο αυτό έκθετα στο θόρυβο είναι πια μόνο (n-m) σύμβολα, με τη διορθωτική ικανότητα t να παραμένει σταθερή. Έτσι έχουμε ένα νέο κώδικα (n-m,k-m) τον οποίο θα συγκρίνουμε με τον γεννήτορά του.

Α/Α	Κώδικας	Παράγοντας Διόρθωσης (δ)	Παράγοντας Περιεκτικότητας σε Πληροφορία (π)
1	(n,k)	t/n	k/n
2	(n-m,k-m)	T n – m	k - m n - m

Είναι φανερό πως η απόδοση (α) ενός κώδικα χαρακτηρίζεται από το μέγεθος

$$\alpha = \delta\pi$$

Θα υπολογίσουμε την απόδοση των κωδίκων 1 και 2 (γεννήτορα και επιβραχυμένου).

$$a_1 = \delta_1 \cdot \pi_1 = \frac{t}{n} \cdot \frac{k}{n} = \frac{t \cdot k}{n^2}$$

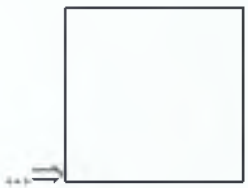
$$\alpha_2 = \delta_2 \cdot \pi_2 = \frac{t(k-m)}{(n-m)^2}$$

Η βελτίωση της απόδοσης του επιβραχυμένου ως προς τον γεννήτορα είναι:

$$\boxed{\beta = \frac{\alpha_2}{\alpha_1} = \frac{n^2(k-m)}{k(n-m)^2}}$$ Παράγοντας βελτίωσης επιβράχυνσης

Για δεδομένα n και k η βελτίωση γίνεται μέγιστη όταν:

$$\frac{d\beta(m)}{dm} = 0 \Rightarrow \frac{-(n-m)^2 + (k-m)\cdot 2\cdot(n-m)}{(n-m)^4} = 0 \Rightarrow \ldots$$



Συνθήκη βέλτιστης επιβράχυνσης

Τότε ο παράγοντας βελτίωσης επιβράχυνσης γίνεται:

$$\beta_{\max} = \frac{n^2}{4k(n-k)}$$ Μέγιστος Παράγοντας βελτίωσης

Από την τελευταία σχέση συμπεραίνουμε ότι συμφέρουσα είναι η επιβράχυνση κωδίκων με μεγάλο μήκος μπλοκ (n) οπότε η βελτίωση είναι μεγαλύτερη.

Η τεχνική της σύμπλεξης κωδίκων μπλοκ[44]

Σκοπός της Σύμπλεξης

Με την τεχνική της Σύμπλεξης Κωδικών Μπλοκ αντιμετωπίζονται περιπτώσεις κατά τις οποίες γίνεται μετάδοση πληροφορίας μέσω τηλεπικοινωνιακών καναλιών στα οποία δρα *Καταιγιστικός Θόρυβος*, θόρυβος δηλαδή που προκαλεί μεγάλο αριθμό αλλοιώσεων σε διαδοχικά σύμβολα (όπως, π.χ. , συμβαίνει κατά την πτώση ενός κεραυνού στη διάρκεια μιας ασύρματης μετάδοσης.)

[44] Peterson, Weldon, "Error Correcting Codes", MIT Press, Cambridge, 1984

Αρχή της Σύμπλεξης

Στην τεχνική της Σύμπλεξης χρησιμοποιούνται λ κωδικά μπλοκ μήκους n - οπότε μιλάμε για σύμπλεξη λ βαθμού- τα σύμβολα των οποίων δεν εκπέμπονται διαδοχικά, αλλά ανά ομάδες ομολόγων από κάθε μπλοκ.

Μειονέκτημα της Σύμπλεξης

Το μειονέκτημα της τεχνικής της σύμπλεξης έγκειται στο γεγονός ότι, προκειμένου να επιτευχθεί, απαιτείται η αποθήκευση των λ κωδικών μπλοκ πριν την εκπομπή τους. Απαιτείται, δηλαδή, μια μονάδα αποθήκευσης (μνήμη) (λη) συμβόλων η οποία αυξάνει τον όγκο και την πολυπλοκότητα της μονάδας Κωδικοποίησης / Αποκωδικοποίησης, και η ανάγκη για την ύπαρξη της οποίας περιορίζει το βαθμό της σύμπλεξης που μπορεί να επιτύχει κανείς στην πράξη.

ΚΕΦΑΛΑΙΟ 4^{Ο}

ΕΦΑΡΜΟΓΕΣ - ΠΡΑΚΤΙΚΗ ΑΞΙΑ

4.1 Ψηφιακή μετάδοση υψηλής ποιότητας

Οι διαρκώς αυξανόμενες απαιτήσεις του σύγχρονου ανθρώπου επιβάλλουν - ιδιαίτερα η μετάδοση δεδομένων (DATA) - πολύ μικρό ποσοστό σφαλμάτων (BER) στις διακινούμενες ψηφιοσειρές. Προς την κατεύθυνση αυτή συμβάλλουν οι Κώδικες Ελέγχου Σφάλματος, ιδιαίτερα όταν η μετάδοση της πληροφορίας γίνεται μέσα από ευαίσθητα και επιβαρυμένα σε θόρυβο κανάλια.

Ασύρματη Μετάδοση

Ιδιαίτερα έκθετη στο θόρυβο είναι η ψηφιακή πληροφορία που διαβιβάζεται μέσω ασύρματων συστημάτων (Radio Links). Κατά την μετάδοση αυτή εμφανίζεται θόρυβος τυχαίος αλλά και καταιγιστικός, τον οποίο αντιμετωπίζουν με επιτυχία οι τεχνικές κωδικοποίησης ελέγχου σφάλματος. Έτσι, ECC Κωδικοποιητές/ Αποκωδικοποιητές (Reed - Solomon και άλλοι) χρησιμοποιούνται σε δορυφορικές ζεύξεις, σε κινητά ραδιοσυστήματα καθώς και στις διαστημικές επικοινωνίες.

Είναι χαρακτηριστικό το γεγονός ότι ένας κώδικας Reed - Solomon που τηλεμετρικά προγραμματίστηκε για εκτέλεση στα κυκλώματα του διαστημοπλοίου Mariner* έσωσε το αντίστοιχο εξερευνητικό πρόγραμμα από βέβαιη αποτυχία όταν η κεντρική κεραία επικοινωνίας με τη Γη καταστράφηκε. Συγκεκριμένα, ο κώδικας Reed - Solomon εξασφάλισε αξιόπιστη μετάδοση των δεδομένων από το Δία (εικόνες κλπ) μέσω δευτερεύουσας κεραίας πολύ μικρότερης απολαβής (άρα και αισθητά μικρότερου εύρους ζώνης).[45]

Ευαίσθητα Ψηφιακά Συστήματα

Κρίσιμη είναι, επίσης, η συνεισφορά της Κωδικοποίησης Ελέγχου σφάλματος σε ευαίσθητα Ψηφιακά Συστήματα, όπως συστήματα μεταφοράς συμπιεσμένων δεδομένων (εικόνας κλπ), σε συστήματα με απαιτητικό συγχρονισμό (συστήματα μεταφοράς κρυπτογραφημένης πληροφορίας) καθώς και στην επικοινωνία υπολογιστών συνδεδεμένων σε δίκτυο (ιδιαίτερα τύπου MAN και WAN [Metropolitan Area Network, Wide Area Network]), όπου αποτελούν την καρδιά του μηχανισμού επανεκπομπής πακέτων δεδομένων (Retransmission). [46]

[45] Zieman, Peterson, "Digital Communications and Spread Spectrum Systems", Macmillan, 1985
[46] Shanmugan, "Ψηφιακά και Αναλογικά Συστήματα Επικοινωνίας" Μετάφραση Κ. Καρούμπαλου, 2003

Ηλεκτρονικός Πόλεμος

Αδιαμφισβήτητη είναι η θέση του ECC και στις επιχειρήσεις του Ηλεκτρονικού Πολέμου. Ισχυροί κώδικες Reed-Solomon σε συνδυασμό με άλλους κώδικες και με τεχνικές Επιβράχυνσης και Σύμπλεξης μπορούν να αποτελέσουν ισχυρότατο εργαλείο εναντίον του ηλεκτρονικού θορύβου που προκαλεί ο εχθρός.[47]

[47] Leach and Malvino, "Ψηφιακά Ηλεκτρονικά", 5η Έκδοση, 2006, Εκδόσεις Τζιόλα

4.2 Ψηφιακή αποθήκευση-αναπαραγωγή

Χαρακτηριστική πρακτική εφαρμογή της τεχνικής ECC αποτελεί το γνωστό μας CD. Επειδή τα φυσικά μεγέθη που αποθηκεύονται σ' ένα Compact Disk είναι πολύ μικρής κλίμακας, και άρα ευάλωτα στο θόρυβο, η αξιόπιστη ανάγνωση και αναπαραγωγή τους επιβάλλει την "προστασία" τους με έναν κώδικα Reed - Solomon. Με τον τρόπο αυτό εξουδετερώνονται αλλοιώσεις της πληροφορίας που μπορούν να προέλθουν από την επικάθιση σκόνης στην επιφάνεια του δισκιδίου, δακτυλικά αποτυπώματα, κ.λπ. Ανάλογη είναι η χρήση κωδίκων ECC και σε άλλα γνωστά μέσα ψηφιακής αποθήκευσης, όπως π.χ. η μαγνητική ταινία τύπου DAT.[48]

[48] Leach and Malvino, "Ψηφιακά Ηλεκτρονικά", 5η Έκδοση, 2006, Εκδόσεις Τζιόλα

Επίλογος-συμπεράσματα

Η εργασία αυτή πραγματεύτηκε τις γνώσεις και τα στοιχεία που απαιτούνται για την κατανόηση του αντικειμένου της ανίχνευσης και διόρθωσης σφαλμάτων στην ψηφιακή μετάδοση δεδομένων. Αναλύθηκαν έννοιες που αφορούσαν τις κατηγορίες των κωδίκων ανίχνευσης σφαλμάτων, τις τεχνικές ανίχνευσης και διόρθωσης. Αφιερώθηκε υποενότητα για την ανάλυση του ζητήματος της επιβράχυνσης των κωδίκων μπλοκ, που είναι και το κύριο θέμα της εργασίας, καθώς και για τις πρακτικές εφαρμογές των παραπάνω συστημάτων ανίχνευσης και διόρθωσης σφαλμάτων.

Από την παραπάνω εργασία κατανοούμε την αναγκαιότητα των κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων, ειδικά στη σημερινή εποχή που η ραγδαία εξέλιξη της τεχνολογίας και των τηλεπικοινωνιών απαιτούν καλύτερης ποιότητας ψηφιακό σήμα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική βιβλιογραφία

1) Ζορκάδης Β., (2002), "Θεωρία Πληροφορίας και Κωδικοποίησης", Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο.

2) Γεώργιος Κων. Κοκκινάκης, (2004), "Εισαγωγή στις Επικοινωνίες".

3) Διπλωματική Εργασία του Φοιτητή Γεώργιου Αγγελόπουλου του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών με Θέμα "Ανάλυση, σχεδιασμός και υλοποίηση κωδίκων διόρθωσης λαθών για τηλεπικοινωνιακές εφαρμογές υψηλών ταχυτήτων", 2009.

4) Ζορκάδης Β., "Θεωρία Πληροφορίας και Κωδικοποίησης", Τόμος Α΄, Ελληνικό Ανοικτό Πανεπιστήμιο, 2002.

5) Μπάρδης Γ., Νικολόπουλος Β., Μπράττος Ι., "Μελέτες – Εφαρμογές Και Υλοποίηση Δικτύων Η/Υ", 1η Έκδοση, 2007, Β. Γκιούρδας Εκδοτική.

Ξένη βιβλιογραφία

6) C. E. Shannon, "A Mathematical Theory of Communication", Bell System.
7) John G. Proakis, "Digital Communications", Fourth Edition.
8) R.W. Hamming, (1950), "Error detection and error correcting codes", Bell Syst. Technology Journal
9) G. Kabatiansky, E. Krouk, S. Semenov, "Error Correcting Coding and Security for Data Networks", Wiley
10) Lin Shu, Daniel J. Costello Jr, "Error Control Coding, Fundamentals and Applications", Prentice Hall 1983
11) Peterson, Weldon, "Error Correcting Codes", MIT Press, Cambridge, 1984
12) Bernard M. J. Leiner, "LDPC Codes – a brief Tutorial", April 8 2005
13) Zieman, Peterson, "Digital Communications and Spread Spectrum Systems", Macmillan, 1985
14) Shanmugan, "Ψηφιακά και Αναλογικά Συστήματα Επικοινωνίας" Μετάφραση Κ. Καρούμπαλου, 2003
15) Leach and Malvino, "Ψηφιακά Ηλεκτρονικά", 5η Έκδοση, 2006, Εκδόσεις Τζιόλα

Ηλεκτρονική βιβλιογραφία

16) http://de.wikipedia.org/wiki/Turbo-Code

17) http://www.eyliko.gr/htmls/diktya/senario4/theory/files/DiktyMetds1Kef2.pdf

18) http://eclass.teilam.gr/claroline/document/document.php

19) http://courses.softlab.ntua.gr/softdev/#lesson2811

20) http://eclass.teilam.gr/claroline/document/document.php

21) http://el.wikipedia.org/wiki/WiMAX

22) http://www.ipet.gr/digitech2/index.php