Περιεχόμενα

Κεφάλαιο 1

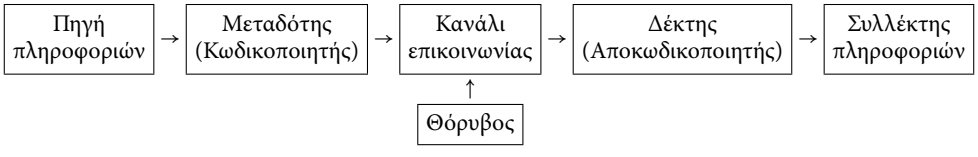
Εισαγωγή στη θεωρία κωδικοποίησης

1.1 Εισαγωγή

Η θεωρία κωδικοποίησης (coding theory) είναι η μελέτη μεθόδων για την αποδοτική και ακριβή μεταβίβαση πληροφοριών από το ένα μέρος στο άλλο. Η θεωρία έχει αναπτυχθεί για ποικίλες εφαρμογές, όπως η ελαχιστοποίηση του θορύβου από τις εγγραφές συμπαγών δίσκων (compact disc, CD), η μετάδοση οικονομικών πληροφοριών μέσω τηλεφωνικών γραμμών, η μετάδοση δεδομένων μεταξύ υπολογιστών ή μεταξύ μνήμης και κεντρικού επεξεργαστή, καθώς και η μετάδοση πληροφοριών από απομακρυσμένες πηγές, όπως είναι οι μετεωρολογικοί ή επικοινωνιακοί δορυφόροι ή το διαστημόπλοιο Voyager, το οποίο έστελνε στη Γη φωτογραφίες από τους πλανήτες Δία και Κρόνο.

Το φυσικό μέσο μέσα από το οποίο μεταδίδεται η πληροφορία ονομάζεται *κανάλι*. Οι τηλεφωνικές γραμμές και η ατμόσφαιρα αποτελούν παραδείγματα καναλιών. Ανεπιθύμητες παρεμβολές, που αποκαλούνται *θόρυβος* (noise), ενδέχεται να προκαλέσουν διαφοροποίηση μεταξύ της μεταδιδόμενης και της παραληφθείσας πληροφορίας. Ο θόρυβος μπορεί να προκληθεί από ηλιακές κηλίδες, αστραπές, τσακίσματα της μαγνητικής ταινίας, βροχές μετεωριτών, φορτωμένες τηλεφωνικές γραμμές, τυχαία ραδιοφωνικά παράσιτα, κακή δακτυλογράφηση, περιορισμένη ακοή, μη καθαρή ομιλία, ή πολλές άλλες αιτίες.

Η θεωρία κωδικοποίησης ασχολείται με το πρόβλημα της ανίχνευσης και της διόρθωσης των λαθών (ή σφαλμάτων) μετάδοσης που προκαλούνται από το θόρυβο στο κανάλι. Στο διάγραμμα που ακολουθεί παρέχεται μια χονδρική ιδέα ενός γενικού συστήματος μετάδοσης πληροφοριών.



Το πιο σημαντικό τμήμα του διαγράμματος για εμάς είναι ο θόρυβος, χωρίς τον οποίο δεν θα ήταν αναγκαία η θεωρία κωδικοποίησης.

Στην πράξη, ο έλεγχος που έχουμε όσον αφορά το θόρυβο είναι η επιλογή ενός καλού καναλιού που θα χρησιμοποιηθεί για τη μετάδοση, καθώς και η χρήση διαφόρων φίλτρων θορύβου για την αντιμετώπιση συγκεκριμένων τύπων παρεμβολών που ενδέχεται να ανακύψουν. Αυτά είναι τεχνικά προβλήματα. Μόλις καταλήξουμε στο καλύτερο μηχανικό σύστημα για την επίλυση των συγκεκριμένων προβλημάτων, μπορούμε να επικεντρώσουμε την προσοχή μας στην κατασκευή του κωδικοποιητή (encoder) και του αποκωδικοποιητή (decoder). Η πρόθεσή μας είναι να τους κατασκευάσουμε με τέτοιο τρόπο ώστε να πετύχουμε:

1. γρήγορη κωδικοποίηση των πληροφοριών,
2. εύκολη μετάδοση των κωδικοποιημένων μηνυμάτων,
3. γρήγορη αποκωδικοποίηση των παραληφθέντων μηνυμάτων,
4. διόρθωση των λαθών που εισάγονται στο κανάλι, και
5. μέγιστη μετάδοση πληροφοριών ανά μονάδα χρόνου.

Ο τέταρτος στόχος είναι και ο πρωταρχικός. Το πρόβλημα είναι ότι δεν είναι γενικά συμβατός με τον πέμπτο, και μπορεί επίσης να μην είναι ιδιαίτερα συμβατός με τους υπόλοιπους τρεις. Έτσι, κάθε λύση επιτυγχάνεται με εξισορρόπηση και των πέντε αντικειμενικών στόχων.

Στις καθημερινές μας προσωπικές επικοινωνίες χρησιμοποιούμε τυπικά λέξεις, γραπτώς ή προφορικώς, που έχουν φτιαχτεί από ένα περιορισμένο αλφάβητο. Έχουμε πληροφορίες που θέλουμε να μεταδώσουμε· τις κωδικοποιούμε σε ακολουθίες λέξεων, οι οποίες εκφράζονται έπειτα με γραπτό ή προφορικό τρόπο. Οι ακολουθίες αποστέλλονται μέσω ενός καναλιού, που είναι συνήθως το διάστημα από το στόμα μέχρι το αυτί ή από το στυλό μέχρι το χαρτί και στη συνέχεια μέχρι το μάτι. Ο θόρυβος μπορεί να προκληθεί από μη καθαρή ομιλία, περιορισμένη ακοή, εσφαλμένη γραμματική, ένα στερεοφωνικό που παίζει σε μεγάλη ένταση, ταυτόχρονη ομιλία από πολλά άτομα, ορθογραφικά λάθη, παρερμηνεία, ή μια ελαττωματική γραφομηχανή. Ο αποκωδικοποιητής είναι η δική μας ανάγνωση (ή ακρόαση) και η κατανόηση των παραληφθέντων μηνυμάτων.

Διαθέτουμε ενσωματωμένους μηχανισμούς διόρθωσης λαθών που ούτε καν φανταζόμαστε. Έστω ότι λαμβάνουμε το μήνυμα «Apt natural. I have a gub.», ένα σημείωμα σε μια ληστεία από την ταινία «Take the money and run» (προβλήθηκε στην Ελλάδα με τίτλο «Ζητείται εγκέφαλος για ληστεία») του Woody Allen. Αφού η αγγλική γλώσσα δεν χρησιμοποιεί όλες τις πιθανές λέξεις με οποιοδήποτε δεδομένο μήκος, θα αναγνωρίσουμε πιθανότατα ότι το «gub» δεν είναι αγγλική λέξη. Μπορούμε με ασφάλεια να υποθέσουμε ότι η λέξη που μεταδόθηκε είναι κα-

τά κάποια έννοια παραπλήσια με το «gub». Άρα, είναι πιο πιθανό να ήταν «gut» ή «gun» ή «tub» παρά «firetruck» ή «rat». Από τα συμφραζόμενα και μόνο του μηνύματος θα επιλέξουμε το «gun» ως την πιο πιθανή λέξη. Η λέξη «Apt» υπάρχει στην αγγλική γλώσσα, αλλά πάλι από τα συμφραζόμενα θα τη διορθώσουμε σε «act». Αν τυχαίνει να είμαστε γνώστες της αγγλικής γλώσσας, θα διορθώσουμε επίσης το «natural» σε «naturally», αν και το συγκεκριμένο λάθος μπορεί να οφείλεται στην πηγή και όχι στο θόρυβο του καναλιού.

Από τους παραπάνω τύπους λαθών, μπορούμε να ασχοληθούμε πιθανώς μόνο με τον πρώτο: δηλαδή να επιλέξουμε (να βρούμε) την πιο πιθανή λέξη που μεταδόθηκε. Η τυπική μέθοδος για την αντιμετώπιση των λαθών βασίζεται στον πλεονασμό (redundancy). Στην εποχή μας, πολλές επιχειρήσεις προσθέτουν συνήθως ψηφία ελέγχου σε αριθμούς αναγνώρισης (identification numbers). Αυτά είναι επιπλέον ψηφία που χρησιμοποιούνται για να ελεγχθεί η ορθότητα διαφόρων δεδομένων ή οι αριθμοί κάποιων λογαριασμών. Αυτή είναι μάλλον και η πιο γνωστή μέθοδος κωδικοποίησης στην καθημερινή ζωή. Θα ασχοληθούμε με πιο πολύπλοκες αλλά παρόμοιες ιδέες.

1.2 Βασικές υποθέσεις

Θα διατυπώσουμε ορισμένους θεμελιώδεις ορισμούς και υποθέσεις που θα ισχύουν σε όλο το βιβλίο.

Σε πολλές περιπτώσεις, οι πληροφορίες προς αποστολή μεταδίδονται με μια ακολουθία από μηδέν και άσους. Οι αριθμοί 0 και 1 αποκαλούνται *ψηφία* (digits). Μια δυαδική λέξη, ή απλά *λέξη*, είναι μια ακολουθία ψηφίων. Ο αριθμός των ψηφίων της λέξης αποτελεί το *μήκος* (length) αυτής. Άρα, η ακολουθία 0110101 είναι μια λέξη μήκους 7. Η μετάδοση της λέξης πραγματοποιείται με την αποστολή των ψηφίων της, το ένα μετά το άλλο, μέσω ενός *δυαδικού καναλιού* (binary channel). Ο όρος «δυαδικό» αναφέρεται στο γεγονός ότι χρησιμοποιούνται μόνο δύο ψηφία, το 0 και το 1. Κάθε ψηφίο μεταδίδεται μηχανικά, ηλεκτρικά, μαγνητικά, ή διαφορετικά, με έναν από τους δύο τύπους εύκολα διαφοροποιήσιμων παλμών.

Ο *δυαδικός κώδικας* (binary code) ορίζεται ως ένα σύνολο C από λέξεις. Ο κώδικας που αποτελείται από όλες τις λέξεις μήκους δύο είναι

$$C = \{00, 10, 01, 11\}.$$

Ο *τμηματικός κώδικας* (block code) είναι ένας κώδικας στον οποίο όλες οι λέξεις έχουν τον ίδιο αριθμό ψηφίων· αυτός ο αριθμός ονομάζεται *μήκος* του κώδικα. Θα μελετήσουμε μόνο τμηματικούς κώδικες. Άρα, για μας, ο όρος *κώδικας* θα αναφέρεται πάντα σε δυαδικό τμηματικό κώδικα. Οι λέξεις που ανήκουν σε δεδομένο

κώδικα C_0 θα αποκαλούνται *κωδικολέξεις* (ή κωδικές λέξεις). Θα συμβολίζουμε τον αριθμό των κωδικολέξεων σε έναν κώδικα C με $|C|$.

Ασκήσεις

1.2.1 Φτιάξτε μια λίστα με όλες τις λέξεις μήκους 3, μήκους 4, και μήκους 5.

1.2.2 Βρείτε ένα μαθηματικό τύπο για το συνολικό αριθμό των λέξεων μήκους n.

1.2.3 Έστω C ο κώδικας που αποτελείται από όλες τις λέξεις μήκους 6, οι οποίες έχουν άρτιο πλήθος άσων. Φτιάξτε μια λίστα με τις κωδικολέξεις του C.

Είναι, επίσης, απαραίτητο να κάνουμε ορισμένες βασικές υποθέσεις για το κανάλι. Αυτές οι υποθέσεις θα μορφοποιήσουν αναγκαστικά τη θεωρία που διατυπώνουμε.

Η πρώτη υπόθεση είναι ότι μια κωδικολέξη μήκους n που αποτελείται από 0 και 1 παραλαμβάνεται πάντα ως λέξη μήκους n που αποτελείται από 0 και 1, αλλά δεν αποκλείεται να είναι διαφορετική από τη λέξη που έχει αποσταλεί.

Η δεύτερη είναι ότι μπορούμε να αναγνωρίσουμε την αρχή της πρώτης λέξης που μεταδόθηκε. Έτσι, αν χρησιμοποιήσουμε κωδικολέξεις μήκους 3 και λάβουμε την ακολουθία 011011001, θα ξέρουμε ότι λάβαμε κατά σειρά τις εξής λέξεις : 011, 011, 001. Αυτή η υπόθεση σημαίνει, ξανά για μήκος 3, ότι το κανάλι δεν μπορεί να παραδώσει την ακολουθία 01101 στο δέκτη, επειδή έχει χαθεί ένα ψηφίο στη συγκεκριμένη περίπτωση.

Η τελευταία υπόθεση είναι ότι ο θόρυβος είναι διεσπαρμένος τυχαία (σε όλο το μήκος της ακολουθίας που παραλήφθηκε) αντί να εμφανίζεται σε δέσμες που ονομάζονται *ριπές* (bursts).[1] Δηλαδή, η πιθανότητα να έχει επηρεαστεί ένα τυχαίο ψηφίο κατά τη μετάδοση (λόγω θορύβου) είναι ίδια ακριβώς με την πιθανότητα οποιουδήποτε άλλου ψηφίου και δεν επηρεάζεται από λάθη που έχουν γίνει σε γειτονικά ψηφία. Αυτή η υπόθεση δεν είναι πολύ ρεαλιστική για πολλά είδη θορύβου, όπως οι αστραπές και οι γρατζουνιές σε CD. Θα μελετήσουμε τελικά και αυτόν τον τύπο θορύβου.

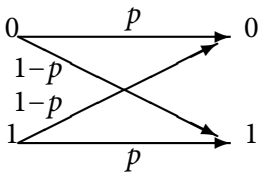
Σε ένα *τέλειο*, ή αθόρυβο κανάλι, κάθε ψηφίο 0 ή 1 που αποστέλλεται είναι πάντοτε αυτό που παραλαμβάνεται. Αν όλα τα κανάλια ήταν τέλεια, η θεωρία κωδικοποίησης δεν θα ήταν απαραίτητη. Όμως ευτυχώς (ή ίσως, δυστυχώς) κανένα κανάλι δεν είναι τέλειο· όλα τα κανάλια είναι θορυβώδη. Κάποια κανάλια είναι λιγότερο θορυβώδη, ή περισσότερο αξιόπιστα, από άλλα.

Ένα δυαδικό κανάλι είναι *συμμετρικό*, αν τα 0 και 1 μεταδίδονται με την ίδια πιθανότητα λάθους· δηλαδή η πιθανότητα να λάβουμε το σωστό ψηφίο είναι ανεξάρτητη από το ποιο ψηφίο, 0 ή 1, μεταδίδεται. Η *αξιοπιστία* ενός δυαδικού

[1] *Σ.τ.Μ.*: Ο όρος *ριπή* έχει καθιερωθεί στη βιβλιογραφία και υποδηλώνει ότι ένας μεγάλος αριθμός λαθών εμφανίζονται πολύ κοντά το ένα στο άλλο. Ουσιαστικά, πρόκειται για έναν *καταιγισμό* λαθών.

συμμετρικού καναλιού (binary symmetric channel, ή ΔΣΚ για συντομία) είναι ένας πραγματικός αριθμός p, με $0 \leq p \leq 1$, ο οποίος συμβολίζει την πιθανότητα να είναι το ψηφίο (0 ή 1) που παραλαμβάνεται ακριβώς εκείνο που έχει αποσταλεί.

Αν λοιπόν το p συμβολίζει την πιθανότητα να είναι το ψηφίο που παραλαμβάνεται ίδιο με το ψηφίο που έχει αποσταλεί, τότε η πιθανότητα να *μην* είναι το ψηφίο που παραλαμβάνεται εκείνο που έχει αποσταλεί είναι ίση με $1 - p$. Το παρακάτω διάγραμμα αποσαφηνίζει τη λειτουργία ενός ΔΣΚ:



Στις περισσότερες περιπτώσεις, είναι ίσως δύσκολο να υπολογίσουμε την ακριβή τιμή του p για δεδομένο κανάλι. Παρόλα αυτά, η πραγματική τιμή του p δεν επηρεάζει σημαντικά τη διατύπωση και το σχηματισμό της θεωρίας.

Θα αποκαλούμε ένα κανάλι πιο αξιόπιστο από κάποιο άλλο, αν η αξιοπιστία του είναι μεγαλύτερη. Προσέξτε ότι για $p = 1$, δεν υπάρχει περίπτωση να αλλαχτεί κάποιο ψηφίο κατά την μετάδοση. Επομένως, το κανάλι είναι τέλειο και δεν μας ενδιαφέρει. Δεν θα μας απασχολήσουν επίσης τα κανάλια με $p = 0$. Οποιοδήποτε κανάλι με $0 < p \leq 1/2$ μπορεί εύκολα να μετατραπεί σε κανάλι με $1/2 \leq p < 1$. *Από τώρα και στο εξής θα υποθέτουμε πάντα ότι χρησιμοποιούμε ένα ΔΣΚ με αξιοπιστία p που ικανοποιεί τη σχέση* $1/2 < p < 1$. (Η περίπτωση $p = 1/2$ θα εξεταστεί στην Άσκηση 1.2.6.)

Ασκήσεις

1.2.4 Εξηγήστε γιατί ένα κανάλι με $p = 0$ δεν έχει ενδιαφέρον.

1.2.5 Εξηγήστε πώς μπορεί ένα κανάλι με πιθανότητα $0 < p \leq 1/2$ να μετατραπεί σε κανάλι με πιθανότητα $1/2 \leq p < 1$.

1.2.6 Τι μπορούμε να πούμε για ένα κανάλι με $p = 1/2$;

1.3 Διόρθωση και ανίχνευση υποδειγμάτων λάθους

Θα μελετήσουμε τώρα τις δυνατότητες διόρθωσης και ανίχνευσης λαθών. Σε αυτή την ενότητα θα αναπτύξουμε διαισθητικά τις έννοιες που εμπλέκονται στη διόρθωση και την ανίχνευση λαθών, ενώ στις επόμενες ενότητες θα υιοθετήσουμε μια πιο τυπική θεώρηση.

Ας υποθέσουμε ότι λαμβάνουμε μια λέξη που δεν είναι κωδικολέξη. Είναι προφανές ότι κάποιο λάθος έχει συμβεί κατά τη διάρκεια της μετάδοσης, άρα *έχουμε*

ανιχνεύσει ότι εμφανίστηκε ένα λάθος (ίσως αρκετά λάθη). Αν όμως λάβουμε μια κωδικολέξη, τότε είναι πιθανό ότι δεν υπήρξαν λάθη κατά τη διάρκεια της μετάδοσης, οπότε είναι αδύνατο να ανιχνεύσουμε κάποιο λάθος.

Η έννοια της διόρθωσης ενός λάθους είναι πιο περίπλοκη. Όπως στο παράδειγμα της εισαγωγής όπου προτιμήσαμε να διορθώσουμε το «gub» σε «gun» παρά σε «rat», θα προσφύγουμε στη διαίσθησή μας για να προτείνουμε ότι κάθε παραληφθείσα λέξη, έστω w, θα πρέπει να *διορθωθεί* σε μια κωδικολέξη που απαιτεί να γίνουν όσο το δυνατόν λιγότερες αλλαγές στη w. (Σε επόμενη ενότητα θα δείξουμε ότι η πιθανότητα να έχει αποσταλεί μια τέτοια κωδικολέξη είναι μεγαλύτερη από ή ίση με την πιθανότητα να έχει αποσταλεί οποιαδήποτε άλλη λέξη). Για να εμπεδώσουμε αυτές τις ιδέες, θα μελετήσουμε συγκεκριμένους κώδικες. Παρατηρήστε ότι η υπόθεσή μας, σύμφωνα με την οποία δεν υπάρχει περίπτωση να χάνονται ή να δημιουργούνται ψηφία κατά τη διάρκεια της μετάδοσης, αποκλείει την αποκωδικοποίηση του «gub» σε «firetruck».

Παράδειγμα 1.3.1 Έστω ο κώδικας $C_1 = \{00, 01, 10, 11\}$. Κάθε λέξη που παραλαμβάνεται είναι κωδικολέξη και ο C_1 δεν μπορεί να ανιχνεύσει κάποιο λάθος. Επίσης, ο C_1 δεν διορθώνει λάθη, αφού κάθε παραληφθείσα λέξη δεν απαιτεί αλλαγές για να γίνει κωδικολέξη.

Παράδειγμα 1.3.2 Τροποποιούμε τον C_1 επαναλαμβάνοντας κάθε κωδικολέξη τρεις φορές. Ο νέος κώδικας είναι

$$C_2 = \{000000, 010101, 101010, 111111\}.$$

Αυτό είναι ένα παράδειγμα *επαναληπτικού* κώδικα (repetition code). Έστω τώρα ότι λαμβάνουμε την ακολουθία 110101. Επειδή δεν είναι κωδικολέξη, μπορούμε να ανιχνεύσουμε ότι έχει συμβεί τουλάχιστον ένα λάθος. Η κωδικολέξη 010101 μπορεί να σχηματιστεί με αλλαγή ενός ψηφίου, αλλά όλες οι άλλες κωδικολέξεις σχηματίζονται με αλλαγή περισσότερων ψηφίων. Συνεπώς, υποθέτουμε ότι η 010101 είναι η πιο πιθανή κωδικολέξη που μεταδόθηκε, άρα διορθώνουμε την 110101 σε 010101. (Μια κωδικολέξη που μπορεί να σχηματιστεί από μια λέξη w με αλλαγή ελάχιστου πλήθους ψηφίων αυτής ονομάζεται *κοντινότερη* κωδικολέξη· η ιδέα θα σχηματοποιηθεί αργότερα). Στην πραγματικότητα, αν μεταδοθεί οποιαδήποτε από τις κωδικολέξεις $c \in C_2$ και σημειωθεί ένα λάθος κατά την διάρκεια της μετάδοσης, τότε η μοναδική κοντινότερη κωδικολέξη της παραληφθείσας λέξης είναι η c· άρα, όταν έχουμε ένα μόνο εσφαλμένο ψηφίο, θα προκύψει μια λέξη που μπορεί εύκολα να διορθωθεί στην αρχική κωδικολέξη που μεταδόθηκε.

Παράδειγμα 1.3.3 Τροποποιούμε τον C_1 προσθέτοντας ένα τρίτο ψηφίο σε κάθε κωδικολέξη έτσι ώστε το πλήθος των άσων σε κάθε κωδικολέξη να είναι άρτιο. Ο κώδικας που προκύπτει είναι

$$C_3 = \{000, 011, 101, 110\}.$$

Το επιπλέον ψηφίο λέγεται ψηφίο *ελέγχου ισοτιμίας* (parity-check digit).[2] Ας υποθέσουμε ότι παραλαμβάνεται η ακολουθία 010· αφού δεν είναι μια κωδικολέξη, έχουμε ανιχνεύσει την εμφάνιση ενός λάθους. Καθεμία από τις κωδικολέξεις 110, 000 και 011 μπορεί να σχηματιστεί με την αλλαγή ενός ψηφίου της παραληφθείσας λέξης. Σε επόμενες ενότητες θα ξεχωρίσουμε τον τρόπο που χειριζόμαστε τις παραληφθείσες λέξεις που είναι κοντινότερες σε μια μοναδική κωδικολέξη (η οποία είναι η κωδικολέξη που έχει κατά πάσα πιθανότητα αποσταλεί), όπως ίσχυε στο Παράδειγμα 1.3.2, και τις παραληφθείσες λέξεις που είναι κοντινότερες σε πολλές κωδικολέξεις, όπως συμβαίνει σε τούτο εδώ το παράδειγμα. Είναι αρκετό σε αυτό το στάδιο να παρατηρήσουμε ότι φαίνεται πιο λογικό να διορθώσουμε την 010 σε μια από τις 110, 000, ή 011 παρά στην 101.

Ασκήσεις

1.3.4 Έστω C ο κώδικας που περιέχει όλες τις κωδικολέξεις μήκους 3. Αν παραληφθεί η 001, βρείτε ποια είναι η πιο πιθανή κωδικολέξη που έχει αποσταλεί.

1.3.5 Στις κωδικολέξεις του κώδικα στην Άσκηση 1.3.4, προσθέστε ένα ψηφίο ελέγχου ισοτιμίας και χρησιμοποιήστε τον κώδικα C που προκύπτει για να απαντήσετε στις παρακάτω ερωτήσεις.

(α) Αν λάβουμε την ακολουθία 1101, μπορούμε να ανιχνεύσουμε κάποιο λάθος;

(β) Αν λάβουμε την 1101, ποιες κωδικολέξεις είναι πιο πιθανό να έχουν μεταδοθεί;

(γ) Υπάρχει κάποια λέξη με μήκος 4 που δεν ανήκει στον κώδικα, αλλά είναι κοντινότερη σε μια μοναδική κωδικολέξη;

1.3.6 Επαναλάβετε κάθε κωδικολέξη του κώδικα C που ορίστηκε στην Άσκηση 1.3.4 τρεις φορές για να σχηματίσετε έναν επαναληπτικό κώδικα με μήκος 9. Βρείτε τις κοντινότερες κωδικολέξεις στις παρακάτω παραληφθείσες λέξεις:

(α) 001000001 (β) 011001011

(γ) 101000101 (δ) 100000010

[2] *Σ.τ.Μ.*: Ο όρος θα μπορούσε να αποδοθεί και ως *ψηφίο ελέγχου αρτιότητας*, αλλά χρησιμοποιούμε τον όρο όπως έχει καθιερωθεί στην ελληνική βιβλιογραφία.

1.3.7 Βρείτε το μέγιστο αριθμό κωδικολέξεων με μήκος $n = 4$ σε έναν κώδικα στον οποίο μπορεί να ανιχνευτεί κάθε μοναδικό λάθος (δηλαδή, ένα μόνο εσφαλμένο ψηφίο κατά την παραλαβή της κωδικολέξης).

1.3.8 Επαναλάβετε την Άσκηση 1.3.7 για $n = 5$, $n = 6$, και για οποιοδήποτε n.

1.4 Βαθμός πληροφορίας

Με βάση την τελευταία ενότητα, είναι φανερό ότι η προσθήκη νέων ψηφίων σε κωδικολέξεις μπορεί να βελτιώσει τις δυνατότητες διόρθωσης και ανίχνευσης λαθών του κώδικα. Ωστόσο, όσο μεγαλύτερο είναι το μήκος των κωδικολέξεων, τόσο περισσότερος χρόνος απαιτείται για τη μετάδοση κάθε μηνύματος. Ο *βαθμός πληροφορίας* (information rate) ή απλά *βαθμός* ενός κώδικα είναι ένας αριθμός που σχεδιάστηκε να μετράει το ποσοστό κάθε κωδικολέξης που μεταφέρει (δηλαδή περιέχει) το πραγματικό μήνυμα. Ο βαθμός πληροφορίας για έναν κώδικα C μήκους n ορίζεται (για δυαδικούς κώδικες) ως

$$\frac{1}{n}\log_2|C|.$$

Επειδή μπορούμε να υποθέσουμε ότι $1 \leq |C| \leq 2^n$, είναι φανερό ότι ο βαθμός πληροφορίας κυμαίνεται μεταξύ 0 και 1· είναι ίσος με 1 αν κάθε λέξη είναι μια κωδικολέξη, και ίσος με 0 αν ισχύει $|C| = 1$.

Για παράδειγμα, οι βαθμοί πληροφορίας για τους κώδικες C_1, C_2, και C_3 της προηγούμενης ενότητας, είναι 1, 1/3, και 2/3 αντίστοιχα. Καθένας από αυτούς τους βαθμούς φαίνεται να σχετίζεται λογικά με τους αντίστοιχους κώδικες, αφού μπορούμε να θεωρήσουμε ότι τα πρώτα 2 από τα 6 ψηφία σε κάθε κωδικολέξη του C_2 μεταφέρουν το μήνυμα, όπως και τα πρώτα 2 από τα 3 ψηφία σε κάθε κωδικολέξη του C_3.

Ασκήσεις

1.4.1 Βρείτε το βαθμό πληροφορίας για κάθε κώδικα στις Ασκήσεις 1.3.4, 1.3.5, και 1.3.6.

1.5 Τα αποτελέσματα της διόρθωσης και ανίχνευσης λαθών

Για να τονίσουμε τα πολύ θετικά αποτελέσματα που έχει η προσθήκη ενός ψηφίου ελέγχου ισοτιμίας στη δυνατότητα ενός κώδικα να ανιχνεύει λάθη, θεωρούμε τους παρακάτω κώδικες.

Ας υποθέσουμε ότι όλες οι 2^{11} λέξεις μήκους 11 είναι κωδικολέξεις· κατά συνέπεια, κανένα λάθος δεν πρόκειται να ανιχνευτεί. Έστω ότι η αξιοπιστία του κα-

ναλιού είναι $p = 1 - 10^{-8}$ και ότι τα ψηφία αποστέλλονται με ρυθμό 10^7 ψηφία ανά δευτερόλεπτο. Επομένως, η πιθανότητα εσφαλμένης μετάδοσης μιας λέξης είναι χονδρικά ίση με $11p^{10}(1-p)$, κατά προσέγγιση ίση με $11/10^8$. Άρα, περίπου

$$\frac{11}{10^8} \cdot \frac{10^7}{11} = 0.1 \text{ λέξεις ανά δευτερόλεπτο}$$

θα μεταδίδονται εσφαλμένα χωρίς να μπορούν να ανιχνευτούν. Δηλαδή μια ολόκληρη εσφαλμένη λέξη κάθε 10 δευτερόλεπτα, 6 λέξεις το λεπτό, 360 λέξεις την ώρα, ή 8640 λέξεις τη μέρα! Αυτό δεν είναι πολύ καλό.

Ας υποθέσουμε τώρα ότι εισάγουμε ένα ψηφίο ελέγχου ισοτιμίας σε κάθε κωδικολέξη, οπότε το πλήθος των άσων σε καθεμία από τις 2048 κωδικολέξεις είναι άρτιο. Κάθε λέξη με ένα λάθος θα ανιχνεύεται πάντα, άρα τουλάχιστον 2 λάθη θα πρέπει να εμφανιστούν σε κάποια λέξη ώστε αυτή να μεταδοθεί εσφαλμένα χωρίς να το αντιληφθούμε. Η πιθανότητα να εμφανιστούν τουλάχιστον δύο λάθη είναι ίση με $1 - p^{12} - 12p^{11}(1-p)$, δηλαδή κατά προσέγγιση ίση με $\binom{12}{2}p^{10}(1-p)^2$, το οποίο είναι περίπου $\frac{66}{10^{16}}$ για $p = 1 - 10^{-8}$. Άρα, $\frac{66}{10^{16}} \cdot \frac{10^7}{12} = 5.5 \times 10^{-9}$ λέξεις ανά δευτερόλεπτο θα μεταδίδονται εσφαλμένα χωρίς να ανιχνεύονται. Αυτό σημαίνει ένα σφάλμα κάθε 2000 μέρες!

Αν είμαστε πρόθυμοι να ελαττώσουμε το βαθμό πληροφορίας επιμηκύνοντας τον κώδικα από 11 σε 12, είναι πολύ πιθανό να ανακαλύπτουμε τα λάθη. Για να αποφασίσουμε αν αυτά τα λάθη συνέβησαν πραγματικά, ίσως χρειαστεί να ζητήσουμε την επαναμετάδοση του μηνύματος. Από φυσικής άποψης, αυτό σημαίνει ότι η μετάδοση πρέπει να καθυστερήσει μέχρι να λάβουμε την επιβεβαίωση, ή ότι τα μηνύματα πρέπει να αποθηκεύονται προσωρινά μέχρι να απαιτήσουμε επαναμετάδοση· και οι δύο περιπτώσεις μπορεί να έχουν υψηλό κόστος σε χρόνο ή αποθηκευτικό χώρο. Υπάρχουν βέβαια και οι περιπτώσεις που η επαναμετάδοση είναι αδύνατη, όπως για παράδειγμα στην αποστολή του Voyager, καθώς και όταν χρησιμοποιούμε CD. Επομένως, αξίζει να ενσωματώνουμε δυνατότητες διόρθωσης λαθών μέσα στον κώδικα, παρά την περαιτέρω αύξηση του μήκους των λέξεων. Αυτές οι δυνατότητες μπορεί να δυσκολέψουν την κωδικοποίηση και αποκωδικοποίηση, αλλά θα μας βοηθήσουν να αποφύγουμε το κρυφό κόστος σε χρόνο ή αποθηκευτικό χώρο που προαναφέραμε.

Ένας απλός τρόπος για να ενσωματώσουμε τη διόρθωση λαθών είναι να φτιάξουμε έναν επαναληπτικό κώδικα στον οποίο κάθε κωδικολέξη μεταδίδεται τρεις φορές διαδοχικά. Οπότε, αν υποθέσουμε ότι το πολύ ένα εσφαλμένο ψηφίο εμφανίζεται σε κάθε κωδικολέξη των 33 ψηφίων, τότε δύο τουλάχιστον από τις τρεις επαναλήψεις θα είναι σωστές. Επειδή οι συγκρίσεις των τριών εντεκαψήφιων λέξεων είναι σχετικά εύκολη διαδικασία, το μοναδικό μειονέκτημα είναι η μείωση του βαθμού πληροφορίας από 1 σε 1/3.

Όμως, το 1/3 είναι μόνο 1/3. Ίσως υπάρχει καλύτερος τρόπος. Παρακάτω θα δούμε ότι είναι δυνατόν να διορθώνουμε κάθε μοναδικό εσφαλμένο ψηφίο εισάγοντας 4 μόνο επιπλέον ψηφία σε κάθε κωδικολέξη των 11 ψηφίων. Ο κώδικας που παράγεται έχει βαθμό πληροφορίας ίσο με 11/15· η βελτίωση είναι σημαντική, με την προϋπόθεση ότι τα πρόσθετα κόστη κωδικοποίησης και αποκωδικοποίησης δεν είναι απαγορευτικά.

Συνεπώς, η αποστολή μας είναι να σχεδιάζουμε κώδικες με λογικούς βαθμούς πληροφορίας, χαμηλό κόστος κωδικοποίησης και αποκωδικοποίησης, και συγκεκριμένες δυνατότητες διόρθωσης ή ανίχνευσης λαθών ώστε να μην απαιτείται επαναμετάδοση του μηνύματος.

1.6 Εύρεση της πιο πιθανής κωδικολέξης που μεταδόθηκε

Ας υποθέσουμε ότι έχουμε μια συνολική αντίληψη της διαδικασίας μετάδοσης, γνωρίζοντας τόσο την κωδικολέξη v που έχει αποσταλεί όσο και τη λέξη w που παραλαμβάνεται. Για δεδομένες κωδικολέξεις v και w, έστω ότι $\phi_p(v, w)$ είναι η πιθανότητα να παραληφθεί η λέξη w, αν η κωδικολέξη v αποσταλεί μέσω ενός ΔΣΚ με αξιοπιστία p. Αφού υποθέτουμε ότι ο θόρυβος κατανέμεται τυχαία, μπορούμε να μεταχειριστούμε τη μετάδοση κάθε ψηφίου ως ανεξάρτητο γεγονός. Άρα, αν οι v και w διαφωνούν σε d ψηφία, τότε $n-d$ ψηφία έχουν μεταδοθεί σωστά και d ψηφία έχουν μεταδοθεί εσφαλμένα, συνεπώς

$$\phi_p(v, w) = p^{n-d}(1-p)^d.$$

Παράδειγμα 1.6.1 Έστω C ένας κώδικας μήκους 5. Τότε για κάθε κωδικολέξη v στο C, η πιθανότητα να παραληφθεί σωστά η v είναι

$$\phi_p(v, v) = p^5.$$

Έστω ότι η κωδικολέξη 10101 ανήκει στον C. Τότε

$$\phi_p(10101, 01101) = p^3(1-p)^2$$

και αν $p = 0.9$, τότε

$$\phi_{0.9}(10101, 01101) = (0.9)^3(0.1)^2 = 0.00729.$$

Ασκήσεις

1.6.2 Υπολογίστε τη $\phi_{0.97}(v, w)$ για καθένα από τα παρακάτω ζεύγη των v και w:

(α) $v = 01101101, w = 10001110$ (β) $v = 1110101, w = 1110101$

(γ) $v = 00101, w = 11010$ (δ) $v = 00000, w = 00000$

(ε) $v = 1011010, w = 0000010$ (στ) $v = 10110, w = 01001$

(ζ) $v = 111101, w = 000010$.

Στην πράξη, γνωρίζουμε τη λέξη w που παραλαμβάνεται, αλλά δεν ξέρουμε την κωδικολέξη v που έχει πραγματικά αποσταλεί. Ωστόσο, κάθε κωδικολέξη v προσδιορίζει μια αντιστοίχιση πιθανοτήτων $\phi_p(v, w)$ για τις λέξεις w. Κάθε τέτοια αντιστοίχιση είναι ένα μαθηματικό μοντέλο και επιλέγουμε το μοντέλο (δηλαδή την κωδικολέξη v) που συμφωνεί περισσότερο με την παρατήρηση — σε αυτή την περίπτωση, εκείνη για την οποία η παραληφθείσα λέξη καθίσταται η πιο πιθανή. Δηλαδή, υποθέτουμε ότι η v έχει αποσταλεί όταν παραληφθεί η w αν ισχύει

$$\phi_p(v, w) = \max\{\phi_p(u, w) : u \in C\}.$$

Το παρακάτω θεώρημα παρέχει ένα απλό κριτήριο για την εύρεση μιας τέτοιας κωδικολέξης v.

Θεώρημα 1.6.3 *Ας υποθέσουμε ότι έχουμε ένα ΔΣΚ με $1/2 < p < 1$. Έστω v_1 και v_2 δύο κωδικολέξεις και w μια λέξη, όλες με μήκος n. Υποθέτουμε ότι οι v_1 και w διαφωνούν σε d_1 θέσεις (ψηφία), και οι v_2 και w σε d_2 θέσεις. Τότε:*

$$\phi_p(v_1, w) \le \phi_p(v_2, w) \text{ αν και μόνο αν } d_1 \ge d_2.$$

Απόδειξη: Έχουμε ήδη αποδείξει ότι $\phi_p(v_1, w) \le \phi_p(v_2, w)$ ανν $p^{n-d_1}(1-p)^{d_1} \le p^{n-d_2}(1-p)^{d_2}$ ανν $(\frac{p}{1-p})^{d_2-d_1} \le 1$ ανν $d_2 \le d_1$ (αφού ισχύει $\frac{p}{1-p} > 1$). □

Η παραπάνω απόδειξη ορίζει τυπικά τη διαδικασία διόρθωσης λέξεων που είχαμε υιοθετήσει μέχρι τώρα ως μια ενστικτωδώς λογική διαδικασία: διορθώνουμε τη λέξη w στην κωδικολέξη που διαφωνεί με τη w σε όσο το δυνατόν λιγότερες θέσεις, αφού μια τέτοια κωδικολέξη είναι εκείνη που έχει κατά πάσα πιθανότητα αποσταλεί, δεδομένου ότι λάβαμε τη w.

Παράδειγμα 1.6.4 Αν η λέξη $w = 00110$ παραληφθεί μέσω ενός ΔΣΚ με $p = 0.98$, ποια από τις κωδικολέξεις 01101, 01001, 10100, 10101 είναι πιθανότερο να έχει αποσταλεί;

v	d (πλήθος διαφορετικών ψηφίων με τη w)	
01101	3	
01001	4	
10100	2	← το μικρότερο d
10101	3	

Με χρήση του παραπάνω πίνακα και σύμφωνα με το Θεώρημα 1.6.3, η 10100 είναι η πιο πιθανή λέξη που έχει αποσταλεί. Σημειώστε ότι δεν είναι ανάγκη να γνωρίζουμε την ακριβή τιμή της αξιοπιστίας p για να εφαρμόσουμε το Θεώρημα 1.6.3· το μόνο που πρέπει να γνωρίζουμε είναι ότι $p > 1/2$.

Ασκήσεις

1.6.5 Έστω ότι παραλαμβάνεται η λέξη $w = 0010110$ μέσω ΔΣΚ με αξιοπιστία $p = 0.90$. Ποια από τις ακόλουθες κωδικολέξεις είναι πιο πιθανό να έχει αποσταλεί;

$$1001011, 1111100, 0001110, 0011001, 1101001.$$

1.6.6 Ποια από τις 8 κωδικολέξεις του κώδικα στην Άσκηση 1.3.6 είναι πιθανότερο να έχει αποσταλεί αν παραληφθεί η $w = 101000101$;

1.6.7 Αν $C = \{01000, 01001, 00011, 11001\}$ και παραληφθεί η λέξη $w = 10110$, ποια κωδικολέξη είναι πιο πιθανό να έχει αποσταλεί;

1.6.8 Επαναλάβετε την Άσκηση 1.6.7, αφού αντικαταστήσετε τον C με $\{010101, 110110, 101101, 100110, 011001\}$ και τη w με 101010.

1.6.9 Ποια από τις κωδικολέξεις $110110, 110101, 000111, 100111, 101000$ είναι πιθανότερο να έχει αποσταλεί αν παραληφθεί η $w = 011001$;

1.6.10 Στο Θεώρημα 1.6.3 υποθέτουμε ότι $1/2 < p < 1$. Τι θα αλλάξει στη διατύπωση του Θεωρήματος 1.6.3, αν αντικαταστήσουμε αυτή την υπόθεση με

(α) $0 < p < 1/2$, (β) $p = 1/2$;

1.7 Στοιχεία βασικής άλγεβρας

Ένα πρόβλημα στο οποίο θα πρέπει να στρέψουμε την προσοχή μας είναι να ανακαλύψουμε έναν αποδοτικό τρόπο για να βρίσκουμε την κωδικολέξη που είναι κοντινότερη σε οποιαδήποτε παραληφθείσα λέξη. Αν ο κώδικας έχει πάρα πολλές κωδικολέξεις, τότε δεν είναι πρακτικό να συγκρίνουμε κάθε παραληφθείσα λέξη w με κάθε κωδικολέξη διαδοχικά για να βρούμε ποια κωδικολέξη συμφωνεί περισσότερο με τη w. Για παράδειγμα, αν ο κώδικας περιέχει 2^{12} κωδικολέξεις (όπως στην αποστολή του Voyager), τότε μια τέτοια διαδικασία αποκωδικοποίησης δεν θα μπορούσε ποτέ να συμβαδίσει με την εισερχόμενη πληροφορία. Για να ξεπεράσουμε αυτό το πρόβλημα, πρέπει να εισαγάγουμε κάποια δομή στους κώδικες.

Έστω $K = \{0, 1\}$ και έστω K^n το σύνολο όλων των δυαδικών λέξεων με μήκος n. Ορίζουμε τη (δυαδική) πρόσθεση και το (δυαδικό) πολλαπλασιασμό στοιχείων του K ως εξής:

$$0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0$$
$$0 \cdot 0 = 0, 1 \cdot 0 = 0, 0 \cdot 1 = 0, 1 \cdot 1 = 1.$$