Θεωρία Πληροφορίας και Κωδικοποίησης

Σημείωση

Το ΕΑΠ είναι υπεύθυνο για την επιμέλεια έκδοσης και την ανάπτυξη των κειμένων σύμφωνα με τη Μεθοδολογία της εξ Αποστάσεως Εκπαίδευσης. Για την επιστημονική αρτιότητα και πληρότητα των συγγραμμάτων την αποκλειστική ευθύνη φέρουν οι συγγραφείς, κριτικοί αναγνώστες και ακαδημαϊκοί υπεύθυνοι που ανέλαβαν το έργο αυτό.

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
Σχολή Θετικών Επιστημών και Τεχνολογίας

Πρόγραμμα Σπουδών
ΠΛΗΡΟΦΟΡΙΚΗ

Θεματική Ενότητα
ΒΑΣΙΚΑ ΖΗΤΗΜΑΤΑ ΔΙΚΤΥΩΝ Η/Υ

Τόμος Α'

Θεωρία Πληροφορίας και Κωδικοποίησης

ΒΑΣΙΛΕΙΟΣ ΖΟΡΚΑΔΗΣ
Διδάκτωρ Πληροφορικής, Ηλεκτρολόγος Μηχανικός

ΠΑΤΡΑ 2002

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Θετικών Επιστημών και Τεχνολογίας

Πρόγραμμα Σπουδών
ΠΛΗΡΟΦΟΡΙΚΗ

Θεματική Ενότητα
ΒΑΣΙΚΑ ΖΗΤΗΜΑΤΑ ΔΙΚΤΥΩΝ Η/Υ

Τόμος Α'
Θεωρία Πληροφορίας και Κωδικοποίησης

Συγγραφή
ΒΑΣΙΛΕΙΟΣ ΖΟΡΚΑΔΗΣ
Διδάκτωρ Πληροφορικής, Ηλεκτρολόγος Μηχανικός

Κριτική Ανάγνωση
ΜΑΡΙΟΣ ΜΑΥΡΟΝΙΚΟΛΑΣ
Επίκουρος Καθηγητής Τμήματος Πληροφορικής
Πανεπιστημίου Κύπρου

Ακαδημαϊκός Υπεύθυνος για την επιστημονική επιμέλεια του τόμου
ΠΑΥΛΟΣ ΣΠΥΡΑΚΗΣ
Καθηγητής Τμήματος Μηχανικών Η/Υ & Πληροφορικής Πανεπιστημίου Πατρών

Επιμέλεια στη μέθοδο της εκπαίδευσης από απόσταση
ΙΩΑΝΝΗΣ ΚΟΥΤΣΟΝΙΚΟΣ

Γλωσσική Επιμέλεια
ΡΩΞΑΝΗ ΚΑΤΣΗ

Τεχνική Επιμέλεια
TYPORAMA

Καλλιτεχνική Επιμέλεια, Σελιδοποίηση
TYPORAMA

Συντονισμός ανάπτυξης εκπαιδευτικού υλικού και γενική επιμέλεια των εκδόσεων
ΟΜΑΔΑ ΕΚΤΕΛΕΣΗΣ ΕΡΓΟΥ ΕΑΠ / 2002

ISBN: 960–538–453–1
Κωδικός Έκδοσης: ΠΛΗ 22/1

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 2

Πηγές Πληροφορίας

ΕΦΑΛΑΙΟ 3

Κανάλια Επικοινωνίας

ΚΕΦΑΛΑΙΟ 5

Κρυπτογραφία και Θεωρία Πληροφορίας

Πρόλογος

Η Θεωρία Πληροφορίας είναι το επιστημονικό πεδίο που ασχολείται με τα μέτρα και τις εφαρμογές της έννοιας της «πληροφορίας». Απαντά, κατά βάση, σε δύο θεμελιώδεις ερωτήσεις: Ποια είναι η μεγαλύτερη δυνατή συμπίεση δεδομένων και ποιος ο μέγιστος δυνατός ρυθμός μετάδοσης σε ένα επικοινωνιακό κανάλι; Όριο της συμπίεσης δεδομένων αποτελεί η μέση ποσότητα πληροφορίας (ή εντροπία), ενώ όριο του ρυθμού μετάδοσης σε ένα κανάλι αποτελεί η χωρητικότητά του. Η Θεωρία Κωδικοποίησης είναι η μελέτη μεθόδων για την αποτελεσματική και ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό. Περαιτέρω, λαμβάνοντας υπόψη και απαιτήσεις εμπιστευτικής μεταφοράς της πληροφορίας, μπορούμε να συμπεριλάβουμε στη Θεωρία Κωδικοποίησης και κρυπτογραφικές μεθόδους.

Το πεδίο της Θεωρίας Πληροφορίας και Κωδικοποίησης, όπως το οριοθετήσαμε ανωτέρω, είναι πολύ ευρύ για να παρουσιαστεί στον τόμο αυτό των 200 περίπου σελίδων. Έτσι, αν και κατεβλήθη προσπάθεια να συμπεριληφθούν τα πλέον βασικά ζητήματα, κατέστη αναπόφευκτη η μη κάλυψη ορισμένων θεμάτων, όπως για παράδειγμα των πρότυπων σχημάτων συμπίεσης JPEG και MPEG, των οποίων η παρουσίαση θα απαιτούσε κείμενα σχετικά μεγάλης έκτασης. Ωστόσο, ο αλγόριθμος κωδικοποίησης του Huffman, που αποτελεί τη βάση των σχημάτων αυτών, παρουσιάζεται επαρκώς στο παρόν βιβλίο. Επίσης, το ραγδαία αναπτυσσόμενο πεδίο της Κρυπτογραφίας δεν ήταν δυνατό καλυφθεί σε ικανοποιητικό βαθμό, παρά μόνον από τη σκοπιά της ασφάλειας κρυπτογραφικών συστημάτων που σχετίζεται με τη Θεωρία Πληροφορίας. Βέβαια, στην Κρυπτογραφία είναι αφιερωμένος ειδικός τόμος στο πλαίσιο της Θεματικής Ενότητας «Προστασία και Ασφάλεια Συστημάτων Υπολογιστών».

Η δημιουργία ενός ευανάγνωστου κειμένου υπήρξε βασικός γνώμονας του τρόπου παρουσίασης της ύλης, κατά τη συγγραφή του βιβλίου αυτού. Προσπάθησα να αποφύγω ένα κείμενο μαθηματικά αυστηρό μεν, αλλά αρκετά δυσνόητο. Επίσης, προσπάθησα να βοηθήσω τον αναγνώστη, συμπεριλαμβάνοντας σύντομες αναδρομές σε μαθηματικά θέματα, στα σημεία που απαιτείται για την κατανόηση της ύλης. Ελπίζω, το αποτέλεσμα της προσπάθειας αυτής να είναι πράγματι ένα «φιλικό» κείμενο, παρόλο που το αντικείμενο το βιβλίου είναι σχετικά «βαρύ».

Το βιβλίο αποτελείται από πέντε κεφάλαια. Το πρώτο κεφάλαιο μας εισάγει στο συντακτικό, το σημασιολογικό και τον πραγματικό τύπο πληροφορίας, στον ορισμό

του μέτρου ποσότητας πληροφορίας που διατυπώθηκε από τον Hartley, σε ένα στοιχειώδες επικοινωνιακό μοντέλο καθώς και ένα λεπτομερές, που αποτελούν το πλαίσιο μέσα στο οποίο παρουσιάζονται οι βασικές αρχές και έννοιες της Θεωρίας Πληροφορίας. Επίσης, μας υπενθυμίζει, πολύ συνοπτικά, βασικά στοιχεία από τη Θεωρία Πιθανοτήτων και μας εισάγει στο μέτρο ποσότητας πληροφορίας του Shannon καθώς και στην επέκτασή του για την περίπτωση πληροφορίας που εκφράζεται ως συνδυασμός δύο τυχαίων μεταβλητών.

Το δεύτερο κεφάλαιο αφιερώνεται στις πηγές πληροφορίας. Πιο συγκεκριμένα, στο κεφάλαιο αυτό περιγράφονται οι διακριτές πηγές πληροφορίας χωρίς μνήμη και τεχνικές κωδικοποίησης γι' αυτές τις πηγές καθώς και οι διακριτές πηγές πληροφορίας με μνήμη και σχετικές τεχνικές κωδικοποίησης. Επίσης, επεκτείνεται ο ορισμός του μέτρου της ποσότητας πληροφορίας στην περίπτωση συνεχούς τυχαίας μεταβλητής και περιγράφονται συνεχείς πηγές πληροφορίας.

Το τρίτο κεφάλαιο πραγματεύεται ζητήματα σχετικά με τα επικοινωνιακά κανάλια. Αφιερώνεται στα διακριτά κανάλια επικοινωνίας και ειδικότερα στη χωρητικότητα και στο ρυθμό μετάδοσης διακριτών καναλιών με μνήμη και χωρίς μνήμη καθώς και στη διατύπωση του θεωρήματος κωδικοποίησης. Επίσης, αφιερώνεται σε αντίστοιχα ζητήματα των συνεχών καναλιών επικοινωνίας.

Το τέταρτο κεφάλαιο ασχολείται με ζητήματα κωδικοποίησης ελέγχου σφάλματος, δηλαδή με την περιγραφή του τρόπου κατασκευής καθώς και της συμπεριφοράς κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων. Ειδικότερα, το κεφάλαιο αυτό παρουσιάζει βασικές αρχές, έννοιες και παραδοχές σχετικά με τους διάφορους τύπους κωδίκων ελέγχου σφάλματος και εξετάζει γραμμικούς κώδικες, κυκλικούς κώδικες, συμπεριλαμβανομένων των κωδίκων BCH και θίγει πολύ συνοπτικά τους κώδικες Reed – Solomon, διόρθωσης καταιγισμών σφαλμάτων και συνελικτικούς κώδικες.

Το πέμπτο κεφάλαιο, τέλος, αναφέρεται σε θέματα προστασίας της πληροφορίας κατά την αποθήκευση και μεταφορά της μέσω του επικοινωνιακού καναλιού. Ειδικότερα, παρουσιάζονται συνοπτικά έννοιες της Κρυπτογραφίας και Κρυπτανάλυσης, τύποι κρυπταναλυτικών επιθέσεων καθώς και ορισμένες κλασικές κρυπτογραφικές τεχνικές και τα σύγχρονα ασύμμετρα κρυπτογραφικά συστήματα RSA και ElGamal. Κυρίως, όμως, εξετάζονται ζητήματα ασφαλείας κρυπτογραφικών συστημάτων από τη σκοπιά της Θεωρίας Πληροφορίας, αλλά και από τη σκοπιά της Θεωρίας Πολυπλοκότητας.

Θα ήθελα να ευχαριστήσω όλους όσοι συνέβαλαν με τον ένα ή τον άλλο τρόπο στην ολοκλήρωση αυτού του βιβλίου. Ιδιαίτερα, θα ήθελα να ευχαριστήσω τον Ακαδη-

μαϊκό Υπεύθυνο καθ. Παύλο Σπυράκη, τον Κριτικό Αναγνώστη καθ. Μάριο Μαυρονικόλα και τον Υπεύθυνο της ΟΕΕ κ. Γιάννη Κουτσονίκο για τις πολύτιμες και εποικοδομητικές παρατηρήσεις και σχόλιά τους. Επίσης, θα ήθελα να ευχαριστήσω την κα Δήμητρα Παρασκευοπούλου, συντονίστρια του προγράμματος σπουδών Πληροφορικής, τη φιλόλογο κα Ρωξάνη Κατσή για τη γλωσσική επιμέλεια καθώς και το Typorama για την καλλιτεχνική επιμέλεια.

Οι όποιες παραλήψεις και λάθη βαρύνουν τον συγγραφέα και μόνον και γι' αυτά παρακαλώ για την κατανόησή σας. Θα εκτιμούσα ιδιαίτερα τη συνεισφορά σας για τον εντοπισμό και τη διόρθωσή τους.

Βασίλης Ζορκάδης

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή στη Θεωρία Πληροφορίας

Σκοπός

Ο σκοπός του κεφαλαίου αυτού είναι να γνωρίσουμε, πρώτα, την εξέλιξη της Θεωρίας Πληροφορίας και στη συνέχεια, μέσα στο πλαίσιο ενός μοντέλου επικοινωνίας και με τη βοήθεια της Θεωρίας Πιθανοτήτων, τις βασικές αρχές και έννοιες αυτής.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *διακρίνετε μεταξύ των τριών διαφορετικών τύπων πληροφορίας,*
- *αναφέρετε δύο σημαντικές επιστημονικές συμβολές στην ανάπτυξη της Θεωρίας Πληροφορίας,*
- *περιγράφετε και εξηγείτε αρχές και έννοιες της Θεωρίας Πληροφορίας,*
- *περιγράφετε και εξηγείτε τα διάφορα μέτρα ποσότητας πληροφορίας.*

Έννοιες κλειδιά

- *συντακτική πληροφορία,*
- *σημασιολογική πληροφορία,*
- *πραγματική πληροφορία,*
- *επικοινωνιακό μοντέλο,*
- *πηγή και προορισμός πληροφορίας,*
- *κωδικοποίηση και αποκωδικοποίηση πηγής,*
- *απαλοιφή και επανακατασκευή δεδομένων,*
- *συμπίεση και αποσυμπίεση δεδομένων,*
- *κρυπτογράφηση και αποκρυπτογράφηση,*
- *κωδικοποίηση και αποκωδικοποίηση καναλιού,*
- *διαμόρφωση και αποδιαμόρφωση,*
- *θόρυβος,*
- *μέτρο ποσότητας πληροφορίας*

Εισαγωγικές παρατηρήσεις

Το κεφάλαιο αυτό αποτελείται από πέντε ενότητες. Στην πρώτη περιγράφονται οι τρεις τύποι πληροφορίας: ο συντακτικός, ο σημασιολογικός και ο πραγματικός, δίνεται ο

ορισμός του μέτρου ποσότητας πληροφορίας που διατυπώθηκε από τον Hartley και θίγεται η συμβολή του Shannon στην ανάπτυξη της σύγχρονης Θεωρίας Πληροφορίας. Στη δεύτερη ενότητα περιγράφεται ένα στοιχειώδες επικοινωνιακό μοντέλο, καθώς και ένα λεπτομερές, που αποτελούν το πλαίσιο μέσα στο οποίο παρουσιάζονται βασικές αρχές και έννοιες της Θεωρίας Πληροφορίας. Στην τρίτη ενότητα περιγράφονται, πολύ συνοπτικά, βασικά στοιχεία από τη Θεωρία Πιθανοτήτων. Στην τέταρτη ενότητα περιγράφεται το μέτρο ποσότητας πληροφορίας του Shannon και παρατίθενται παραδείγματα υπολογισμού αυτής. Τέλος, στην πέμπτη ενότητα επεκτείνεται ο ορισμός του μέτρου ποσότητας πληροφορίας του Shannon για την περίπτωση πληροφορίας που εκφράζεται ως συνδυασμός δύο τυχαίων μεταβλητών.

1.1 Η εξέλιξη της Θεωρίας Πληροφορίας

Θεωρία Πληροφορίας είναι το πεδίο εκείνο που ασχολείται με την έννοια της «πληροφορίας», τα μέτρα και τις εφαρμογές της.

Πιο συγκεκριμένα, στα θέματα που απασχολούν τη Θεωρία Πληροφορίας συγκαταλέγονται η ποσότητα συντακτικής πληροφορίας (ή εντροπία) και οι μονάδες μέτρησης αυτής, η ροή πληροφορίας σε κανάλια και τα θεμελιώδη όρια της ποσότητας πληροφορίας που μπορούν να μεταδοθούν, δηλαδή η χωρητικότητα καναλιών, που αποτελεί το μέγιστο δυνατό ρυθμό μετάδοσης. Ακόμα, θέματα που απασχολούν είναι η κατασκευή συστημάτων επεξεργασίας και επικοινωνίας πληροφορίας που μπορούν να προσεγγίσουν αυτά τα ανωτέρω όρια κ.ά.

1.1.1 Τύποι πληροφορίας

Η **συντακτική** πληροφορία σχετίζεται με τα σύμβολα και τις σχέσεις μεταξύ αυτών, από τα οποία αποτελούνται τα μηνύματα. Η **σημασιολογική** πληροφορία σχετίζεται με τη σημασία και η **πραγματική** με τη χρήση και τη δυνατή επίπτωση των μηνυμάτων. Έτσι, ενώ ο συντακτικός τύπος της πληροφορίας αναφέρεται στη μορφή, ο σημασιολογικός και ο πραγματικός αναφέρονται στο περιεχόμενο. Ας εξετάσουμε, στη συνέχεια, τις ακόλουθες προτάσεις για να αποσαφηνίσουμε αυτές τις έννοιες.

1. Η Άννα πήγε με ψαρόβαρκα από το λιμάνι της Πάργας στο Χρυσογυάλι.
2. Η ψαρόβαρκα μετέφερε την Άννα από το λιμάνι της Πάργας στο Χρυσογυάλι.
3. Στα ελληνικά πελάγη πνέουν άνεμοι ισχύος 5 – 9 μποφόρ.
4. Στο Ιόνιο πέλαγος πνέουν άνεμοι ισχύος 5 – 6 μποφόρ, στο ΒΑ Αιγαίο 6 – 7 μποφόρ, στο Ν. Αιγαίο 8 – 9 μποφόρ και στο Κρητικό πέλαγος 7 – 8 μποφόρ.

Οι δύο πρώτες προτάσεις διαφοροποιούνται ως προς τη σύνταξη και είναι ταυτόσημες ως προς τη σημασία, προσφέρουν δηλαδή την ίδια πληροφόρηση. Αντίθετα, οι δύο τελευταίες προτάσεις διαφέρουν όχι μόνο ως προς τη σύνταξη αλλά και ως προς το περιεχόμενο. Η τέταρτη πρόταση είναι πιο ακριβής από την τρίτη, προσφέρει επομένως περισσότερη πληροφόρηση. Η πραγματική διάσταση της πληροφορίας εξαρτάται κυρίως από το δεδομένο γενικό πλαίσιο. Δηλαδή, η σημασία της τρίτης και της τέταρτης πρότασης είναι σημαντική και ενδιαφέρουσα για όσους βρίσκονται στην Ελλάδα και όχι για κάποιους που βρίσκονται στην Αυστραλία. Ιδιαίτερα, η ακρίβεια της τέταρτης πρότασης μπορεί να καθορίσει επιλογές των ναυτιλλομένων στα ελληνικά πελάγη.

Όπως θα δούμε στη συνέχεια, η Θεωρία Πληροφορίας αναφέρεται στη συντακτική

πληροφορία, δηλαδή η πληροφορία εξαρτάται από την πιθανότητα εμφάνισης των μηνυμάτων και όχι από τη σημασία τους.

1.1.2 Το μέτρο ποσότητας πληροφορίας του Hartley

Καθοριστική συμβολή στην ανάπτυξη της Θεωρίας Πληροφορίας είχαν οι Shannon και Wiener. Ιδιαίτερα ο πρώτος θεωρείται ως ο πατέρας αυτής, θέτοντας τις βάσεις της με το επιστημονικό του άρθρο «A mathematical theory of communication», το 1948.

Του άρθρου του Shannon προηγήθηκε η προσπάθεια του Hartley να ορίσει ένα «μέτρο ποσότητας πληροφορίας». Σύμφωνα με την πρόταση του Hartley, η «ποσότητα πληροφορίας» διαμορφώνεται από τη διαδοχική επιλογή συμβόλων ή λέξεων από ένα δεδομένο σύνολο. Ας υποθέσουμε ότι σχηματίζουμε λέξεις ή μηνύματα αποτελούμενα από v σύμβολα από ένα αλφάβητο N συμβόλων. Τότε μπορούμε να επιλέξουμε N^v διαφορετικές λέξεις.

Ποσότητα πληροφορίας

Ο Hartley όρισε την ποσότητα πληροφορίας (ή πληροφορικό περιεχόμενο) ως το δεκαδικό λογάριθμο του πλήθους των διαφορετικών λέξεων που μπορούν να σχηματιστούν, αποτελούμενες από ένα δεδομένο πλήθος συμβόλων. Στην περίπτωση μηνυμάτων μήκους κ συμβόλων από ένα αλφάβητο με N σύμβολα, η ποσότητα πληροφορίας είναι ίση με

$$H(N^k) = \log(N^k) = k \log N.$$

Για μηνύματα μήκους 1 συμβόλου, από το ανωτέρω αλφάβητο, η ποσότητα πληροφορίας είναι

$$H(N^1) = \log(N).$$

Οι ανωτέρω σχέσεις ανταποκρίνονται στη διαίσθησή μας ότι η ποσότητα πληροφορίας ενός μηνύματος αποτελούμενου από κ σύμβολα θα πρέπει να είναι κ φορές μεγαλύτερη από αυτή ενός μηνύματος που αποτελείται από 1 σύμβολο. Αυτός είναι, άλλωστε, ο λόγος που επελέγη η λογαριθμική συνάρτηση στον ορισμό της ποσότητας πληροφορίας, αφού πληροί τη σχέση

$$f(x^y) = yf(x).$$

Με βάση του λογάριθμου το 10, η μονάδα της ποσότητας πληροφορίας είναι η decit (decimal unit) ή Hartley. Αν χρησιμοποιήσουμε φυσικό λογάριθμο, η μονάδα είναι

το *nat* (natural unit). Εξετάζοντας ως παράδειγμα το σχηματισμό μηνυμάτων μήκους ενός συμβόλου από ένα αλφάβητο αποτελούμενο από 10 σύμβολα, η ποσότητα πληροφορίας κάθε μηνύματος είναι ίση με

$$H(N^1) = \log_{10} 10 = 1 \text{ decit.}$$

Με βάση του λογάριθμου το 2, η μονάδα της ποσότητας πληροφορίας καλείται bit (binary unit). Αν τώρα εξετάσουμε ως παράδειγμα το σχηματισμό μηνυμάτων μήκους ενός συμβόλου από ένα αλφάβητο αποτελούμενο από δύο σύμβολα, τότε η ποσότητα πληροφορίας είναι

$$H(N^1) = \log_2 N = \log_2 2 = 1 \text{ bit.}$$

Δραστηριότητα 1.1

Προσπαθήστε να περιγράψετε την ποσότητα πληροφορίας του Hartley. Αν δεν τα καταφέρετε, μελετήστε και πάλι το αντίστοιχο τμήμα αυτής της ενότητας.

Άσκηση αυτοαξιολόγησης 1.1

Θεωρούμε ότι έχουμε ένα αλφάβητο αποτελούμενο από 32 σύμβολα. Από αυτό το αλφάβητο σχηματίζουμε μηνύματα μήκους 2 συμβόλων. Να υπολογιστεί η ποσότητα πληροφορίας των μηνυμάτων σε μονάδες decit και bit.

Ο Hartley επηρεάστηκε από το νόμο που, σχεδόν ταυτόχρονα, είχαν διατυπώσει ο Nyquist στις Ηνωμένες Πολιτείες της Αμερικής και ο Kupfmuller στη Γερμανία, το 1924. Σύμφωνα με αυτό το νόμο, η μετάδοση σημάτων τηλεγράφου σ' ένα δεδομένο ρυθμό απαιτεί ένα καθορισμένο εύρος συχνοτήτων. Ο Hartley στον ορισμό του δε διακρίνει διαφορετικές πιθανότητες για τα σύμβολα που απαρτίζουν το αλφάβητο, θεωρεί την επιλογή καθενός εξ αυτών κατά το σχηματισμό ενός μηνύματος ως ίσης πιθανότητας γεγονός.

Αντίθετα, ο Shannon εισήγαγε την έννοια της πιθανότητας στον ορισμό της ποσότητας πληροφορίας και έθεσε τις βάσεις της σύγχρονης Θεωρίας Πληροφορίας. Η επιλογή κάθε συμβόλου συνδέεται με κάποια, στη γενική περίπτωση, διαφορετική πιθανότητα. Έτσι, ο ορισμός του Hartley είναι μια ειδική περίπτωση του ορισμού του Shannon για την ποσότητα πληροφορίας.

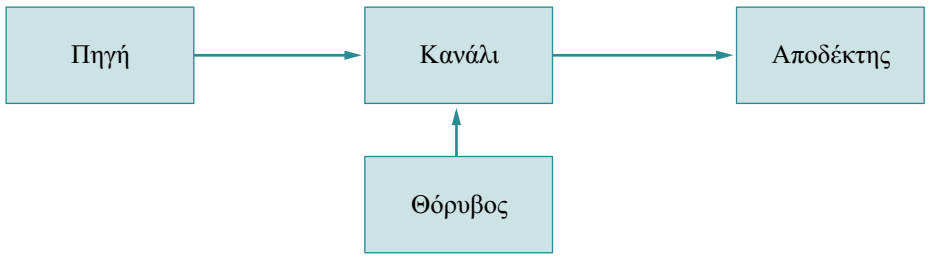
1.2 Το επικοινωνιακό μοντέλο

Στην ενότητα αυτή θα γνωρίσουμε πρώτα ένα στοιχειώδες επικοινωνιακό μοντέλο, το οποίο στη συνέχεια θα περιγράψουμε με περισσότερη λεπτομέρεια. Το επικοινωνιακό μοντέλο απαιτεί το πλαίσιο στο οποίο εντάσσονται τα θέματα που θα μας απασχολήσουν στο παρόν σύγγραμμα.

1.2.1 Στοιχειώδες επικοινωνιακό μοντέλο

Σε κάθε επικοινωνιακή διεργασία λαμβάνει χώρα ροή πληροφορίας μεταξύ ενός αποστολέα και ενός αποδέκτη. Η πληροφορία αυτή μπορεί να έχει διάφορες μορφές, όπως ηλεκτρισμού, μουσικής, λέξεων ή εικόνων. Η μεταφορά της πληροφορίας επιτυγχάνεται, στη γενική περίπτωση, με τη βοήθεια ενός δικτύου μετάδοσης. Έτσι, τα βασικά μέρη ενός επικοινωνιακού μοντέλου είναι ο αποστολέας ή πηγή πληροφορίας, το κανάλι ή δίκτυο μετάδοσης και ο παραλήπτης ή προορισμός αυτής.

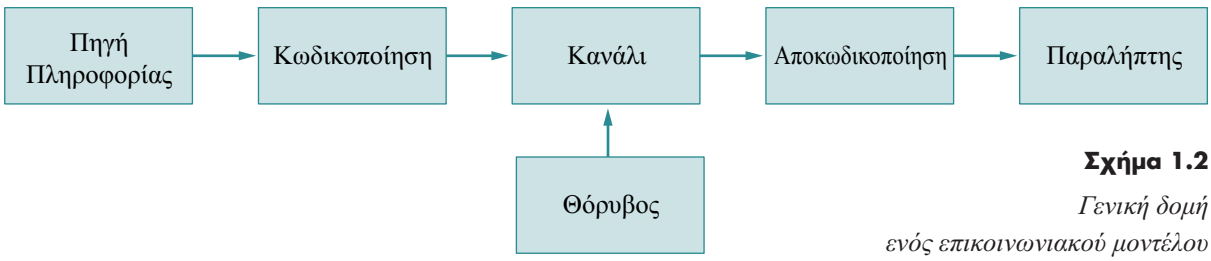
Η αποθήκευση της πληροφορίας παίζει σήμερα σημαντικό ρόλο. Αν και κατά κανόνα δεν είναι ζήτημα μετάδοσης, μπορεί ωστόσο να περιγραφεί ως μέρος του καναλιού ή δικτύου μετάδοσης. Η πληροφορία κατά τη μετάδοσή της μπορεί να αλλοιωθεί από την επενέργεια του θορύβου πάνω στο κανάλι. Ένα στοιχειώδες επικοινωνιακό μοντέλο φαίνεται στο Σχήμα 1.1.



Σχήμα 1.1
Βασικό επικοινωνιακό μοντέλο

Η μεταφορά της πληροφορίας θα πρέπει να είναι, ως ένα βαθμό, χωρίς σφάλματα. Γι' αυτό πρέπει να είναι δυνατή η διόρθωση σφαλμάτων ή η μεταφορά να είναι τόσο καλή, ώστε να μην υπεισέρχονται παρά μόνο ασήμαντα σφάλματα που είναι ανεκτά. Μια τέλεια, δηλαδή χωρίς σφάλματα, μεταφορά δεν είναι δυνατή για σήματα ομιλίας, μουσικής ή video. Μπορούν μόνο να τεθούν απαιτήσεις ως προς το μέγεθος της απόκλισης του σήματος που λαμβάνει ο αποδέκτης από το σήμα που έχει αποστείλει ο μεταδότης. Η απαιτούμενη ποιότητα μεταφοράς της πληροφορίας οδηγεί στην επιλογή κατάλληλου μέσου μεταφοράς ή καναλιού και επιβάλλει οριακές συνθήκες προσαρμογής του καναλιού στον αποστολέα και τον παραλήπτη. Μια από τις σημαντικές επιδιώξεις σχεδιαστών επικοινωνιακών συστημάτων είναι η ελαχιστο-

ποίηση των απωλειών πληροφορίας στο κανάλι και η βέλτιστη επανάκτηση πληροφορίας που έχει προσβληθεί από θόρυβο. Για την επίτευξη της επιδίωξης αυτής χρησιμοποιούνται τεχνικές κωδικοποίησης στην πλευρά του αποστολέα και αντίστοιχες τεχνικές αποκωδικοποίησης στην πλευρά του αποδέκτη. Λαμβάνοντας υπόψη την κωδικοποίηση και την αποκωδικοποίηση, οδηγούμαστε στη γενική δομή ενός επικοινωνιακού μοντέλου που παρουσιάζεται στο Σχήμα 1.2.



Σχήμα 1.2
Γενική δομή ενός επικοινωνιακού μοντέλου

1.2.2 Λεπτομερές επικοινωνιακό μοντέλο

Στη συνέχεια θα επιχειρήσουμε πιο λεπτομερή περιγραφή των λειτουργιών του αποστολέα και του παραλήπτη.

Καταρχήν θεωρούμε ως δεδομένα την πηγή πληροφορίας, τον προορισμό, το κανάλι με τα φυσικά χαρακτηριστικά του και την πηγή του θορύβου που επενεργεί στο επικοινωνιακό κανάλι. Σκοπός της πηγής πληροφορίας ή του αποστολέα είναι να καταστήσει την πληροφορία κατάλληλη για μετάδοση μέσω του δεδομένου καναλιού. Από την άλλη πλευρά, ο αποδέκτης έχει ως σκοπό τη διόρθωση σφαλμάτων τα οποία προέκυψαν κατά τη μεταφορά της πληροφορίας στο επικοινωνιακό κανάλι εξαιτίας του θορύβου και, επίσης, τη μετατροπή της πληροφορίας σε τέτοια μορφή που να είναι κατάλληλη για τον παραλήπτη. Έτσι, μπορούμε να διακρίνουμε στην πλευρά του μεταδότη ή αποστολέα τέσσερις λειτουργίες:

1. Εφόσον δεν είναι σημαντικό για τον παραλήπτη το σύνολο της πληροφορίας που έχει δημιουργηθεί από την πηγή, θα πρέπει να αφαιρεθεί το μη χρήσιμο μέρος από την προς μεταφορά πληροφορία. Αυτή η λειτουργία καλείται **απαλοιφή δεδομένων** (data reduction). Η πληροφορία που απομένει για μεταφορά καλείται αποτελεσματική (ή ουσιαστική) πληροφορία.
2. Πολλές φορές, η ουσιαστική πληροφορία μπορεί να αποτελέσει αντικείμενο περαιτέρω επεξεργασίας για την αναπαράστασή της με όσο το δυνατόν πιο συμπυκνωμένο τρόπο. Σ' αυτό στοχεύει μια δεύτερη λειτουργία, αυτή της **συμπίεσης**.

3. Η τρίτη λειτουργία, αυτή της **κρυπτογράφησης**, εφαρμόζεται όταν επιδιώκεται η προστασία του περιεχομένου από υποκλοπή ή σκόπιμη παραποίηση.
4. Η τελευταία λειτουργία, στην πλευρά του αποστολέα, στοχεύει στην προστασία από σφάλματα που δημιουργούνται κατά τη μεταφορά της πληροφορίας στο επικοινωνιακό κανάλι εξαιτίας της επενέργειας του θορύβου σ' αυτό. Για το λόγο αυτό προστίθεται ειδική πληροφορία και μεταφέρεται από το κανάλι μαζί με την ουσιαστική πληροφορία για την ανίχνευση και, πολλές φορές, διόρθωση σφαλμάτων. Αυτή η τέταρτη λειτουργία καλείται **κωδικοποίηση καναλιού**.

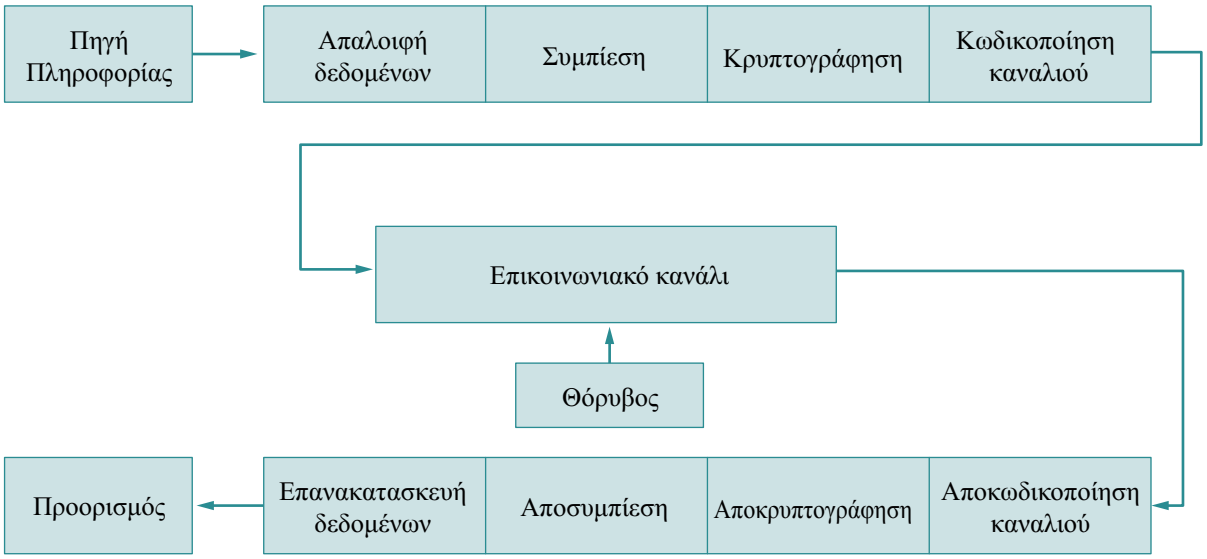
Το επικοινωνιακό κανάλι μεταφέρει και αποδίδει την πληροφορία, ενδεχομένως με σφάλματα στον αποδέκτη. Στην πλευρά του αποδέκτη, οι λειτουργίες εκτελούνται με αντίστροφη σειρά.

1. Η πρώτη λειτουργία, η **αποκωδικοποίηση καναλιού**, επιτρέπει τον έλεγχο ύπαρξης σφαλμάτων και, ενδεχομένως, διόρθωσης αυτών.
2. Η δεύτερη λειτουργία, η **αποκρυπτογράφηση**, επαναφέρει την πληροφορία σε τέτοιον τρόπο αναπαράστασης, που επιτρέπει την αποκάλυψη της σημασίας και, ενδεχομένως, επιτρέπει τον έλεγχο ύπαρξης παραποίησης (μη επιτρεπτής τροποποίησης).
3. Στην περίπτωση συμπίεσης της πληροφορίας στην πλευρά του μεταδότη, η λειτουργία της **αποσυμπίεσης** εκτελείται στον αποδέκτη.
4. Τέλος, η τέταρτη λειτουργία, αυτή της **επανακατασκευής των δεδομένων** (data reconstruction), φέρει την πληροφορία σε μορφή κατάλληλη για τον παραλήπτη.

Λαμβάνοντας υπόψη τις ανωτέρω λειτουργίες, μπορούμε να οδηγηθούμε στο λεπτομερές επικοινωνιακό μοντέλο που παρουσιάζεται στο Σχήμα 1.3.

Δραστηριότητα 1.2

Προσπαθήστε να περιγράψετε συνοπτικά το επικοινωνιακό μοντέλο και τους τρόπους επεξεργασίας που υποβάλλεται η πληροφορία στο μεταδότη και τον παραλήπτη. Αν δεν τα καταφέρετε, μελετήστε και πάλι την Ενότητα 1.2 και συμβουλευτείτε τη σχετική παράγραφο της σύνοψης.



Σχήμα 1.3
Λεπτομερές επικοινωνιακό μοντέλο

1.3 Στοιχεία Πιθανοτήτων

Σκοπός

Σκοπός της ενότητας αυτής είναι να επαναφέρουμε στη μνήμη μας βασικά στοιχεία από τη Θεωρία Πιθανοτήτων που απαιτούνται στους ορισμούς των μέτρων ποσότητας πληροφορίας και στη μελέτη ζητημάτων της Θεωρίας Πληροφορίας.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει την ενότητα αυτή, θα μπορείτε να:

- *περιγράψετε και εξηγήσετε τη διακριτή και τη συνεχή τυχαία μεταβλητή,*
- *διακρίνετε μεταξύ της συνάρτησης πιθανότητας μάζας και της συνάρτησης πυκνότητας πιθανότητας,*
- *εξηγήσετε τις έννοιες της συνδυασμένης (ή από κοινού), οριακής (ή ακραίας) και υπό συνθήκη πιθανότητας,*
- *ερμηνεύσετε το θεώρημα του Bayes.*

Έννοιες κλειδιά

- *τυχαίο πείραμα και δειγματικός χώρος,*
- *διακριτή και συνεχής τυχαία μεταβλητή,*
- *συνάρτηση κατανομής και πυκνότητας πιθανότητας,*
- *υπό συνθήκη, συνδυασμένη και οριακή πιθανότητα,*
- *Θεώρημα του Bayes,*
- *στατιστική ανεξαρτησία.*

Το αποτέλεσμα ενός τυχαίου πειράματος, όπως, παραδείγματος χάρη, της ρίψης ενός ζαριού ή κέρματος, δεν είναι εκ των προτέρων βέβαιο. Τα ατομικά αδιαίρετα αποτελέσματα, όπως στην περίπτωση του ζαριού το 1, 2, 3, 4, 5 και 6, λέγονται εκβάσεις ή στοιχειώδη ή απλώς ενδεχόμενα ή δειγματικά σημεία. Έτσι και η επιλογή από την πηγή πληροφορίας των συμβόλων ενός μηνύματος είναι ένα τυχαίο πείραμα και τα σύμβολα τα δειγματικά σημεία. Το σύνολο των στοιχειωδών ενδεχομένων ενός τυχαίου πειράματος λέγεται δειγματικός χώρος. Στην περίπτωση της ρίψης του ζαριού ο δειγματικός χώρος είναι το σύνολο $S = \{1, 2, 3, 4, 5, 6\}$ και στην περίπτωση

επιλογής ενός συμβόλου κατά το σχηματισμό μηνύματος από πηγή πληροφορίας είναι το αλφάβητο που χρησιμοποιείται. Ένα υποσύνολο του δειγματικού χώρου, δηλαδή μια συλλογή εκβάσεων ή απλών ενδεχομένων ή δειγματικών σημείων, στην περίπτωση του ζαριού το $S_1 = \{1, 4\}$, ή μια λέξη στην περίπτωση της πηγής, λέγεται γεγονός ή συμβάν. Υποθέτουμε ότι μπορούν να προσδιοριστούν όλα τα ενδεχόμενα που ενδιαφέρουν. Αν θεωρήσουμε ότι ένα γεγονός E αποτελείται από ν δειγματικά σημεία και ότι όλα τα σημεία του δειγματικού χώρου είναι N και ισοπίθανα, τότε ορίζουμε ως πιθανότητα του E το λόγο ν/N. Αυτός είναι ο κλασικός ορισμός της πιθανότητας. Σε οποιοδήποτε εισαγωγικό βιβλίο στη Θεωρία Πιθανοτήτων μπορείτε να βρείτε και τον εμπειρικό και τον αξιωματικό ορισμό.

Τυχαία μεταβλητή είναι μια μονοσήμαντη συνάρτηση με πεδίο ορισμού ένα δειγματικό χώρο S και πεδίο τιμών ένα υποσύνολο των πραγματικών αριθμών. Μια τυχαία μεταβλητή λέγεται διακριτή αν το σύνολο των τιμών της είναι πεπερασμένο ή απείρως αριθμήσιμο. (Απείρως αριθμήσιμο σημαίνει πως το σύνολο των δυνατών τιμών μπορεί να τεθεί σε μία προς μία αντιστοιχία με το σύνολο των ακέραιων αριθμών.) Οι συνεχείς τυχαίες μεταβλητές αντιστοιχούν σε συνεχείς δειγματικούς χώρους.

Έστω ένα τυχαίο πείραμα S με δειγματοχώρο $S = \{s_1, s_2, \ldots, s_n\}$ και η διακριτή τυχαία μεταβλητή X με πεδίο τιμών $X = \{x_1, x_2, \ldots, x_n\}$. Κάθε γεγονός s_i μπορεί να συμβεί με πιθανότητα $P(S = s_i) = P(X = x_i) = p_i$. Η $P(X = x_i) = p_i$ λέγεται συνάρτηση πιθανότητας μάζας και το σύνολο των πιθανοτήτων αυτών είναι $P = \{p_1, p_2, \ldots, p_n\}$. Η συνάρτηση πιθανότητας μάζας πληροί τις ακόλουθες θεμελιώδεις απαιτήσεις:

1. $p(x_i) \geq 0$, για κάθε i

2. $$\sum_{1}^{n} p(x_i) = 1.$$

Η συνάρτηση κατανομής αθροιστικής πιθανότητας μιας διακριτής τυχαίας μεταβλητής X δίνεται από τη σχέση

$$F(X \leq x) = \sum_{x_i \leq x} p(x_i)\,, \text{ για κάθε } x \in (-\infty, \infty).$$

Αντίστοιχα, η συνάρτηση κατανομής μιας συνεχούς τυχαίας μεταβλητής δίνεται από τη σχέση

$$F(X \leq x) = P[X \in (-\infty, x)] = \int_{-\infty}^{x} f(y)dy\,, \text{ για κάθε } x \in (-\infty, \infty).$$

Η μη αρνητική συνάρτηση $f(x)$ καλείται συνάρτηση πυκνότητας πιθανότητας της συνεχούς τυχαίας μεταβλητής X. Για τη συνάρτηση πυκνότητας πιθανότητας ισχύουν τα εξής:

$$\int_B f(x)dx = P(X \in B) \text{ και } \int_{-\infty}^{\infty} f(x)dx = 1.$$

Η συνάρτηση κατανομής της συνεχούς τυχαίας μεταβλητής έχει τις ακόλουθες ιδιότητες:

1. $0 \le F(X \le x) \le 1$, για κάθε x
2. Η συνάρτηση κατανομής είναι μη φθίνουσα, δηλαδή αν $x_i \le x_k$, τότε
$$F(X \le x_i) \le F(X \le x_k)$$
3. $\lim_{x\to\infty} F(X \le x) = 1$ και $\lim_{x\to\infty} F(X \le x) = 0$.

Μερικές φορές συνδυάζουμε n τυχαία πειράματα σε ένα σύνθετο ή ενδιαφερόμαστε για n τυχαίες μεταβλητές ταυτόχρονα. Στη συνέχεια θα περιορίσουμε τη συζήτηση σε δύο πειράματα ή τυχαίες μεταβλητές. Σ' αυτή την περίπτωση έχουμε δύο δειγματικούς χώρους, έστω X και Y, όπου ο δειγματικός χώρος Y αναφέρεται στο αντίστοιχο πείραμα ή στην αντίστοιχη διακριτή τυχαία μεταβλητή, $Y = \{y_1, y_2, ..., y_m\}$. Η κατανομή πιθανότητας της Y είναι $P(Y) = \{p(y_1),\ p(y_2),\ ...,\ p(y_m)\}$, δηλαδή $p(y_i) = P(Y = y_i)$.

Ας εξετάσουμε τώρα το πείραμα (X, Y) με δειγματικό χώρο το σύνολο των συνδυασμών (x, y). Ορίζουμε ως συνάρτηση συνδυασμένης πιθανότητας μάζας την $p_{ij} = P(X = x_i,\ Y = y_j)$, που δίνει την πιθανότητα να ισχύει: $X = x_i$ και $Y = y_j$. Από τη συνάρτηση συνδυασμένης πιθανότητας μάζας p_{ij} μπορούν να υπολογιστούν οι συναρτήσεις ακραίας πιθανότητας μάζας $p(x_i)$ και $p(y_j)$:

$$p(x_i) = \sum_{j=1}^{m} p_{ij} \text{ και } p(y_j) = \sum_{i=1}^{n} p_{ij}.$$

Παράδειγμα 1.1

Υποθέτουμε ότι οι X και Y είναι διακριτές τυχαίες μεταβλητές και ότι η συνάρτηση συνδυασμένης πιθανότητας μάζας δίνεται από τη σχέση

$$p_{ij} = \frac{x_i y_j}{27},\ \text{για}\ X = \{1, 2\}\ \text{και}\ Y = \{2,\ 3,\ 4\}.$$

Τότε οι συναρτήσεις ακραίας πιθανότητας μάζας υπολογίζονται ως ακολούθως:

$$p(x_i) = \sum_{y=2}^{4} \frac{x_i y}{27},\ \text{για}\ x_1 = 1,\ x_2 = 2\ \text{και}\ \ p(y_i) = \sum_{x=1}^{2} \frac{x y_j}{27},\ \text{για}\ y_1 = 2,\ y_2 = 3,\ y_3 = 4.$$

Ένας άλλος τύπος πιθανότητας είναι η υπό συνθήκη πιθανότητα. Αυτή προκύπτει όταν το αποτέλεσμα ενός πειράματος *Y* αποτελεί τη συνθήκη για ένα άλλο πείραμα *X*. Ας εξετάσουμε ως παράδειγμα το εξής ερώτημα: Ποια η πιθανότητα της εμφάνισης του συμβόλου «α» κατά τη λήψη μηνύματος στην ελληνική γλώσσα όταν ο παραλήπτης έλαβε ήδη το τμήμα «θάλασσ». Είναι πολύ υψηλή, αφού το επόμενο γράμμα μπορεί να είναι «α» ή «ε» (θάλασσα ή θάλασσες). Η εμφάνιση γραμμάτων σε λέξεις συνήθως εξαρτάται από τα γράμματα που ήδη έχουν εμφανιστεί. Έτσι, υπάρχει μικρή πιθανότητα το γράμμα «κ» να ακολουθείται από το «β». Τουναντίον, είναι υψηλή η πιθανότητα το «κ» να ακολουθείται από «α». Η συνάρτηση υπό συνθήκη πιθανότητας μάζας $p(x_i / y_j)$, που δίνει την πιθανότητα $X = x_i$ δεδομένου του $Y = y_i$, ορίζεται ως ακολούθως: [Η $p(x_i, y_j)$ είναι η συνάρτηση συνδυασμένης πιθανότητας μάζας που δίνει την πιθανότητα $X = x_i$ και $Y = y_j$.]

$$p(x_i / y_j) = \frac{p(x_i, y_j)}{p(y_j)},\ \text{εφόσον}\ \ p(y_j) > 0.$$

Αντίστοιχα, η συνάρτηση υπό συνθήκη πιθανότητας μάζας $p(y_j / x_i)$, που δίνει την πιθανότητα $Y = y_i$ δεδομένου του $X = x_i$, δίνεται από τη σχέση

$$p(y_j / x_i) = \frac{p(x_i, y_j)}{p(x_i)},\ \text{εφόσον}\ \ p(x_i) > 0.$$

Από τις σχέσεις αυτές προκύπτει η συνάρτηση συνδυασμένης πιθανότητας μάζας:

$$p(x_i, y_j) = p(x_i / y_j)\, p(y_j) = p(y_j / x_i)\, p(x_i).$$

Αναφορικά με την υπό συνθήκη πιθανότητα μάζας ισχύει και η σχέση

$$\sum_{i=1}^{n} p(x_i / y_j) = 1.$$

Άσκηση αυτοαξιολόγησης 1.2

Δίνονται δύο συνεχείς τυχαίες μεταβλητές, οι X και Y, και η συνδυασμένη συνάρτηση πυκνότητας πιθανότητάς τους

$$f(x,y)=\begin{cases}4xy \text{ για } x\geq 0, y\geq 0 \text{ και } x+y=1\\ 0 \qquad \text{άλλως}\end{cases}$$

Να υπολογίσετε τις συναρτήσεις πυκνότητας πιθανότητας $f(x)$ και $f(y)$.

Όταν δίνεται η υπό συνθήκη πιθανότητα μάζας $p(y_j / x_i)$ και η $p(x_i)$ και θέλουμε να προσδιορίσουμε την $p(x_i / y_j)$, μπορούμε να χρησιμοποιήσουμε το θεώρημα του Bayes. Όπως είδαμε προηγουμένως, ισχύει

$$p(x_i, y_j) = p(x_i / y_j)p(y_j) = p(y_j / x_i)p(x_i).$$

Αν είναι $p(y_j) > 0$, τότε η ακόλουθη σχέση επιτρέπει τον προσδιορισμό της $p(x_i / y_j)$:

$$p(x_i / y_j) = \frac{p(y_j / x_i)p(x_i)}{p(y_j)} = \frac{p(y_j / x_i)p(x_i)}{\sum_{i=1}^{n} p(x_i)p(y_j / x_i)}.$$

Δύο τυχαίες μεταβλητές X και Y είναι ανεξάρτητες η μια από την άλλη αν ισχύει η σχέση

$$p(x_i, y_j) = p(x_i)p(y_j).$$

Σ' αυτή την περίπτωση ισχύει $p(x_i / y_j) = p(x_i)$ και $p(y_j / x_i) = p(y_j)$.

1.4 Το Μέτρο Πληροφορίας του Shannon

Σκοπός

Σκοπός της ενότητας αυτής είναι να γνωρίσουμε το μέτρο ποσότητας πληροφορίας του Shannon και να περιγράψουμε και επεξηγήσουμε τις ιδιότητες αυτού.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει την ενότητα αυτή, θα είστε σε θέση να:

- *περιγράψετε και επεξηγήσετε το μέτρο ποσότητας πληροφορίας του Shannon,*
- *αναφέρετε τέσσερις ιδιότητες του μέτρου ποσότητας πληροφορίας του Shannon,*
- *υπολογίσετε την ποσότητα πληροφορίας τυχαίων μεταβλητών.*

Έννοιες κλειδιά

- *Μέση (ποσότητα) πληροφορίας ή εντροπία ή μέσο πληροφορικό περιεχόμενο*

Το μέτρο ποσότητας πληροφορίας του Hartley, που γνωρίσαμε στην Ενότητα 1.1, δε λαμβάνει υπόψη διαφορετικές πιθανότητες για την επιλογή των συμβόλων που απαρτίζουν ένα μήνυμα. Η εισαγωγή, από τον Shannon, της έννοιας της πιθανότητας στον ορισμό του μέτρου ποσότητας πληροφορίας, που πραγματεύεται αυτή η ενότητα, έθεσε τις βάσεις για την ανάπτυξη της σύγχρονης Θεωρίας Πληροφορίας. Ο Shannon γενίκευσε, λοιπόν, τον ορισμό της ποσότητας πληροφορίας του Hartley, επιτρέποντας διαφορετικές πιθανότητες εμφάνισης των συμβόλων σε μηνύματα και κατ΄ επέκταση και των διαφόρων μηνυμάτων. Η συσχέτιση της έννοιας της πιθανότητας με τον ορισμό του μέτρου ποσότητας πληροφορίας είναι εύλογη. Αν θεωρήσουμε ένα τυχαίο πείραμα με δειγματοχώρο του οποίου τα γεγονότα είναι ισοπίθανα, τότε υπάρχει μεγάλη αβεβαιότητα για το αποτέλεσμα. Αντίθετα, αν ο δειγματοχώρος έχει ένα στοιχείο με πολύ μεγάλη πιθανότητα, τότε το να συμβεί αυτό το γεγονός προσφέρει πολύ λιγότερη πληροφορία απ’ ό,τι το να συμβεί ένα από τ’ άλλα γεγονότα.

1.4.1 Ορισμός του μέτρου πληροφορίας του Shannon

Μέση ποσότητα πληροφορίας ή μέση πληροφορία ή μέσο πληροφορικό περιεχόμενο

Αν X είναι μια διακριτή τυχαία μεταβλητή με δειγματοχώρο $X = \{x_1, x_2, \ldots, x_n\}$ και συνάρτηση πιθανότητας μάζας $p(x_i)$, τότε η μέση ποσότητα πληροφορίας (ή μέση πληροφορία ή μέσο πληροφορικό περιεχόμενο) της X, $H(X)$, δίνεται από τη σχέση

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i).$$

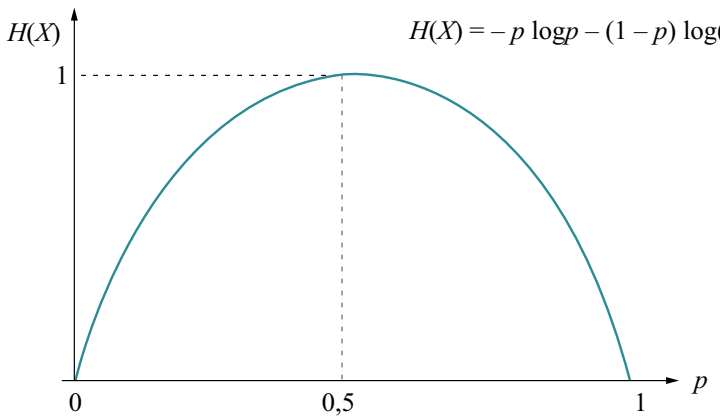
Η μέση πληροφορία ονομάζεται και **εντροπία**.

Στην περίπτωση μιας διακριτής τυχαίας μεταβλητής X με δύο ενδεχόμενα, π.χ. εκπομπή ενός από δύο δυνατά μηνύματα και πιθανότητες αυτών p και $(1–p)$, αντίστοιχα, η εντροπία είναι

$$H(X) = -p \log p - (1-p) \log(1-p).$$

Όπως μπορούμε να συνάγουμε από τον ορισμό της εντροπίας, η ποσότητα πληροφορίας (ή το πληροφορικό περιεχόμενο) ενός γεγονότος x_i της τυχαίας μεταβλητής X είναι ίσο με τον αρνητικό λογάριθμο της πιθανότητας εμφάνισής του $p(x_i)$, δηλαδή ίσο με $(-\log p(x_i))$. Επομένως, η ποσότητα πληροφορίας ενός γεγονότος είναι αντιστρόφως ανάλογη της πιθανότητας εμφάνισής του.

Η γραφική παράσταση του Σχήματος 1.4 δείχνει τη συμπεριφορά της μέσης ποσότητας πληροφορίας ως συνάρτηση της πιθανότητας p. (Η μονάδα μέτρησης της μέσης ποσότητας πληροφορίας είναι το bit, δηλαδή ο λογάριθμος είναι με βάση το 2.)



Σχήμα 1.4
Η μέση ποσότητα πληροφορίας ως συνάρτηση της p

Παρατηρούμε στη γραφική παράσταση (Σχήμα 1.4) ότι η μέση πληροφορία παίρνει τη μέγιστη τιμή, που ισούται με ένα, όταν τα δύο γεγονότα μπορούν να συμβούν με την ίδια πιθανότητα, δηλαδή $p = \frac{1}{2}$. Από την άλλη πλευρά, αν $p = 1$ ή $p = 0$, τότε η εντροπία είναι 0, αφού το τελικό αποτέλεσμα (η έκβαση του πειράματος) είναι βέβαιο.

Παράδειγμα 1.2

Ας εξετάσουμε δύο τυχαία πειράματα X και Y. Θεωρούμε ότι το X έγκειται στην επιλογή και αποστολή ενός μηνύματος από ένα δειγματικό χώρο με, συνολικά, τρία μηνύματα, $X = \{x_1, x_2, x_3\}$ και κατανομή πιθανοτήτων $P(X) = \{0,1,\ 0,5,\ 0,4\}$. Τα μηνύματα αυτά έχουν ως ακολούθως: x_1 = η άφιξη της πτήσης είναι στις 08:30, x_2 = η άφιξη της πτήσης είναι στις 08:45 και x_3 = η άφιξη της πτήσης είναι στις 08:15. Το τυχαίο πείραμα Y, επίσης, έγκειται στην επιλογή και αποστολή ενός μηνύματος, εκ τριών δυνατών, $Y = \{y_1, y_2, y_3\}$ και έχει κατανομή πιθανοτήτων $P(Y) = \{0,4,\ 0,1,\ 0,5\}$. Για τα μηνύματα αυτά ισχύει: y_1 = αύριο αναμένεται αύξηση των πωλήσεων, y_2 = αύριο αναμένεται μείωση των πωλήσεων και y_3 = αύριο δεν αναμένεται αύξηση ή μείωση των πωλήσεων. Η μέση ποσότητα πληροφορίας της X και της Y δίνεται από τις ακόλουθες σχέσεις, αντίστοιχα:

$$H(X) = -0,1 \log 0,1 - 0,5 \log 0,5 - 0,4 \log 0,4.$$

$$H(Y) = -0,4 \log 0,4 - 0,1 \log 0,1 - 0,5 \log 0,5.$$

Παρατηρούμε ότι είναι ίσες. Επομένως, καθοριστικές είναι οι πιθανότητες που επιλέγονται και αποστέλλονται τα μηνύματα και όχι η σημασία τους, κάτι που είχαμε επισημάνει και στην Ενότητα 1.1.

Παράδειγμα 1.3

Υποθέτουμε ότι η εικόνα τερματικού γραφικών αποτελείται από 1024 γραμμές και κάθε γραμμή από 1024 στοιχεία εικόνας (pixels, picture elements). Έτσι, μια απλή εικόνα αποτελείται από, συνολικά, 1024×1024 pixels. Αν κάθε στοιχείο της εικόνας μπορεί να έχει ένα από 256 χρώματα, τότε υπάρχουν $256^{1048576}$ διαφορετικές εικόνες. Αν υποθέσουμε, ακόμα, ότι η εμφάνιση των διαφόρων εικόνων είναι ίσης πιθανότητας γεγονότα, τότε η μέση ποσότητα πληροφορίας δίνεται από

$$H(X) = \log 256^{1048576} = 1048576 \log 2^8 = 2^{23} \text{ bits.}$$

Άσκηση αυτοαξιολόγησης 1.3

Να υπολογίσετε τη μέση ποσότητα της πληροφορίας που περιέχεται στο άθροισμα της ρίψης δύο ζαριών. Αποτελέσματα όπως (4, 2) και (2, 4) θεωρούνται διαφορετικά.

1.4.2 Ιδιότητες της μέσης ποσότητας πληροφορίας

Οι ιδιότητες της μέσης (ποσότητας) πληροφορίας, που έχουν τεθεί και ως απαιτήσεις κατά τον ορισμό της, δηλαδή κατά την αναζήτηση από τον Shannon και άλλους ερευνητές της κατάλληλης συνάρτησης, διακρίνονται στις ακόλουθες:

1. Η μέση πληροφορία $H(X)$ είναι συνεχής στο p, κάτι που μπορούμε να δούμε στην προηγούμενη γραφική παράσταση του Σχήματος 1.4.
2. Η μέση πληροφορία $H(X)$ είναι συμμετρική, δηλαδή η διάταξη των πιθανοτήτων δεν την επηρεάζει, όπως είδαμε στο Παράδειγμα 2. Έτσι, διαφορετικές τυχαίες μεταβλητές με κατανομές πιθανοτήτων που προέρχονται από μεταθέσεις της ίδιας κατανομής πιθανοτήτων έχουν ίση εντροπία. Σε ορισμένες περιπτώσεις, ακόμα και διαφορετικές κατανομές πιθανοτήτων οδηγούν στην ίδια μέση ποσότητα πληροφορίας.
3. Η εντροπία $H(X)$ παίρνει τη μέγιστη τιμή όταν όλα τα ενδεχόμενα είναι ισοπίθανα. Τότε, η αβεβαιότητα είναι η μέγιστη δυνατή και, κατά συνέπεια, η επιλογή ενός μηνύματος προσφέρει τη μέγιστη δυνατή μέση πληροφορία.
4. Η εντροπία είναι προσθετική (additive). Η ιδιότητα αυτή αναφέρεται στην περίπτωση κατά την οποία δύο ανεξάρτητες τυχαίες μεταβλητές X και Y συνδυάζονται. Τότε, για τη συνδυασμένη ποσότητα πληροφορίας ισχύει

$$H(X,Y) = H(X) + H(Y).$$

Η σχέση $H(X,Y) = H(X) + H(Y)$ μπορεί να δειχθεί αν χρησιμοποιήσουμε τον ορισμό της μέσης πληροφορίας. Σύμφωνα με τον ορισμό ισχύει

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij} \log p_{ij}.$$

Αφού οι δύο τυχαίες μεταβλητές είναι ανεξάρτητες, ισχύει $p_{ij} = p(x_i)p(y_j)$ και έτσι έχουμε

$$
\begin{aligned}
H(X,Y) &= -\sum_{i=1}^{n}\sum_{j=1}^{m} p_i p_j \log p_i p_j \\
&= -\sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j \left(\log p_i + \log p_j\right) \\
&= -\sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j \left(\log p_i\right) - \sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j \left(\log p_j\right) \\
&= -\sum_{i=1}^{n} p_i \log p_i \sum_{j=1}^{m} p_j - \sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j \log p_j \\
&= -\sum_{i=1}^{n} p_i \log p_i - \sum_{j=1}^{m} p_j \log p_j \\
&= H(X) + H(Y).
\end{aligned}
$$

Οι Chaundy και MacLeod [CHA60] έδειξαν ότι οι ιδιότητες, ιδιαίτερα η τέταρτη, ικανοποιούνται μόνο από τη συνάρτηση $-\sum p \log p$, που διατύπωσε ο Shannon. (Η απόδειξη της μοναδικότητας δεν είναι απλή. Το άρθρο των Chaundy και MacLeod, που αναφέρεται σ' αυτή την απόδειξη, περιέχεται στα πρακτικά Edinburgh Math. Soc. Notes, 43, 1960, pp. 7 – 8.)

Στη συνέχεια θα δούμε δύο προτάσεις για την εντροπία. Η πρώτη αναφέρεται στη μέγιστη τιμή της μέσης ποσότητας πληροφορίας, στην οποία αναφερθήκαμε προηγουμένως, και η δεύτερη στο ότι η μέση ποσότητα πληροφορίας είναι μη αρνητική. X είναι μια τυχαία μεταβλητή με δειγματοχώρο $X = \{x_1, x_2, ..., x_n\}$ και κατανομή πιθανοτήτων $P = \{p_1, p_2, ..., p_n\}$.

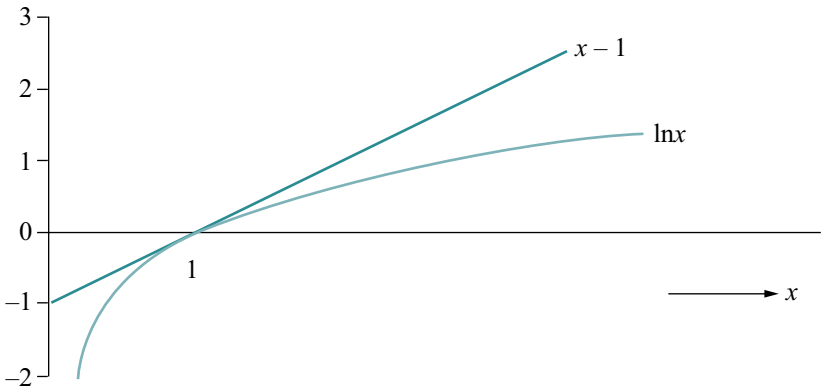
Πρόταση 1.1

Για μια τυχαία μεταβλητή X ισχύει $H(X) \leq \log n$.

$H(X) = \log n$ αν $p_i = \dfrac{1}{n}$, για όλα τα i.

Απόδειξη: Για κάθε θετικό αριθμό ισχύει, όπως φαίνεται στο Σχήμα 1.5, $\ln x \leq x - 1$. Λαμβάνοντας υπόψη την ανισότητα αυτή, μπορούμε να έχουμε την ακόλουθη σχέση:

$$\log x = \frac{\ln x}{\ln 2} \leq (x-1)\frac{\ln e}{\ln 2} = (x-1)\log e.$$



Σχήμα 1.5
Γραφική παράσταση της $\ln x \le x-1$

Αναφορικά με τη μέση ποσότητα πληροφορίας ισχύει η ακόλουθη σχέση:

$$H(X)-\log n=-\sum_{i=1}^{n}p_i\log p_i-\log n=-\sum_{i=1}^{n}p_i(\log p_i+\log n)$$
$$=-\sum_{i=1}^{n}p_i\log(np_i)=\sum_{i=1}^{n}p_i\log\left(\frac{1}{np_i}\right).$$

Με τη βοήθεια της ανωτέρω ανισότητας μπορούμε να γράψουμε

$$H(X)-\log n\le\sum_{i=1}^{n}p_i\left(\frac{1}{np_i}-1\right)\log e=\left(\sum_{i=1}^{n}p_i\frac{1}{np_i}-\sum_{i=1}^{n}p_i\right)\log e$$
$$=\left(n\frac{1}{n}-1\right)\log e=0.$$

Από την τελευταία σχέση έχουμε τη ζητούμενη:

$$H(X)\le\log n.$$

Η ισότητα ισχύει για $\frac{1}{np_i}=1\Rightarrow p_i=\frac{1}{n}$, αφού $\ln x=x-1$, αν $x=1$.

Πρόταση 1.2

Η μέση ποσότητα πληροφορίας είναι μη αρνητική, $H(X)\ge 0$.

Απόδειξη: Η πιθανότητα p_i παίρνει τιμές στο διάστημα [0, 1]. Έτσι, δεν μπορεί να είναι αρνητική. Από την άλλη πλευρά, ο λογάριθμός της είναι μικρότερος ή ίσος του μηδενός. Έτσι, το γινόμενο $p_i \log p_i$ είναι μη θετικό. Επομένως, η ποσότητα πληροφορίας είναι μη αρνητική.

Άσκηση αυτοαξιολόγησης 1.4

Δίνεται μια διακριτή τυχαία μεταβλητή με δειγματοχώρο $X = \{x_1, x_2, x_3, x_4\}$. Ζητούνται οι κατανομές πιθανοτήτων που οδηγούν στη μέγιστη και την ελάχιστη ποσότητα πληροφορίας της X.

1.5 Συνδυασμένη, Υπό Συνθήκη και Αμοιβαία Πληροφορία

Σκοπός

Σκοπός αυτής της ενότητας είναι να γνωρίσουμε την επέκταση του μέτρου ποσότητας πληροφορίας του Shannon και για δύο τυχαίες μεταβλητές.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει την ενότητα αυτή, θα είστε σε θέση να:

- *περιγράψετε και εξηγήσετε τη συνδυασμένη ποσότητα πληροφορίας,*
- *περιγράψετε και εξηγήσετε την υπό συνθήκη ποσότητα πληροφορίας,*
- *περιγράψετε και εξηγήσετε την αμοιβαία ποσότητα πληροφορίας,*
- *υπολογίσετε τα μέτρα αυτά της ποσότητας πληροφορίας δύο τυχαίων μεταβλητών.*

Έννοιες κλειδιά

- *συνδυασμένη πληροφορία,*
- *υπό συνθήκη πληροφορία,*
- *αμοιβαία πληροφορία.*

1.5.1 Η συνδυασμένη ποσότητα πληροφορίας

Πολλές φορές μάς ενδιαφέρει να εξετάσουμε την ποσότητα πληροφορίας ενός συνδυασμού δύο τυχαίων μεταβλητών, δηλαδή ενός πειράματος που αποτελείται από δύο υποπειράματα, όπως είδαμε στην τέταρτη ιδιότητα του μέτρου ποσότητας πληροφορίας του Shannon και στην Άσκηση αυτοαξιολόγησης 3 με τη ρίψη των δύο ζαριών. Ένα τυχαίο πείραμα (X, Y) έχει ως δυνατά αποτελέσματα όλους του συν-

δυασμούς των αποτελεσμάτων των $X = \{x_1, x_2, ..., x_n\}$ και $Y = \{y_1, y_2, ..., y_m\}$, επομένως το δειγματοχώρο

$$(X,Y) = \{(x_1, y_1),(x_1, y_2),\ldots,(x_1, y_m),\ldots,(x_n, y_1),(x_n, y_2),\ldots,(x_n, y_m)\}.$$

Η κατανομή πιθανοτήτων δίνεται από

$$P = \{p(x_1, y_1),..., p(x_1, y_m),..., p(x_n, y_1),..., p(x_n, y_m)\}.$$

Συνδυασμένη ποσότητα πληροφορίας (ή συνδυασμένη πληροφορία)

Αν (X, Y) είναι ένα τυχαίο πείραμα με δισδιάστατο δειγματοχώρο και κατανομή πιθανοτήτων όπως ανωτέρω, τότε η συνδυασμένη πληροφορία $H(X, Y)$ ορίζεται ως η μέση τιμή

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j)\log p(x_i, y_j).$$

Αν είναι γνωστές όλες οι συνδυασμένες πιθανότητες $p(x_i, y_j)$, τότε μπορούν να υπολογιστούν οι ακραίες πιθανότητες $p(x_i)$ και $p(y_j)$, όπως είδαμε στην Ενότητα 1.3, και επομένως οι **ακραίες ποσότητες πληροφορίας** $H(X)$ και $H(Y)$. Ο ορισμός της μέσης ποσότητας πληροφορίας μπορεί να επεκταθεί και για περισσότερες από δύο διαστάσεις. Σε κάθε περίπτωση λαμβάνουμε υπόψη όλους τους δυνατούς συνδυασμούς αποτελεσμάτων και, εφόσον γνωρίζουμε τις πιθανότητες αυτών, μπορούμε να υπολογίσουμε τη συνδυασμένη ποσότητα πληροφορίας. Για τρεις τυχαίες μεταβλητές (X, Y, Z) με συνδυασμένες πιθανότητες $p(x_i, y_j, z_k)$ η συνδυασμένη ποσότητα πληροφορίας δίνεται από τη σχέση

$$H(X,Y,Z) = -\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i, y_j, z_k)\log p(x_i, y_j, z_k).$$

Εναλλακτικά, μπορούμε να θεωρήσουμε ότι τα ενδεχόμενα, v, του τρισδιάστατου πειράματος είναι όλοι οι δυνατοί συνδυασμοί των τριών τυχαίων μεταβλητών και επομένως το πλήθος αυτών είναι ίσο με lmn. Οι αντίστοιχες πιθανότητες είναι $p(v_1)$, $p(v_2)$, …, $p(v_{lmn})$ και η συνδυασμένη πληροφορία δίνεται από τη σχέση

$H(X,Y,Z) = -\sum_{i=1}^{lmn} p(v_i)\log p(v_i)$. Το τελευταίο άθροισμα είναι ίσο με το άθροισμα που προκύπτει από τον προηγούμενο τύπο, αφού κάθε $p(v_h)$ ισούται με κάποια $p(x_i, y_j, z_k)$.

Παράδειγμα 1.4

Ας εξετάσουμε ένα τρισδιάστατο τυχαίο πείραμα το οποίο συνίσταται στη ρίψη, ταυτόχρονα, τριών κερμάτων. Η συνδυασμένη ποσότητα πληροφορίας της ταυτόχρονης ρίψης των τριών κερμάτων μπορεί να υπολογιστεί ως ακολούθως:

Οι δυνατοί συνδυασμοί είναι οκτώ, αφού τα δυνατά αποτελέσματα της ρίψης κάθε κέρματος είναι δύο, κεφαλή ή γράμμα. Θεωρώντας ότι κατά τη ρίψη ενός κέρματος το κάθε αποτέλεσμα έχει ίση πιθανότητα να λάβει χώρα, η πιθανότητα για κάθε συνδυασμό είναι 1/8. Επομένως, η συνδυασμένη ποσότητα πληροφορίας υπολογίζεται από

$$H(X,Y,Z) = -\sum_{1}^{lmn} p(v_i)\log p(v_i) = -\sum_{1}^{8} \frac{1}{8}\log\frac{1}{8} = 3 \text{ bits.}$$

Άσκηση αυτοαξιολόγησης 1.5

Ένα τυχαίο πείραμα τεσσάρων διαστάσεων συνίσταται στη ρίψη, ταυτόχρονα, τεσσάρων κερμάτων. Να υπολογιστεί η συνδυασμένη ποσότητα πληροφορίας της ταυτόχρονης ρίψης των τεσσάρων κερμάτων. Θεωρούμε ότι κατά τη ρίψη ενός κέρματος το κάθε αποτέλεσμα έχει ίση πιθανότητα να λάβει χώρα.

1.5.2 Η υπο συνθήκη ποσότητα πληροφορίας

Επίσης, μας ενδιαφέρει, αρκετές φορές, να υπολογίσουμε την ποσότητα πληροφορίας μιας τυχαίας μεταβλητής, X, όταν δίνεται το αποτέλεσμα μιας άλλης τυχαίας μεταβλητής, Y. Αυτή καλείται **υπό συνθήκη ποσότητα πληροφορία**ς της X ως προς την Y. Η υπό συνθήκη ποσότητα πληροφορίας του αποτελέσματος x_i αν είναι γνωστό ότι έχει λάβει χώρα το αποτέλεσμα y_j δίνεται από

$$H(x_i / y_j) = -\log p(x_i / y_j).$$

Η μέση τιμή τής υπό συνθήκη ποσότητας πληροφορίας της τυχαίας μεταβλητής X, δεδομένου του αποτελέσματος y_j, δίνεται από

$$H(X / y_j) = -\sum_{i=1}^{n} p(x_i / y_j) \log p(x_i / y_j).$$

Λαμβάνοντας υπόψη όλα τα δυνατά αποτελέσματα της Y, μπορούμε να υπολογίσουμε τη μέση τιμή τής υπό συνθήκη ποσότητας πληροφορίας της X, με δεδομένο το αποτέλεσμα της Y, ως ακολούθως:

$$H(X / Y) = \sum_{j=1}^{m} p(y_j) H(X / y_j) = -\sum_{j=1}^{m} p(y_j) \sum_{i=1}^{n} p(x_i / y_j) \log p(x_i / y_j)$$

$$= -\sum_{i=1}^{n} \sum_{j=1}^{m} p(y_j) p(x_i / y_j) \log p(x_i / y_j).$$

Λαμβάνοντας ακόμα υπόψη τη σχέση $p(a / b) = p(a, b) / p(b)$, η οποία αναφέρεται στη συνδυασμένη πιθανότητα δύο τυχαίων μεταβλητών και τις υπό συνθήκη και τις ακραίες πιθανότητες αυτών, μπορούμε να οδηγηθούμε στον ακόλουθο ορισμό:

Η υπό συνθήκη ποσότητα πληροφορίας (ή υπό συνθήκη πληροφορία)

Η (μέση) υπό συνθήκη ποσότητα πληροφορίας του τυχαίου πειράματος X, με δεδομένο το αποτέλεσμα του πειράματος Y, δίνεται από

$$H(X / Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \log p(x_i / y_j).$$

Αντίστοιχα, η υπό συνθήκη ποσότητα πληροφορίας του τυχαίου πειράματος Y, με δεδομένο το αποτέλεσμα του πειράματος X, δίνεται από

$$H(Y / X) = -\sum_{j=1}^{m} \sum_{i=1}^{n} p(x_i, y_j) \log p(y_j / x_i).$$

Άσκηση αυτοαξιολόγησης 1.6

Δίνονται δύο τυχαίες μεταβλητές, X και Y, με δύο δυνατά αποτελέσματα η καθεμία. Οι συνδυασμένες πιθανότητες δίνονται από

$$p(x_1, y_1) = \frac{1}{8}, \quad p(x_1, y_2) = \frac{1}{8}, \quad p(x_2, y_1) = \frac{1}{2} \text{ και } \quad p(x_2, y_2) = \frac{1}{4}.$$

1. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το αποτέλεσμα της τυχαίας μεταβλητής X; Ποια όταν μας γνωστοποιείται το αποτέλεσμα της Y;
2. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το αποτέλεσμα του σύνθετου τυχαίου πειράματος (X, Y);
3. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το αποτέλεσμα της Y, αν γνωρίζουμε το αποτέλεσμα της X;

Η συνδυασμένη και η υπό συνθήκη ποσότητα πληροφορίας είναι μη αρνητική. Η υπό συνθήκη ποσότητα πληροφορίας $H(X/Y)$ είναι μικρότερη ή ίση της $H(X)$. Η ισότητα ισχύει αν οι X και Y είναι ανεξάρτητες. Η απόδειξη αυτής της ανισότητας θα αποτελέσει το θέμα της επόμενης άσκησης.

Άσκηση αυτοαξιολόγησης 1.7

Να δείξετε ότι για δύο τυχαίες μεταβλητές X και Y ισχύει η ανισότητα

$$H(X/Y) \le H(X).$$

Η επόμενη πρόταση εκφράζει τη σχέση που υφίσταται μεταξύ των ακραίων, συνδυασμένων και υπό συνθήκη ποσοτήτων πληροφορίας.

Πρόταση 1.3

Για δύο τυχαίες μεταβλητές X και Y ισχύει

$$H(X,Y) = H(X) + H(Y/X) = H(Y) + H(X/Y).$$

Απόδειξη: Σύμφωνα με τον ορισμό της $H(X, Y)$ ισχύει

$$\begin{aligned} H(X,Y) &= -\sum_{i=1}^{1}\sum_{j=1}^{m} p(x_i,y_j)\log p(x_i,y_j) = -\sum_{i=1}^{1}\sum_{j=1}^{m} p(x_i,y_j)\log p(x_i)p(y_j/x_i) \\ &= -\sum_{i=1}^{1}\sum_{j=1}^{m} p(x_i,y_j)\log p(x_i) - \sum_{i=1}^{1}\sum_{j=1}^{m} p(x_i,y_j)\log p(y_j/x_i) \\ &= H(X) + H(Y/X). \end{aligned}$$

Κατά τον ίδιο τρόπο αποδεικνύεται και η σχέση $H(X,Y) = H(Y) + H(X/Y)$.

Άσκηση αυτοαξιολόγησης 1.8

Μια τράπουλα έχει 52 χαρτιά. Αυτά χωρίζονται σε τέσσερις κατηγορίες: τα μπαστούνια, τα σπαθιά, τις κούπες και τα καρό, με δεκατρία χαρτιά η καθεμία. Τα μπαστούνια και τα σπαθιά είναι μαύρου χρώματος και τα υπόλοιπα κόκκινου χρώματος. Το τυχαίο πείραμα συνίσταται στο τράβηγμα ενός χαρτιού από την τράπουλα. Θεωρούμε ότι για το κάθε χαρτί η πιθανότητα να είναι αποτέλεσμα του τυχαίου πειράματος είναι η ίδια.

1. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται μόνο το χρώμα του χαρτιού;
2. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το χρώμα και η κατηγορία στην οποία ανήκει το χαρτί;
3. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το χρώμα, η κατηγορία και ο αριθμός του χαρτιού;
4. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται ο αριθμός αν γνωρίζουμε ήδη το χρώμα του.
5. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται η κατηγορία αν το χρώμα του χαρτιού είναι ήδη γνωστό;

1.5.3 Η αμοιβαία ποσότητα πληροφορίας

Το τελευταίο ζήτημα αυτής της ενότητας αφορά στον ορισμό ενός μέτρου αμοιβαίας πληροφορίας δύο τυχαίων μεταβλητών X, Y. Η αμοιβαία πληροφορία είναι ένα μέτρο της ποσότητας πληροφορίας που μια τυχαία μεταβλητή περιέχει για μια άλλη τυχαία μεταβλητή ή ένα μέτρο της εξάρτησης μεταξύ δύο τυχαίων μεταβλητών.

Η αμοιβαία ποσότητα πληροφορίας (ή αμοιβαία πληροφορία)

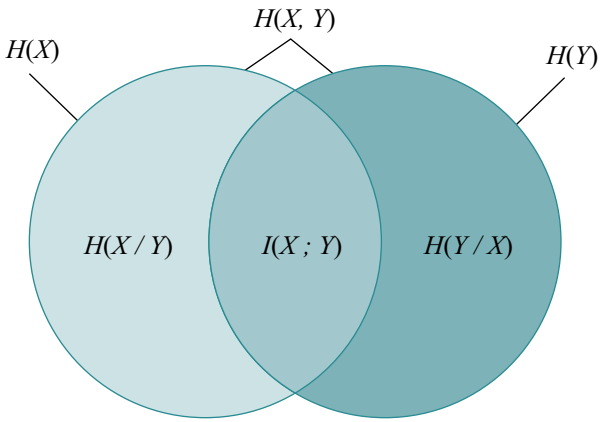
Η αμοιβαία πληροφορία δύο τυχαίων μεταβλητών X και Y ορίζεται από τη σχέση

$$I(X;Y) = H(Y) - H(Y/X)$$
$$= \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i)p(y_j)}.$$

Από τον ορισμό της αμοιβαίας πληροφορίας έχουμε

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ &= H(X) - H(X/Y) = H(Y) - H(X/Y). \end{aligned}$$

Παρατηρούμε πως η αμοιβαία ποσότητα πληροφορίας δύο ανεξάρτητων τυχαίων μεταβλητών είναι $I(X;Y) = 0$. Από την άλλη πλευρά, αν η X είναι πλήρως εξαρτημένη από την Y, δηλαδή $H(X/Y) = 0$, τότε $I(X;Y) = H(X) = H(Y)$. Το Σχήμα 1.6 παρουσιάζει τις σχέσεις μεταξύ των διαφόρων μέτρων ποσότητας πληροφορίας.



Σχήμα 1.6
Σχέσεις μεταξύ των μέτρων ποσότητας πληροφορίας

Παράδειγμα 1.5

Θεωρούμε ένα ψηφιακό επικοινωνιακό κανάλι που χρησιμοποιεί ως εισόδους και εξόδους τα σύμβολα «μηδέν» και «ένα». Οι συνδυασμένες πιθανότητες της δυαδικής εισόδου και εξόδου αυτού είναι

$$p(x_1,y_1) = p(x_1,y_2) = p(x_2,y_1) = p(x_2,y_2) = \frac{1}{4}.$$

Να βρεθούν τα διάφορα μέτρα πληροφορίας και η αμοιβαία ποσότητα πληροφορίας.

Απάντηση: Οι ακραίες πιθανότητες είναι $p(x_1) = p(x_2) = \frac{1}{2}$ και $p(y_1) = p(y_2) = \frac{1}{2}$. Τα μέτρα ποσότητας πληροφορίας είναι $H(X) = H(Y) = 1$ και $H(X,Y) = 2$. Από τις ποσότητες αυτές μπορούμε να υπολογίσουμε την αμοιβαία πληροφορία $I(X;Y) = H(X) + H(Y) - H(X,Y) = 0.$

Άσκηση αυτοαξιολόγησης 1.9

Υπολογίστε την αμοιβαία πληροφορία των δύο τυχαίων μεταβλητών X και Y της Άσκησης αυτοαξιολόγησης 6.

Μέχρι τώρα περιγράψαμε και εξηγήσαμε στις Ενότητες 1.4 και 1.5 τη μέση πληροφορία ή εντροπία μιας τυχαίας μεταβλητής, τη συνδυασμένη πληροφορία, την υπό συνθήκη και την αμοιβαία πληροφορία δύο τυχαίων μεταβλητών. Στον Πίνακα 1.1 θα συνοψίσουμε τους μαθηματικούς ορισμούς των διαφόρων αυτών μέτρων ποσότητας πληροφορίας και τις σχέσεις που ισχύουν μεταξύ αυτών.

Πίνακας 1.1

Μέτρα ποσότητας πληροφορίας και σχέσεις μεταξύ αυτών

Μέτρα ποσότητας πληροφορίας	**Μαθηματικός ορισμός (X, Y τυχαίες μεταβλητές)**	**Σχέσεις μεταξύ των διαφόρων μέτρων**
Μέση πληροφορία ή εντροπία	$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i)$	$H(X) \le \log n$ $H(X) \ge 0$
Συνδυασμένη πληροφορία	$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log p(x_i, y_j)$	$H(X,Y) = H(Y) + H(X/Y)$ $= H(X) + H(X/Y)$
Υπό συνθήκη πληροφορία	$H(X/Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log p(x_i / y_j)$	$H(X/Y) \le H(X)$
Αμοιβαία πληροφορία	$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i)p(y_j)}$	$I(X;Y) = H(X) + H(Y) - H(X,Y)$ $= H(X) - H(X/Y)$ $= H(Y) - H(Y/X)$

Άσκηση αυτοαξιολόγησης 1.10

Σύμφωνα με στατιστικές ιατρικών εξετάσεων, το 80% των ασθενών εμφανίζει χοληστερίνη υπεράνω του επιτρεπτού ορίου. Από τους ασθενείς που εμφανίζουν υψηλή χοληστερίνη ένα ποσοστό 75% κάνει δουλειά γραφείου, ενώ από τους ασθενείς με χαμηλό επίπεδο χοληστερίνης ένα ποσοστό 50% κάνει δουλειά γραφείου.

1. Ποια η ποσότητα πληροφορίας που λαμβάνει κάποιος αν του ειπωθεί το αποτέλεσμα μιας ιατρικής εξέτασης ως προς το επίπεδο χοληστερίνης;
2. Ποια η ποσότητα πληροφορίας που προσφέρεται όταν γνωστοποιείται αν κάποιος με υψηλή χοληστερίνη κάνει δουλειά γραφείου ή όχι;
3. Ποια η ποσότητα πληροφορίας που προσφέρει η γνωστοποίηση ότι κάποιος έχει υψηλή χοληστερίνη ως προς το αν κάνει δουλειά γραφείου ή όχι;

Άσκηση αυτοαξιολόγησης 1.11

Θεωρούμε και πάλι ένα ψηφιακό επικοινωνιακό κανάλι, όπως στο Παράδειγμα 5.

Δίνονται οι ακόλουθες πιθανότητες $p(x_1)=\frac{1}{2}$, $p(y_1/x_1)=\frac{3}{4}$, $p(y_1/x_2)=\frac{1}{4}$, όπου τα x_1, y_1 αναφέρονται στο σύμβολο «μηδέν» και τα x_2, y_2 στο σύμβολο «ένα».

1. Ποια ποσότητα πληροφορίας λαμβάνουμε αν μας γνωστοποιείται ποιο σύμβολο έχει ληφθεί στην έξοδο όταν γνωρίζουμε ότι στην είσοδο έχει σταλεί το «ένα»;
2. Ποια ποσότητα πληροφορίας λαμβάνουμε αν μας γνωστοποιείται ποιο σύμβολο έχει ληφθεί στην έξοδο όταν γνωρίζουμε ποιο σύμβολο είχε σταλεί στην είσοδο;
3. Ποια ποσότητα πληροφορίας λαμβάνουμε αν μας γνωστοποιείται ποιο σύμβολο έχει σταλεί στην είσοδο και ποιο σύμβολο έχει ληφθεί στην έξοδο;
4. Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται ποιο σύμβολο έχει σταλεί στην είσοδο όταν γνωρίζουμε ποιο σύμβολο έχει ληφθεί στην έξοδο;

Σύνοψη

Η Θεωρία Πληροφορίας είναι το επιστημονικό πεδίο που ασχολείται με τα μέτρα και τις εφαρμογές της έννοιας της «πληροφορίας». Απαντά, κατά βάση, σε δύο θεμελιώδεις ερωτήσεις: Ποια είναι η μεγαλύτερη δυνατή συμπίεση δεδομένων και ποιος ο μέγιστος δυνατός ρυθμός μετάδοσης σε ένα επικοινωνιακό κανάλι; Όριο της συμπίεσης δεδομένων αποτελεί η ποσότητα πληροφορίας (ή εντροπία), και του ρυθμού μετάδοσης σε ένα κανάλι η χωρητικότητά του.

Υπάρχουν τρεις τύποι πληροφορίας: ο συντακτικός, ο σημασιολογικός και ο πραγματικός. Η Θεωρία Πληροφορίας αναφέρεται στη συντακτική πληροφορία. Ο πρώτος που διατύπωσε ορισμό ενός μέτρου ποσότητας πληροφορίας είναι ο Hartley. Ακολούθησαν οι εργασίες των Shannon και Wiener. Ιδιαίτερα ο Shannon, συσχετίζοντας το μέτρο της πληροφορίας με την έννοια της πιθανότητας, θεωρείται ως ο πατέρας της σύγχρονης Θεωρίας Πληροφορίας.

Σε κάθε επικοινωνία λαμβάνει χώρα μεταφορά πληροφορίας από μια πηγή σ' έναν αποδέκτη, μέσω ενός καναλιού. Στο κανάλι επενεργεί θόρυβος, με αποτέλεσμα την αλλοίωση της μεταφερόμενης πληροφορίας. Για να είναι δυνατή η ανίχνευση και διόρθωση σφαλμάτων, θα πρέπει η πληροφορία να τύχει, στην πλευρά του μεταδότη, κατάλληλης επεξεργασίας ή κωδικοποίησης και, επομένως, αποκωδικοποίησης στον αποδέκτη. Επίσης, για την καλύτερη δυνατή αξιοποίηση ενός επικοινωνιακού καναλιού με περιορισμένη χωρητικότητα, η πληροφορία υποβάλλεται, στην πλευρά του αποστολέα, σε συμπίεση και στον αποδέκτη σε αποσυμπίεση. Τέλος, για την προστασία του περιεχομένου από υποκλοπή ή από σκόπιμη παραποίηση, η πληροφορία μπορεί να κρυπτογραφείται από το μεταδότη και να αποκρυπτογραφείται από τον παραλήπτη.

Η Θεωρία Πληροφορίας χρησιμοποιεί ως βασικό μαθηματικό εργαλείο τη Θεωρία Πιθανοτήτων. Απαραίτητες έννοιες από τη Θεωρία Πιθανοτήτων είναι αυτές του τυχαίου πειράματος, της διακριτής και συνεχούς τυχαίας μεταβλητής, της συνάρτησης κατανομής και πυκνότητας πιθανότητας. Ακόμη, οι έννοιες της συνδυασμένης, υπό συνθήκη και ακραίας πιθανότητας χρησιμοποιούνται στους ορισμούς διαφόρων μέτρων ποσότητας πληροφορίας και το θεώρημα του Bayes στους υπολογισμούς τους.

Ο Shannon όρισε τη μέση ποσότητα πληροφορίας ή μέση πληροφορία ή εντροπία μιας διακριτής τυχαίας μεταβλητής ως το αρνητικό άθροισμα των γινομένων της πιθανότητας κάθε γεγονότος με το λογάριθμό της. Η συνάρτηση αυτή είναι μη αρνητική, συνεχής, συμμετρική, προσθετική και παίρνει τη μέγιστη τιμή της όταν όλα τα γεγονότα έχουν ίση πιθανότητα να συμβούν.

Πολλές φορές μάς ενδιαφέρει η ποσότητα πληροφορίας συνδυασμού δύο ή περισσό-

τερων τυχαίων μεταβλητών. Για τις περιπτώσεις αυτές ορίστηκε η συνδυασμένη, η υπό συνθήκη και η αμοιβαία πληροφορία. Το συνδυασμένο μέτρο ποσότητας πληροφορίας ορίζεται, όπως η μέση πληροφορία, για όλους τους δυνατούς συνδυασμούς αποτελεσμάτων και πιθανοτήτων, αντίστοιχα. Το υπό συνθήκη μέτρο ποσότητας πληροφορίας αναφέρεται σε μία τυχαία μεταβλητή, δεδομένου του αποτελέσματος μιας άλλης τυχαίας μεταβλητής. Τέλος, η αμοιβαία πληροφορία είναι ένα μέτρο εξάρτησης μεταξύ δύο τυχαίων μεταβλητών.

Βιβλιογραφία

ΠΡΟΤΑΣΕΙΣ ΜΕΛΕΤΗΣ

Το βιβλίο του F. M. Reza «An Introduction to Information Theory», που εκδόθηκε το 1961 από τον εκδ. οίκο Dover Publications, περιγράφει μεταξύ άλλων την εξέλιξη της Θεωρίας Πληροφορίας έως το έτος έκδοσής του, καθώς και αναφορές στους επιστήμονες με σημαντική συμβολή στην ανάπτυξη αυτής. Επίσης, περιγράφει τα διάφορα μέτρα πληροφορίας αναλυτικά και αναφέρεται εκτενώς στις ιδιότητες και τις σχέσεις που ισχύουν μεταξύ αυτών. Η κλασική εργασία του Shannon, που δημοσιεύτηκε για πρώτη φορά το 1948 [SHA48] πραγματεύεται τα θέματα που γνωρίσαμε σ' αυτό το κεφάλαιο πολύ εύληπτα. Σε πιο προχωρημένο επίπεδο καλύπτεται η θεματολογία μας στα βιβλία των Abramson [ABR63] και Gallager [GAL68].

Ελληνική βιβλιογραφία

[1] [SHA79]K. S. Shanmugan: *Ψηφιακά και Αναλογικά Συστήματα Επικοινωνίας*, Μετάφραση – Επιμέλεια Κ. Καρούμπαλου, Αθήνα, Εκδ. Γ. Πνευματικού, 1979.

Ξενόγλωσση βιβλιογραφία

[1] [ABR63] N. Abramson: *Information Theory and Coding*, New York, McGraw – Hill, 1963.

[2] [ASH65] R. B. Ash: *Information Theory*, Dover Publications, 1965.

[3] [COT91] T. M. Cover, J. A. Thomas: *Elements of Information Theory*, John Willey & Sons, 1991.

[4] [CHA60] Chaundy T. W. and MacLeod J. B: «On a Functional Equation», *Proc. Edinburgh Mathematical Society Notes*, 43, 1960, pp. 7 – 8.

[5] [GAL68] R. G. Gallager: *Information Theory and Reliable Communication*, New York, John Wiley, 1968.

[6] [LUB97] J. C. A. Van der Lubbe: *Information Theory*, Cambridge University Press, 1997.

[7] [SHA48] C. E. Shannon: «Mathematical Theory of Communication», *Bell System Technical Journal*, vol. 27, 1948, pp. 379 – 423, 623 – 656.

ΚΕΦΑΛΑΙΟ 2

Πηγές Πληροφορίας

Σκοπός

Ο σκοπός του κεφαλαίου αυτού είναι να περιγραφούν οι διακριτές πηγές πληροφορίας με και χωρίς μνήμη, οι συνεχείς πηγές πληροφορίας, καθώς και τεχνικές κωδικοποίησης για την όσο το δυνατόν συμπυκνωμένη αναπαράσταση της πληροφορίας τέτοιων πηγών.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *υπολογίζετε την εντροπία, τη μέγιστη ποσότητα πληροφορίας, τον πλεονασμό και το μέσο ρυθμό πληροφορίας διακριτής πηγής πληροφορίας χωρίς μνήμη και με μνήμη,*
- *εξετάζετε αν δεδομένοι κώδικες είναι μη ιδιάζοντες (non – singular), μοναδικά αποκωδικοποιήσιμοι και άμεσοι και να υπολογίζετε την επίδοσή τους,*
- *εξηγείτε τρεις αλγόριθμους κωδικοποίησης και να σχηματίζετε κώδικες που βασίζονται σ' αυτούς,*
- *υπολογίζετε την εντροπία καταστάσεων πηγών Markoff και την εντροπία πηγών Markoff,*
- *διατυπώνετε το θεώρημα που συσχετίζει τη μέση ποσότητα πληροφορίας μηνυμάτων με την εντροπία διακριτής πηγής με μνήμη,*
- *υπολογίζετε τον πλεονασμό, τον πλεονασμό εξάρτησης και τον ολικό πλεονασμό διακριτών πηγών με μνήμη,*
- *υπολογίζετε την εντροπία συνεχών πηγών, καθώς και να διατυπώνετε ένα θεώρημα σχετικά με τη μέγιστη τιμή της εντροπίας.*

Έννοιες κλειδιά

- *διακριτή πηγή πληροφορίας,*
- *αλφάβητο πηγής,*
- *κωδική λέξη,*
- *μέσο πληροφορικό περιεχόμενο συμβόλων διακριτής πηγής χωρίς μνήμη,*
- *μέσο πληροφορικό περιεχόμενο μηνυμάτων διακριτής πηγής με μνήμη,*
- *πλεονασμός διακριτής πηγής,*

- *κωδικοποίηση πηγής ή συμπίεση*,
- *ρυθμός πληροφορίας διακριτής πηγής*,
- *πλεονασμός εξάρτησης διακριτής πηγής με μνήμη*,
- *ολικός πλεονασμός διακριτής πηγής με μνήμη*,
- *μη ιδιάζοντες* (*non – singular*) *κώδικες*,
- *μοναδικά αποκωδικοποιήσιμοι κώδικες*,
- *άμεσος κώδικας*,
- *ανισότητα Kraft*,
- *επίδοση κώδικα*,
- *εντροπία πηγών Markoff*,
- *εντροπία καταστάσεων πηγών Markoff*,
- *συνεχή μέτρα ποσότητας πληροφορίας*,
- *μέγιστη εντροπία τυχαίων σημάτων*

Εισαγωγικές παρατηρήσεις

Το κεφάλαιο αυτό αποτελείται από τρεις ενότητες. Στην πρώτη ενότητα περιγράφονται οι διακριτές πηγές πληροφορίας χωρίς μνήμη και τεχνικές κωδικοποίησης γι' αυτές τις πηγές. Στη δεύτερη ενότητα περιγράφονται οι διακριτές πηγές πληροφορίας με μνήμη και σχετικές τεχνικές κωδικοποίησης. Τέλος, στην τρίτη ενότητα επεκτείνεται ο ορισμός του μέτρου της ποσότητας πληροφορίας στην περίπτωση συνεχούς τυχαίας μεταβλητής και περιγράφονται συνεχείς πηγές πληροφορίας.

2.1 Διάκριτες πηγές πληροφορίας χωρίς μνήμη

Με τον όρο **διακριτή πηγή πληροφορίας** εννοούμε μια πηγή πληροφορίας που παράγει ακολουθίες συμβόλων (ή γραμμάτων). Το σύνολο των συμβόλων ονομάζεται **αλφάβητο πηγής**. Τα σύμβολα δημιουργούνται από την πηγή σε διακριτές χρονικές στιγμές. Για το λόγο αυτό και λόγω του πεπερασμένου πλήθους των συμβόλων η πηγή ονομάζεται διακριτή. Μια ομάδα διαδοχικών συμβόλων ονομάζεται **μήνυμα ή λέξη**.

Η επιλογή ενός συμβόλου κατά τη δημιουργία μηνυμάτων από την πηγή λαμβάνει χώρα με κάποια πιθανότητα. Θεωρούμε πως οι πιθανότητες επιλογής των συμβόλων παραμένουν αμετάβλητες με το πέρασμα του χρόνου, δηλαδή είναι ανεξάρτητες του χρόνου. Επίσης, θεωρούμε πως η επιλογή ενός συμβόλου δεν εξαρτάται από τα προηγούμενα σύμβολα του μηνύματος. Ακριβώς γι' αυτό το λόγο, δηλαδή το ότι η πιθανότητα επιλογής ενός συμβόλου κατά τη δημιουργία ενός μηνύματος από την πηγή είναι σταθερή και ανεξάρτητη από τις επιλογές των προηγούμενων συμβόλων, η διακριτή πηγή πληροφορίας ονομάζεται **διακριτή πηγή πληροφορίας χωρίς μνήμη**. Αντίθετα, η στατιστική εξάρτηση της επιλογής ενός συμβόλου από προηγούμενα σύμβολα του μηνύματος χαρακτηρίζει μια **πηγή με μνήμη**.

Στη συνέχεια θα συμβολίζουμε τα σύμβολα με $s_1, s_2, \ldots, s_n$, όπου n το πλήθος των συμβόλων του αλφαβήτου και με S το αλφάβητο. Τα μηνύματα θα συμβολίζονται με $m_1, m_2, \ldots, m_q$, όπου q το πλήθος των δυνατών μηνυμάτων και το σύνολο όλων των μηνυμάτων θα συμβολίζεται με M. Αν κάθε μήνυμα αποτελείται από l σύμβολα, τότε το πλήθος των δυνατών μηνυμάτων, q, είναι ίσο με n^l. Επίσης, με p_i συμβολίζουμε την αμετάβλητη στο χρόνο πιθανότητα επιλογής του συμβόλου s_i.

Στις επόμενες υποενότητες, θα εξετάσουμε την ποσότητα πληροφορίας (ή πληροφορικό περιεχόμενο) των συμβόλων και των μηνυμάτων της πηγής, τον πλεονασμό της πηγής και θα μελετήσουμε γενικά ζητήματα και ειδικές στρατηγικές κωδικοποίησης, καθώς και την έννοια των πιο πιθανών μηνυμάτων.

2.1.1 Ποσοότητα πληροφορίας της πηγής

Όπως ήδη είπαμε, τα μηνύματα που παράγονται από τις πηγές πληροφορίας αποτελούνται από ακολουθίες συμβόλων. Αν και τα μηνύματα είναι αυτά που ενδιαφέρουν τόσο τους αποστολείς όσο και τους τελικούς παραλήπτες, τα επικοινωνιακά συστήματα ασχολούνται με το καθένα από τα σύμβολα που απαρτίζουν τα μηνύματα. Για παράδειγμα, αν στέλνουμε ένα μήνυμα με ηλεκτρονικό ταχυδρομείο, ο παραλήπτης ενδιαφέρεται κυρίως για τις λέξεις και τις προτάσεις, ενώ το σύστημα επι-

κοινωνίας έχει να κάνει με το καθένα από τα σύμβολα (γράμματα) που το αποτελούν. Επομένως, από τη σκοπιά των επικοινωνιακών συστημάτων υπάρχει ενδιαφέρον για την ποσότητα πληροφορίας (πληροφορικό περιεχόμενο) των συμβόλων που παράγει η πηγή.

Η **μέση ποσότητα πληροφορίας (ή το μέσο πληροφορικό περιεχόμενο ή η εντροπία) συμβόλων** που δημιουργούνται από μια διακριτή πηγή χωρίς μνήμη με αλφάβητο $S = \{s_1, s_2, \ldots, s_n\}$, όπου n το πλήθος των συμβόλων του αλφαβήτου και p_i η πιθανότητα επιλογής του συμβόλου s_i, δίνεται από την ακόλουθη σχέση:

$$H(S) = -\sum_{i=1}^{n} p_i \log p_i \text{ bits / symbol.} \tag{2.1}$$

Η **μέγιστη μέση ποσότητα πληροφορίας των συμβόλων** που μπορεί να παραχθεί από μια διακριτή πηγή πληροφορίας χωρίς μνήμη δίνεται από τη σχέση (2.2). Όπως είδαμε στην Πρόταση 1 / Κεφάλαιο 1, στην Υποενότητα 1.4.2, η μέγιστη ποσότητα πληροφορίας μιας τυχαίας μεταβλητής επιτυγχάνεται όταν τα δυνατά ενδεχόμενα είναι ισοπίθανα. Κατ' ανάλογο τρόπο, η μέγιστη εντροπία των συμβόλων της πηγής επιτυγχάνεται όταν οι πιθανότητες επιλογής τους είναι ίσες:

$$\max H(S) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = \log n \text{ bits / symbol.} \tag{2.2}$$

Ο **πλεονασμός της διακριτής πηγής** ορίζεται από τη σχέση (2.3), όπου $H(S)$ είναι το μέσο πληροφορικό περιεχόμενο της πηγής με αλφάβητο αποτελούμενο από n σύμβολα:

$$red = 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{H(S)}{\log n}. \tag{2.3}$$

Αφού η εντροπία είναι μικρότερη ή ίση της μέγιστης εντροπίας μιας πηγής, ο πλεονασμός της πηγής λαμβάνει τιμές στο διάστημα [0, 1].

Λαμβάνοντας υπόψη ότι η πηγή παράγει σύμβολα με ρυθμό r_s symbols/sec, ορίζουμε το μέσο ρυθμό πληροφορίας της πηγής, R, ως το γινόμενο του ρυθμού συμβόλων με το μέσο πληροφορικό περιεχόμενο των συμβόλων της πηγής:

$$R = r_s H(S) \text{ bits / sec.} \tag{2.4}$$

Παράδειγμα 2.1

Μια δυαδική πηγή χωρίς μνήμη εκπέμπει (παράγει) τα δύο σύμβολα 0 και 1 σε στα-

τιστικά ανεξάρτητες ακολουθίες με πιθανότητες 0,75 και 0,25, αντίστοιχα. Να υπολογιστούν η εντροπία, η μέγιστη μέση ποσότητα πληροφορίας, και ο πλεονασμός της πηγής.

Απάντηση: Το αλφάβητο της πηγής είναι $S = \{0, 1\}$ και οι αντίστοιχες πιθανότητες συμβόλων 3/4 *και* 1/4. Οι εξισώσεις (2.1), (2.2) και (2.3) μάς επιτρέπουν να υπολογίσουμε την εντροπία, τη μέγιστη μέση ποσότητα πληροφορίας, καθώς και τον πλεονασμό της πηγής:

$$H(S) = -\sum_{i=1}^{2} p_i \log p_i = -\frac{3}{4}\log\frac{3}{4} - \frac{1}{4}\log\frac{1}{4} = 0{,}81 \text{ bit / symbol},$$

$$\max H(S) = \log 2 = 1 \text{ bit / symbol},$$

$$red = 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{0{,}81}{1} = 0{,}19.$$

Άσκηση αυτοαξιολόγησης 2.1

Βρείτε το μέσο πληροφορικό περιεχόμενο (εντροπία), τη μέγιστη μέση ποσότητα πληροφορίας και τον πλεονασμό διακριτής πηγής χωρίς μνήμη που παράγει τα σύμβολα X, Ψ και Ω με ρυθμό 1.000 σύμβολα το δευτερόλεπτο και πιθανότητες 0,25, 0,5 και 0,25, αντίστοιχα. Επίσης, υπολογίστε το μέσο ρυθμό πληροφορίας της πηγής.

Επίσης, μπορούμε να ορίσουμε το **μέσο πληροφορικό περιεχόμενο μηνυμάτων της πηγής** κατά ανάλογο τρόπο. $M = \{m_1, m_2, \ldots, m_q\}$ είναι το σύνολο των δυνατών μηνυμάτων, q το πλήθος των δυνατών μηνυμάτων ($q = n^l$, όπου n το πλήθος των συμβόλων του αλφαβήτου) και $P = \{p(m_1), p(m_2), \ldots, p(m_q)\}$ η κατανομή πιθανοτήτων:

$$H(M) = -\sum_{i=1}^{q} p(m_i) \log p(m_i) \text{ bits / message} \qquad (2.5)$$

Παράδειγμα 2.2

Υποθέτουμε ότι η δυαδική πηγή του Παραδείγματος 1 παράγει μηνύματα αποτελούμενα από δύο σύμβολα. Να υπολογιστεί το μέσο πληροφορικό περιεχόμενο των μηνυμάτων της πηγής.

Απάντηση: Προφανώς τα δυνατά μηνύματα είναι τέσσερα, $M = \{(00), (01), (10),$

(11)}. Η πιθανότητα εκπομπής (παραγωγής) καθενός από τα μηνύματα είναι ίση με το γινόμενο των πιθανοτήτων των συμβόλων από τα οποία αποτελείται, αφού οι ακολουθίες συμβόλων (μηνύματα) είναι στατιστικά ανεξάρτητες (πηγή χωρίς μνήμη). Επομένως, $P = \{(9/16), (3/16), (3/16), (1/16)\}$. Για τον υπολογισμό του μέσου πληροφορικού περιεχομένου μηνυμάτων της πηγής χρησιμοποιούμε την εξίσωση (2.5):

$$H(M) = -\sum_{i=1}^{4} p(m_i) \log p(m_i)$$

$$= -\frac{9}{16}\log\frac{9}{16} - \frac{3}{16}\log\frac{3}{16} - \frac{3}{16}\log\frac{3}{16} - \frac{1}{16}\log\frac{1}{16} = 1{,}63 \text{ bits / message.}$$

Συγκρίνοντας τα αποτελέσματα των Παραδειγμάτων 1 και 2, παρατηρούμε ότι το μέσο πληροφορικό περιεχόμενο της πηγής σε επίπεδο μηνυμάτων είναι διπλάσιο από αυτό σε επίπεδο συμβόλων. Αυτό είναι ακριβώς όπως το περιμέναμε, αφού τα μηνύματα αποτελούνται από δύο σύμβολα. Ισχύει, λοιπόν, η ακόλουθη σχέση για μηνύματα αποτελούμενα από q σύμβολα:

$$H(M) = qH(S).$$

Τη σχέση αυτή μπορείτε να την επιβεβαιώσετε με τα αποτελέσματα της Άσκησης αυτοαξιολόγησης 2 και για μηνύματα αποτελούμενα από τρία σύμβολα.

Άσκηση αυτοαξιολόγησης 2.2

Υποθέτουμε μια δυαδική πηγή χωρίς μνήμη που εκπέμπει μηνύματα αποτελούμενα από τρία σύμβολα. Οι πιθανότητες επιλογής των συμβόλων 0 και 1 είναι 3/4 και 1/4, αντίστοιχα (όπως και στα Παραδείγματα 1 και 2). Να υπολογιστεί το μέσο πληροφορικό περιεχόμενο των μηνυμάτων της πηγής.

2.1.2 Κωδικοποίηση πηγής

Σύμφωνα με το επικοινωνιακό μοντέλο (Υποενότητα 1.2.2), τη δημιουργία των μηνυμάτων από την πηγή ακολουθεί η απαλοιφή δεδομένων για την απομάκρυνση της μη σχετικής για τον προορισμό πληροφορίας. Εδώ, ωστόσο, υποθέτουμε ότι η πηγή παράγει μηνύματα που ενδιαφέρουν τον προορισμό στην ολότητά τους, και έτσι δεν θα μας απασχολήσει το ζήτημα αυτό.

Για την καλύτερη δυνατή απόδοση των επικοινωνιακών συστημάτων, επιδιώκεται η όσο το δυνατόν πιο συμπυκνωμένη αναπαράσταση των μηνυμάτων, η οποία επιτυγχάνεται με την αφαίρεση του πλεονασμού που εμπεριέχεται σ' αυτά. Αυτή η διαδι-

κασία ονομάζεται **κωδικοποίηση πηγής**. Στην περιγραφή του λεπτομερούς επικοινωνιακού μοντέλου (Σχήμα 1.3, Υποενότητα 1.2.2) χρησιμοποιήθηκε ο όρος **συμπίεση** αντί του όρου κωδικοποίηση πηγής, που επίσης συνηθίζεται στη βιβλιογραφία.

Πιο συγκεκριμένα, **κωδικοποίηση πηγής** είναι η διαδικασία μετατροπής των ακολουθιών συμβόλων που παράγει η πηγή σε ακολουθίες συμβόλων κάποιου κώδικα (συνήθως δυαδικές ακολουθίες), έτσι ώστε να αφαιρείται ο πλεονασμός και να προκύπτει συμπιεσμένη αναπαράσταση των μηνυμάτων. Επειδή εξετάζουμε πηγές χωρίς μνήμη, δηλαδή ανεξάρτητες ακολουθίες συμβόλων, το ενδιαφέρον μας ως προς την κωδικοποίηση μετατοπίζεται από τα μηνύματα στα σύμβολα. Όπως θα πετύχουμε στη συνέχεια τη μετατροπή συμβόλων πηγής σε ακολουθίες κωδικών συμβόλων, θα μπορούσαμε να πετύχουμε και τη μετατροπή μηνυμάτων της πηγής σε ακολουθίες κωδικών συμβόλων.

Τα διαφορετικά κωδικά σύμβολα που χρησιμοποιούμε για τη μετατροπή των συμβόλων ή ακολουθιών συμβόλων της πηγής σε ακολουθίες κωδικών συμβόλων απαρτίζουν το επονομαζόμενο **κωδικό αλφάβητο**. Καθώς το δυαδικό αλφάβητο έχει, όπως γνωρίζουμε, τα σύμβολα 0 και 1, η κωδικοποίηση οδηγεί, στην περίπτωση αυτή, σε μετατροπή των συμβόλων ή ακολουθιών συμβόλων της πηγής σε δυαδικές ακολουθίες. Κατά την κωδικοποίηση, λοιπόν, το κάθε σύμβολο που παράγεται από την πηγή αναπαρίσταται με μια **ακολουθία κωδικών συμβόλων** (ή μια **κωδική λέξη**). **Κώδικας** είναι το σύνολο των κωδικών λέξεων και η αντιστοίχηση αυτών με τα σύμβολα (ή τις ακολουθίες συμβόλων αν πρόκειται για κωδικοποίηση μηνυμάτων) της πηγής.

Παράδειγμα 2.3

Ένας πολύ γνωστός κώδικας είναι αυτός του Morse, ο οποίος χρησιμοποιεί ένα κωδικό αλφάβητο με τα εξής τέσσερα σύμβολα: τελεία (dot), παύλα (dash), διάστημα γράμματος (letter space) και διάστημα λέξης (word space). Η εκπομπή μιας τελείας συνίσταται στη μετάδοση σήματος διάρκειας μιας μονάδας του χρόνου, η οποία ακολουθείται από παύση μετάδοσης διάρκειας ακόμα μιας μονάδας του χρόνου. Στην περίπτωση της εκπομπής μιας παύλας, η μετάδοση σήματος διαρκεί τρεις μονάδες του χρόνου και η εκπομπή της παύλας ολοκληρώνεται με παύση μετάδοσης διάρκειας μιας μονάδας του χρόνου. Όσο για το διάστημα γράμματος, αυτό συνίσταται από παύση μετάδοσης διάρκειας τριών μονάδων του χρόνου, ενώ το διάστημα λέξης από παύση μετάδοσης διάρκειας έξι μονάδων του χρόνου. Στον κώδικα Μορς κωδικές λέξεις μικρού μήκους αναπαριστούν γράμματα του αγγλικού αλφάβητου που εμφανίζονται με υψηλή συχνότητα (μια απλή τελεία, «.», αναπαριστά το Ε και μια

τελεία και μια παύλα, «. – », το Α), ενώ, αντίθετα, κωδικές λέξεις μεγάλου μήκους αναπαριστούν γράμματα με χαμηλή συχνότητα εμφάνισης («—..» ή «dash dash dot dot» αναπαριστά το Z). Μεταξύ διαφορετικών γραμμάτων ή των αντίστοιχων κωδικών λέξεων παρεμβάλλονται τα διαστήματα γραμμάτων (letter space) και μεταξύ λέξεων του μηνύματος ή των αντίστοιχων ακολουθιών κωδικών λέξεων παρεμβάλλονται τα διαστήματα λέξεων (word space). Όσο για το σημείο στίξης «τελεία», αυτό αναπαρίσταται από την κωδική λέξη «. – . – . – » ή «dot dash dot dash dot dash».

Αν όλες οι κωδικές λέξεις είναι διαφορετικές, ο κώδικας χαρακτηρίζεται ως **μη ιδιάζων** (non – singular). Αν και οι δυνατές ακολουθίες κωδικών λέξεων είναι διαφορετικές, ο κώδικας είναι **μοναδικά αποκωδικοποιήσιμος** (uniquely decodable). Αν, τέλος, ένας μοναδικά αποκωδικοποιήσιμος κώδικας επιτρέπει την άμεση αποκωδικοποίηση κάθε κωδικοποιημένου συμβόλου (μιας κωδικής λέξης) μόλις λαμβάνεται στον προορισμό (χωρίς να πρέπει να ληφθεί και η επόμενη ή επόμενες κωδικές λέξεις), τότε χαρακτηρίζεται ως **άμεσος κώδικας** (instantaneous code).

Παράδειγμα 2.4

Υποθέτουμε μια διακριτή πηγή χωρίς μνήμη με τέσσερα σύμβολα, τα Φ, Χ, Ψ και Ω. Επίσης, ένα κωδικό αλφάβητο αποτελούμενο από τα σύμβολα 0 και 1. Τέσσερις διαφορετικές τεχνικές κωδικοποίησης, I, II, III και IV οδηγούν στους δυαδικούς κώδικες που παρατίθενται στη συνέχεια.

	I	II	III	IV
Φ	0	00	0	0
Χ	11	01	10	01
Ψ	00	10	110	011
Ω	01	11	1110	0111

Να εξεταστεί αν οι κώδικες αυτοί είναι μη ιδιάζοντες, μοναδικά αποκωδικοποιήσιμοι και άμεσοι.

Απάντηση: Προφανώς όλοι οι κώδικες είναι μη ιδιάζοντες, αφού ο καθένας αποτελείται από διαφορετικές κωδικές λέξεις. Ο κώδικας I δεν είναι μοναδικά αποκωδικοποιήσιμος, αφού η ακολουθία κωδικών λέξεων 0000 μπορεί να ληφθεί για τις ακολουθίες συμβόλων της πηγής «ΦΦΦΦ» ή «ΦΦΨ» ή «ΨΨ». Αντίθετα, οι υπόλοιποι κώδικες είναι μοναδικά αποκωδικοποιήσιμοι, δηλαδή όλοι οι δυνατοί συνδυασμοί κωδικών λέξεων είναι διαφορετικοί. Ο κώδικας II γιατί οι λέξεις του έχουν το ίδιο μήκος (2 κωδικά σύμβολα) και οι κώδικες III και IV γιατί η κάθε κωδική λέξη ολο-

κληρώνεται με το «0» ή αρχίζει με το «0», αντίστοιχα. Τέλος, οι κώδικες ΙΙ και ΙΙΙ είναι άμεσοι. Ο κώδικας ΙΙ γιατί κάθε κωδικοποιημένο σύμβολο πηγής αναπαρίσταται από δύο δυαδικά σύμβολα, που μόλις ληφθούν στον προορισμό μπορούν άμεσα να αποκωδικοποιηθούν στο αντίστοιχο σύμβολο. Ο κώδικας ΙΙΙ γιατί, μόλις ληφθεί το δυαδικό ψηφίο «0», αυτό ως τελευταίο ψηφίο της ακολουθίας και όλα τα «1» που προηγήθηκαν μπορούν να αποκωδικοποιηθούν άμεσα στο αντίστοιχο σύμβολο της πηγής. Αντίθετα, ο κώδικας IV δεν είναι άμεσος, αφού για την αποκωδικοποίηση μιας κωδικής λέξης δεν αρκεί να ληφθεί και το τελευταίο σύμβολο (ψηφίο) αυτής της λέξης, αλλά θα πρέπει να ληφθεί και το πρώτο ψηφίο της επόμενης κωδικής λέξης που αρχίζει με το «0», αφού μόνο τότε αναγνωρίζεται ότι ολοκληρώθηκε προηγουμένως η λήψη μιας κωδικής λέξης στον προορισμό και, επομένως, μόνο τότε είναι δυνατή η αποκωδικοποίησή της, και όχι άμεσα με τη λήψη του τελευταίου ψηφίου.

Ένας κώδικας, του οποίου κωδικές λέξεις αποτελούν προθέματα άλλων κωδικών λέξεων δεν μπορεί να είναι άμεσος, αφού η ολοκλήρωση της λήψης τους στον προορισμό δεν μπορεί να αναγνωριστεί και, επομένως, η αποκωδικοποίηση δεν μπορεί να επιτευχθεί άμεσα. Ο κώδικας IV του Παραδείγματος 4 έχει τις κωδικές λέξεις «0», «01», «011» και «0111». Ο παραλήπτης, όταν λάβει το σύμβολο «0», δε γνωρίζει αν πρόκειται για την πρώτη κωδική λέξη ή είναι το πρώτο ψηφίο μιας από τις υπόλοιπες. Επίσης, αν λάβει «01» δε γνωρίζει αν πρόκειται για τη δεύτερη κωδική λέξη ή αν είναι τα δύο πρώτα ψηφία της τρίτης ή της τέταρτης κωδικής λέξης κ.ο.κ. Επομένως, δεν είναι δυνατή η άμεση αποκωδικοποίηση, αφού θα πρέπει πρώτα να αναγνωριστεί η ολοκλήρωση της λήψης μιας κωδικής λέξης, που επιτυγχάνεται με τη λήψη του πρώτου ψηφίου της επόμενης κωδικής λέξης.

Επιθυμούμε ασφαλώς την κατασκευή άμεσων κωδίκων με το ελάχιστο προσδοκώμενο μήκος για τη συμπιεσμένη αναπαράσταση των συμβόλων μιας πηγής. Είναι, βέβαια, φανερό από την αμέσως προηγούμενη παράγραφο και το Παράδειγμα 4 ότι δεν μπορούμε να έχουμε πολύ μικρές κωδικές λέξεις για όλα τα σύμβολα της πηγής και ο κώδικας να είναι άμεσος, αφού κάποιες θα είναι προθέματα άλλων. Η ανισότητα του Kraft, που ακολουθεί, περιορίζει το σύνολο των δυνατών μηκών των κωδικών λέξεων για να είναι ένας κώδικας άμεσος.

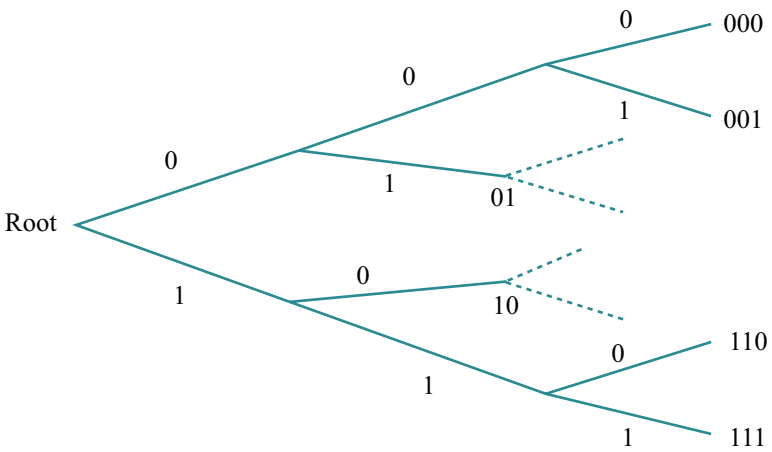
Ανισότητα του Kraft

Για κάθε άμεσο κώδικα με πλήθος συμβόλων του κωδικού αλφάβητου q και μήκη των κωδικών λέξεων l_i, όπου $i = 1, 2, \ldots, n$ και n το πλήθος των συμβόλων της πηγής, ισχύει η ακόλουθη ανισότητα (2.6). Αντίστροφα, δεδομένου ενός συνόλου μηκών κωδικών λέξεων που ικανοποιούν την ανισότητα (2.6), υπάρχει ένας άμεσος κώδι-

κας με κωδικές λέξεις που έχουν αυτά τα μήκη.

$$\sum_{i=1}^{n} q^{-l_i} \leq 1. \tag{2.6}$$

Απόδειξη: Ας παρατηρήσουμε μια δεντρική δομή, της οποίας κάθε κόμβος έχει q παιδιά. Τα κλαδιά του δέντρου αναπαριστούν τα σύμβολα του κωδικού αλφάβητου και τα φύλλα τις κωδικές λέξεις. Η διαδρομή από τη βάση του δέντρου (root) προς ένα κόμβο – φύλλο περιγράφει τα κωδικά σύμβολα από τα οποία αποτελείται η κωδική λέξη που αναπαρίσταται από τον κόμβο αυτό. Στο Σχήμα 2.1 παρουσιάζεται ένα παράδειγμα δεντρικής δομής για $q = 2$.



Σχήμα 2.1
Δυαδική δεντρική δομή

Αν l_{max} είναι το μέγιστο μήκος κωδικών λέξεων, τότε όλοι οι κόμβοι του δέντρου στο επίπεδο αυτό είναι είτε κωδικές λέξεις είτε (άμεσοι ή μακρινοί) απόγονοι κωδικών λέξεων. Το πλήθος των απογόνων μιας κωδικής λέξης του επιπέδου l_i που βρίσκονται στο επίπεδο l_{max} είναι ίσο με τη δύναμη του πλήθους των κωδικών συμβόλων q στη διαφορά $(l_{max} - l_i)$. Καθένα από τα σύνολα αυτά απογόνων δεν έχει κοινό στοιχείο με οποιοδήποτε από τα υπόλοιπα. Επίσης, το άθροισμα των απογόνων όλων των κωδικών λέξεων οι οποίοι βρίσκονται στο επίπεδο l_{max} δεν μπορεί να ξεπεράσει τη δύναμη του q στο l_{max}, αφού αυτός είναι ο αριθμός των κόμβων – φύλλων στο επίπεδο l_{max} αν έχουμε πλήρη ανάπτυξη της δεντρικής δομής. Επομένως, για το άθροισμα των απογόνων όλων των κωδικών λέξεων στο επίπεδο l_{max} ισχύει

$$\sum_i q^{l_{\max} - l_i} \leq q^{l_{\max}} \quad \text{ή} \quad \sum_i q^{-l_i} \leq 1.$$

Αντίστροφα, αν δίνονται τα μήκη κωδικών λέξεων, $l_1, l_2, \ldots, l_n$, που ικανοποιούν την

ανισότητα του Kraft, τότε μπορούμε να κατασκευάσουμε ένα δέντρο όπως αυτό του Σχήματος 2.1. Με τη βοήθεια του δέντρου μπορούμε να προσδιορίσουμε κωδικές λέξεις με τα δεδομένα μήκη που απαρτίζουν έναν άμεσο κώδικα. Πιο συγκεκριμένα, τον πρώτο κόμβο του δέντρου μήκους l_1 τον χαρακτηρίζουμε ως κωδική λέξη 1 και διαγράφουμε όλους τους απογόνους του από το δέντρο, το δεύτερο κόμβο μήκους l_2 τον χαρακτηρίζουμε κωδική λέξη 2 και διαγράφουμε τους απογόνους του από το δέντρο κ.ο.κ. Κατ' αυτόν τον τρόπο μπορούμε να κατασκευάσουμε έναν άμεσο κώδικα με τα δεδομένα μήκη κωδικών λέξεων.

Η ανισότητα του Kraft υποδηλώνει ότι υπάρχει άμεσος κώδικας με μήκη κωδικών λέξεων l_i και όχι ότι κάθε κώδικας με μήκη λέξεων l_i είναι άμεσος.

ΘΕΩΡΗΜΑ 2.1 (ΘΕΩΡΗΜΑ ΚΩΔΙΚΟΠΟΙΗΣΗΣ ΠΗΓΗΣ)

Θεωρούμε ένα κωδικό αλφάβητο αποτελούμενο από q σύμβολα και n κωδικές λέξεις των n συμβόλων της πηγής, καθώς και τις πιθανότητες εμφάνισης των συμβόλων της πηγής $P = \{p_1, p_2, \ldots, p_n\}$. Αν ισχύει η (2.6), τότε ισχύει και η ακόλουθη ανισότητα (l_i είναι τα μήκη και $H(C)$ το μέσο πληροφορικό περιεχόμενο των κωδικών λέξεων ή των συμβόλων της πηγής):

$$\frac{H(C)}{\log q} \leq \sum_{i=1}^{n} p_i l_i. \tag{2.7}$$

Απόδειξη:

$$\begin{aligned} H(C) - \log q \sum_{i=1}^{n} p_i l_i &= -\sum_{i=1}^{n} \left(p_i \log p_i + p_i l_i \log q \right) = -\sum_{i=1}^{n} p_i \log\left(p_i q^{l_i} \right) \\ &= \sum_{i=1}^{n} p_i \log\left(\frac{1}{p_i q^{l_i}} \right) = \sum_{i=1}^{n} p_i \frac{\ln\left(\frac{1}{p_i q^{l_i}} \right)}{\ln 2}. \end{aligned} \tag{2.8}$$

Λαμβάνοντας υπόψη την ισχύ της $\ln a \leq a - 1$ για α > 0 (δείτε Σχήμα 1.5, Υποενότητα 1.4.2), ακολουθεί από τη σχέση (2.8):

$$\sum_{i=1}^{n} p_i \ln\left(\frac{1}{p_i q^{l_i}} \right) \leq \sum_{i=1}^{n} p_i \left(\frac{1}{p_i q^{l_i}} - 1 \right) = \sum_{i=1}^{n} q^{-l_i} - 1.$$

Επομένως, από τη (2.6) ακολουθεί η ισχύς της ανισότητας (2.7). (Το μέσο πληροφορικό περιεχόμενο των κωδικών λέξεων είναι προφανώς ίσο με το μέσο πληροφορικό περιεχόμενο των συμβόλων της πηγής.)

Σύμφωνα με το θεώρημα κωδικοποίησης πηγής, λοιπόν, το μέσο μήκος των κωδικών λέξεων δεν μπορεί να είναι μικρότερο από το μέσο πληροφορικό περιεχόμενο της πηγής σε μονάδα μέτρησης που προκύπτει με βάση του λογάριθμου το q.

Δραστηριότητα 2.1

Προσπαθήστε να ελαχιστοποιήσετε το μέσο μήκος των κωδικών λέξεων, $\Sigma p_i l_i$, για όλα τα μήκη, $l_1, l_2, \ldots, l_n$, που ικανοποιούν την ανισότητα του Kraft. (Το πρόβλημα αυτό θα μας απασχολήσει στη συνέχεια.)

Ας εξετάσουμε τώρα το πρόβλημα εύρεσης του άμεσου κώδικα με το ελάχιστο μέσο μήκος κωδικών λέξεων για μια δεδομένη πηγή. Το **πρόβλημα** αυτό είναι ένα τυπικό πρόβλημα αριστοποίησης, το οποίο διατυπώνεται ως εξής: **Ελαχιστοποίησε το μέσο μήκος των κωδικών λέξεων**, $\Sigma p_i l_i$, για όλους τους ακέραιους, $l_1, l_2, \ldots, l_n$, που ικανοποιούν την ανισότητα του Kraft.

Αν παραβλέψουμε καταρχήν το ότι τα μήκη των κωδικών λέξεων είναι ακέραιοι αριθμοί, τα οποία συμβολίζουμε τώρα με $l^*_1, l^*_2, \ldots, l^*_n$ και θεωρήσουμε την ισότητα στη σχέση (2.6), αφού αυτή προκύπτει για τα μικρότερα μήκη, τότε το πρόβλημά μας, της αριστοποίησης, διατυπώνεται ως πρόβλημα ελαχιστοποίησης της ακόλουθης ποσότητας:

$$Y = \sum_{i=1}^{n} p_i l_i^* + c\left(\sum_{i=1}^{n} q^{-l_i^*}\right)$$

Υπολογίζοντας τη μερική παράγωγο ως προς l^*_i, λαμβάνουμε

$$\frac{\partial Y}{\partial l_i^*} = p_i - q^{-l_i^*} c \ln q.$$

Θέτοντας την πρώτη μερική παράγωγο ίση με μηδέν, λαμβάνουμε

$$q^{-l_i^*} = \frac{p_i}{c \ln q}.$$

Αφού το άθροισμα των αρνητικών δυνάμεων του q ως προς τα μήκη είναι ίσο με τη μονάδα, το c είναι ίσο με $1/lnq$ και, επομένως, ισχύει αναφορικά με τα άριστα μήκη

$$p_i = q^{-l_i^*} \text{ και } \; l_i^* = \log_q p_i.$$

Αυτή η επιλογή μη ακέραιων αριθμών για τα μήκη των κωδικών λέξεων οδηγεί σε μέση τιμή που είναι ίση με το μέσο πληροφορικό περιεχόμενο των συμβόλων της πηγής, αφού $\Sigma p_i l_i^* = -\Sigma p_i \log_q p_i = H_q(S)$. Ωστόσο, αφού τα μήκη των κωδικών λέξεων είναι ακέραιοι αριθμοί, πρέπει να είναι ακέραιοι αριθμοί και οι ποσότητες $-\log_q p_i$ για να είναι δυνατή η άριστη κωδικοποίηση και, κατά συνέπεια, να ισχύει η ισότητα στη σχέση (2.7). Στην περίπτωση που η ποσότητα $-\log_q p_i$ δεν είναι ακέραιος αριθμός, ο αμέσως μεγαλύτερος ακέραιος αριθμός του λογάριθμου επιλέγεται ως μήκος της αντίστοιχης κωδικής λέξης, δηλαδή της i – στής κωδικής λέξης, l_i, τέτοιος ώστε

$$-\log_q p_i \le l_i \le -\log_q p_i + 1.$$

Μπορούμε να ορίσουμε τώρα ένα μέτρο της ποιότητας του κώδικα, την **επίδοσή** του, η οποία πλησιάζει τόσο πιο πολύ την τιμή 1 όσο πιο αποδοτικός είναι ο κώδικας. Την τιμή 1 λαμβάνει στην περίπτωση της άριστης λύσης που θίξαμε προηγουμένως.

Επίδοση του κώδικα

Η επίδοση, α, ενός κώδικα ορίζεται ως ο λόγος του μέσου πληροφορικού περιεχομένου των συμβόλων της πηγής (ή των κωδικών λέξεων) προς το γινόμενο του μέσου μήκους των κωδικών λέξεων με το λογάριθμο του πλήθους των κωδικών συμβόλων:

$$a = \frac{H(C)}{\left(\sum_{i=1}^{n} p_i l_i\right) \log q}. \tag{2.9}$$

Παράδειγμα 2.5

Υποθέτουμε μια διακριτή πηγή χωρίς μνήμη με τέσσερα σύμβολα, τα Φ, Χ, Ψ και Ω. Επίσης, ένα κωδικό αλφάβητο αποτελούμενο από τα σύμβολα 0 και 1. Οι πιθανότητες των τεσσάρων συμβόλων της πηγής είναι όλες 1/4. Να υπολογιστεί η επίδοση του κώδικα που παρατίθεται στη συνέχεια.

Σύμβολα Πηγής	Κωδικές Λέξεις
Φ	00
Χ	01
Ψ	10
Ω	11

Απάντηση: Το μέσο πληροφορικό περιεχόμενο της πηγής και το (μέσο) μήκος των

κωδικών λέξεων είναι 2 bits, καθώς και το πλήθος των κωδικών συμβόλων. Επομένως, η επίδοση του κώδικα είναι α = 1.

Άσκηση αυτοαξιολόγησης 2.3

Για την πηγή του Παραδείγματος 5 να υπολογιστεί η επίδοση του κώδικα αν οι πιθανότητες των συμβόλων της πηγής Φ, Χ, Ψ και Ω είναι 1/2, 1/4, 1/8 και 1/8, αντίστοιχα. Επίσης, για την ίδια πηγή να υπολογιστεί η επίδοση του κώδικα «1», «01», «001», και «000».

2.1.3 Αλγόριθμοι κωδικοποίησης

Υπάρχουν πολλοί αλγόριθμοι για την εύρεση αποδοτικών κωδίκων. Σ' αυτούς συγκαταλέγονται οι αλγόριθμοι κωδικοποίησης του Fano, του Shannon και του Huffman, των Gilbert – Moore και ο αλγόριθμος αριθμητικής κωδικοποίησης. Οι αλγόριθμοι κωδικοποίησης συνδυάζονται με άλλες τεχνικές για τη δημιουργία σχημάτων συμπίεσης, όπως τα πρότυπα σχήματα συμπίεσης JPEG και MPEG, στα οποία χρησιμοποιείται ο αλγόριθμος του Huffman. Τα πρότυπα JPEG και MPEG βρίσκουν εφαρμογή για τη συμπίεση εικόνας και βίντεο, αντίστοιχα. Στη συνέχεια θα ασχοληθούμε μόνο με τους τρεις πρώτους από τους ανωτέρω αλγορίθμους κωδικοποίησης.

Ο Αλγόριθμος Κωδικοποίησης του Fano

Ο αλγόριθμος κωδικοποίησης του Fano (ή Shannon – Fano) αποτελείται από τα ακόλουθα βήματα:

1. Τα σύμβολα της πηγής (ή τα μηνύματα αν η κωδικοποίηση αφορά τα μηνύματα) διατάσσονται σε τάξη φθίνουσας πιθανότητας.
2. Στη συνέχεια, τα σύμβολα χωρίζονται σε τόσες ομάδες όσα και τα κωδικά σύμβολα, κατά τέτοιον τρόπο ώστε να προκύπτουν το δυνατόν ίσες αθροιστικές πιθανότητες εμφάνισης των συμβόλων της πηγής για όλες τις ομάδες. (Οι ομάδες συγκροτούνται από συνεχόμενα στη διάταξη σύμβολα.) Στην περίπτωση δυαδικού κώδικα, τα n σύμβολα της πηγής χωρίζονται σε 2 ομάδες, επιλέγοντας το k έτσι ώστε η ακόλουθη διαφορά των αθροιστικών πιθανοτήτων εμφάνισης των συμβόλων των δύο ομάδων να ελαχιστοποιείται:

$$\left| \sum_{i=1}^{k} p_i - \sum_{i=k+1}^{n} p_i \right|.$$

3. Για κάθε ομάδα συμβόλων της πηγής, επιλέγεται ένα από τα κωδικά σύμβολα ως το πρώτο των κωδικών λέξεων που θα προκύψουν.
4. Για κάθε ομάδα συμβόλων της πηγής επαναλαμβάνονται τα βήματα 2 και 3 έως ότου η κάθε ομάδα αποτελείται από μόνο ένα σύμβολο. Σε κάθε επανάληψη του βήματος 3, επιλέγεται ένα ακόμα κωδικό σύμβολο για το σχηματισμό των κωδικών λέξεων.

Ο αλγόριθμος κωδικοποίησης του Fano μπορεί να οδηγήσει σε άριστους κώδικες αν είναι δυνατή η επαναλαμβανόμενη διαίρεση των ομάδων συμβόλων σε ακριβώς ισοπίθανες (υπο)ομάδες (στο βήμα 2 του αλγόριθμου). Αν αυτό δεν είναι δυνατόν, ο κώδικας που προκύπτει δεν είναι άριστος. Ωστόσο, αν η απαίτηση αυτή ικανοποιείται προσεγγιστικά, τότε και ο κώδικας που προκύπτει χαρακτηρίζεται από ικανοποιητική επίδοση. Προφανώς ο αλγόριθμος του Fano τερματίζει στην περίπτωση πεπερασμένου πλήθους συμβόλων (ή μηνυμάτων), αφού η επανάληψη των βημάτων 2 και 3 δεν ξεπερνάει το πλήθος τους.

Παράδειγμα 2.6

Υποθέτουμε μια πηγή που παράγει τέσσερα σύμβολα, τα Φ, Χ, Ψ και Ω με πιθανότητες 1/2, 1/4, 1/8 και 1/8, αντίστοιχα. Να σχηματιστούν δυαδικές κωδικές λέξεις για τα σύμβολα αυτά στη βάση του αλγόριθμου κωδικοποίησης του Fano.

Απάντηση

Τα σύμβολα δίνονται ήδη διαταγμένα κατά φθίνουσα πιθανότητα εκπομπής από την πηγή. Παρατηρούμε ότι το σύμβολο Φ έχει πιθανότητα παραγωγής 1/2. Επομένως, η πρώτη ομάδα περιέχει μόνο το σύμβολο Φ και η δεύτερη όλα τα υπόλοιπα σύμφωνα με το βήμα 2 του αλγόριθμου. (Έχουμε δύο ομάδες αφού πρόκειται για δυαδική κωδικοποίηση.) Επιλέγουμε το «0» ως το πρώτο κωδικό σύμβολο της κωδικής λέξης της πρώτης ομάδας και το «1» ως το πρώτο κωδικό σύμβολο των κωδικών λέξεων της δεύτερης ομάδας. Αφού η πρώτη ομάδα αποτελείται από μόνο ένα σύμβολο πηγής, το Φ, ολοκληρώθηκε ήδη ο σχηματισμός της κωδικής του λέξης, που είναι το «0». Η δεύτερη ομάδα αποτελείται από 3 σύμβολα πηγής και έτσι πρέπει να συνεχίσουμε με την προηγούμενη διαδικασία. Χωρίζουμε τα τρία αυτά σύμβολα σε δύο (υπο)ομάδες, έτσι ώστε για την κάθε ομάδα να προκύπτει όσο γίνεται η ίδια πιθανότητα, κάτι που είναι δυνατόν με ακρίβεια στην προκειμένη περίπτωση. Στην πρώτη υποομάδα ανήκει το σύμβολο Χ, ενώ στη δεύτερη τα υπόλοιπα δύο. Κατά τον ίδιο τρόπο, όπως προηγουμένως, το κωδικό σύμβολο «0» χρησιμοποιείται για την κωδική λέξη της πρώτης ομάδας και το «1» για τις κωδικές λέξεις της δεύτερης

ομάδας. Ο σχηματισμός της κωδικής λέξης του συμβόλου Χ ολοκληρώνεται σ' αυτό το βήμα και είναι «10». Αντίθετα, για τα σύμβολα της δεύτερης υποομάδας πρέπει να επαναλάβουμε τα βήματα 2 και 3. Έτσι, προκύπτουν οι κωδικές λέξεις «110» και «111» για τα Ψ και Ω, αντίστοιχα. Στον ακόλουθο πίνακα παρατίθενται τα σύμβολα της πηγής, οι πιθανότητές τους και οι κωδικές λέξεις που σχηματίστηκαν.

Σύμβολα Πηγής	Πιθανότητες	Κωδικές Λέξεις
Φ	1/2	0
Χ	1/4	10
Ψ	1/8	110
Ω	1/8	111

Άσκηση αυτοαξιολόγησης 2.4

Δίνεται μια πηγή που παράγει 10 σύμβολα s_1, …, s_{10}, με πιθανότητες παραγωγής 1/4, 1/4, 1/8, 1/8, 1/16, 1/16, 1/32, 1/32, 1/32 και 1/32, αντίστοιχα. Να σχηματιστούν κωδικές λέξεις με τη βοήθεια του αλγόριθμου κωδικοποίησης του Fano.

Ο Αλγόριθμος Κωδικοποίησης του Shannon

Ο αλγόριθμος κωδικοποίησης του Shannon μπορεί να χρησιμοποιηθεί, όπως και οι άλλοι αλγόριθμοι, για την κωδικοποίηση των συμβόλων ή των μηνυμάτων της πηγής. Αποτελείται δε από τα ακόλουθα βήματα:

1. Τα σύμβολα (ή τα μηνύματα) διατάσσονται σε τάξη φθίνουσας πιθανότητας, όπως και στην περίπτωση του αλγόριθμου του Fano.
2. Για κάθε σύμβολο S_j, του οποίου η πιθανότητα εμφάνισης είναι $p(s_j)$, υπολογίζεται η αθροιστική πιθανότητα P_i, που ορίζεται από τη σχέση ($P_i = 0$):

$$P_i = \sum_{j=1}^{i-1} p(s_j).$$

3. Το πλήθος των κωδικών συμβόλων της κωδικής λέξης η οποία αναπαριστά το σύμβολο της πηγής S_i είναι ίσο με τον ακέραιο αριθμό l_i, που πληροί την ακόλουθη ανισότητα:

$$\log \frac{1}{p(s_i)} \le l_i < 1 + \log \frac{1}{p(s_i)}$$

4. Η κωδική λέξη c_i του συμβόλου της πηγής S_i είναι το δυαδικό ανάπτυγμα του κλάσματος P_i (μόνο τα πρώτα l_i bits του αναπτύγματος), δηλαδή $c_i = (P_i)_{binary\ li\ bits}$.

(Για το δυαδικό ανάπτυγμα ενός κλάσματος ισχύει το εξής:

$$\frac{a_1}{2} + \frac{a_2^2}{2^2} + \ldots + \frac{a_k^k}{2^k} = .a_1 a_2 \ldots a_k \text{ όπου } a_j \text{ είναι 0 ή 1.)}$$

Παράδειγμα 2.7

Δίνεται η πηγή της Άσκησης αυτοαξιολόγησης 4. Να σχηματιστούν οι αντίστοιχες κωδικές λέξεις με τη βοήθεια του αλγόριθμου του Shannon.

Απάντηση

Πρώτα διατάσσουμε τα σύμβολα της πηγής σε τάξη φθίνουσας πιθανότητας. Στη συνέχεια υπολογίζουμε τις αθροιστικές πιθανότητες P_i σύμφωνα με το βήμα 2 του αλγόριθμου. Ακολουθεί ο καθορισμός του μήκους κάθε κωδικής λέξης σύμφωνα με το βήμα 3. Το μήκος της κωδικής λέξης που αναπαριστά το σύμβολο S_1 πρέπει να είναι ίσο με 2, αφού ο λογάριθμος του αντιστρόφου της πιθανότητας εμφάνισής του είναι ίσος με 2. Το ίδιο μήκος προκύπτει και για την κωδική λέξη που αναπαριστά το S_2, αφού και αυτό έχει ίση πιθανότητα εμφάνισης. Για το S_3 προκύπτει μήκος κωδικής λέξης ίσο με 3, κ.ο.κ. Το επόμενο βήμα (4) είναι το δυαδικό ανάπτυγμα των αθροιστικών πιθανοτήτων P_i και ο σχηματισμός των κωδικών λέξεων που αναπαριστούν τα σύμβολα S_i. Το $P_1 = 0$ και, επομένως, έχει το ανάπτυγμα .00000 και η κωδική λέξη που αναπαριστά το S_1 και έχει μήκος 2 bits σχηματίζεται από τα δύο πρώτα δυαδικά ψηφία του δυαδικού αναπτύγματος, δηλαδή τα «00». Το $P_2 = 1/4$ γράφεται $(0/2^1) + (1/2^2) + (0/2^3) + (0/2^4) + (0/2^5)$ και το δυαδικό του ανάπτυγμα είναι οι αριθμητές των κλασμάτων, δηλαδή .01000 και επομένως η κωδική λέξη του συμβόλου S_2 μήκους 2 bits είναι «01». Κατά τον ίδιο τρόπο σχηματίζονται και οι κωδικές λέξεις των υπόλοιπων συμβόλων της πηγής. Οι στήλες του ακόλουθου πίνακα περιέχουν τα σύμβολα της πηγής διαταγμένα σε τάξη φθίνουσας πιθανότητας εμφάνισης, τις πιθανότητες εμφάνισής τους, τις αθροιστικές πιθανότητες, τα μήκη των κωδικών λέξεων, τα δυαδικά αναπτύγματα και τις αντίστοιχες κωδικές λέξεις.

Σύμβολα Πηγής	Πιθανότητες Συμβόλων	P_i	Μήκος l_i	Ανάπτυγμα του P_i	Κωδικές Λέξεις
S_1	1/4	$P_1 = 0$	$l_1 = 2$	.00000	00
S_2	1/4	$P_2 = 1/4$	$l_2 = 2$	.01000	01
S_3	1/8	$P_3 = 1/2$	$l_3 = 3$	.10000	100
S_4	1/8	$P_4 = 5/8$	$l_4 = 3$	.10100	101
S_5	1/16	$P_5 = 3/4$	$l_5 = 4$	.11010	1100
S_6	1/16	$P_6 = 13/16$	$l_6 = 4$	.11010	1101
S_7	1/32	$P_7 = 7/8$	$l_7 = 5$	.11100	11100
S_8	1/32	$P_8 = 29/32$	$l_8 = 5$	.11101	11101
S_9	1/32	$P_9 = 15/16$	$l_9 = 5$	.11110	11110
S_{10}	1/32	$P_{10} = 31/32$	$l_{10} = 5$	.11111	11111

Αν συγκρίνουμε την απάντηση της Άσκησης αυτοαξιολόγησης 4 και του Παραδείγματος 7 παρατηρούμε ότι και ο αλγόριθμος του Fano και ο αλγόριθμος του Shannon οδηγούν στις ίδιες κωδικές λέξεις. Ωστόσο, αυτό δεν ισχύει πάντοτε. Στο Παράδειγμα 8 μπορούμε να δούμε μια τέτοια περίπτωση.

Παράδειγμα 2.8

Δίνεται μια πηγή με τέσσερα σύμβολα, τα Φ, Χ, Ψ και Ω, και πιθανότητες παραγωγής τους 0,4, 0,3, 0,2 και 0,1, αντίστοιχα. Να σχηματιστούν κωδικές λέξεις με τον αλγόριθμο του Shannon και τον αλγόριθμο του Fano.

Απάντηση

Σύμβολα Πηγής	Πιθανότητες Συμβόλων	P_i	Μήκος l_i	Ανάπτυγμα του P_i	Κώδικας Shannon	Κώδικας Fano
Φ	0,4	$P_1 = 0$	$l_1 = 2$	.0000	00	0
Χ	0,3	$P_2 = 0,4$	$l_2 = 2$	.01100..	01	10
Ψ	0,2	$P_3 = 0,7$	$l_3 = 3$	.10110..	101	110
Ω	0,1	$P_4 = 0,9$	$l_4 = 4$	.11100..	1110	111

Άσκηση αυτοαξιολόγησης 2.5

Δίνεται μια πηγή που παράγει 15 σύμβολα με πιθανότητες 27/128 τα δύο πρώτα, 9/128 τα επόμενα έξι, 3/128 τα ακόλουθα έξι και 2/128 το τελευταίο σύμβολο. Να σχηματιστούν κωδικές λέξεις με τη βοήθεια του αλγόριθμου του Shannon και του αλγόριθμου του Fano.

Ο Αλγόριθμος Κωδικοποίησης του Huffman

Ένας άριστος κώδικας για δεδομένες πιθανότητες εμφάνισης των συμβόλων της πηγής μπορεί να προκύψει με τη βοήθεια ενός απλού αλγόριθμου κωδικοποίησης, αυτού του Huffman. Μπορεί να δειχθεί ότι κανένας άλλος αλγόριθμος δεν μπορεί να οδηγήσει στην κατασκευή κώδικα με μικρότερο μέσο μήκος κωδικών λέξεων για ένα δεδομένο αλφάβητο της πηγής. Σύμφωνα με τον αλγόριθμο του Huffman, για τη δυαδική κωδικοποίηση των συμβόλων της πηγής ακολουθούνται τα επόμενα βήματα:

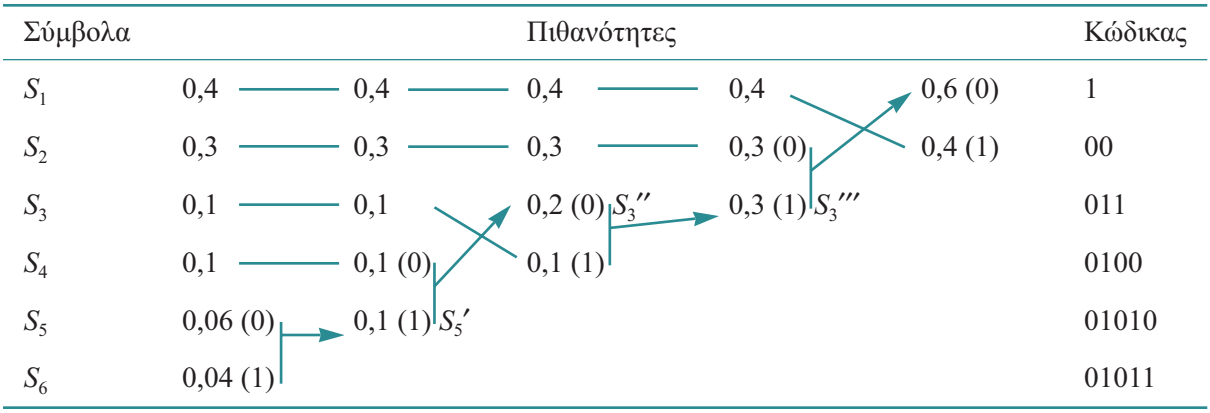
1. Τα σύμβολα της πηγής διατάσσονται κατά φθίνουσα πιθανότητα εκπομπής.
2. Τα δύο τελευταία σύμβολα της πηγής με τη μικρότερη πιθανότητα παραγωγής ενώνονται σε ένα, πιθανότητας ίσης με το άθροισμα των πιθανοτήτων των δύο αυτών συμβόλων, με αποτέλεσμα τη μείωση κατά ένα του πλήθους των συμβόλων του αλφάβητου της πηγής.
3. Τα βήματα 1 και 2 επαναλαμβάνονται έως ότου το αλφάβητο της πηγής αποτελείται μόνο από δύο σύμβολα. Σ' αυτά τα δύο σύμβολα αποδίδονται τα 0 και 1 του δυαδικού κώδικα.
4. Ένα «0» και ένα «1» αποδίδονται στη θέση του ενός και του άλλου συμβόλου, αντίστοιχα, τα οποία στο βήμα 2 συγχωνεύτηκαν σε ένα. Το βήμα αυτό αφορά σε όλες τις συγχωνεύσεις.
5. Οι κωδικές λέξεις των συμβόλων σχηματίζονται από όλα τα ψηφία «0» και «1» που σχετίζονται με αυτά τα σύμβολα (από το τέλος προς την αρχή), δηλαδή από τα ψηφία που έχουν αποδοθεί απευθείας σε αυτά ή στα συγχωνευμένα σύμβολα που συμμετέχουν.

Παράδειγμα 2.9

Δίνεται μια πηγή που παράγει έξι σύμβολα με πιθανότητες 0,4, 0,3, 0,1, 0,1, 0,06 και 0,04. Να σχηματιστεί κώδικας αυτών των συμβόλων με τη βοήθεια του αλγόριθμου του Huffman.

Απάντηση

Σύμφωνα με τον αλγόριθμο, πρώτα διατάσσουμε τα έξι σύμβολα σε τάξη φθίνουσας πιθανότητας εκπομπής. Η πρώτη στήλη του ακόλουθου πίνακα περιέχει τα σύμβολα και η δεύτερη στήλη τις πιθανότητές τους. Στο επόμενο βήμα, τα σύμβολα S_5 και S_6, με τις μικρότερες πιθανότητες, ενώνονται σε ένα με πιθανότητα ίση με το άθροισμα αυτών των πιθανοτήτων, δηλαδή ίση με 0,1. Τώρα διατάσσονται εκ νέου τα σύμβολα λαμβάνοντας υπόψη την ένωση των S_5 και S_6 στο S_5'. Έτσι, προκύπτει η τρίτη στήλη του πίνακα, όπου το σύνθετο σύμβολο είναι το πέμπτο, το S_5'. Στο επόμενο βήμα, το S_5' και το S_4 συγχωνεύονται στο S_3'', αφού έχουν τις μικρότερες πιθανότητες και τα εναπομείναντα σύμβολα διατάσσονται και πάλι. Έτσι, προκύπτει η τέταρτη στήλη του πίνακα (ή η τρίτη στήλη των πιθανοτήτων), όπου το νέο σύνθετο σύμβολο είναι στη θέση 3, το S_3'', και στη θέση 4 βρίσκεται το αρχικό S_3. Επαναλαμβάνουμε εκ νέου τα βήματα της συγχώνευσης και διάταξης των συμβόλων που έχουν απομείνει και έτσι προκύπτει η πέμπτη στήλη του πίνακα, όπου στη θέση 3 έχουμε το S_3''', το οποίο είναι η ένωση του S_3'' και του αρχικού S_3. Με επανάληψη της ένωσης των δύο τελευταίων συμβόλων και της διάταξης αυτών κατά φθίνουσα πιθανότητα προκύπτει η τελευταία στήλη πιθανοτήτων, όπου στη θέση 1 έχουμε την ένωση του S_3''' με το αρχικό σύμβολο S_2 και στη θέση 2 το αρχικό σύμβολο S_1. Ξεκινώντας από την τελευταία στήλη των πιθανοτήτων, αποδίδουμε στα σύμβολα που απέμειναν το «0» και το «1», αντίστοιχα. Στην προηγούμενη στήλη πιθανοτήτων σημειώνουμε επίσης δίπλα στα σύμβολα που ενώθηκαν το «0» και το «1», κ.ο.κ. Τώρα είμαστε σε θέση να σχηματίσουμε τις κωδικές λέξεις. Το σύμβολο S_1 αναπαρίσταται με την κωδική λέξη «1», το σύμβολο S_2 με την κωδική λέξη «00», που προκύπτει από το «0» της τελευταίας και από το «0» της προτελευταίας στήλης πιθανοτήτων. Το S_3, αφού περιέχεται στο ενωμένο σύμβολο της τελευταίας στήλης, έχει ως πρώτο κωδικό σύμβολο το «0». Επειδή περιέχεται και στο τρίτο συγχωνευμένο σύμβολο της προτελευταίας στήλης, έχει ως δεύτερο κωδικό σύμβολο το «1» και επίσης έχει ως τελευταίο κωδικό σύμβολο το «1», που αποδόθηκε σ' αυτό στην τρίτη στήλη πιθανοτήτων, όπου όμως καταλαμβάνει την τέταρτη θέση. Επομένως, η κωδική λέξη του συμβόλου S_3 είναι η «011». Κατά τον ίδιο τρόπο σχηματίζουμε και τις κωδικές λέξεις των υπόλοιπων συμβόλων της πηγής.



Άσκηση αυτοαξιολόγησης 2.6

Μια πηγή παράγει 8 διαφορετικά σύμβολα, τα S_1, ..., S_8, με πιθανότητες 1/2, 1/4, 1/8, 1/16, 1/32, 1/64, 1/128 και 1/128. Αυτά κωδικοποιούνται ως 000, 001, 010, 011, 100, 101, 110 και 111, αντίστοιχα. Ζητούνται:

1. η εντροπία της πηγής,
2. η επίδοση αυτού του κώδικα,
3. να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Huffman.
4. Να υπολογιστεί και να σχολιαστεί η επίδοση του κώδικα Huffman.

Οι αλγόριθμοι κωδικοποίησης που γνωρίσαμε μπορούν να εφαρμοστούν ακόμα και στην περίπτωση κωδικού αλφαβήτου με περισσότερα των δύο συμβόλων, και όχι μόνο των δυαδικών ψηφίων «0» και «1». Η Άσκηση αυτοαξιολόγησης 7 σάς ζητά να εφαρμόσετε έναν εξ αυτών για κωδικά αλφάβητα αποτελούμενα από τρία και τέσσερα σύμβολα.

Άσκηση αυτοαξιολόγησης 2.7

Μια πηγή παράγει 8 σύμβολα, όπως στην προηγούμενη άσκηση, με πιθανότητες τώρα 0,32, 0,24, 0,20, 0,09, 0,05, 0,04, 0,04 και 0,02. Ζητούνται τα ακόλουθα:

1. Να σχηματιστεί ένας κώδικας με κωδικό αλφάβητο αποτελούμενο από δύο σύμβολα με τη βοήθεια του αλγόριθμου του Fano.
2. Να σχηματιστεί ένας κώδικας με κωδικό αλφάβητο αποτελούμενο από τρία

σύμβολα με τη βοήθεια του αλγόριθμου του Fano.

3. Να σχηματιστεί ένας κώδικας με κωδικό αλφάβητο αποτελούμενο από τέσσερα σύμβολα με τη βοήθεια του αλγόριθμου του Fano.

2.1.4 Το πλήθος των πιο πιθανών μηνυμάτων

Στην Υποενότητα 2.1.1 ορίσαμε το μέσο πληροφορικό περιεχόμενο των μηνυμάτων της πηγής. Θεωρήσαμε ως $M = \{m_1, m_2, \ldots, m_n\}$ το σύνολο των δυνατών μηνυμάτων, όπου n το πλήθος αυτών ($n = q^l$, l το μήκος των μηνυμάτων σε σύμβολα και q το πλήθος των συμβόλων του αλφαβήτου) και $p(m_1), p(m_2), \ldots, p(m_n)$ οι αντίστοιχες πιθανότητες εκπομπής των μηνυμάτων. Καθώς το μήκος των μηνυμάτων αυξάνει, ορισμένα μηνύματα έχουν αμελητέα πιθανότητα εκπομπής, σε αντίθεση με τα υπόλοιπα, που εμφανίζονται να έχουν περίπου την ίδια πιθανότητα. Τότε είναι που αναφερόμαστε στο **πλήθος των πιο πιθανών (τυπικών) μηνυμάτων**.

Ας υποθέσουμε ότι μ_i είναι το πλήθος εμφάνισης ενός συμβόλου s_i σε ένα μήνυμα m, μήκους l συμβόλων. Τότε, αν k είναι το πλήθος των διαφορετικών συμβόλων που εμφανίζονται σε ένα τυχαίο μήνυμα m (για μεγάλο l θεωρούμε k=9), η πιθανότητα εκπομπής του m δίνεται από

$$p(m) = \prod_{i=1}^{k} p(s_i)^{\mu_i}, \text{ όπου } l = \sum_{i=1}^{k} \mu_i.$$

Λαμβάνοντας υπόψη το νόμο των μεγάλων αριθμών, σύμφωνα με τον οποίο $\mu_i/l \to p(s_i)$, δηλαδή $\mu_i \approx lp(s_i)$ και παίρνοντας τους λογάριθμους στην προηγούμενη σχέση έχουμε τα ακόλουθα:

$$\begin{aligned} \log p(m) &= \log\left\{\prod_{i=1}^{k} p(s_i)^{\mu_i}\right\} \\ &\approx \log\left\{\prod_{i=1}^{9} p(s_i)^{lp(s_i)}\right\} \\ &= l\left\{\sum_{i=1}^{9} p(s_i)\log p(s_i)\right\} = -lH(S). \end{aligned}$$

Έτσι, ο λογάριθμος της πιθανότητας εκπομπής ενός τυπικού μηνύματος ισούται (προσεγγιστικά) με το γινόμενο της εντροπίας της πηγής με το μήκος του μηνύματος.

Πρόκειται, με άλλα λόγια, για μια προσεγγιστική έκφραση της μέσης τιμής του λογάριθμου της πιθανότητας εκπομπής μηνυμάτων ως συνάρτησης του μήκους τους και της εντροπίας της πηγής.

Σχετικά με την κατάταξη των μηνυμάτων σε δύο κατηγορίες, στα πιο πιθανά και τα υπόλοιπα, διατυπώθηκε η ακόλουθη πρόταση από τους Shannon – MacMillan. Επίσης, μια δεύτερη πρόταση αναφέρεται στο πλήθος των πιο πιθανών μηνυμάτων διακριτής πηγής χωρίς μνήμη.

Πρόταση 2.1 (Θεώρημα των Shannon – MacMillan)

Για μια διακριτή πηγή χωρίς μνήμη με αλφάβητο S και εντροπία $H(S)$ μπορεί να βρεθεί ένα μήκος μηνυμάτων l_0, με $\varepsilon > 0$ και $\delta > 0$, έτσι ώστε τα μηνύματα της πηγής με μήκος $l \geq l_0$ να κατατάσσονται σε δύο κατηγορίες:

1. Ένα σύνολο S', με άθροισμα των πιθανοτήτων όλων των μηνυμάτων που περιέχει μικρότερο του ε.
2. Ένα σύνολο S'', το οποίο περιέχει τα υπόλοιπα (πιο πιθανά) μηνύματα και των οποίων οι πιθανότητες ικανοποιούν την ανισότητα

$$\left| \frac{-\log p(m)}{l} - H(S) \right| \leq \delta.$$

Η απόδειξη είναι σχετικά σύνθετη και για το λόγο αυτό παραλείπεται. Για μικρές τιμές του ε, το σύνολο S'' περιέχει όλα τα μηνύματα με υψηλή πιθανότητα εκπομπής και για το λόγο αυτό ονομάζεται **σύνολο των πιο πιθανών μηνυμάτων**. Ισχύει επομένως η σχέση $1-\varepsilon \leq p(S'') \leq 1$.

Η ακόλουθη πρόταση θέτει όρια στο πλήθος των μηνυμάτων που περιέχονται στο σύνολο αυτό.

Πρόταση 2.2

Για το πλήθος των μηνυμάτων, M, που περιέχονται στο σύνολο των πιο πιθανών μηνυμάτων ισχύει η ακόλουθη ανισότητα:

$$(1-e)2^{l\left(H(S)-\delta\right)} \leq M \leq 2^{l\left(H(S)+\delta\right)}.$$

Απόδειξη

Από την ακόλουθη σχέση

$$\left|\frac{-\log p(m)}{l} - H(S)\right| \leq \delta$$

έχουμε

$$2^{-l\left(H(S)+\delta\right)} \leq p(m) \leq 2^{-l\left(H(S)-\delta\right)}$$

και επομένως

$$\sum_{m\in S''} 2^{-l\left(H(S)+\delta\right)} \leq \sum_{m\in S''} p(m) \leq \sum_{m\in S''} 2^{-l\left(H(S)-\delta\right)} \text{ ή}$$
$$M2^{-l\left(H(S)+\delta\right)} \leq p(S'') \leq M2^{-l\left(H(S)-\delta\right)}.$$

Λαμβάνοντας υπόψη και τη σχέση $1-\varepsilon \leq p(S'') \leq 1$ έχουμε

$$1-\varepsilon \leq M2^{l\left(H(S)-\delta\right)}$$
$$M2^{l\left(H(S)+\delta\right)} \leq 1.$$

Επομένως, το πλήθος των πιο πιθανών μηνυμάτων μπορεί να υπολογιστεί προσεγγιστικά, για πολύ μικρές τιμές των ε και δ, ως εξής:

$$M \approx 2^{lH(S)} \tag{2.10}$$

Δραστηριότητα 2.2

Προσπαθήστε να διατυπώσετε τις σχέσεις που υφίστανται μεταξύ του πλήθους των πιο πιθανών μηνυμάτων, του πλήθους των δυνατών μηνυμάτων και της μέγιστης εντροπίας μιας πηγής. (Στη συνέχεια δίνεται η απάντηση στο ερώτημα αυτό.)

Αν τα σύμβολα μιας πηγής παράγονται με ίση πιθανότητα, τότε η εντροπία της πηγής είναι μέγιστη και ίση με το λογάριθμο του πλήθους των συμβόλων της πηγής. Σ' αυτή την περίπτωση το M παίρνει τη μέγιστη τιμή του και είναι ίσο με το πλήθος των δυνατών μηνυμάτων, δηλαδή

$$M_{\max} = 2^{l\log q} = q^l.$$

Για κάθε πηγή με εντροπία μικρότερη της μέγιστης για δεδομένο πλήθος συμβόλων

($\log q$) το πλήθος των πιο πιθανών μηνυμάτων θα είναι μικρότερο του πλήθους των δυνατών μηνυμάτων μιας πηγής.

2.2 Διάκριτες πηγές πληροφορίας με μνήμη

Στην Ενότητα 2.1 γνωρίσαμε πηγές χωρίς μνήμη. Ωστόσο, σχεδόν όλες οι πραγματικές πηγές πληροφορίας παράγουν ακολουθίες συμβόλων που είναι στατιστικά εξαρτημένες, όπως τα μηνύματα φυσικών γλωσσών. Για παράδειγμα, σε ελληνικά κείμενα η πιθανότητα το «τ» να ακολουθείται από το «α» είναι πολύ υψηλή, να ακολουθείται από το «π» όμως μηδενική. Επίσης, η πιθανότητα ένα οποιοδήποτε σύμβολο να είναι το «α» ανέρχεται στο 11,7%, να είναι όμως το «ψ» μόλις στο 0,1%.

Στην περίπτωση της διακριτής πηγής με μνήμη, λοιπόν, υφίσταται εξάρτηση μεταξύ των διαδοχικών συμβόλων κατά την παραγωγή τους από την πηγή. Η εξάρτηση αυτή μπορεί να υφίσταται για μακρές ακολουθίες συμβόλων. Συνήθως, όμως, υποθέτουμε ότι η εξάρτηση υφίσταται για έναν περιορισμένο αριθμό συμβόλων. Έτσι, μπορούν να χρησιμοποιηθούν Μαρκοβιανές αλυσίδες ως στατιστικά υποδείγματα (μοντέλα) για τις πηγές πληροφορίας.

Η ενότητα αυτή αποτελείται από τρεις υποενότητες. Στην πρώτη υποενότητα περιγράφονται συνοπτικά οι διαδικασίες Markoff, στη δεύτερη υποενότητα θα ασχοληθούμε με την εντροπία των πηγών Markoff και στην τρίτη με ζητήματα κωδικοποίησης αυτών.

2.2.1 Πηγές Markoff

Μια τυχαία διαδικασία είναι μια ακολουθία (ή οικογένεια) τυχαίων μεταβλητών Y_1, Y_2, ..., Y_n. Γενικά, μπορεί να υφίσταται οποιαδήποτε εξάρτηση μεταξύ των τυχαίων μεταβλητών της ακολουθίας. Η τυχαία διαδικασία χαρακτηρίζεται από τη συνάρτηση πιθανότητας μάζας

$$P\{(Y_1, Y_2, \ \ldots, Y_n) = (y_1, y_2, \ \ldots, y_n)\} = p(y_1, y_2, \ \ldots, y_n).$$

Ένα παράδειγμα τυχαίας διαδικασίας με εξάρτηση μεταξύ των τυχαίων μεταβλητών είναι η διαδικασία Markoff. Στη διαδικασία Markoff μια τυχαία μεταβλητή εξαρτάται από την αμέσως προηγούμενή της στην ακολουθία και είναι υπό συνθήκη ανεξάρτητη από όλες τις άλλες.

Ορισμός διαδικασίας Markoff

Μια διακριτή τυχαία διαδικασία Y_1, Y_2, ..., Y_n χαρακτηρίζεται ως διαδικασία Markoff (Μαρκοβιανή αλυσίδα) αν, για $n = 1, 2, \ldots$

$$P(Y_{n+1} = y_{n+1} \mid Y_n = y_n, Y_{n-1} = y_{n-1}, \ \ldots, Y_1 = y_1) = P(Y_{n+1} = y_{n+1} \mid Y_n = y_n). \qquad (2.11)$$

Στην περίπτωση της διαδικασίας Markoff η συνάρτηση πιθανότητας μάζας μπορεί να γραφεί ως

$$p(y_1, y_2, \ \ldots, y_n) = p(y_1)\, p(y_2 \mid y_1)\, p(y_3 \mid y_2) \ldots p(y_n \mid y_{n-1}).$$

Ορισμός: Η διαδικασία Markoff χαρακτηρίζεται ως χρονικά αμετάβλητη (time invariant) αν η υπό συνθήκη πιθανότητα $p(y_{n+1} \mid y_n)$ δεν εξαρτάται από το n, δηλαδή για $n = 1, 2, \ldots$

$$P(Y_{n+1} = b \mid Y_n = a) = P(Y_2 = b \mid Y_1 = a).$$

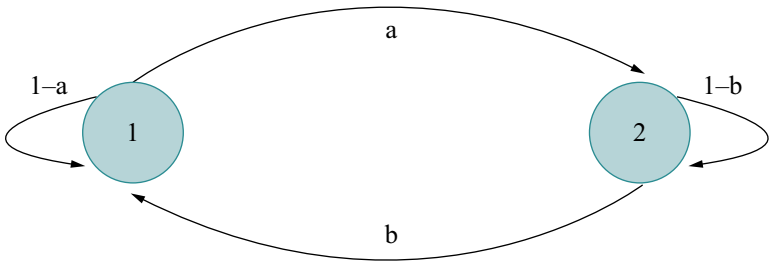
Μια τυχαία διαδικασία συμβολίζεται και με $\{Y_n\}$. Αν $\{Y_i\}$ είναι μια Μαρκοβιανή αλυσίδα, τότε η Y_n αναπαριστά την **κατάστασή** της στο χρόνο n. Μια αμετάβλητη στο χρόνο Μαρκοβιανή αλυσίδα περιγράφεται πλήρως από την αρχική της κατάσταση και από τον πίνακα των πιθανοτήτων μετάβασης $P = [P_{ij}]$, όπου $P_{ij} = P\{Y_{n+1} = j \mid Y_n = i\}$ και i, j οι τιμές των τυχαίων μεταβλητών οι οποίες ανήκουν στο σύνολο των δυνατών καταστάσεων $\{1, 2, \ldots, m\}$. (Οι δυνατές καταστάσεις μπορεί να είναι μεμονωμένες τιμές ή συνδυασμοί τιμών. Συνήθως αριθμούνται και χρησιμοποιείται ως σύμβολό τους ο αντίστοιχος αριθμός.) Ο πίνακας των πιθανοτήτων μετάβασης καλείται και **πίνακας μετάβασης** (ή μετάπτωσης). Η πιθανότητα της Μαρκοβιανής αλυσίδας να βρίσκεται τη χρονική στιγμή n στην κατάσταση i συμβολίζεται με $p_i(n)$, δηλαδή $p_i(n) = P_i(Y_n = i)$. Αν ισχύει $p_i(n) = p_i(n + 1) = \pi_i$ για κάθε κατάσταση, τότε η Μαρκοβιανή αλυσίδα χαρακτηρίζεται στατική. Για μια στατική Μαρκοβιανή αλυσίδα ισχύει μεταξύ του διανύσματος των πιθανοτήτων των καταστάσεων $\boldsymbol{\pi}$ και του πίνακα μετάπτωσης $\boldsymbol{P}$ η σχέση $\boldsymbol{\pi P} = \boldsymbol{\pi}$.

Παράδειγμα 2.10

Ας θεωρήσουμε μια Μαρκοβιανή αλυσίδα με δύο καταστάσεις και με πίνακα μετάβασης (Σχήμα 2.2)

$$P = \begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix} = \begin{bmatrix} 1-a & a \\ b & 1-b \end{bmatrix}.$$

Να υπολογιστούν οι πιθανότητες π_1 και π_2, δηλαδή οι πιθανότητες να βρίσκεται η Μαρκοβιανή αλυσίδα στην κατάσταση 1 και 2, αντίστοιχα.



Σχήμα 2.2
Μαρκοβιανή αλυσίδα δύο καταστάσεων

Απάντηση

Αφού δίνεται ο πίνακας μετάβασης, οι πιθανότητες των δύο καταστάσεων μπορούν να υπολογιστούν με τη βοήθεια της σχέσης $\boldsymbol{\pi P} = \boldsymbol{\pi}$. Επομένως,

$$\begin{bmatrix}\pi_1 & \pi_2\end{bmatrix}\begin{bmatrix}P_{11} & P_{12}\\ P_{21} & P_{22}\end{bmatrix} = \begin{bmatrix}\pi_1(1-a)+\pi_2 b & \pi_1 a+\pi_2(1-b)\end{bmatrix} = \begin{bmatrix}\pi_1 & \pi_2\end{bmatrix}.$$

Λαμβάνοντας ακόμα υπόψη ότι $\pi_1 + \pi_2 = 1$, μπορούμε να υπολογίσουμε τις ζητούμενες πιθανότητες των δύο καταστάσεων της Μαρκοβιανής αλυσίδας:

$$\pi_1(1-a)+\pi_2 b = \pi_1 \underset{\pi_2 = 1-\pi_1}{\Rightarrow} -\pi_1 a + b - \pi_1 b = 0 \Rightarrow \pi_1 = \frac{b}{a+b},$$

$$\pi_1 a+\pi_2(1-b) = \pi_2 \underset{\pi_2 = 1-\pi_1}{\Rightarrow} -\pi_2 a + a - \pi_2 b = 0 \Rightarrow \pi_2 = \frac{a}{a+b}.$$

Οι Μαρκοβιανές αλυσίδες μπορούν να χρησιμοποιηθούν ως στατιστικά υποδείγματα διακριτών πηγών με μνήμη (π.χ. τηλέτυπο). Οι πηγές οι οποίες μπορούν να αναπαρασταθούν (μοντελοποιηθούν) με Μαρκοβιανές αλυσίδες ονομάζονται και **πηγές Markoff**.

Θεωρούμε πως η εκπομπή ενός συμβόλου από την πηγή Markoff λαμβάνει χώρα κατά τη διάρκεια κάποιου χρονικού διαστήματος. Στην αρχή αυτού του διαστήματος, το οποίο λέγεται και **διάστημα συμβόλου**, η πηγή βρίσκεται σε μια από τις m δυνατές καταστάσεις.

Σε κάθε χρονικό διάστημα συμβόλου, η πηγή αλλάζει κατάσταση, δηλαδή μεταβαίνει από την κατάσταση που βρισκόταν στην αρχή του διαστήματος συμβόλου σε αυτή που συνεπάγεται το σύμβολο που εκπέμφθηκε. Η πιθανότητα αυτής της μετάβασης (μετάπτωσης) έστω από την κατάσταση i στην κατάσταση j, P_{ij}, εξαρτάται από την αρχική (παρούσα) κατάσταση i και την τελική (μελλοντική) κατάσταση j, είναι όμως ανεξάρτητη από τις προηγούμενες καταστάσεις (2.11). Σε κάθε αλλαγή κατάστασης, λοιπόν, η πηγή εκπέμπει κάποιο σύμβολο.

Η Y_i είναι μια διακριτή τυχαία μεταβλητή και αναπαριστά την κατάσταση του συστή-

ματος, δηλαδή τα σύμβολα που εκπέμφθηκαν στα τελευταία l διαστήματα συμβόλων, όπου l είναι ο αριθμός των προηγούμενων συμβόλων που επηρεάζουν το επόμενο που θα παραχθεί από την πηγή (λέγεται και βάθος πηγής). Το πλήθος των δυνατών καταστάσεων της πηγής είναι $m = q^l$, όπου q το πλήθος των συμβόλων της πηγής. Σε μια Μαρκοβιανή αλυσίδα πρώτης τάξης ($l = 1$) το πλήθος των καταστάσεων της πηγής είναι ίσο με το πλήθος των συμβόλων του αλφάβητου της πηγής ($m = q$). Λέγοντας λοιπόν στην περίπτωση Μαρκοβιανής αλυσίδας πρώτης τάξης ότι η πηγή είναι στην κατάσταση i, εννοούμε ότι έχει λάβει χώρα ως τελευταία εκπομπή αυτή του συμβόλου s_i. Αντίστοιχα, λέγοντας ότι η πηγή μεταβαίνει από την κατάσταση i στην κατάσταση j, εννοούμε ότι μετά την εκπομπή του συμβόλου s_i εκπέμπεται το σύμβολο s_j. Σε μια Μαρκοβιανή αλυσίδα δεύτερης τάξης ($l = 2$), όπου η επιλογή του υπό εκπομπή συμβόλου εξαρτάται μόνο από τα δύο τελευταία σύμβολα, το πλήθος των καταστάσεων της πηγής είναι ίσο με το τετράγωνο του πλήθους των συμβόλων ($m = q^2$). Ανάλογα, στην περίπτωση Μαρκοβιανής αλυσίδας τρίτης τάξης το πλήθος των καταστάσεων της πηγής είναι ίσο με την τρίτη δύναμη του πλήθους των συμβόλων κ.ο.κ.

Για τις πιθανότητες των καταστάσεων της πηγής ισχύει η ακόλουθη σχέση, αφού υποθέτουμε χρονικά αμετάβλητες διαδικασίες Markoff (Μαρκοβιανές αλυσίδες):

$$p_j(k+1) = \sum_{i=1}^{m} p_i(k) P_{ij},$$

όπου $p_i(k)$ η πιθανότητα να βρίσκεται το σύστημα στην κατάσταση i κατά την αρχή του k – στού διαστήματος συμβόλου (ή τη χρονική στιγμή k).

Οι διακριτές πηγές Markoff παριστάνονται συχνά με γράφους, όπως στο Παράδειγμα 10, και ειδικότερα οι καταστάσεις παριστάνονται με κόμβους του γράφου και οι μεταβάσεις (μεταπτώσεις) με ακμές που συνδέουν την αρχική με την τελική κατάσταση.

2.2.2 Εντροπία των πηγών Markoff

Στην υποενότητα αυτή θα ορίσουμε την εντροπία και το ρυθμό πληροφορίας των πηγών Markoff. Επίσης, θα ορίσουμε την εντροπία των μηνυμάτων της πηγής και θα διατυπώσουμε ένα θεώρημα για τη σχέση μεταξύ της εντροπίας των μηνυμάτων και της εντροπίας των συμβόλων της πηγής.

Εντροπία της πηγής Markoff

Η εντροπία της πηγής ορίζεται ως ο μέσος όρος της εντροπίας των συμβόλων που εκπέμπονται από κάθε κατάσταση. Η εντροπία των συμβόλων που εκπέμπονται από την κατάσταση i, $H(K_i)$, δίνεται από την ακόλουθη σχέση:

$$H(K_i) = -\sum_{j=1}^{m} P_{ij} \log P_{ij} \text{ bits / symbol.} \tag{2.12}$$

Η εντροπία της πηγής, που είναι ο μέσος όρος της εντροπίας των καταστάσεων, είναι επομένως

$$H(S) = \sum_{i=1}^{m} p_i H(K_i) = -\sum_{i=1}^{m} p_i \sum_{j=1}^{m} P_{ij} \log P_{ij} \text{ bits / symbol.} \tag{2.13}$$

Μπορούμε, επίσης, να ορίσουμε το μέσο ρυθμό πληροφορίας της πηγής, R, που δίνεται από την επόμενη σχέση, όπου r_s είναι ο ρυθμός εκπομπής συμβόλων της πηγής:

$$R = r_s H(S) \text{ bits / sec}$$

Ακόμα, μπορούμε να ορίσουμε τη **μέση ποσότητα πληροφορίας μηνυμάτων** της πηγής ως ακολούθως, όπου το άθροισμα αναφέρεται σε όλα τα μηνύματα μήκους N συμβόλων και $p(m_i)$ συμβολίζει την πιθανότητα εκπομπής του μηνύματος m_i:

$$H(M) = -\sum_{i} p(m_i) \log p(m_i). \tag{2.14}$$

Διαιρώντας τη μέση ποσότητα πληροφορίας μηνυμάτων της πηγής με το μήκος τους, παίρνουμε τη μέση ποσότητα πληροφορίας των συμβόλων της πηγής:

$$H_N = \frac{1}{N} H(M). \tag{2.15}$$

Η ακόλουθη πρόταση συσχετίζει τη μέση ποσότητα πληροφορίας μηνυμάτων της πηγής, $H(M)$, με το μήκος των μηνυμάτων N και με την εντροπία της πηγής, $H(S)$.

Πρόταση 2.3

Για τη μέση ποσότητα πληροφορίας των συμβόλων της πηγής H_N, η οποία είναι μια μονότονα αύξουσα συνάρτηση του N, ισχύει

$$\lim_{N \to \infty} H_N = H(S) \text{ bits / symbol.} \tag{2.16}$$

Άσκηση αυτοαξιολόγησης 2.8

Μια πηγή με μνήμη εκπέμπει τα σύμβολα $s_1 = \varphi$, $s_2 = \chi$ και $s_3 = \psi$. Η παραγωγή των συμβόλων σχηματίζει μια στατική Μαρκοβιανή αλυσίδα πρώτης τάξης. Ο πίνακας μετάβασης είναι

$$P = \begin{bmatrix} P_{11} = P(\varphi/\varphi) & P_{12} = P(\varphi/\chi) & P_{13} = P(\varphi/\psi) \\ P_{21} = P(\chi/\varphi) & P_{22} = P(\chi/\chi) & P_{23} = P(\chi/\psi) \\ P_{31} = P(\psi/\varphi) & P_{32} = P(\psi/\chi) & P_{33} = P(\psi/\psi) \end{bmatrix} = \begin{bmatrix} 0 & 0,2 & 0,8 \\ 0,5 & 0,1 & 0,4 \\ 0,5 & 0 & 0,5 \end{bmatrix}$$

Να υπολογιστούν:

1. Οι πιθανότητες παραγωγής των συμβόλων φ, χ και ψ.
2. Η εντροπία της πηγής.
3. Το μέσο πληροφορικό περιεχόμενο μηνυμάτων αποτελούμενων από δύο σύμβολα.

2.2.3 Ζητήματα κωδικοποίησης των πηγών Markoff

Στην Υποενότητα 2.1.1 ορίσαμε την έννοια του πλεονασμού, που αποτελεί ένα μέτρο της ποιότητας της πηγής χωρίς μνήμη. Κατά ανάλογο τρόπο μπορούμε να ορίσουμε, για τις πηγές με μνήμη, το μέτρο του **πλεονασμού εξάρτησης**:

$$red_{\varepsilon\xi} = 1 - \frac{H_{\text{με μνήμη}}(S)}{H_{\text{χωρίς μνήμη}}(S)} \tag{2.17}$$

Επίσης, μπορούμε να ορίσουμε το μέτρο του **ολικού πλεονασμού**, το οποίο αναφέρεται στην εντροπία της πηγής με μνήμη σε σύγκριση με τη μέγιστη δυνατή εντροπία της πηγής χωρίς μνήμη, που επιτυγχάνεται για ίσες πιθανότητες εκπομπής όλων των συμβόλων:

$$red_{o\lambda} = 1 - \frac{H_{\text{με μνήμη}}(S)}{\max H_{\text{χωρίς μνήμη}}(S)} = 1 - \frac{H_{\text{με μνήμη}}(S)}{\log q} \tag{2.18}$$

Οι αλγόριθμοι κωδικοποίησης, τους οποίους εξετάσαμε στην Υποενότητα 2.1.3, μπορούν να χρησιμοποιηθούν και στις πηγές με μνήμη. Η εφαρμογή τους σε μηνύματα ή συνδυασμούς συμβόλων μήκους ίσου με το βάθος της πηγής (δείτε Υποενότητα 2.2.1) οδηγούν σε πιο αποδοτικούς κώδικες από ότι η εφαρμογή σε μεμονωμένα σύμβολα της πηγής. Αυτό μπορούμε να το δούμε και στο Παράδειγμα 11.

Παράδειγμα 2.11

Μια διακριτή πηγή με μνήμη παράγει μια Μαρκοβιανή αλυσίδα πρώτης τάξης. Το αλφάβητο της πηγής αποτελείται από τα σύμβολα φ, χ και ψ. Ο πίνακας μετάβασης είναι

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & 0 & \frac{3}{4} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}.$$

Να υπολογιστούν οι πιθανότητες εκπομπής των συμβόλων της πηγής, οι συνδυασμένες πιθανότητες εκπομπής μηνυμάτων αποτελούμενων από δύο σύμβολα και να σχηματιστούν κωδικές λέξεις με το δυαδικό κωδικό αλφάβητο για τα δυνατά μηνύματα δύο συμβόλων σύμφωνα με τον αλγόριθμο του Fano.

Απάντηση

Από τον πίνακα μετάβασης μπορούμε να υπολογίσουμε τις ακραίες πιθανότητες εκπομπής των συμβόλων της πηγής, οι οποίες ταυτίζονται με τις πιθανότητες κατάστασης της πηγής Markoff ($\boldsymbol{\pi P} = \boldsymbol{\pi}$, δείτε και το Παράδειγμα 10). Για το λόγο αυτό πρέπει να επιλύσουμε το ακόλουθο σύστημα εξισώσεων:

$$p(\varphi) = p(\varphi)P(\varphi/\varphi) + p(x)P(\varphi/x) + p(\psi)P(\varphi/\psi)$$

$$p(\chi) = p(\varphi)P(\chi/\varphi) + p(x)P(\chi/x) + p(\psi)P(\chi/\psi)$$

$$p(\psi) = p(\varphi)P(\psi/\varphi) + p(x)P(\psi/x) + p(\psi)P(\psi/\psi)$$

$$p(\varphi) + p(x) + p(\psi) = 1.$$

Τα αποτελέσματα είναι: $p(\varphi) = 10/27$, $p(\chi) = 8/27$, και $p(\psi) = 9/27$.

Από τον πίνακα μετάβασης και τις πιθανότητες των καταστάσεων της πηγής (ή εκπομπής των συμβόλων), $p(\varphi)$, $p(\chi)$ και $p(\psi)$ μπορούμε να υπολογίσουμε τις συνδυασμένες πιθανότητες εκπομπής των δυνατών μηνυμάτων των αποτελούμενων από δύο σύμβολα. Στον ακόλουθο πίνακα παρατίθενται οι συνδυασμένες πιθανότητες και οι κωδικές λέξεις που προκύπτουν από την εφαρμογή του αλγόριθμου του Fano.

Μήνυμα	Πιθανότητα	Κωδική Λέξη
χψ	6/27	00
φφ	5/27	01
φχ	5/27	100
ψφ	3/27	101
ψχ	3/27	110
ψψ	3/27	1110
χφ	2/27	1111
φψ	0	–
χχ	0	–

Το μέσο μήκος των κωδικών λέξεων υπολογίζεται από το μήκος των κωδικών λέξεων λαμβανομένων υπόψη των πιθανοτήτων παραγωγής των αντίστοιχων μηνυμάτων. Επομένως, $L = 75/27 = 2{,}78$ bits/message ή 1,39 bits/symbol. Η συνδυασμένη ποσότητα πληροφορίας, $H(X,Y)$, είναι ίση με 2,72 bits/message. Επομένως, η αποδοτικότητα, $\alpha = H(X,Y)/L$, είναι περίπου ίση με 0,98. Αν είχαμε εφαρμόσει τον αλγόριθμο του Fano σε επίπεδο συμβόλων και όχι μηνυμάτων, θα είχε προκύψει ένα μέσο μήκος κωδικών λέξεων περίπου ίσο με 3,26 bits/message, το οποίο είναι μεγαλύτερο από το 2,78 bits/message, που λάβαμε ανωτέρω. Συνεπώς, η κωδικοποίηση των συμβόλων σε σύγκριση με αυτή των μηνυμάτων θα οδηγούσε σε μείωση της αποδοτικότητας (περίπου 0,76).

Άσκηση αυτοαξιολόγησης 2.9

Να υπολογιστούν ο πλεονασμός, ο πλεονασμός εξάρτησης και ο ολικός πλεονασμός της διακριτής πηγής που δίνεται στην Άσκηση αυτοαξιολόγησης 8. (Για τον υπολογισμό του πλεονασμού, θεωρούμε την πηγή χωρίς μνήμη.)

2.3 Συνεχείς πηγές πληροφορίας

Στην ενότητα αυτή θα συζητήσουμε θέματα σχετικά με συνεχείς πηγές πληροφορίας, και πιο συγκεκριμένα σχετικά με συνεχή μέτρα ποσότητας πληροφορίας.

Η συνεχής ποσότητα πληροφορίας ορίζεται κατά ανάλογο τρόπο με τη διακριτή ποσότητα πληροφορίας. Αυτό είναι εύλογο, αφού μια συνεχής συνάρτηση πυκνότητας πιθανότητας μπορεί να προσεγγιστεί από τιμές πιθανοτήτων που είναι σταθερές σε διαστήματα μήκους Δx.

Ορισμός συνεχούς ποσότητας πληροφορίας

Η μέση ποσότητα πληροφορίας, $H(X)$, μιας συνεχούς τυχαίας μεταβλητής X με συνάρτηση πυκνότητας πιθανότητας $f(x)$ δίνεται από τη σχέση

$$H(X) = -\int_{-\infty}^{\infty} f(x) \log f(x) dx. \tag{2.19}$$

Κατά την εξέταση της διακριτής ποσότητας πληροφορίας, στο Κεφάλαιο 1, αναζητήσαμε τις πιθανότητες που την καθιστούν μέγιστη. Ανάλογα, μπορούμε να διερευνήσουμε τα χαρακτηριστικά που πρέπει να πληροί η συνάρτηση πυκνότητας πιθανότητας για να καταστεί η συνεχής ποσότητα πληροφορίας μέγιστη. Ωστόσο, ο τρόπος εξαγωγής της συνάρτησης πυκνότητας πιθανότητας που οδηγεί στη μέγιστη μέση ποσότητα πληροφορίας, καθώς και στην τιμή της στην περίπτωση της συνεχούς ποσότητας πληροφορίας, είναι διαφορετικός απ' αυτόν που ακολουθείται στην περίπτωση της διακριτής ποσότητας πληροφορίας. Αυτό οφείλεται σε επιπρόσθετους περιορισμούς που επιβάλλονται στις συνεχείς τυχαίες μεταβλητές, Αυτοί οι περιορισμοί μπορεί να αναφέρονται σε φραγμένο εύρος ή σε σταθερή ισχύ. Στη συνέχεια θα διατυπώσουμε ένα σχετικό θεώρημα.

ΘΕΩΡΗΜΑ 2.2

Η ποσότητα πληροφορίας, $H(X)$, ενός σήματος με φραγμένο εύρος, $(-E, +E)$ γίνεται μέγιστη και ίση με $\log 2E$ αν ισχύει η σχέση $f(x) = 1/(2E)$.

Απόδειξη

Για την απόδειξη του θεωρήματος αρκεί να προσδιορίσουμε τη συνάρτηση πυκνότητας πιθανότητας, $f(x)$, που οδηγεί στη μεγιστοποίηση της συνεχούς ποσότητας πληροφορίας του σήματος, $H(X)$, που ορίζεται με τον τύπο (2.19). Αφού το σήμα έχει φραγμένο εύρος, το ολοκλήρωμα της συνάρτησης πυκνότητας πιθανότητας στο διάστημα $(-E, +E)$ είναι ίσο με 1, δηλαδή

$$\int_{-E}^{+E} f(x) dx = 1$$

Στη συνέχεια ορίζουμε τη συνάρτηση $B(x)$ και σχηματίζουμε την παράγωγό της ως προς $f(x)$, την οποία θέτουμε ίση με 0:

$$B(x)' = \left[-f(x)\log f(x) + \varepsilon f(x)\right]' = -\log f(x) - \log e + \varepsilon = 0$$

Από την τελευταία σχέση λαμβάνουμε

$$\ln f(x) = \frac{\varepsilon}{\log e} - 1 = q, \text{ επομένως } f(x) = e^q,$$

$$\int_{-E}^{+E} f(x)dx = \int_{-E}^{+E} e^q dx = 1 \Rightarrow \left[\mathrm{e}^q x\right]_{-E}^{+E} = e^q 2E = 1, \text{ επομένως } f(x) = \frac{1}{2E}.$$

$$H(X) = -\int_{-E}^{+E} \frac{1}{2E}\log\left(\frac{1}{2E}dx\right) = \log 2E.$$

Η αντικατάσταση της $f(x)$ στην $H(X)$ οδηγεί στη ζητούμενη μέγιστη τιμή:

Επομένως, στην περίπτωση σήματος με φραγμένο εύρος η ομοιόμορφη συνάρτηση πυκνότητας πιθανότητας οδηγεί στη μέγιστη τιμή της συνεχούς ποσότητας πληροφορίας.

Όπως στην περίπτωση των διακριτών μέτρων ποσότητας πληροφορίας, έτσι και στην περίπτωση των συνεχών μέτρων μπορούμε να ορίσουμε τη **συνδυασμένη**, την **υπό συνθήκη** και την **αμοιβαία ποσότητα πληροφορίας**.

Έστω X και Y συνεχείς τυχαίες μεταβλητές και $f(x)$ και $f(y)$ οι συναρτήσεις πυκνότητας πιθανότητάς τους, $f(x,y)$ είναι η συνδυασμένη συνάρτηση πυκνότητας πιθανότητας και $f(x/y)$ και $f(y/x)$ οι υπό συνθήκη συναρτήσεις πυκνότητας πιθανότητας. Στη συνέχεια θα ορίσουμε τη συνδυασμένη ποσότητα πληροφορίας, καθώς και την υπό συνθήκη και την αμοιβαία ποσότητα πληροφορίας δύο τυχαίων μεταβλητών.

Η **συνδυασμένη ποσότητα πληροφορίας**, $H(X,Y)$, των τυχαίων μεταβλητών X και Y ορίζεται από τον ακόλουθο τύπο:

$$H(X,Y) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log f(x,y)dxdy \tag{2.20}$$

Η **υπό συνθήκη ποσότητα πληροφορίας**, $H(X/Y)$, των τυχαίων μεταβλητών X και Y ορίζεται από τον ακόλουθο τύπο:

$$H(X/Y) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log f(x/y)dxdy \tag{2.21}$$

Η **αμοιβαία ποσότητα πληροφορίας**, $I(X,Y)$, των τυχαίων μεταβλητών X και Y ορί-

ζεται ως ακολούθως:

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{2.22}$$

Οι (2.20), (2.21) και (2.22) οδηγούν αναφορικά με την αμοιβαία ποσότητα πληροφορίας στην ακόλουθη σχέση:

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log\frac{f(x,y)}{f(x)f(y)}\,dxdy \tag{2.23}$$

Άσκηση αυτοαξιολόγησης 2.10

Δίνεται η συνδυασμένη συνάρτηση πυκνότητας πιθανότητας, $f(x,y)$, των τυχαίων μεταβλητών X και Y :

$$f(x,y) = \begin{cases} \frac{1}{4}, & 0 \le x \le 2 \text{ και } 0 \le y \le 4 - 2x \\ 0, & \text{διαφορετικά} \end{cases}$$

Να υπολογιστούν οι ακραίες, η συνδυασμένη, η υπό συνθήκη και η αμοιβαία ποσότητα πληροφορίας των X και Y.

Σύνοψη

Στο κεφάλαιο αυτό εξετάσαμε ζητήματα σχετικά με διακριτές και συνεχείς πηγές πληροφορίας. Οι διακριτές πηγές πληροφορίας χωρίς μνήμη εκπέμπουν στατιστικά ανεξάρτητες ακολουθίες συμβόλων. Αντίθετα, οι πηγές με μνήμη εμφανίζουν στατιστική εξάρτηση μεταξύ των συμβόλων σε μια δεδομένη ακολουθία.

Στα μέτρα που χαρακτηρίζουν μια διακριτή πηγή συγκαταλέγονται το μέσο πληροφορικό περιεχόμενο των συμβόλων, καθώς και η μέγιστη τιμή του, ο πλεονασμός της πηγής και η μέση ποσότητα πληροφορίας των μηνυμάτων. Οι ακολουθίες συμβόλων της πηγής μετατρέπονται στο πλαίσιο της διαδικασίας κωδικοποίησης πηγής σε ακολουθίες κωδικών συμβόλων. Η κωδικοποίηση έχει ως στόχο την κατά το δυνατόν συμπιεσμένη αναπαράσταση των μηνυμάτων με απομάκρυνση του υπάρχοντος πλεονασμού για την πιο αποτελεσματική αξιοποίηση του καναλιού επικοινωνίας. Οι κώδικες μπορεί να είναι μη ιδιάζοντες, μοναδικά αποκωδικοποιήσιμοι ή άμεσοι. Ένα μέτρο χαρακτηρισμού κωδίκων είναι η επίδοσή τους. Οι αλγόριθμοι κωδικοποίησης, με τη βοήθεια των οποίων σχηματίζουμε κώδικες, είναι πολλοί και διάφοροι, όπως ο αλγόριθμος του Fano, του Shannon, του Huffman, του Gilbert – Moore, ο αριθμητικός κώδικας και αλγόριθμος κωδικοποίησης βασισμένος στην επέκταση αλφαβήτων.

Για τη μελέτη διακριτών πηγών με μνήμη, όπου υφίσταται στατιστική εξάρτηση μεταξύ των διαδοχικών συμβόλων κατά την εκπομπή τους από την πηγή, χρησιμοποιήσαμε Μαρκοβιανές αλυσίδες ως μαθηματικά υποδείγματα. Η εντροπία, ο ρυθμός πληροφορίας των συμβόλων και η μέση ποσότητα πληροφορίας των μηνυμάτων αποτελούν χαρακτηριστικά μέτρα πηγών με μνήμη, καθώς επίσης και ο πλεονασμός εξάρτησης και ο ολικός πλεονασμός.

Τα συνεχή μέτρα ποσότητας πληροφορίας ορίζονται κατ' ανάλογο τρόπο με τα διακριτά. Η μέγιστη τιμή της ποσότητας πληροφορίας τυχαίων σημάτων προσδιορίζεται αφού ληφθούν υπόψη οι περιορισμοί στους οποίους υπόκεινται οι συνεχείς τυχαίες μεταβλητές, όπως το φραγμένο εύρος ή η σταθερή ισχύς.

Βιβλιογραφία

ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΜΕΛΕΤΗ

[1] [SHA79] K. Sam Shammungen: *Ψηφιακά και Αναλογικά Συστήματα Επικοινωνίας*, Μετάφραση – επιμέλεια: Κ. Καρούμπαλου, Αθήνα, Εκδ. Γ. Πνευματικού, αγγλόφωνη έκδοση John Wiley & Sons, 1979.

Στην Ενότητα 4.2 του βιβλίου μπορείτε να βρείτε περιγραφή των πηγών Markoff και στην Ενότητα 4.3 περιγραφή του αλγόριθμου κωδικοποίησης του Shannon.

[2] [COT91] T. M. Cover, J. A. Thomas: *Elements of Information Theory*, John Willey & Sons, 1991.

Το Κεφάλαιο 3 επεξηγεί την έννοια των πιο πιθανών μηνυμάτων. Το Κεφάλαιο 4 περιγράφει, μεταξύ άλλων, τις πηγές Markoff. Στο Κεφάλαιο 5 μπορείτε να βρείτε την απόδειξη της ανισότητας του Kraft, διάφορα θέματα σχετικά με κώδικες, καθώς και περιγραφή και σύγκριση διαφόρων αλγόριθμων κωδικοποίησης, όπως του Huffman και του Shannon – Fano. Τέλος, το Κεφάλαιο 9 αναφέρεται στα συνεχή μέτρα ποσότητας πληροφορίας.

[3] [LUB97] J. C. A. van der Lubbe: *Information Theory*, Cambridge University Press, 1997.

Το Κεφάλαιο 2 του βιβλίου αυτού είναι αφιερωμένο σε θέματα σχετικά με τις διακριτές πηγές πληροφορίας χωρίς μνήμη, όπως την έννοια του πλεονασμού, την ανισότητα του Kraft, το θεώρημα κωδικοποίησης του Shannon και αλγόριθμους κωδικοποίησης. Το Κεφάλαιο 3 εξετάζει τις πηγές Markoff και θέματα κωδικοποίησης διακριτής πηγής με μνήμη. Το Κεφάλαιο 5 είναι αφιερωμένο στις συνεχείς πηγές πληροφορίας.

[4] [WEL98] R. B. Wells, *Applied Coding and Information Theory for Engineers*, Prentice Hall, 1998.

Στο βιβλίο αυτό, εκτός της θεωρίας, μπορείτε να βρείτε και λεπτομερή παραδείγματα. Το Κεφάλαιο 1 είναι αφιερωμένο στις διακριτές πηγές και τα αντίστοιχα μέτρα πληροφορίας και το Κεφάλαιο 9 αναφέρεται στα θεωρήματα κωδικοποίησης του Shannon.

[5] [ABR48]C. E. Shannon: «Mathematical Theory of Communication», *Bell System Technical Journal*, vol. 27, 1948, pp. 379 – 423, 623 – 656.

Το θεώρημα κωδικοποίησης και απλά παραδείγματα κωδίκων περιέχονται στην

εργασία αυτή. Επίσης, περιγράφεται και ο αλγόριθμος κωδικοποίησης του Fano (ή Shannon – Fano).

Άλλη βιβλιογραφία

[1] [ABR63] N. Abramson: *Information Theory and Coding*, New York, MacGraw Hill, 1963.

[2] [BLA87] R. E. Blahut: *Principles and Practice of Information Theory*, Mass., Addison – Wesley, Reading, 1987.

[3] [JON00] G. A. Jones, J. M. Jones: *Information and Coding Theory*, Springer Verlag, 2000.

[4] [ROM96] S. Roman: *Introduction to Coding and Information Theory*, Springer Verlag, 1996.

ΚΕΦΑΛΑΙΟ 3

Κανάλια Επικοινωνίας

Σκοπός

Ο σκοπός του κεφαλαίου αυτού είναι να εξετάσουμε θέματα σχετικά με το μέγιστο ρυθμό μετάδοσης και την κωδικοποίηση πληροφορίας καναλιών επικοινωνίας.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *υπολογίζετε την αμοιβαία πληροφορία μεταξύ του σήματος εισόδου και του σήματος εξόδου διακριτών καναλιών επικοινωνίας, καθώς και το ρυθμό μετάδοσης πληροφορίας από αυτά,*
- *υπολογίζετε τη χωρητικότητα διακριτών καναλιών χωρίς μνήμη,*
- *διατυπώνετε το θεμελιώδες θεώρημα της Θεωρίας Πληροφορίας,*
- *ορίζετε τη χωρητικότητα διακριτών καναλιών με μνήμη και να υπολογίζετε την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση πληροφορίας μέσω αυτών,*
- *υπολογίζετε την αμοιβαία πληροφορία μεταξύ του σήματος εισόδου και του σήματος εξόδου συνεχών καναλιών χωρίς μνήμη, καθώς και τη χωρητικότητά τους,*
- *υπολογίζετε τη χωρητικότητα ή το άνω φράγμα της χωρητικότητας συνεχών καναλιών χωρίς μνήμη,*
- *διατυπώνετε το θεώρημα κωδικοποίησης για συνεχή κανάλια επικοινωνίας.*

Έννοιες κλειδιά

- *διακριτά και συνεχή κανάλια επικοινωνίας,*
- *χωρητικότητα καναλιών επικοινωνίας,*
- *υπόδειγμα καναλιού επικοινωνίας,*
- *δυαδικό συμμετρικό κανάλι,*
- *αβεβαιότητα καναλιού επικοινωνίας,*
- *ρυθμός μετάδοσης,*
- *ενθόρυβο κανάλι επικοινωνίας,*
- *καταιγισμός σφαλμάτων,*
- *αθροιστικός γκαουσιανός λευκός θόρυβος,*
- *πιθανότητα εμφάνισης σφάλματος,*
- *προσθετικός και πολλαπλασιαστικός θόρυβος,*
- *αθροιστικό κανάλι επικοινωνίας.*

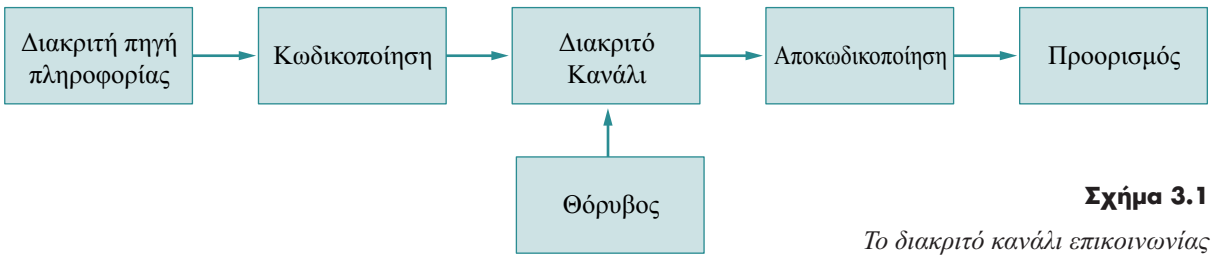
Εισαγωγικές παρατηρήσεις

Στο κεφάλαιο αυτό θα ασχοληθούμε με τη μελέτη ζητημάτων καναλιών επικοινωνίας. Θα αναπτύξουμε μοντέλα (μαθηματικά υποδείγματα) για τα διακριτά και τα συνεχή κανάλια επικοινωνίας και θα ορίσουμε την έννοια της χωρητικότητας ενός διακριτού και ενός συνεχούς καναλιού επικοινωνίας. Η χωρητικότητα είναι η πιο σημαντική παράμετρος ενός καναλιού επικοινωνίας, αφού υποδηλώνει το μέγιστο ρυθμό με τον οποίο μπορούν να μεταδοθούν δεδομένα μέσω αυτού. Επίσης, στη μελέτη μας θα λάβουμε υπόψη το θόρυβο ως παράγοντα που επηρεάζει τη μετάδοση δεδομένων και θα διατυπώσουμε τα θεωρήματα κωδικοποίησης διακριτών και συνεχών καναλιών.

Το κεφάλαιο χωρίζεται σε δύο ενότητες. Η πρώτη ενότητα αφιερώνεται στα διακριτά κανάλια επικοινωνίας, και ειδικότερα στη χωρητικότητα και στο ρυθμό μετάδοσης διακριτών καναλιών με μνήμη και χωρίς μνήμη, καθώς και στη διατύπωση του θεωρήματος κωδικοποίησης. Η δεύτερη ενότητα αφιερώνεται σε αντίστοιχα ζητήματα των συνεχών καναλιών επικοινωνίας.

3.1 Διάκριτα κανάλια επικοινωνίας

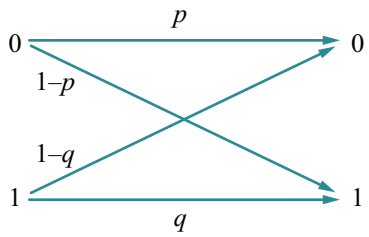
Η πηγή παράγει πληροφορία σε μορφή που δεν είναι κατάλληλη για την άμεση μετάδοσή της μέσω του καναλιού. Για το λόγο αυτό η πληροφορία υποβάλλεται σε ειδική επεξεργασία, την επονομαζόμενη «κωδικοποίηση του καναλιού», που θα μας απασχολήσει λεπτομερώς στο Κεφάλαιο 4 και τη μετατροπή σε ένα σήμα προσαρμοσμένο στις φυσικές ιδιότητες του καναλιού. Ωστόσο, το σήμα μπορεί, κατά τη μετάδοσή του, να αλλοιωθεί εξαιτίας του θορύβου. Προηγουμένως όμως, όπως είδαμε στο Κεφάλαιο 2, η παραγόμενη από την πηγή πληροφορία αποτελεί αντικείμενο επεξεργασίας για την απομάκρυνση του μη ενδιαφέροντος μέρους της (μείωση δεδομένων) και για τη συμπίεσή της (κωδικοποίηση πηγής). Στο Σχήμα 3.1 μπορούμε να δούμε ένα απλό μοντέλο του διακριτού καναλιού επικοινωνίας (δείτε και το Σχήμα 1.2), το οποίο αποτελεί τη βάση για την περαιτέρω συζήτησή μας σ' αυτή την ενότητα.



Σχήμα 3.1
Το διακριτό κανάλι επικοινωνίας

Όπως είδαμε στο Κεφάλαιο 2, ένα σύμβολο (ή ακολουθία συμβόλων) μετά την παραγωγή του από την πηγή αποτελεί αντικείμενο κωδικοποίησης, που οδηγεί στην αναπαράστασή του από μια κωδική λέξη. Η κωδική λέξη, δηλαδή η ακολουθία κωδικών συμβόλων, είναι η είσοδος του καναλιού επικοινωνίας. Αντίστοιχα, η έξοδος του καναλιού είναι επίσης μια ακολουθία κωδικών συμβόλων. Ωστόσο, η ακολουθία κωδικών συμβόλων εξόδου μπορεί να είναι διαφορετική από την ακολουθία εισόδου, εξαιτίας σφαλμάτων του καναλιού που οφείλονται κυρίως στο θόρυβο.

Το διακριτό κανάλι περιγράφεται πλήρως με ένα σύνολο πιθανοτήτων p_i και p_{ij}, όπου p_i είναι η πιθανότητα να έχουμε στην είσοδο του καναλιού το i – οστό σύμβολο του κωδικού αλφαβήτου και p_{ij} η πιθανότητα το i – οστό σύμβολο στην είσοδο να ληφθεί στην έξοδο σαν j – οστό. Στην περίπτωση του δυαδικού κωδικού αλφαβήτου, το μαθηματικό υπόδειγμα του διακριτού καναλιού φαίνεται στο Σχήμα 3.2.



Σχήμα 3.2
Το δυαδικό κανάλι

Το ανωτέρω μαθηματικό υπόδειγμα αναπαριστά την είσοδο του καναλιού με μία δυαδική τυχαία μεταβλητή X, όπου οι δύο τιμές της παριστάνονται από τους δύο κόμβους στην αριστερή πλευρά του γράφου (Σχήμα 3.2). Επίσης, η έξοδος του καναλιού αναπαρίσταται από τη δυαδική τυχαία μεταβλητή Y, όπου και πάλι οι δύο τιμές της παριστάνονται από τους δύο κόμβους στη δεξιά πλευρά του γράφου (Σχήμα 3.2). Οι δυνατές διασυνδέσεις μεταξύ των κόμβων της εισόδου και της εξόδου του καναλιού είναι τέσσερις. Οι οριζόντιες διασυνδέσεις φανερώνουν πως το κωδικό σύμβολο εισόδου εξέρχεται αναλλοίωτο από το κανάλι επικοινωνίας, ενώ οι διαγώνιες διασυνδέσεις ότι το κωδικό σύμβολο εισόδου αλλοιώνεται στο κανάλι και εξέρχεται από αυτό με διαφορετική τιμή. Έστω x_i το κωδικό σύμβολο εισόδου και y_j το κωδικό σύμβολο εξόδου του καναλιού, με $i, j = 1, 2$ και $x_1 = y_1 = 0$ και $x_2 = y_2 = 1$, τότε $p(x_i)$ και $p(y_j)$ είναι οι πιθανότητες να έχουμε στην είσοδο την τιμή x_i και στην έξοδο την τιμή y_j, αντίστοιχα. Ακόμα, $p_{ij} = p(y_j/x_i) = p(x_i/y_j)$ συμβολίζει, όπως είπαμε πιο πάνω, την πιθανότητα το i – οστό σύμβολο στην είσοδο του καναλιού να εξέρχεται από αυτό ως το j – οστό κωδικό σύμβολο. Επομένως, από το μοντέλο του δυαδικού καναλιού έχουμε $p_{11} = p$, $p_{12} = (1 - p)$, $p_{21} = (1 - q)$ και $p_{22} = q$ (Σχήμα 3.2). Αν ισχύει $p = q$, τότε μιλάμε για το **δυαδικό συμμετρικό κανάλι**, δηλαδή η πιθανότητα το «0» να μεταφέρεται από το κανάλι ως «0» είναι ίση με την πιθανότητα το «1» να μεταφέρεται ως «1». Στην περίπτωση του δυαδικού συμμετρικού καναλιού, αφού η πιθανότητα ορθής μετάδοσης είναι p, η πιθανότητα εμφάνισης σφάλματος είναι ίση με $1 - p$. Στη γενική περίπτωση του δυαδικού καναλιού, η πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση, την οποία συμβολίζουμε ως p_{error}, μπορεί να υπολογιστεί ως ακολούθως:

$$p_{error} = p(X = x_1 = 0,\ Y = y_2 = 1) + p(X = x_2 = 1,\ Y = y_1 = 0)$$
$$= p(x_1)\, p_{12} + p(x_2)\, p_{21}.$$

Με τη βοήθεια των σχέσεων που γνωρίσαμε στο Κεφάλαιο 1 μπορούμε να υπολογίσουμε τη μέση ποσότητα πληροφορίας (ή εντροπία, ή μέσο πληροφορικό περιεχόμενο) της εισόδου και της εξόδου του καναλιού, καθώς επίσης και την υπό συνθήκη ποσότητα πληροφορίας της εξόδου, με δεδομένη την είσοδο του καναλιού και τη συνδυασμένη και την αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου:

$$H(Y) = -\sum_{j=1}^{2} p(y_j) \log p(y_j).$$

$$H(X) = -\sum_{i=1}^{2} p(x_i) \log p(x_i).$$

$$H(X,Y) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(x_i, y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(y_j)p(x_i / y_j)\log p(y_j)p(x_i / y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i)p(y_j / x_i)\log p(x_i)p(y_j / x_i)$$
$$= H(X / Y) + H(Y) = H(Y / X) + H(X).$$

$$H(X / Y) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(x_i / y_j)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(y_j)p(x_i / y_j)\log p(x_i / y_j).$$

$$H(Y / X) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(y_j / x_i)$$
$$= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i)p(y_j / x_i)\log p(y_j / x_i).$$

$$I(X;Y) = H(Y) - H(Y / X) = H(X) - H(X / Y).$$

Η υπό συνθήκη ποσότητα πληροφορίας $H(X/Y)$ καλείται και **αβεβαιότητα**, αφού εκφράζει ακριβώς το πόσο αβέβαιοι είμαστε ως προς το σύμβολο της εισόδου x αν στην έξοδο έχει ληφθεί το y. Η υπό συνθήκη εντροπία είναι, λοιπόν, ένα μέτρο της μέσης αβεβαιότητας ως προς X, όταν είναι γνωστό το Y. Επίσης, η $H(Y/X)$ μπορεί να ιδωθεί ως η μέση αβεβαιότητα ως προς το y αν το x είναι γνωστό, η οποία οφείλεται στην επενέργεια του θορύβου. Οι μέσες ποσότητες πληροφορίας $H(X)$ και $H(Y)$ αντιπροσωπεύουν το μέσο αριθμό bits ανά σύμβολο (που απαιτούνται για την κωδικοποίηση της εισόδου και της εξόδου του καναλιού, αντίστοιχα).

Από την άλλη πλευρά, η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού μπορεί να θεωρηθεί ως η αβεβαιότητα ως προς το σύμβολο x πριν από τη λήψη του y, μειωμένη κατά την αβεβαιότητα που παραμένει ως προς x μετά τη λήψη και με δεδομένο το y. Επομένως, η αμοιβαία πληροφορία σχετίζεται με την ποσότητα πληροφορίας που μεταφέρεται από το κανάλι. Αντί του συμβολισμού $I(X;Y)$ χρησιμοποιείται και ο συμβολισμός R, και τότε μιλάμε για το **ρυθμό μετάδοσης**. Σ' ένα κανάλι χωρίς θόρυβο οι υπό συνθήκη ποσότητες πληροφορίας $H(X/Y)$ και $H(Y/X)$

είναι ίσες με μηδέν και επομένως η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού λαμβάνει τη μέγιστη τιμή της, η οποία είναι $H(X)$.

Οι πιθανότητες p_{ij} ή $p(y_j/x_i)$ ή $p(x_i/y_j)$ αντιπροσωπεύουν την επίδραση του θορύβου στο κανάλι επικοινωνίας και είναι αυτές ακριβώς που το χαρακτηρίζουν. Οι πιθανότητες αυτές σχηματίζουν τον πίνακα πιθανοτήτων μετάβασης του καναλιού, που ονομάζουμε και **πίνακα μετάβασης του καναλιού**. Ωστόσο, η αμοιβαία ποσότητα πληροφορίας $I(X;Y)$ εξαρτάται επίσης από τις πιθανότητες εμφάνισης των συμβόλων εισόδου $p(x_i)$, και επομένως είναι διαφορετική για διαφορετικές πιθανότητες εμφάνισης των συμβόλων εισόδου σ' ένα δεδομένο κανάλι.

Παράδειγμα 3.1

Ζητείται να υπολογιστεί η αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου ενός δυαδικού συμμετρικού καναλιού με δεδομένες τις πιθανότητες $p(x_1 = 0) = a$, $p(y_1 = 0) = b$ και $p(0/0) = p(1/1) = p$.

Απάντηση: Από τις δεδομένες πιθανότητες υπολογίζουμε πολύ εύκολα και τις πιθανότητες να έχουμε στην είσοδο και στην έξοδο το σύμβολο «1», $p(x_2 = 1) = 1 - a$, $p(y_2 = 1) = 1 - b$ και τις πιθανότητες εμφάνισης σφάλματος $p(1/0) = p(0/1) = 1 - p$. Με την εφαρμογή των ανωτέρω σχέσεων μπορούμε τώρα να υπολογίσουμε την αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου του καναλιού:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y/X) \\ &= -\beta\log\beta - (1-\beta)\log(1-\beta) \\ &\quad -\alpha p\log p - \alpha(1-p)\log(1-p) - (1-\alpha)(1-p)\log(1-p) - (1-\alpha)p\log p \\ &= -\beta\log\beta - (1-\beta)\log(1-\beta) - (1-p)\log(1-p) - p\log p. \end{aligned}$$

Παρατηρούμε ότι στο αποτέλεσμα δεν περιλαμβάνεται η παράμετρος α (ή θα μπορούσε να εκφραστεί ως συνάρτηση μόνον του α και p), αφού το συμμετρικό δυαδικό κανάλι χαρακτηρίζεται πλήρως από τις παραμέτρους β και p (ή α και p).

3.1.1 Χωρητικότητα καναλιού χωρίς μνήμη

Η αβεβαιότητα (μέσο πληροφορικό περιεχόμενο) συμβόλου ή μηνύματος που έχει εισέλθει στο κανάλι αλλά δεν έχει ληφθεί ακόμα στην έξοδο είναι ίση με $H(X)$. Από την άλλη πλευρά, μετά τη λήψη στην έξοδο, η αβεβαιότητα (πληροφορικό περιεχόμενο) ενός συμβόλου ή μηνύματος που μεταδόθηκε είναι ίση $H(X/Y)$. Επομένως, το πληροφορικό περιεχόμενο που μεταδόθηκε μέσω του καναλιού είναι ίσο με τη διαφορά των πληροφορικών περιεχομένων που αναφέραμε, $H(X) - H(X/Y)$. Η **χωρητικότητα του ενθόρυβου καναλιού** ορίζεται ως το μέγιστο πληροφορικό περιεχόμενο που μπορεί να μεταδοθεί από το κανάλι.

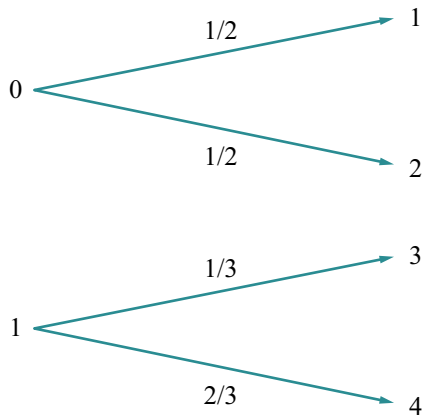
Χωρητικότητα ενθόρυβου καναλιού

Η χωρητικότητα ενός διακριτού ενθόρυβου καναλιού χωρίς μνήμη δίνεται από την ακόλουθη σχέση:

$$C = \max_{p(x)} I(X;Y) = \max_{p(x)} \{H(X) - H(X/Y)\} \\ = \max_{p(x)} \{H(Y) - H(Y/X)\} \text{ bits / symbol.} \quad (3.1)$$

Η μέγιστη τιμή προσδιορίζεται από τη σύγκριση όλων των δυνατών κατανομών εισόδου $p(x)$.

Η χωρητικότητα ενός καναλιού χωρίς θόρυβο ισούται με τη μέγιστη τιμή του $H(X)$, που συνεπάγεται ίσες πιθανότητες για όλα τα κωδικά σύμβολα, όπως είδαμε στο Κεφάλαιο 1. Στην περίπτωση του δυαδικού καναλιού: $C = \log 2 = 1$ *bit*/code_symbol, και στην περίπτωση καναλιού με q κωδικά σύμβολα: $C = \log q$ bits/code_symbol. (Εδώ αναφερόμαστε πλέον στα κωδικά σύμβολα τα οποία αποτελούν την είσοδο και την έξοδο του επικοινωνιακού καναλιού.)



Σχήμα 3.3
Ενθόρυβο κανάλι χωρίς επικαλυπτόμενες εξόδους

Παράδειγμα 3.2

Θεωρούμε ένα κανάλι επικοινωνίας του οποίου καθεμία από τις δύο δυνατές εισόδους μπορεί να ληφθεί στην έξοδο ως μία από δύο διαφορετικές τιμές (δείτε Σχήμα 3.3). Να υπολογιστεί η χωρητικότητα του καναλιού.

Απάντηση

Αν και το κανάλι αυτό εμφανίζεται να είναι ενθόρυβο, στην πραγματικότητα δεν είναι, αφού από το σύμβολο της εξόδου μπορούμε να συμπεράνουμε με βεβαιότητα το σύμ-

βολο της εισόδου. Επομένως, η χωρητικότητα αυτού του καναλιού είναι επίσης ίση με 1 bit/μετάδοση. Η χωρητικότητα είναι ίση με τη μέγιστη τιμή του $H(X)$, αφού η ποσότητα πληροφορίας $H(X/Y)$ ισούται με το 0. Η μέγιστη τιμή $H(X)$ λαμβάνεται για ισοπίθανα σύμβολα εισόδου, δηλαδή για $p(x_1 = 0) = 1/2$ και $p(x_2 = 1) = 1/2$.

Η χωρητικότητα του καναλιού μπορεί να εκφραστεί σε bits/sec αν πολλαπλασιάσουμε το ρυθμό των μεταδιδόμενων συμβόλων r με την (3.1):

$$\begin{aligned} C &= \max_{p(x)} I(X;Y)r \\ &= \max_{p(x)} \{H(X) - H(X/Y)\} r \text{ bits/sec} \end{aligned} \tag{3.2}$$

Άσκηση αυτοαξιολόγησης 3.1

Να υπολογιστεί η χωρητικότητα του διακριτού καναλιού του Παραδείγματος 1. Δίνεται ο ρυθμός μετάδοσης, $r = 1$ symbol/sec.

Μπορούμε, επίσης, να ορίσουμε τη χωρητικότητα διακριτού καναλιού χωρίς θόρυβο.

Χωρητικότητα καναλιού χωρίς θόρυβο

Η χωρητικότητα ενός διακριτού καναλιού χωρίς θόρυβο δίνεται από την ακόλουθη σχέση:

$$C = \lim_{T \to \infty} \frac{\log N(T)}{T} \text{ bits/sec} \tag{3.3}$$

όπου $N(T)$ είναι το πλήθος των επιτρεπτών μηνυμάτων χρονικής διάρκειας T.

Όπως είπαμε πιο πάνω, η χωρητικότητα του διακριτού καναλιού χωρίς θόρυβο με q κωδικά σύμβολα είναι $C = \log q$ bits/code_symbol. Αν υποθέσουμε ότι η μετάδοση κάθε κωδικού συμβόλου έχει μια διάρκεια d, τότε η χωρητικότητα του καναλιού (3.2) σε bits/sec δίνεται από την ακόλουθη σχέση:

$$C = \frac{\log q}{d} \text{ bits/sec.} \tag{3.4}$$

Αν εξετάσουμε ως μηνύματα κωδικές λέξεις μήκους l κωδικών συμβόλων και χρονικής διάρκειας T, τότε το πλήθος των δυνατών κωδικών λέξεων ισούται με $N(T) = q^l$, όπου q είναι ο αριθμός των συμβόλων του κωδικού αλφάβητου. Αφού η μέση

διάρκεια των συμβόλων είναι d και των κωδικών λέξεων T, ισχύει η σχέση $T = dl$. Η αντικατάσταση των $N(T) = q^l$ και $T = dl$ στην (3.3) οδηγεί στην (3.4). Λαμβάνοντας υπόψη ότι ο χρόνος μετάδοσης ενός κωδικού συμβόλου είναι ίσος με τον αντίστροφο του ρυθμού μετάδοσης, δηλαδή $d = 1/r$, και ότι στην περίπτωση του καναλιού χωρίς θόρυβο η ποσότητα πληροφορίας $H(Y/X)$ είναι ίση με μηδέν, συμπεραίνουμε ότι ο ορισμός της χωρητικότητας του ενθόρυβου καναλιού (3.1 ή 3.2) αποτελεί και γενίκευση του ορισμού της χωρητικότητας του καναλιού χωρίς θόρυβο.

Παράδειγμα 3.3

Θεωρούμε ένα ενθόρυβο κανάλι, την ενθόρυβη γραφομηχανή (noisy typewriter), της οποίας τα σύμβολα εισόδου καθώς και τα σύμβολα εξόδου είναι τα 24 γράμματα του ελληνικού αλφαβήτου. Ένα σύμβολο κατά τη μετάδοσή του είτε λαμβάνεται αναλλοίωτο στην έξοδο με πιθανότητα 1/2 είτε ως το επόμενό του στο αλφάβητο με πιθανότητα επίσης 1/2. Για παράδειγμα, το Α λαμβάνεται είτε ως Α είτε ως Β, με πιθανότητα 1/2. Να υπολογιστεί η χωρητικότητα αυτού του καναλιού επικοινωνίας.

Απάντηση

Τα 24 γράμματα τα αριθμούμε, ξεκινώντας από το 1 για το Α, το 2 για το Β κ.ο.κ. Αν από τα 24 σύμβολα της εισόδου χρησιμοποιούμε για μετάδοση μόνο τα σύμβολα που αντιστοιχούν σε περιττούς αριθμούς, τότε μπορούμε να πετύχουμε μετάδοση χωρίς σφάλματα, αφού κάθε είσοδος έχει δύο δυνατές εξόδους μη επικαλυπτόμενες με αυτές των άλλων (όπως στο Σχήμα 3.3). Στην περίπτωση αυτή η χωρητικότητα είναι ίση με log12 bits/*μετάδοση*. Τη χωρητικότητα της ενθόρυβης γραφομηχανής μπορούμε να την υπολογίσουμε και με τη βοήθεια του τύπου (3.1): $C = \max[H(X) - H(X/Y)] = \max H(X) - 1 = \log 24 - 1 = \log 2 + \log 12 - 1 = \log 12$ bits/*μετάδοση*, που επιτυγχάνεται για ομοιόμορφη κατανομή των συμβόλων εισόδου.

Παράδειγμα 3.4

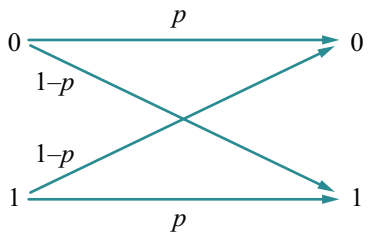
Δίνεται το δυαδικό συμμετρικό κανάλι του Σχήματος 3.4. Να υπολογιστεί το άνω φράγμα της αμοιβαίας πληροφορίας μεταξύ της εισόδου και της εξόδου και να εκφραστεί η χωρητικότητα ως συνάρτηση της πιθανότητας p (δείτε και το Παράδειγμα 1).

Απάντηση

Μπορούμε να υπολογίσουμε το άνω φράγμα της αμοιβαίας πληροφορίας ως ακολούθως:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y/X) = H(Y) - \Sigma p(x) H(Y/X = x) = \\ &= H(Y) - \Sigma p(x) H(p) = H(Y) - H(p) \leq 1 - H(p). \end{aligned}$$

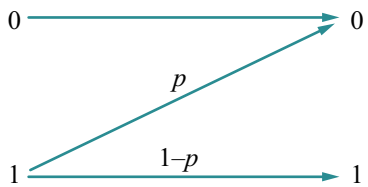
Η ανισότητα προκύπτει αφού η Y είναι δυαδική τυχαία μεταβλητή και επομένως η μέγιστη τιμή της εντροπίας της είναι ίση 1. Η ποσότητα $H(p)$ είναι συνάρτηση μόνο της παραμέτρου p: $H(Y/X) = H(p) = -p\log p - (1-p)\log(1-p)$. Η ισότητα επιτυγχάνεται για ομοιόμορφη κατανομή της εισόδου. Τότε, η χωρητικότητα του δυαδικού συμμετρικού καναλιού είναι $C = 1 - H(p)$ bits/*μετάδοση*.



Σχήμα 3.4
Το δυαδικό συμμετρικό κανάλι

Άσκηση αυτοαξιολόγησης 3.2

Το δυαδικό κανάλι Z ονομάζεται έτσι γιατί μεταφέρει το ένα από τα δύο κωδικά σύμβολα χωρίς σφάλμα, δηλαδή με πιθανότητα 1. Έστω ένα δυαδικό κανάλι Z με πιθανότητες $p(x_1 = 0) = 1 - a$, $p(x_2 = 1) = a$ και $p(y_1|x_1) = p(0/0) = 1$, $p(y_2|x_2) = p(1|1) = 1 - p$ και $p(y_1|x_2) = p(0/1) = p$ (δείτε Σχήμα 3.5). Ζητούνται η ποσότητα πληροφορίας της εισόδου, η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου και η χωρητικότητα του καναλιού. Ο ρυθμός μετάδοσης συμβόλων είναι $r =$ 1 symbol/sec.



Σχήμα 3.5
Το δυαδικό κανάλι Z

Άσκηση αυτοαξιολόγησης 3.3

Δίνεται ένα διακριτό κανάλι χωρίς μνήμη. Το κωδικό αλφάβητο αποτελείται από 4 κωδικά σύμβολα, τα 0, 1, 2 και 3. Οι πιθανότητες εμφάνισης στην είσοδο του καναλιού των κωδικών συμβόλων 0 και 1 είναι $p/2$, ενώ των συμβόλων 2 και 3 είναι $q/2$. Ακόμη, οι πιθανότητες ορθής μετάδοσης των κωδικών συμβόλων 0 και 1 από το κανάλι είναι ίση με 1, ενώ των κωδικών συμβόλων 2 και 3 είναι ίση με p. Τέλος, η πιθανότητα να εισέλθει στην είσοδο του καναλιού το σύμβολο 2 και να εξέλθει το σύμβολο 3 είναι ίση με $1 - p$ και το 3 στην είσοδο να εξέλθει ως 2 είναι

επίσης $1 - p$. Οι πιθανότητες αυτές μετάβασης $p_{ij} = p(y_j/x_i) = p(x_i/y_j)$ περιέχονται στον ακόλουθο πίνακα μετάβασης του καναλιού.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 1-p \\ 0 & 0 & 1-p & p \end{bmatrix}.$$

Να βρεθεί μια σχέση που πρέπει να πληροί η πιθανότητα q (ή η p) για την οποία η αμοιβαία πιθανότητα μεταξύ της εισόδου και της εξόδου του καναλιού παίρνει τη μέγιστη τιμή.

Δραστηριότητα 3.1

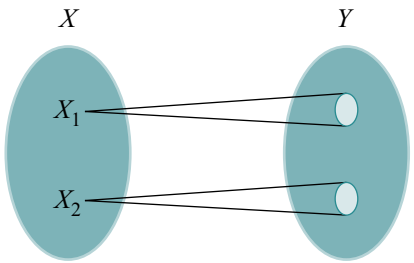
Προσπαθήστε να διατυπώσετε τρεις ιδιότητες της χωρητικότητας καναλιού επικοινωνίας και να σχολιάσετε τους τρόπους υπολογισμού αυτής, στη βάση των όσων εξετάσαμε μέχρι τώρα.

Η χωρητικότητα ενός καναλιού με θόρυβο είναι, βεβαίως, μικρότερη από αυτή ενός καναλιού χωρίς θόρυβο. Θα μπορούσαμε να αναρωτηθούμε γιατί ορίσαμε τη χωρητικότητα ενός ενθόρυβου καναλιού, αφού κατά τη μετάδοση υπεισέρχονται σφάλματα. Ο λόγος είναι γιατί μπορούμε σε κάποιες περιπτώσεις να μειώσουμε κατά βούληση την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση. Τη μείωση της πιθανότητας σφάλματος την επιτυγχάνουμε με την αύξηση του πλεονασμού κατά την κωδικοποίηση. Το ζήτημα αυτό αποτελεί αντικείμενο του ακόλουθου θεωρήματος κωδικοποίησης του Shannon, το οποίο περιγράφουμε στην υποενότητα που ακολουθεί.

3.1.2 Θεώρημα κωδικοποίησης

Σε ένα διακριτό ενθόρυβο κανάλι χωρίς μνήμη υπεισέρχονται σφάλματα κατά τη μετάδοση μηνυμάτων. Η πιθανότητα εμφάνισης σφαλμάτων μπορεί να μειωθεί αν η πληροφορία μεταδίδεται σε μορφή που ενσωματώνει πλεονασμό. Θα περιμέναμε για τη μείωση της πιθανότητας εμφάνισης σφάλματος σχεδόν στο μηδέν να απαιτείται ενσωμάτωση πλεονασμού, που θα οδηγούσε σε μείωση του ρυθμού μετάδοσης επίσης στο μηδέν. Ωστόσο, σύμφωνα με το θεώρημα του Shannon, είναι δυνατή η μετάδοση πληροφορίας με ρυθμό C μέσω του καναλιού με όσο μικρή πιθανότητα σφάλματος επιθυμούμε.

Όμως, ας προσπαθήσουμε πρώτα να αποκτήσουμε μια διαισθητική ιδέα του γιατί μπορούν να μεταδοθούν C bits μέσω του καναλιού.



Σχήμα 3.6
Μετάδοση ακολουθιών εισόδου μήκους l συμβόλων

Η βασική ιδέα είναι ότι κάθε κανάλι είναι όπως η ενθόρυβη γραφομηχανή του Παραδείγματος 3, με ένα υποσύνολο εισόδων που παράγουν στην έξοδο διαφορετικές ακολουθίες. Για κάθε τυπική (πιθανή) ακολουθία εισόδου X μήκους l συμβόλων υπάρχουν περίπου $2^{lH(Y/X)}$ δυνατές ακολουθίες εξόδου Y, όλες με την ίδια πιθανότητα (δείτε Σχήμα 3.6). Εμείς επιθυμούμε να μην υπάρχουν δύο ακολουθίες εισόδου X οι οποίες οδηγούν στην ίδια ακολουθία εξόδου Y, γιατί σε μια τέτοια περίπτωση δε θα μπορούσαμε να συμπεράνουμε από την ακολουθία εξόδου ποια ακολουθία εισόδου μεταδόθηκε. Γνωρίζουμε ότι το πλήθος των πιθανών (ή τυπικών) ακολουθιών εξόδου είναι προσεγγιστικά ίσο με $2^{lH(Y)}$ (Υποενότητα 2.1.4). Αν το σύνολο αυτό των τυπικών ακολουθιών εξόδου Y το χωρίσουμε σε σύνολα μεγέθους $2^{lH(Y/X)}$, καθένα εκ των οποίων αντιστοιχεί σε διαφορετική ακολουθία εισόδου X, τότε το πλήθος των διαφορετικών αυτών συνόλων είναι μικρότερο ή ίσο με $2^{lH(X)}/2^{lH(Y/X)} = 2^{l[H(X) - H(Y/X)]} = 2^{lI(X;Y)}$. Επομένως, μπορούμε να μεταδώσουμε το πολύ $2^{lI(X;Y)}$ ακολουθίες εισόδου, μήκους l συμβόλων, οι οποίες είναι με βεβαιότητα αναγνωρίσιμες στην έξοδο.

Η ανωτέρω διαισθητική περιγραφή αναφέρεται σε ένα άνω φράγμα της χωρητικότητας. Στη συνέχεια θα εξετάσουμε το ιδιαίτερα σημαντικό αποτέλεσμα της Θεωρίας Πληροφορίας, το δεύτερο θεώρημα κωδικοποίησης του Shannon. Για την απόδειξη του θεωρήματος θα χρησιμοποιήσουμε τα επιχειρήματα της προηγούμενης παραγράφου σε μια πιο αυστηρή εκδοχή.

ΘΕΩΡΗΜΑ 3.1

Δεύτερο Θεώρημα Κωδικοποίησης του Shannon ή Θεμελιώδες Θεώρημα της Θεωρίας Πληροφορίας

Σε ένα κανάλι χωρίς μνήμη χωρητικότητας C, είναι δυνατή η μετάδοση ποσότητας πληροφορίας $H(X)$ διακριτής πηγής με οσοδήποτε μικρή πιθανότητα σφάλματος θέλουμε, αν ισχύει $H(X) \leq C$.

Αντίστροφα, είναι αδύνατο να μεταδοθεί πληροφορία με ρυθμό μεγαλύτερο της χωρητικότητας, $H(X)>C$, ανεξαρτήτως της κωδικοποίησης που χρησιμοποιείται, χωρίς να αυξάνεται ανεξέλεγκτα ο αριθμός των σφαλμάτων.

Απόδειξη

Εξετάζουμε πρώτα την περίπτωση μιας διακριτής πηγής με εντροπία $H(X)$ και με τέτοια κατανομή πιθανοτήτων των συμβόλων εισόδου ώστε να ισχύει $C = H(X) – H(X/Y)$. (Η χωρητικότητα εκφράζεται σε bits/*symbol*. Αν είχαμε λάβει υπόψη και το ρυθμό μετάδοσης r, τότε η χωρητικότητα θα εκφραζόταν σε bits/*sec*.) Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην είσοδο του καναλιού είναι ίσο με $M_x = 2^{lH(X)}$, όπου όλα τα μηνύματα είναι ισοπίθανα (Υποενότητα 2.1.4). Ανάλογα, το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην έξοδο του καναλιού είναι ίσο με $M_y = 2^{lH(Y)}$. Ένα μήνυμα $m(y)$ που λαμβάνεται στην έξοδο του ενθόρυβου καναλιού μπορεί να προέρχεται από ένα πλήθος μηνυμάτων εισόδου $m(x)$ εξαιτίας του θορύβου. Το πλήθος των πιο πιθανών μηνυμάτων εισόδου που οδηγούν στη λήψη του ίδιου μηνύματος εξόδου είναι ίσο με $M_{x/y} = 2^{lH(X/Y)}$.

Αν $rI(X;Y) = C$, δηλαδή η πηγή προσαρμόζεται ιδανικά στο κανάλι, τότε το πλήθος των πιο πιθανών μηνυμάτων που μεταδίδονται είναι ίσο με $M_C = 2^{lC}$. Στην περίπτωση μη ιδανικής προσαρμογής, ισχύει $M_R = 2^{lR}$, όπου $rI(X;Y) = R$. Με την τελευταία αυτή περίπτωση, της μη ιδανικής προσαρμογής, δηλαδή $R < C$, θα ασχοληθούμε στη συνέχεια.

Η πιθανότητα μεταφοράς ενός μηνύματος $m(x_i)$, το οποίο ανήκει στο σύνολο των πιο πιθανών μηνυμάτων M_x, από το κανάλι ισούται με την πιθανότητα να ανήκει το μήνυμα $m(x_i)$ στο σύνολο των μηνυμάτων που μεταφέρονται από το κανάλι M_R. Η πιθανότητα αυτή υπολογίζεται ως εξής:

$$p(m(x_i) \in M_R) = \frac{2^{lR}}{2^{lH(X)}} = 2^{l(R-H(X))} \tag{3.5}$$

Από την άλλη πλευρά, το πλήθος των μηνυμάτων εισόδου που οδηγούν, κατά μέσο όρο, στη λήψη του ίδιου μηνύματος στην έξοδο $m(y)$ δίνεται από $M_{x/y}$. Τώρα επιλέγουμε τυχαία ένα μήνυμα εισόδου $m(x_i)$. Αν υπάρχει τουλάχιστον ένα άλλο μήνυμα $m(x_j)$, εκτός του $m(x_i)$, το οποίο να ανήκει τόσο στο $M_{x/y}$ όσο και στο $M_R = 2^{lR}$ που μπορεί να οδηγήσει στη λήψη του ίδιου μηνύματος $m(y_i)$, τότε μπορεί να συμβεί σφάλμα. Η πιθανότητα της εμφάνισης ενός σφάλματος είναι

$$
\begin{aligned}
p_{error} &= p\left\{m(x_j) \in (M_{x/y} \cap M_R), j \neq i\right\} \\
&\leq \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p\left[(m(x_j) \in M_{x/y}) \cap (m(x_j) \in M_R)\right] \\
&= \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p(m(x_j) \in M_{x/y}) p(m(x_j) \in M_R) \\
&\leq \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} p(m(x_j) \in M_R) = \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} \frac{2^{lR}}{2^{lH(X)}} = \sum_{\substack{j=1 \\ j\neq i}}^{M_{x/y}} 2^{l\left(R-H(X)\right)} = \left\{M_{x/y} - 1\right\} 2^{l\left(R-H(X)\right)}
\end{aligned}
$$

Αφού $R < C$, έχουμε $R = C - \varepsilon = H(X) - H(X/Y) - \varepsilon$, όπου ε είναι ένας θετικός σταθερός αριθμός. Επομένως, η πιθανότητα σφάλματος ικανοποιεί την ακόλουθη ανισότητα:

$$p_{error} \leq \left\{2^{lH\left(X|Y\right)} - 1\right\} 2^{l\left(-H\left(X|Y\right)-\varepsilon\right)} \leq 2^{-l\varepsilon}.$$

Από την τελευταία σχέση προκύπτει ότι η πιθανότητα εμφάνισης λάθους μπορεί να γίνει οσοδήποτε μικρή επιθυμούμε, αρκεί να επιλέξουμε κατάλληλα μεγάλο μήκος l.

Το δεύτερο μέρος του θεωρήματος μπορεί να δειχθεί ως ακολούθως: Αν είναι $H(X) > C$, τότε η αβεβαιότητα $H(X/Y)$ είναι μεγαλύτερη του μηδενός και τουλάχιστον ίση με $H(X) - C$. Για να το αποδείξουμε, ας υποθέσουμε καταρχήν το αντίθετο, δηλαδή ότι η αβεβαιότητα $H(X/Y)$ είναι μικρότερη της ποσότητας $H(X) - C$. Αλλά τότε θα έπρεπε να ισχύει $H(X/Y) = H(X) - C - \varepsilon$, για κάποιο θετικό αριθμό ε. Επομένως, $H(X/Y) = H(X) - C - \varepsilon$ και $H(X) - H(X/Y) = C + \varepsilon$. Όμως, αφού η χωρητικότητα είναι η μέγιστη τιμή της ποσότητας $H(X) - H(X/Y)$, η τελευταία σχέση δεν μπορεί να ισχύει. Άρα, η αβεβαιότητα $H(X/Y)$ είναι μεγαλύτερη του μηδενός και τουλάχιστον ίση της διαφοράς $H(X) - C$, δηλαδή $H(X/Y) = H(X) - C + \varepsilon$. Επομένως, δεν είναι δυνατή η μετάδοση με ρυθμό $H(X) > C$.

Η απόδειξη του θεωρήματος βασίζεται στην έννοια των πιο πιθανών ή τυπικών μηνυμάτων, που εξετάσαμε στην Υποενότητα 2.1.4. Μια πιο αυστηρή απόδειξη του Θεωρήματος 3.1 θα ήταν ιδιαίτερα σύνθετη.

Δραστηριότητα 3.2

Προσπαθήστε να συνοψίσετε σε μερικές γραμμές το Θεμελιώδες Θεώρημα της Θεωρίας της Πληροφορίας. Μια ενδεικτική απάντηση δίνεται στη συνέχεια.

Σύμφωνα με το Θεώρημα 3.1, όλοι οι ρυθμοί μετάδοσης οι οποίοι είναι μικρότεροι της χωρητικότητας μπορούν να επιτευχθούν. Πιο συγκεκριμένα, για κάθε ρυθμό μετάδοσης R < C υπάρχει τρόπος κωδικοποίησης καναλιού με μέγιστη πιθανότητα σφάλματος κατά τη μετάδοση η οποία τείνει στο μηδέν. Αντίστροφα, οποιαδήποτε κωδικοποίηση καναλιού και αν χρησιμοποιήσουμε, για να τείνει η μέγιστη πιθανότητα σφάλματος στο μηδέν, πρέπει ο ρυθμός μετάδοσης να είναι μικρότερος ή ίσος της χωρητικότητας.

Με το Θεώρημα 3.1 αποδείξαμε ότι είναι δυνατή η μετάδοση χωρίς σφάλματα, χωρίς ωστόσο να αναφερθούμε στο πώς επιτυγχάνεται. Βέβαια, επειδή δεν μπορούμε να έχουμε πολύ μεγάλα μήκη μηνυμάτων (και κωδικών λέξεων) για να πετύχουμε μετάδοση χωρίς σφάλματα, θα πρέπει να υπολογίζουμε με κάποιες πιθανότητες σφαλμάτων, που κυμαίνονται ανάλογα με την εφαρμογή από περίπου 10^{-14} έως 10^{-3}. Στην πράξη χρησιμοποιούνται **κώδικες ελέγχου σφάλματος (κωδικοποίηση καναλιού)** για τη μείωση των σφαλμάτων που εμφανίζονται κατά τη μετάδοση στα κανάλια επικοινωνίας. Με τους κώδικες ελέγχου σφάλματος θα ασχοληθούμε στο Κεφάλαιο 4.

Άσκηση αυτοαξιολόγησης 3.4

Ποιες από τις προτάσεις που ακολουθούν είναι σωστές και ποιες όχι; Επιλέξτε «Σωστό» ή «Λάθος», ανάλογα με την περίπτωση.

	Σωστό	Λάθος
Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην είσοδο του καναλιού είναι ίσο με $M_x = 2^{lH(X)}$.	❑	❑
Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην έξοδο του καναλιού είναι ίσο με $M_y = 2^{lH(Y)}$.	❑	❑
Το πλήθος των πιο πιθανών μηνυμάτων εισόδου που οδηγούν στη λήψη του ίδιου μηνύματος εξόδου είναι ίσο με $M_{y/x} = 2^{lH(Y/X)}$.	❑	❑
Στην περίπτωση μη ιδανικής προσαρμογής της πηγής στο κανάλι, ισχύει $M_R = 2^{lR}$, όπου $rI(X;Y) = R$.	❑	❑
Αναφορικά με την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση ενός τυχαίου μηνύματος, ισχύει η ανισότητα: $p_{error} > 2^{-l\varepsilon}$, όπου ε θετικός σταθερός αριθμός.	❑	❑

3.1.3 Διάκριτα κανάλια με μνήμη

Στις προηγούμενες υποενότητες εξετάσαμε κανάλια χωρίς μνήμη, δηλαδή κανάλια στα οποία η εμφάνιση ενός σφάλματος κατά τη μετάδοση ενός συμβόλου δεν επηρεάζει τη μετάδοση των επόμενων συμβόλων. Οι περισσότεροι από τους κώδικες ελέγχου σφάλματος που εφαρμόζονται βασίζονται στην παραδοχή ότι τα σφάλματα εμφανίζονται ως ανεξάρτητα τυχαία γεγονότα. Ωστόσο, σε πολλά κανάλια τα σφάλματα εκδηλώνονται μάλλον συσχετισμένα. Αυτό οφείλεται και στο ότι χρησιμοποιούνται πολύ υψηλοί ρυθμοί μετάδοσης, που έχουν ως αποτέλεσμα υφιστάμενες ατέλειες των επικοινωνιακών συστημάτων να προκαλούν σειρές διαδοχικών σφαλμάτων. Για παράδειγμα, σε μαγνητικά και οπτικά μέσα αποθήκευσης, που χαρακτηρίζονται από υψηλές πυκνότητες αποθήκευσης, αυτές έχουν ως αποτέλεσμα την εμφάνιση ακολουθιών διαδοχικών σφαλμάτων όταν παρουσιάζονται βλάβες. Επίσης, τα τηλεφωνικά κανάλια επηρεαζόμενα από τις διατάξεις μεταγωγής συμπεριφέρονται ως κανάλια με μνήμη.

Στα κανάλια με μνήμη εκδηλώνονται, ορισμένες φορές, ξαφνικοί θόρυβοι, που επικρατούν του θορύβου Gauss και προκαλούν καταιγισμούς σφαλμάτων. Τα φαινόμενα των θορύβων είναι πολύπλοκα και γι' αυτό κάνουν δύσκολο το λεπτομερή χαρακτηρισμό των καναλιών με μνήμη.

Αμέσως μετά τον ορισμό της χωρητικότητας του διακριτού καναλιού με μνήμη θα γνωρίσουμε ένα μαθηματικό υπόδειγμα το οποίο είχε σχετική επιτυχία για το χαρακτηρισμό των καταιγισμών σφαλμάτων στα κανάλια με μνήμη.

Ορισμός χωρητικότητας διακριτού καναλιού με μνήμη

Ορίζουμε τη χωρητικότητα του διακριτού καναλιού με μνήμη υποθέτοντας ακολουθίες κωδικών συμβόλων στην είσοδο και στην έξοδο μήκους L, ως ακολούθως:

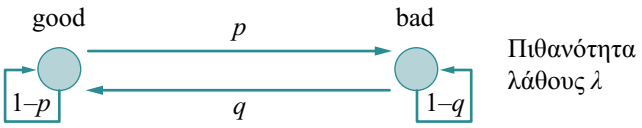
$$C = \lim_{L\to\infty} \frac{1}{L} \max_{p(x_1 \ldots x_L)} I(X_1 \ldots X_L; Y_1 \ldots Y_L) \tag{3.6}$$

Η μέγιστη τιμή της αμοιβαίας πληροφορίας προκύπτει από τη σύγκριση των κατανομών πιθανοτήτων όλων των κωδικών ακολουθιών εισόδου μήκους L.

Κατά κανόνα, ο υπολογισμός και η αξιολόγηση της χωρητικότητας καναλιών με μνήμη είναι αρκετά σύνθετη υπόθεση. Για το λόγο αυτό θα περιοριστούμε στη συνέχεια στην εξέταση δυαδικών καναλιών.

Η εμφάνιση μιας ακολουθίας συσχετισμένων σφαλμάτων ονομάζεται «καταιγισμός» (burst). Ως μήκος του καταιγισμού εννοούμε το μήκος από το πρώτο μέχρι και το

τελευταίο σφάλμα. Για τη μελέτη των καναλιών με μνήμη μπορούμε να χρησιμοποιήσουμε στατιστικές μεθόδους ή υποδείγματα (μοντέλα) που δημιουργούν ακολουθίες σφαλμάτων παρόμοιες με αυτές των καναλιών. Τέτοια είναι τα υποδείγματα τα οποία αποτελούνται από μια Μαρκοβιανή αλυσίδα με συγκεκριμένο αριθμό καταστάσεων και τις αντίστοιχες πιθανότητες μετάβασης. Αυτά ονομάζονται, μερικές φορές στη βιβλιογραφία, και «υποδείγματα Gilbert». Το πιο απλό μοντέλο αυτού του τύπου βλέπουμε στο Σχήμα 3.7.



Σχήμα 3.7
Ένα μαθηματικό υπόδειγμα για κανάλια με μνήμη

Το μοντέλο του Σχήματος 3.7 έχει δύο καταστάσεις, την κατάσταση «good» και την κατάσταση «bad». Υποθέτουμε ότι ο ρυθμός μετάδοσης των δυαδικών ψηφίων είναι ίσος με 1 *symbol*/*sec*. Αν είμαστε στην κατάσταση «good» στην αρχή του χρονικού διαστήματος συμβόλου $t = n$, τότε το δυαδικό ψηφίο που μεταδίδεται λαμβάνεται χωρίς λάθος στην έξοδο. Αμέσως μετά, στην αρχή του επόμενου χρονικού διαστήματος συμβόλου $t = n + 1$, αποφασίζεται αν θα παραμείνει στην κατάσταση «good» με πιθανότητα $1 - p$ ή θα μεταπέσει στην κατάσταση «bad» με πιθανότητα p. Αν παραμείνει στην κατάσταση «good», έχουμε και πάλι ορθή μετάδοση ενός δυαδικού ψηφίου. Αντίθετα, αν μεταπέσει στην κατάσταση «bad», τότε η μετάδοση του δυαδικού ψηφίου είναι ορθή με πιθανότητα $1 - \lambda$ και εσφαλμένη με πιθανότητα λ (δείτε Σχήμα 3.7). Μετά τη μετάδοση, στην αρχή του χρονικού διαστήματος συμβόλου $t = n + 2$ αποφασίζεται αν θα παραμείνει στην κατάσταση «bad» με πιθανότητα $1 - q$ ή θα μεταπέσει στην κατάσταση «good» με πιθανότητα q. Παρατηρούμε ότι το μοντέλο προβλέπει πάντα ορθή μετάδοση στην κατάσταση «good» και ορθή ή εσφαλμένη μετάδοση στην κατάσταση «bad».

Ας προσπαθήσουμε να αναλύσουμε τώρα το μοντέλο αυτό (μοντέλο Gilbert). Από τις δύο καταστάσεις του Σχήματος 3.7 μπορούμε να υπολογίσουμε τις πιθανότητες να βρίσκεται το κανάλι στις καταστάσεις «good» και «bad», καθώς επίσης και την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση. Μεταξύ των πιθανοτήτων κατάστασης και των πιθανοτήτων μετάπτωσης ισχύουν οι ακόλουθες σχέσεις (δείτε την Υποενότητα 2.2.1 για τις Μαρκοβιανές αλυσίδες):

$$p(good) + p(bad) = 1,$$

$$p(good)p + p(good)(1 - p) = p(good)(1 - p) + p(bad)q,$$

$$p(bad)q + p(bad)(1 - q) = p(bad)(1 - q) + p(good)p.$$

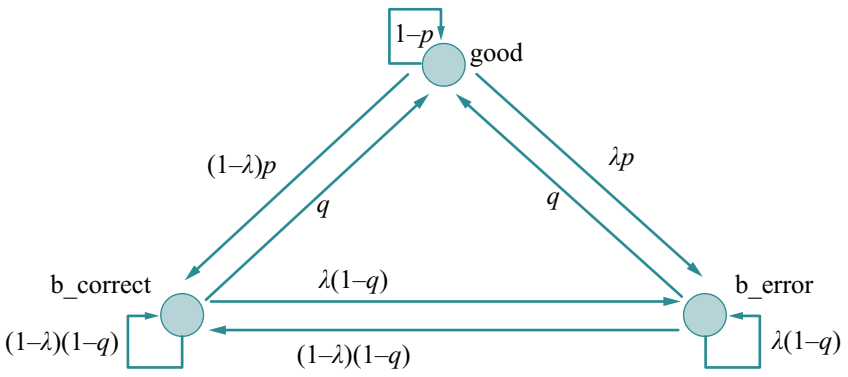
Από το ανωτέρω σύστημα εξισώσεων μπορούν να υπολογιστούν οι πιθανότητες των καταστάσεων και από την πιθανότητα της κατάστασης «bad», $p(bad)$, λαμβανομένης υπόψη της πιθανότητας εσφαλμένης μετάδοσης στην κατάσταση «bad», υπολογίζεται η πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση, p_{error}. Παρατηρούμε ότι, ενώ η δεδομένη πιθανότητα λ αναφέρεται στην εσφαλμένη μετάδοση όταν το κανάλι είναι στην κατάσταση «bad», η p_{error} αναφέρεται στην πιθανότητα εσφαλμένης μετάδοσης ανεξαρτήτως της κατάστασης στην οποία βρίσκεται.

$$p(good) = \frac{q}{p+q}.$$

$$p(bad) = \frac{p}{p+q}.$$

$$p_{error} = \lambda p(bad) = \lambda \frac{p}{p+q}.$$

Μπορούμε να επεκτείνουμε το πλήθος των καταστάσεων του μοντέλου του Σχήματος 3.7 σε τρεις, διακρίνοντας την κατάσταση «bad» σε δύο υποκαταστάσεις: της ορθής (b_correct) και της εσφαλμένης (b_error) μετάδοσης (Σχήμα 3.8). Κατ' αυτόν τον τρόπο η ανάλυση της Μαρκοβιανής αλυσίδας του Σχήματος 3.8 οδηγεί στον υπολογισμό των καταστάσεων $p(good)$, $p(b\_correct)$ και $p(b\_error)$. Το άθροισμα των $p(b\_correct)$ και $p(b\_error)$ είναι η $p(bad)$ και $p(b\_error)$ είναι η p_{error}. Επομένως, το επεκτεταμένο μοντέλο του Σχήματος 3.8 με τις τρεις καταστάσεις επιτρέπει επίσης τον υπολογισμό των πιθανοτήτων καλής, κακής και εσφαλμένης μετάδοσης, δηλαδή των $p(good)$, $p(bad)$ και p_{error}.



Σχήμα 3.8
Το υπόδειγμα Gilbert με τρεις καταστάσεις

Το ανωτέρω μοντέλο γίνεται πιο σύνθετο όταν προβλέπονται περισσότερες των τριών καταστάσεων, οι οποίες είναι απαραίτητες για την ανάλυση της συμπεριφοράς των ακολουθιών σφαλμάτων.

Παράδειγμα 3.5

Για το μοντέλο του Σχήματος 3.7 δίνονται $p = 0{,}02$, $q = 0{,}1$ και $\lambda = 0{,}2$. Ζητούνται οι πιθανότητες $p(good)$, $p(bad)$ και p_{error}.

Απάντηση

Με εφαρμογή των σχετικών τύπων μπορούμε εύκολα να υπολογίσουμε τις ζητούμενες πιθανότητες: $p(good) = (q/(p + q)) = (0{,}1/0{,}12) = 0{,}83$, $p(bad) = (p/(p + q)) = 0{,}17$ και $p_{error} = \lambda\, p(bad) = 0{,}034$.

Άσκηση αυτοαξιολόγησης 3.5

Για το μοντέλο του Σχήματος 3.7 δίνονται $p = 0{,}01$, $q = 0{,}2$ και $\lambda = 0{,}1$. Να μετασχηματίσετε το μοντέλο του Σχήματος 3.7 σε αυτό του Σχήματος 3.8 με τις τρεις καταστάσεις και να υπολογίσετε τις πιθανότητες $p(good)$, $p(b\_correct)$, $p(b\_error)$ και p_{error}.

3.2 Συνεχή κανάλια επικοινωνίας

Στα συνεχή επικοινωνιακά κανάλια η κωδικοποίηση και η αποκωδικοποίηση ερμηνεύονται διαφορετικά απ' ό,τι στα διακριτά κανάλια. Με την κωδικοποίηση εννοούμε διαμόρφωση πλάτους και συχνότητας ή τη φραγή εύρους με τη χρήση φίλτρων. Με τη διαμόρφωση το σήμα που παράγεται από την πηγή μετατρέπεται σε μορφή κατάλληλη για το συνεχές κανάλι.

Όπως στην περίπτωση του διακριτού καναλιού, κατά τη μετάδοση του σήματος στο συνεχές κανάλι επενεργεί προσθετικός ή και πολλαπλασιαστικός θόρυβος. Για το λόγο αυτό το μεταδιδόμενο σήμα θα πρέπει να επανακατασκευαστεί στην έξοδο από το διαστρεβλωμένο σήμα που λαμβάνεται.

Ο προσθετικός θόρυβος με τον οποίο ασχολούμαστε στο σύγγραμμα αυτό εμφανίζεται πιο συχνά από τον πολλαπλασιαστικό. Μπορεί δε να είναι γκαουσιανός ή κρουστικός. Ο γκαουσιανός θόρυβος είναι θερμικός ή βολής από τις διατάξεις και από ακτινοβολία που λαμβάνεται από την κεραία λήψης. Ο κρουστικός θόρυβος, από την άλλη πλευρά, οφείλεται σε μεταβατικά φαινόμενα στη λειτουργία των διακοπτών και χαρακτηρίζεται από μεγάλα διαστήματα χωρίς θόρυβο που διακόπτονται από καταιγισμούς παλμών θορύβου μεγάλου πλάτους.

Στις επόμενες υποενότητες θα εξετάσουμε θέματα σχετικά με τη χωρητικότητα συνεχών καναλιών χωρίς μνήμη, το θεώρημα κωδικοποίησης συνεχών καναλιών και ζητήματα σχετικά με τη χωρητικότητα συνεχών καναλιών με μνήμη.

3.2.1 Χωρητικότητα συνεχών καναλιών χωρίς μνήμη

Στην είσοδο του καναλιού έχουμε ένα συνεχές σήμα $x(t)$ και στην έξοδο επίσης ένα σήμα $y(t)$. Θα υποθέσουμε N δείγματα αυτών των σημάτων. Για τη συνάρτηση πυκνότητας πιθανότητας του σήματος που λαμβάνεται στην έξοδο του καναλιού $y(t)$ με δεδομένο το σήμα εισόδου $x(t)$, ισχύει

$$f(y/x) = f(y_1, \ldots, y_N / x_1, \ldots, x_N).$$

Αν ένα δείγμα του σήματος εξόδου εξαρτάται μόνο από το αντίστοιχο δείγμα του σήματος εισόδου, τότε μιλάμε για συνεχή κανάλια χωρίς μνήμη. Σ' αυτή την περίπτωση τα μέτρα ποσότητας πληροφορίας που μας ενδιαφέρουν μπορούν να οριστούν στη βάση ενός ζεύγους δειγμάτων X και Y. (Τα X και Y είναι τυχαίες μεταβλητές που αναπαριστούν τα δείγματα των σημάτων εισόδου και εξόδου $x(t)$ και $y(t)$.) Όπως και στην περίπτωση των συνεχών πηγών πληροφορίας, μπορούμε να ορίσουμε την αμοιβαία ποσότητα πληροφορίας μεταξύ των συνεχών τυχαίων μεταβλητών που αναπαριστούν τα δείγματα εισόδου και της εξόδου. Ωστόσο, παρ' όλο που ο τύπος που ακολουθεί είναι ίδιος με αυτόν που γνωρίσαμε στο Κεφάλαιο 2, η ερμηνεία του είναι διαφορετική, αφού συσχετίζει το δείγμα εισόδου με αυτό της εξόδου. Στην κατωτέρω σχέση, με $f(x,y)$ συμβολίζεται η συνδυασμένη συνάρτηση πυκνότητας πιθανότητας των τυχαίων μεταβλητών X και Y.

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log\frac{f(x,y)}{f(x)f(y)}\,dxdy.$$

Η αμοιβαία ποσότητα πληροφορίας καλείται και «ρυθμός μετάδοσης πληροφορίας», αφού πρόκειται για την ποσότητα πληροφορίας που μεταφέρεται μέσω του καναλιού. Επίσης, ισχύουν και οι γνωστές σχέσεις μεταξύ της αμοιβαίας ποσότητας πληροφορίας και των ακραίων εντροπιών και των υπό συνθήκη ποσοτήτων πληροφορίας ή της συνδυασμένης ποσότητας πληροφορίας.

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y). \qquad (3.7)$$

Ορισμός χωρητικότητας συνεχούς καναλιού χωρίς μνήμη

Ορίζουμε τη χωρητικότητα του συνεχούς καναλιού ως τη μέγιστη τιμή της αμοιβαίας πληροφορίας μεταξύ της εισόδου και της εξόδου ή του ρυθμού μετάδοσης, που μπορεί να επιτευχθεί συνδέοντας όλες τις πηγές πληροφορίας στο κανάλι και λαμβάνοντας υπόψη τους υφιστάμενους περιορισμούς.

$$C = \max_{f(x)} I(X;Y) = \max_{f(x)}\{H(Y) - H(Y/X)\}. \qquad (3.8)$$

Η μέγιστη τιμή της αμοιβαίας πληροφορίας προκύπτει από τη σύγκριση των συναρτήσεων πυκνότητας πιθανότητας των δειγμάτων του σήματος εισόδου. Ωστόσο, ο υπολογισμός της χωρητικότητας ενός συνεχούς καναλιού είναι δύσκολος.

Στη συνέχεια θα εξετάσουμε τη γενική περίπτωση των αθροιστικών καναλιών, όπου ο στατιστικά ανεξάρτητος θόρυβος $n(t)$ προστίθεται στο μεταδιδόμενο σήμα $x(t)$, και θα ολοκληρώσουμε την υποενότητα με την ειδική περίπτωση του προσθετικού γκαουσιανού λευκού θορύβου. Στη γενική περίπτωση, ισχύει αναφορικά με τις συναρτήσεις πυκνότητας πιθανότητας του σήματος εισόδου, του σήματος εξόδου και του θορύβου η ακόλουθη σχέση ($X + N = Y$):

$$f(y/x) = f(x + n/x) = f(n/x).$$

Αφού ο θόρυβος είναι στατιστικά ανεξάρτητος του σήματος εισόδου, η υπό συνθήκη συνάρτηση πιθανότητας του δείγματος του θορύβου με δεδομένο το δείγμα του σήματος εισόδου μπορεί να εκφραστεί μόνο ως προς τα σήματα εισόδου και εξόδου.

$$f(y/x) = f(n/x) = f(n) = f(y - x).$$

Στην περίπτωση του αθροιστικού καναλιού, η επενέργεια του θορύβου στη χωρητικότητα του καναλιού αντανακλάται στην υπό συνθήκη ποσότητα πληροφορίας $H(Y/X)$. Μπορούμε να υπολογίσουμε την ποσότητα πληροφορίας $H(Y/X)$ ως εξής [δείτε Ενότητα 2.3, σχέση (2.21)]:

$$\begin{aligned} H(Y/X) &= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log f(y/x)\,dx\,dy \\ &= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(y/x)\log f(y/x)\,dx\,dy \\ &= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(n)\log f(n)\,dx\,dn \\ &= -\int_{-\infty}^{\infty} f(n)\log f(n)\,dn = H(N). \end{aligned}$$

Επομένως, η χωρητικότητα του αθροιστικού καναλιού μπορεί να εκφραστεί ως συνάρτηση της μέγιστης μέσης ποσότητας πληροφορίας της εξόδου και της μέσης ποσότητας πληροφορίας του θορύβου.

$$C = \max_{f(x)} I(X;Y) = \max_{f(x)}\{H(Y) - H(N)\} = \max_{f(x)} H(Y) - H(N).$$

Άσκηση αυτοαξιολόγησης 3.6

Σε ένα αθροιστικό συνεχές κανάλι δίνονται οι ακόλουθες συναρτήσεις πυκνότητας πιθανότητας του σήματος εισόδου και του θορύβου.

$$f(x)=\begin{cases}\frac{1}{8}, & -4\le x\le 4\\ 0, & x>4,\ x<\text{-}4.\end{cases}$$

$$f(n)=\begin{cases}\frac{1}{2}, & -1\le x\le 1\\ 0, & x>1,\ x<-1.\end{cases}$$

Να υπολογιστούν οι μέσες ποσότητες πληροφορίας των σημάτων εισόδου, εξόδου και του θορύβου, η συνδυασμένη ποσότητα πληροφορίας και η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου και η υπό συνθήκη ποσότητα πληροφορίας της εισόδου με δεδομένη την έξοδο. Επίσης, να εκφραστεί η χωρητικότητα ως συνάρτηση μόνο της μέγιστης τιμής της εντροπίας της εξόδου.

Συνεχίζουμε με την ειδική περίπτωση του **αθροιστικού γκαουσιανού λευκού θορύβου**. Πιο συγκεκριμένα, θα προσπαθήσουμε να εκφράσουμε τη χωρητικότητα συνεχών καναλιών όταν επενεργεί μόνο αθροιστικός λευκός θόρυβος. Υποθέτουμε, λοιπόν, όπως και ανωτέρω, ότι ο θόρυβος είναι αθροιστικός και ανεξάρτητος του σήματος εισόδου. Επιπρόσθετα, ο λευκός θόρυβος χαρακτηρίζεται από μια γκαουσιανή συνάρτηση πυκνότητας πιθανότητας $N(0, \sigma)$, δηλαδή μηδενικής μέσης τιμής, και από σταθερή ισχύ πυκνότητας φάσματος στο εύρος ζώνης W. Επίσης, ο λευκός θόρυβος χαρακτηρίζεται από εσωτερική ανεξαρτησία, δηλαδή τα δείγματα του θορύβου είναι στατιστικά ανεξάρτητα και, επομένως, κάθε δείγμα του θορύβου μπορεί να εξεταστεί ξεχωριστά από τα υπόλοιπα δείγματα.

Αφού η συνάρτηση πυκνότητας πιθανότητας του λευκού θορύβου είναι αυτή της κανονικής κατανομής με μηδενική μέση τιμή, η ποσότητα πληροφορίας αυτού είναι ίση με τη μέγιστη ποσότητα πληροφορίας σήματος συνεχούς πηγής πληροφορίας με σταθερή ισχύ. Η μέγιστη ποσότητα πληροφορίας μιας συνεχούς πηγής πληροφορίας με σταθερή ισχύ, σ^2, είναι ίση με $H(X) = \log(\sigma\sqrt{2\pi e})$ και ισχύει για κανονική συνάρτηση πυκνότητας πιθανότητας, $f(x)$. Το αποτέλεσμα αυτό μπορούμε να το επεκτείνουμε και να το εκφράσουμε σε bits/sec λαμβάνοντας υπόψη το πλήθος των δειγμάτων M, το οποίο είναι ίσο με το διπλάσιο του εύρους ζώνης του σήματος W, δηλαδή $M = 2W$.

$$
\begin{aligned}
H(N) &= \log\left(\sigma\sqrt{2\pi e}\right) \text{ bits / δείγμα} \\
&= M\frac{1}{2}\log\left(2\pi e\sigma^2\right) \text{ bits / sec} \\
&= 2\mathrm{W}\frac{1}{2}\log\left(2\pi e\sigma^2\right) = \mathrm{W}\log\left(2\pi e\sigma^2\right) \text{ bits / sec.}
\end{aligned}
$$

Από την άλλη πλευρά, η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος της εξόδου λαμβάνεται όταν είναι κανονικά κατανεμημένο, με ισχύ σ^2_y. Αλλά τότε, αφού και ο λευκός θόρυβος ακολουθεί την κανονική κατανομή, το σήμα εισόδου πρέπει να είναι και αυτό γκαουσιανό. Επομένως, αφού $Y = X + N$ και $\sigma^2_y = \sigma^2_x + \sigma^2_n$, η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εισόδου ως προς τη συνάρτηση πυκνότητας πιθανότητας του σήματος εισόδου δίνεται από την ακόλουθη σχέση:

$$
\begin{aligned}
\max_{f(x)} H(Y) &= \log\sqrt{\sigma_x^2+\sigma_n^2}\left(\sqrt{2\pi e}\right) \text{ bits / δείγμα} \\
&= \frac{1}{2}\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / δείγμα} \\
&= \mathrm{W}\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / sec.}
\end{aligned}
$$

Έχοντας υπολογίσει την ποσότητα πληροφορίας του λευκού θορύβου και τη μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εξόδου για την περίπτωση περιορισμένης μέσης ισχύος, μπορούμε πλέον να υπολογίσουμε τη χωρητικότητα του συνεχούς καναλιού με αθροιστικό λευκό θόρυβο:

$$
\begin{aligned}
C &= \max_{f(x)}\left\{H(Y)\right\} - H(N) \text{ bits / sec} \\
&= W\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} - W\log\left\{2\pi e\sigma_n^2\right\} \\
&= W\log\frac{\sigma_x^2+\sigma_n^2}{\sigma_n^2} = W\log\left\{1+\frac{\sigma_x^2}{\sigma_n^2}\right\} \text{ bits / sec.}
\end{aligned}
$$

Παρατηρούμε ότι, μειώνοντας το εύρος ζώνης W και ταυτόχρονα αυξάνοντας το λόγο της ισχύος του σήματος εισόδου προς την ισχύ του λευκού θορύβου ή αντίστροφα, η χωρητικότητα μπορεί να διατηρηθεί η ίδια.

Παράδειγμα 3.6

Ζητείται ο υπολογισμός της χωρητικότητας ενός καναλιού επικοινωνίας με διαθέσιμο εύρος 3300 Hz και λόγο ισχύος σήματος εισόδου προς την ισχύ του θορύβου ίσο με 1023. Ο θόρυβος είναι γκαουσιανός και λευκός.

Απάντηση

Αφού ο θόρυβος είναι γκαουσιανός και λευκός, η χωρητικότητα μπορεί να υπολογιστεί ως ακολούθως: $C = 3300\log(1 + 1023) = 33000$ bits/*sec*.

Άσκηση αυτοαξιολόγησης 3.7

Το σήμα εισόδου ενός συνεχούς καναλιού είναι γκαουσιανό με μηδενική μέση τιμή και διακύμανση ίση με τη μονάδα, $N(0, 1)$. Κατά τη μετάδοση του σήματος επενεργεί αθροιστικός λευκός θόρυβος, του οποίου η συνάρτηση πυκνότητας πιθανότητας είναι η εξής: $f(n) = n^2$ αν $|n| \leq a$ και $f(n) = 0$ αν $|n| > a$. Ζητούνται η ποσότητα πληροφορίας του θορύβου και το άνω φράγμα της χωρητικότητας του καναλιού.

Ορισμός χωρητικότητας συνεχούς καναλιού με μνήμη

Ορίζουμε τη χωρητικότητα του συνεχούς καναλιού με μνήμη ως τη μέγιστη τιμή της αμοιβαίας ποσότητας πληροφορίας μεταξύ διανύσματος δειγμάτων της εισόδου και διανύσματος δειγμάτων της εξόδου ή του ρυθμού μετάδοσης ως προς τη συνάρτηση πυκνότητας πιθανότητας του διανύσματος των δειγμάτων.

$$C = \lim_{N \to \infty} \max_{f(x_1, \ldots, x_N)} I(X_1, \ldots, X_N / Y_1, \ldots, Y_N).$$

3.2.2 Θεώρημα κωδικοποίησης συνεχών καναλιών

Όπως στην περίπτωση των διακριτών καναλιών, έτσι και στην περίπτωση των συνεχών καναλιών είναι δυνατή η μετάδοση πληροφορίας με οσοδήποτε μικρή πιθανότητα εμφάνισης σφάλματος. Αυτό διατυπώνεται στο ακόλουθο θεώρημα κωδικοποίησης του Shannon για τα συνεχή κανάλια, το οποίο είναι ανάλογο του θεωρήματος του Shannon για τα διακριτά κανάλια (Θεώρημα 3.1).

ΘΕΩΡΗΜΑ 3.2 ΘΕΩΡΗΜΑ ΚΩΔΙΚΟΠΟΙΗΣΗΣ ΣΥΝΕΧΩΝ ΚΑΝΑΛΙΩΝ

Είναι δυνατή η μεταφορά ποσότητας πληροφορίας $H(X)$ (bits/*sec*) μέσω συνεχούς καναλιού χωρητικότητας C, στο οποίο επενεργεί λευκός γκαουσιανός θόρυβος, με οσοδήποτε μικρή πιθανότητα εμφάνισης σφάλματος επιθυμούμε, αν ισχύει $H(X) < C$.

Δε θα συζητήσουμε την απόδειξη του θεωρήματος, επειδή είναι σχετικά σύνθετη και ξεφεύγει από το πλαίσιο του παρόντος συγγράμματος.

Άσκηση αυτοαξιολόγησης 3.8

Ένα τερματικό συνδέεται με έναν ηλεκτρονικό υπολογιστή μέσω τηλεφωνικής γραμμής. Το εύρος ζώνης της τηλεφωνικής γραμμής είναι ίσο με 3000 *Hz* και ο λόγος των διακυμάνσεων της εισόδου προς το θόρυβο είναι ίσος με 15 *db*. Αν από το τερματικό αποστέλλονται ανεξάρτητες ακολουθίες χαρακτήρων, από ένα σύνολο 256 ισοπίθανων χαρακτήρων, να υπολογιστεί η χωρητικότητα του καναλιού και να βρεθεί ο μέγιστος ρυθμός με τον οποίο μπορούν να μεταδοθούν δεδομένα με αμελητέα πιθανότητα εμφάνισης σφαλμάτων.

3.2.3 Συνεχή κανάλια με μνήμη

Στην Υποενότητα 3.2.1 συζητήσαμε ζητήματα σχετικά με τη χωρητικότητα συνεχών καναλιών χωρίς μνήμη. Ιδιαίτερα για την περίπτωση λευκού γκαουσιανού θορύβου με επίπεδη (σταθερή) φασματική πυκνότητα ισχύος η χωρητικότητα προσδιορίστηκε ως συνάρτηση των ισχύων του σήματος εισόδου και του θορύβου. Τώρα θα εξετάσουμε και πάλι συνεχή κανάλια στα οποία επενεργεί λευκός γκαουσιανός θόρυβος χωρίς όμως επίπεδη φασματική πυκνότητα ισχύος. Τα δείγματα, λοιπόν, δεν είναι στατιστικά ανεξάρτητα, δηλαδή έχουμε κανάλι με μνήμη.

Για τον προσδιορισμό της χωρητικότητας συνεχούς καναλιού με μνήμη θα πρέπει να λάβουμε υπόψη τις φασματικές πυκνότητες ισχύος του στοχαστικού σήματος εισόδου και του θορύβου.

Υποθέτουμε ότι το στοχαστικό σήμα εισόδου και ο θόρυβος ακολουθούν γκαουσιανή κατανομή και ότι είναι φραγμένα ως προς την ισχύ και το εύρος ζώνης. Μεταξύ της ισχύος και της φασματικής πυκνότητας ισχύος ισχύει η ακόλουθη σχέση, όπου W είναι το εύρος ζώνης του σήματος εισόδου και του θορύβου:

$$\sigma_x^2 = \frac{1}{2\pi}\int_{-2\pi W}^{2\pi W} \Phi_x(\omega)d\omega,$$

$$\sigma_n^2 = \frac{1}{2\pi}\int_{-2\pi W}^{2\pi W} \Phi_n(\omega)d\omega.$$

Αν χωρίσουμε το φάσμα σε τόσο μικρά τμήματα $\Delta\omega$ ώστε να μπορεί να ληφθεί σ' αυτά ως σταθερό, τότε μπορούμε να θεωρήσουμε τα αντίστοιχα σήματα εξόδου ως ασυσχέτιστα μεταξύ τους. Η μέση ισχύς ανά τμήμα $\Delta\omega$ είναι

$$\sigma_{x_i}^2 = \frac{1}{2\pi}\Phi_{x_i}(\omega_i)\Delta\omega,$$
$$\sigma_{n_i}^2 = \frac{1}{2\pi}\Phi_{n_i}(\omega_i)\Delta\omega.$$

Τώρα υποθέτουμε ότι το πλήθος των τμημάτων $\Delta\omega$ είναι ίσο με M, όπου $M = 4\pi W/\Delta\omega$ και επομένως $W = M\omega_i$ και $\omega_i = \Delta\omega/4\pi$. Για τον υπολογισμό της χωρητικότητας κάθε τμήματος $\Delta\omega$ λαμβάνουμε υπόψη και την υφιστάμενη στατιστική ανεξαρτησία μεταξύ των διαφόρων δειγμάτων:

$$C_i = \omega_i \log\left\{1 + \frac{\sigma_{x_i}^2}{\sigma_{n_i}^2}\right\} = \frac{\Delta\omega}{4\pi}\log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}.$$

Η χωρητικότητα όλου του φάσματος μεταξύ $-2\pi W$ και $2\pi W$ δίνεται από

$$C = \sum_{i=1}^{M} C_i = \frac{\Delta\omega}{4\pi}\sum_{i=1}^{M}\log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}.$$

Αν πάρουμε το όριο για $\Delta\omega \to 0$, τότε έχουμε

$$C = \frac{1}{4\pi}\int_{-2\pi W}^{2\pi W}\log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}d\omega \text{ bits / sec.}$$

Αν ισχύει $\Phi_x(\omega) = \Phi_x(-\omega)$, τότε

$$C = \frac{1}{2\pi}\int_{0}^{2\pi W}\log\left\{1 + \frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}d\omega \text{ bits / sec.}$$

Η χωρητικότητα εξαρτάται, λοιπόν, από το φάσμα του σήματος εισόδου, καθώς και από το φάσμα του θορύβου. Τα ερωτήματα που συνήθως απασχολούν σχεδιαστές επικοινωνιακών συστημάτων αναφέρονται, από τη μια πλευρά, στη μέγιστη τιμή της χωρητικότητας όταν δίνονται τα φάσματα εισόδου και θορύβου και, από την άλλη πλευρά, στο φάσμα του σήματος εισόδου που οδηγεί σε μεγιστοποίηση της χωρητικότητας όταν δίνεται μόνο το φάσμα του θορύβου.

Στη συνέχεια θα δούμε την απάντηση στο πρώτο ερώτημα. Η χωρητικότητα του καναλιού λαμβάνει τη μέγιστη τιμή αν το άθροισμα των φασμάτων του σήματος εισόδου και του θορύβου είναι ίσο με το λόγο του αθροίσματος των ισχύων τους προς το διπλάσιο του εύρους ζώνης και σταθερό.

$$\Phi_x(\omega)+\Phi_n(\omega)=\frac{\sigma_x^2+\sigma_n^2}{2W}=\ \text{σταθερό}.$$

Τότε η μέγιστη χωρητικότητα του καναλιού δίνεται από

$$C=W\log\left\{\frac{\sigma_x^2+\sigma_n^2}{2W}\right\}-\frac{1}{2\pi}\int_0^{2\pi W}\log\Phi_n(\omega)d\omega.$$

Άσκηση αυτοαξιολόγησης 3.9

Δίνεται το φάσμα ενός στοχαστικού σήματος εισόδου $x(t)$, καθώς επίσης και του θορύβου που επενεργεί σε ένα συνεχές κανάλι με μνήμη. Να προσδιοριστεί η χωρητικότητα του καναλιού και η μέγιστη τιμή της.

$$\Phi_\chi(\omega)=\begin{cases}4,\ \text{αν}\ 0<|\omega|<\pi W\\ 8,\ \text{αν}\ \pi W<|\pi|<2\pi W\\ 0,\ \text{διαφορετικά}\end{cases}$$

$$\Phi_n(\omega=\begin{cases}1,\ \text{αν}\ 0<|\omega|<\frac{2}{3}\pi W\\ 2,\ \text{αν}\ \frac{2}{3}\pi W<|\pi|<\frac{4}{3}\pi W\\ 4,\ \text{αν}\ \frac{4}{3}\pi W<|\pi|<2\pi W\\ 0,\ \text{διαφορετικά}\end{cases}$$

Σύνοψη

Τα διακριτά και συνεχή κανάλια επικοινωνίας αποτέλεσαν το αντικείμενο μελέτης αυτού του κεφαλαίου, και κυρίως ο μέγιστος ρυθμός μετάδοσης, δηλαδή η χωρητικότητά τους.

Τα κανάλια επικοινωνίας μελετώνται με τη βοήθεια μαθηματικών υποδειγμάτων, τα οποία περιγράφονται πλήρως με τον πίνακα των πιθανοτήτων μετάβασης. Ένα απλό υπόδειγμα καναλιού επικοινωνίας, το δυαδικό συμμετρικό κανάλι χαρακτηρίζεται από ίσες πιθανότητες ορθής μεταφοράς των δύο ψηφίων, του '0' και του '1'.

Ο ρυθμός μετάδοσης καναλιού επικοινωνίας ορίζεται ως η ποσότητα που προκύπτει από την εντροπία του σήματος εξόδου μειωμένη κατά την αβεβαιότητά του, δηλαδή την υπό συνθήκη ποσότητα πληροφορίας του σήματος εξόδου με δεδομένο το σήμα εισόδου (σε bits/*sec). Η αβεβαιότητα οφείλεται στην επενέργεια του θορύβου, γι' αυτό κανάλια χωρίς θόρυβο έχουν μεγαλύτερη χωρητικότητα από τα ενθόρυβα κανάλια.*

Σύμφωνα με το θεμελιώδες θεώρημα κωδικοποίησης του Shannon, είναι δυνατή η μετάδοση ποσότητας πληροφορίας διακριτής πηγής μέσω καναλιού επικοινωνίας, με αμελητέα πιθανότητα σφάλματος, αν η ποσότητα πληροφορίας του σήματος εισόδου (ή της πηγής σε bits/*sec) είναι μικρότερη της χωρητικότητας του καναλιού.*

Ο υπολογισμός της χωρητικότητας διακριτών καναλιών με μνήμη δυσχεραίνεται από την πολυπλοκότητα των φαινομένων του θορύβου. Για τη μελέτη της επενέργειας του θορύβου, ιδιαίτερα για το χαρακτηρισμό των καταιγισμών σφαλμάτων, έχουν αναπτυχθεί κατάλληλα μαθηματικά υποδείγματα.

Στα συνεχή κανάλια, σε αντίθεση με τα διακριτά, η κωδικοποίηση και η αποκωδικοποίηση εννοούνται διαφορετικά, δηλαδή αναφέρονται στη διαμόρφωση πλάτους και συχνότητας ή τη φραγή εύρους με τη χρήση φίλτρων. Η χωρητικότητα των συνεχών καναλιών ορίζεται κατ' ανάλογο τρόπο με αυτή των διακριτών.

Σύμφωνα με το θεώρημα κωδικοποίησης συνεχών καναλιών, που είναι ανάλογο αυτού των διακριτών καναλιών, είναι δυνατή η μεταφορά ποσότητας πληροφορίας (bits/*sec*), *με οσοδήποτε μικρή πιθανότητα σφάλματος, αν είναι μικρότερη της χωρητικότητας.*

Τέλος, για τον προσδιορισμό της χωρητικότητας συνεχών καναλιών με μνήμη πρέπει να ληφθούν υπόψη οι φασματικές πυκνότητες ισχύος του σήματος εισόδου και του θορύβου. Το βασικό ερώτημα των σχεδιαστών επικοινωνιακών συστημάτων είναι η μεγιστοποίηση της χωρητικότητας με κατάλληλη επιλογή του σήματος εισόδου όταν δίνεται το φάσμα του θορύβου.

Βιβλιογραφία για περαιτέρω μελέτη

[1] [SHA79] K. Sam Shammungen: *Ψηφιακά και Αναλογικά Συστήματα Επικοινωνίας*, Μετάφραση – επιμέλεια: Κ. Καρούμπαλου, Αθήνα, Εκδ. Γ. Πνευματικού, αγγλόφωνη έκδοση John Wiley & Sons, 1979.

Στην Ενότητα 4.4 του βιβλίου μπορείτε να βρείτε μια συνοπτική εισαγωγή στα κανάλια επικοινωνίας, στην Ενότητα 4.5 περιγραφή των διακριτών καναλιών και στην Ενότητα 4.6 περιγραφή των συνεχών καναλιών επικοινωνίας.

[2] [COT91] T. M. Cover, J. A. Thomas: *Elements of Information Theory*, John Willey & Sons, 1991.

Το Κεφάλαιο 8 είναι αφιερωμένο στη χωρητικότητα διακριτών καναλιών επικοινωνίας. Στο Κεφάλαιο αυτό αποδεικνύεται το Θεμελιώδες Θεώρημα της Θεωρίας Πληροφορίας με μεγαλύτερη αυστηρότητα από ό,τι η απόδειξη που γνωρίσαμε. Επίσης, σε αυτό περιέχονται αρκετά παραδείγματα καναλιών επικοινωνίας και η διαισθητική περιγραφή του θεωρήματος κωδικοποίησης, την οποία γνωρίσαμε. Το Κεφάλαιο 10 αναφέρεται στο γκαουσιανό κανάλι επικοινωνίας (συνεχές).

[3] [LUB97] J. C. A. van der Lubbe: *Information Theory*, Cambridge University Press, 1997.

Το διακριτό επικοινωνιακό κανάλι με μνήμη και χωρίς μνήμη περιγράφεται στο Κεφάλαιο 4. Στο Κεφάλαιο αυτό περιέχεται και η απλή απόδειξη του Θεωρήματος Κωδικοποίησης, την οποία υιοθετήσαμε. Το Κεφάλαιο 6 του βιβλίου αυτού είναι αφιερωμένο στα συνεχή κανάλια επικοινωνίας.

[4] [WEL98] R. B. Wells: *Applied Coding and Information Theory for Engineers*, Prentice Hall, 1998.

Στο βιβλίο αυτό μπορείτε να βρείτε εκτός της θεωρίας και λεπτομερή παραδείγματα. Το Κεφάλαιο 2 είναι αφιερωμένο στα κανάλια επικοινωνίας και στο πιο σημαντικό τους χαρακτηριστικό, τη χωρητικότητα. Το Κεφάλαιο 9 αναφέρεται και στο δεύτερο θεώρημα κωδικοποίησης του Shannon.

[5] [SHA48] C. E. Shannon: «Mathematical Theory of Communication», *Bell System Technical Journal*, vol. 27, 1948, pp. 379 – 423, 623 – 656. Στην εργασία αυτή περιέχεται το δεύτερο θεώρημα κωδικοποίησης, του οποίου η απόδειξη βασίζεται στην έννοια των πιο πιθανών μηνυμάτων.

Άλλη βιβλιογραφία

[1] [ABR63] N. Abramson: *Information Theory and Coding*, New York, MacGraw Hill, 1963.

[2] [BLA87] R. E. Blahut: *Principles and Practice of Information Theory*, Mass., Addison – Wesley, Reading, 1987.

[3] [GAL68] R. G. Gallager: *Information Theory and Reliable Communication*, New York, Wiley, 1968

[4] [JON00] G. A. Jones, J. M. Jones: *Information and Coding Theory*, Springer Verlag, 2000.

[5] [ROM96] S. Roman: *Introduction to Coding and Information Theory*, Springer Verlag, 1996.

ΚΕΦΑΛΑΙΟ 4

Κωδικοποίηση Ελέγχου Σφάλματος

Σκοπός

Το κεφάλαιο αυτό έχει ως στόχο την περιγραφή του τρόπου κατασκευής καθώς και της συμπεριφοράς κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *εξηγήσετε το αντικείμενο της Θεωρίας Κωδικοποίησης.*
- *περιγράψετε διαδικασίες κωδικοποίησης και αποκωδικοποίησης γραμμικών κωδίκων.*
- *περιγράψετε διαδικασίες κωδικοποίησης και αποκωδικοποίησης κυκλικών κωδίκων καθώς και τη διαδικασία αποκωδικοποίησης των BCH κωδίκων.*
- *αναφέρετε τους κώδικες Reed – Solomon, διόρθωσης καταιγιστικών σφαλμάτων και συνελικτικούς.*

Έννοιες κλειδιά

- *Θεωρία Κωδικοποίησης,*
- *Κώδικες ελέγχου σφάλματος,*
- *Γραμμικοί κώδικες,*
- *Κυκλικοί κώδικες,*
- *BCH κώδικες,*
- *Reed – Solomon κώδικες,*
- *Κώδικες διόρθωσης καταιγιστικών σφαλμάτων,*
- *Συνελικτικοί κώδικες.*

Εισαγωγικές παρατηρήσεις

Η κωδικοποίηση πηγής που μας απασχόλησε στο Κεφάλαιο 2 επιδιώκει την απομάκρυνση του πλεονασμού από την έξοδο της πηγής, δηλαδή την όσο το δυνατόν πιο συμπυκνωμένη αναπαράσταση των μηνυμάτων. Αντίθετα, κατά την κωδικοποίηση καναλιού, με την οποία θα ασχοληθούμε στο κεφάλαιο αυτό, προστίθεται όσος πλεονασμός είναι απαραίτητος ώστε να μειωθεί η ολική πιθανότητα σφάλματος μετάδοσης στην επιθυμητή τιμή. Με άλλα λόγια, η κωδικοποίηση καναλιού είναι μια καλά

υπολογισμένη χρήση πλεονασμού με επιδίωξη την ανίχνευση και τη διόρθωση σφαλμάτων κατά τη μετάδοση της πληροφορίας στο κανάλι επικοινωνίας.

Το κεφάλαιο αυτό αποτελείται από τέσσερις ενότητες. Στην πρώτη ενότητα, θα εξετάσουμε βασικές αρχές, έννοιες και παραδοχές σχετικά με τους διάφορους τύπους κωδίκων ελέγχου σφάλματος, στη δεύτερη ενότητα θα μελετήσουμε τους γραμμικούς κώδικες, στην τρίτη ενότητα τους κυκλικούς κώδικες, συμπεριλαμβανομένων των κωδίκων BCH και στην τέταρτη ενότητα θα αναφερθούμε πολύ συνοπτικά στους Reed – Solomon κώδικες, στους κώδικες διόρθωσης καταιγισμών σφαλμάτων και στους συνελικτικούς κώδικες.

4.1 Εισαγωγή στη Θεωρία Κωδικοποίησης

Σκοπός

Η ενότητα αυτή έχει ως στόχο την εισαγωγή βασικών αρχών και όρων της Θεωρίας Κωδικοποίησης.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *να ορίσετε τους ισομήκεις κώδικες (ή κώδικες μπλοκ) και να αναφέρετε δύο παραδοχές που γίνονται στη Θεωρία Κωδικοποίησης.*
- *εξηγήσετε τις έννοιες της αξιοπιστίας καναλιού, του ρυθμού πληροφορίας, του βάρους μιας λέξης και της απόστασης μεταξύ δύο λέξεων.*
- *εξηγήσετε τη διαδικασία αποκωδικοποίησης μέγιστης πιθανότητας στις δύο της εκδοχές, της πλήρους και της ατελούς αποκωδικοποίησης.*
- *εξηγήσετε τις έννοιες του προτύπου σφάλματος και να διατυπώσετε ένα θεώρημα σχετικό με κώδικες ανίχνευσης σφάλματος και ένα θεώρημα σχετικό με κώδικες διόρθωσης σφάλματος.*

Έννοιες κλειδιά

- *Ισομήκεις κώδικες ή Κώδικες μπλοκ,*
- *αξιοπιστία καναλιού,*
- *ρυθμός πληροφορίας,*
- *βάρος λέξης,*
- *απόσταση μεταξύ δύο λέξεων,*
- *αποκωδικοποίηση μέγιστης πιθανότητας,*
- *πρότυπο σφάλματος,*
- *απόσταση κώδικα.*

Η **Θεωρία Κωδικοποίησης** είναι η μελέτη μεθόδων για την αποτελεσματική και ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό. Η ανάπτυξη της θεωρίας οφείλεται στις σχετικές απαιτήσεις εφαρμογών, όπως της μεταφοράς οικο-

νομικών πληροφοριών μέσω τηλεφωνικών γραμμών, μεταφοράς δεδομένων από έναν ηλεκτρονικό υπολογιστή σε άλλο ή από τη μνήμη στην κεντρική μονάδα επεξεργασίας και μεταφοράς δεδομένων από δορυφόρους ή διαστημικά σκάφη στη Γη.

Όπως είδαμε στο Κεφάλαιο 1, το φυσικό μέσο, δια του οποίου μεταδίδεται η πληροφορία, ονομάζεται κανάλι επικοινωνίας. Παραδείγματα καναλιών είναι οι τηλεφωνικές γραμμές και η ατμόσφαιρα. Δυστυχώς, στα κανάλια επικοινωνίας επενεργεί θόρυβος, ο οποίος προκαλεί αλλοίωση της μεταδιδόμενης πληροφορίας. Η Θεωρία Κωδικοποίησης ασχολείται με το πρόβλημα της ανίχνευσης και της διόρθωσης σφαλμάτων μετάδοσης, τα οποία προκαλούνται από το θόρυβο στα επικοινωνιακά κανάλια. Στο Σχήμα 1.3 / Κεφάλαιο 1 απεικονίζεται ένα λεπτομερές επικοινωνιακό μοντέλο. Τα μέρη του διαγράμματος αυτού, τα οποία θα μας απασχολήσουν στο παρόν κεφάλαιο, είναι η κωδικοποίηση και η αποκωδικοποίηση του καναλιού.

Η ενότητα αυτή χωρίζεται σε τέσσερις υποενότητες. Η πρώτη υποενότητα αναφέρεται σε βασικές παραδοχές και βασικούς ορισμούς της Θεωρίας Κωδικοποίησης, η δεύτερη στην αποκωδικοποίηση μέγιστης πιθανότητας, η τρίτη σε κώδικες ανίχνευσης σφαλμάτων και η τέταρτη σε κώδικες διόρθωσης σφαλμάτων.

4.1.1 Παραδοχές και ορισμοί

Όπως είδαμε και στο Κεφάλαιο 2, ένας δυαδικός κώδικας, C, είναι ένα σύνολο κωδικών λέξεων. Οι κωδικές λέξεις είναι ακολουθίες δυαδικών ψηφίων. Για παράδειγμα, ο κώδικας που απαρτίζεται από όλες τις λέξεις μήκους δύο ψηφίων είναι $C = \{00, 10, 01, 11\}$. Ένας κώδικας ονομάζεται **ισομήκης κώδικας (ή κώδικας μπλοκ)** αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος. Στο κεφάλαιο αυτό θα μας απασχολήσουν μόνο κώδικες μπλοκ. Το πλήθος των κωδικών λέξεων ενός κώδικα C συμβολίζεται με $|C|$.

Σχετικά με το κανάλι κάνουμε **δύο παραδοχές**, καθοριστικές για την ανάπτυξη της θεωρίας κωδικοποίησης. Σύμφωνα με την πρώτη παραδοχή, μια κωδική λέξη μήκους n δυαδικών ψηφίων, που εισέρχεται στο κανάλι, λαμβάνεται στην έξοδό του ως λέξη μήκους και πάλι n δυαδικών ψηφίων, αν και η ακολουθία εισόδου του καναλιού μπορεί να διαφέρει από αυτή της εξόδου του καναλιού. Επίσης, χωρίς δυσκολία διαπιστώνεται, από το δέκτη, η αρχή της πρώτης λέξης μιας ακολουθίας κωδικών λέξεων που μεταδίδεται μέσω του καναλιού. Για παράδειγμα, αν στο κανάλι μεταδίδεται η δυαδική ακολουθία 010011, τότε στην έξοδό του λαμβάνεται η ακολουθία 010011 ή κάποια άλλη του ιδίου μήκους, όχι όμως η ακολουθία 10011 ή κάποια άλλη μικρότερου μήκους, επειδή χάθηκε το 1ο ψηφίο (το «0») της 1ης λέξης της ακολουθίας. Επομένως, η πρώτη παραδοχή αναφέρεται στη δυνατότητα του δέκτη να λάβει

όλες τις λέξεις που μεταδόθηκαν, με ή χωρίς σφάλματα.

Η δεύτερη παραδοχή αναφέρεται στο ότι τα σφάλματα, δηλαδή ο θόρυβος, εμφανίζονται διασκορπισμένα κατά τυχαίο τρόπο και όχι σε συστάδες (ή καταιγισμούς, bursts). Με άλλα λόγια, η πιθανότητα να αλλοιωθεί ένα bit κατά τη μετάδοση εξ αιτίας του θορύβου είναι η ίδια με αυτή οποιουδήποτε άλλου bit και δεν επηρεάζεται από σφάλματα σε γειτονικά δυαδικά ψηφία. Αυτή η παραδοχή δεν είναι ιδιαίτερα ρεαλιστική, αν λάβουμε υπόψη φυσικά φαινόμενα όπως αστραπές ή ακόμα και «γρατσουνιές» δίσκων, που οδηγούν σε καταιγισμούς σφαλμάτων. Η δεύτερη παραδοχή ισχύει σε όλες τις ενότητες του κεφαλαίου, πλην της Ενότητας 4.4.2 που αναφέρεται σε κώδικες διόρθωσης καταιγιστικών σφαλμάτων.

Στην Ενότητα 3.1 αναφερθήκαμε στο δυαδικό συμμετρικό κανάλι (Binary Symmetric Channel, BSC), στο οποίο η πιθανότητα το «0» να μεταφέρεται από το κανάλι ως «0» είναι ίση με την πιθανότητα το «1» να μεταφέρεται ως «1». Η **αξιοπιστία** του καναλιού είναι ο πραγματικός αριθμός p, $0 \leq p \leq 1$, όπου p είναι η πιθανότητα της ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού. Ένα κανάλι χαρακτηρίζεται πιο αξιόπιστο από ένα άλλο αν η πιθανότητα p, δηλαδή η αξιοπιστία του, είναι πιο υψηλή. Ωστόσο, αν $p = 1$ (ή $p = 0$) τότε δεν υπάρχει περίπτωση σφάλματος (ή πάντοτε υπεισέρχεται σφάλμα) και επομένως το κανάλι αυτό δε θα μας απασχολήσει. Επειδή κάθε κανάλι αξιοπιστίας p, $0 < p \leq 1/2$, μπορεί να μετατραπεί σε ένα κανάλι με $1/2 \leq p < 1$, στο κεφάλαιο αυτό θα ασχοληθούμε με δυαδικά συμμετρικά κανάλια με $1/2 < p < 1$. (Η περίπτωση $p = 1/2$ δεν επιτρέπει την εξαγωγή οποιουδήποτε αξιοποιήσιμου αποτελέσματος.)

Ο **ρυθμός πληροφορίας** ενός κώδικα είναι το ποσοστό της κωδικής λέξης που μεταφέρει το μήνυμα. Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα C μήκους n είναι ίσος με $(1/n)\log_2|C|$. Αφού $1 \leq |C| \leq 2^n$, ο ρυθμός πληροφορίας παίρνει τιμές μεταξύ 0 και 1, την τιμή 1 αν $|C| = 2^n$ δηλαδή κάθε λέξη n δυαδικών ψηφίων είναι κωδική λέξη και την τιμή 0 αν $|C| = 1$.

Παράδειγμα 4.1

Ζητούνται οι ρυθμοί πληροφορίας των κωδίκων $C_1 = \{00, 10, 01, 11\}$, $C_2 = \{000, 010, 101, 111\}$ και $C_3 = \{000000, 000010, 110001, 111111\}$.

Απάντηση

Αφού τα μήκη των κωδικών λέξεων των κωδίκων C_1, C_2 και C_3 είναι 2, 3 και 6, αντίστοιχα και το πλήθος των κωδικών λέξεων όλων των κωδίκων είναι ίσο με 4, οι αντί-

στοιχοι ρυθμοί πληροφορίας είναι:

$$(1/n_1)\log_2|C_1| = (1/2)\log_2 4 = 1,$$

$$(1/n_2)\log_2|C_2| = (1/3)\log_2 4 = (2/3) \text{ και}$$

$$(1/n_3)\log_2|C_3| = (1/6)\log_2 4 = (1/3).$$

Άσκηση αυτοαξιολόγησης 4.1

Εξηγήστε γιατί δεν μας ενδιαφέρει στην κωδικοποίηση ένα κανάλι αξιοπιστίας $p = 0$ και πώς μπορούμε να μετατρέψουμε ένα κανάλι με $0 < p \leq 1/2$ σε ένα κανάλι με $1/2 \leq p < 1$.

Ας προσπαθήσουμε τώρα να αποκτήσουμε μια πρώτη, διαισθητική, εικόνα της ανίχνευσης και της διόρθωσης σφαλμάτων. Ας υποθέσουμε πρώτα ότι χρησιμοποιούμε για τη μετάδοση τον κώδικα $C_1 = \{00, 10, 01, 11\}$. Αν τώρα κατά τη μετάδοση της ακολουθίας 0010, ο παραλήπτης λαμβάνει στην έξοδο του καναλιού την ακολουθία 0111, δεν μπορεί να ξέρει αν έχει υπεισέλθει κάποιο σφάλμα, αφού «01» και «11» είναι κωδικές λέξεις που θα μπορούσαν να είχαν σταλεί από τον αποστολέα. Δεν μπορεί, επομένως, να επιτευχθεί η ανίχνευση, πόσο μάλλον η διόρθωση σφαλμάτων. Αν σε κάθε κωδική λέξη του κώδικα C_1 προσθέσουμε ακόμα ένα ψηφίο ελέγχου ισοτιμίας, δηλαδή το ψηφίο εκείνο για το οποίο προκύπτει άρτιο πλήθος του «1» στην κωδική λέξη, λαμβάνουμε τον κώδικα $C_2 = \{000, 101, 011, 110\}$.

Η χρήση του κώδικα C_2 επιτρέπει, σε ορισμένες περιπτώσεις, την ανίχνευση σφαλμάτων. Για παράδειγμα, αν αποστέλλεται η κωδική λέξη «000» και ο παραλήπτης λαμβάνει τη λέξη «001», η οποία δεν είναι κωδική λέξη, τότε ανιχνεύει το σφάλμα. Η διόρθωση όμως του σφάλματος δεν είναι εύκολη, αφού η λέξη «001» μπορεί να προκύψει με αλλαγή ενός ψηφίου από τις κωδικές λέξεις «000», «011» και «101». Αλλά και η ανίχνευση σφαλμάτων δεν είναι πάντοτε δυνατή με τη χρήση του κώδικα C_2, για παράδειγμα, αν αποστέλλεται και πάλι η κωδική λέξη «000» και λαμβάνεται στην έξοδο η κωδική λέξη «011» ή οποιαδήποτε άλλη κωδική λέξη. Η ανίχνευση του σφάλματος (ή των σφαλμάτων) είναι μόνο δυνατή αν στην έξοδο του καναλιού λαμβάνεται κάποια λέξη, η οποία όμως δεν είναι και κωδική λέξη.

Αν τώρα κάνουμε χρήση του κώδικα $C_3 = \{000000, 101010, 010101, 111111\}$, ο οποίος προκύπτει από τον κώδικα C_1 , με τριπλή επανάληψη κάθε κωδικής λέξης, είναι δυνατή και η ανίχνευση και η διόρθωση σφαλμάτων. Για παράδειγμα, αν αποστέλλεται η κωδική λέξη «000000» και λαμβάνεται στην έξοδο η λέξη «000010»,

αφού η τελευταία δεν είναι κωδική λέξη, ανιχνεύουμε την ύπαρξη τουλάχιστον ενός σφάλματος. Αλλάζοντας μόνο ένα δυαδικό ψηφίο της λέξης «000010» μπορούμε να λάβουμε την κωδική λέξη «000000», αλλά θα πρέπει να αλλάξουμε περισσότερα ψηφία για να λάβουμε οποιαδήποτε από τις άλλες κωδικές λέξεις. Για το λόγο αυτό θεωρούμε ότι η πιο πιθανή κωδική λέξη που μεταδόθηκε είναι η «000000» και διορθώνουμε επομένως τη λέξη «000010» στην κωδική λέξη «000000». Διαπιστώνουμε λοιπόν ότι εφόσον κατά τη μετάδοση οποιασδήποτε από τις κωδικές λέξεις του κώδικα C_3 υπεισέλθει ένα μόνο σφάλμα, ο παραλήπτης μπορεί να ανιχνεύσει και να διορθώσει το σφάλμα. Αν υπεισέλθουν περισσότερα σφάλματα, τότε η διόρθωση και σε ορισμένες περιπτώσεις και η ανίχνευση δεν είναι δυνατή και με τον κώδικα C_3.

Άσκηση αυτοαξιολόγησης 4.2

Υποθέτουμε ότι χρησιμοποιούμε τον κώδικα C = {000000000, 011011011, 101101101, 110110110}, ο οποίος προκύπτει με τριπλή επανάληψη κάθε κωδικής λέξης του C_2 = {000, 011, 101, 110}. Ζητούνται οι περιπτώσεις κατά τις οποίες δεν ανιχνεύονται σφάλματα κατά τη μετάδοση καθώς και περιπτώσεις κατά τις οποίες σφάλματα ανιχνεύονται, αλλά δεν μπορεί να επιτευχθεί διόρθωσή τους χωρίς επανάληψη της μετάδοσης. Επίσης, ζητούνται οι κωδικές λέξεις, οι οποίες είναι οι εγγύτερες (πλησιέστερες) στις λέξεις «100000001», «111011111», «111101001» και «010110111».

Ορισμός 4.1 Βάρος (Weight)

Βάρος Hamming ή απλά **βάρος**, $wt(x)$, μιας λέξης x μήκους n ψηφίων ονομάζεται το πλήθος των ψηφίων της λέξης, τα οποία είναι ίσα με το «1». Το βάρος παίρνει τιμές από 0 έως n.

Ορισμός 4.2 Απόσταση (Distance)

Απόσταση Hamming ή απλά **απόσταση**, $d(x, y)$, μεταξύ δύο λέξεων x και y του ιδίου μήκους n ονομάζεται το πλήθος των θέσεων, στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου. Η απόσταση παίρνει τιμές από 0 έως n.

Παράδειγμα 4.2

Δίνονται οι λέξεις x_1 = 000000, x_2 = 000010, x_3 = 110001 και x_4 = 111111. Ζητούνται τα βάρη όλων των λέξεων καθώς και οι αποστάσεις $d(x_1, x_2)$, $d(x_1, x_3)$, $d(x_2, x_3)$ και $d(x_3, x_4)$.

Απάντηση

Η λέξη $x_1 = 000000$ δεν περιέχει κανένα '1' και επομένως $wt(000000) = 0$ και η λέξη $x_2 = 000010$ περιέχει ένα '1' και άρα $wt(000010) = 1$. Επίσης, $wt(110001) = 3$ και $wt(111111) = 6$. Αναφορικά με την απόσταση $d(x_1, x_2)$, παρατηρούμε ότι οι λέξεις $x_1 = 000000$ και $x_2 = 000010$ διαφέρουν μόνο σε μία θέση (την πέμπτη) και επομένως $d(000000, 000010) = 1$. Επίσης, $d(000000, 110001) = 3$, $d(000010, 110001) = 4$ και $d(110001, 111111) = 3$.

Ορισμός 4.3 Πρόσθεση και Πολλαπλασιασμός

Μεταξύ των δυαδικών λέξεων ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού ως ακολούθως:

$0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1$ και $1 + 1 = 0$

$0 . 0 = 0, 0 . 1 = 0, 1 . 0 = 0$ και $1 . 1 = 1$.

Παράδειγμα 4.3

Δίνονται και πάλι οι λέξεις $x_1 = 000000$, $x_2 = 000010$, $x_3 = 110001$ και $x_4 = 111111$. Ζητούνται οι $x_1 + x_2$, $x_2 + x_3$, $x_3 + x_4$, $x_1 \cdot x_4$, $x_2 \cdot x_3$ και $x_3 \cdot x_4$.

Απάντηση

Είναι $x_1 + x_2 = 000000 + 000010 = 000010$, $x_2 + x_3 = 000010 + 110001 = 110011$, $x_3 + x_4 = 110001 + 111111 = 001110$, $x_1 \cdot x_4 = 000000 \cdot 111111 = 000000$, $x_2 \cdot x_3 = 000010 \cdot 110001 = 000000$ και $x_3 \cdot x_4 = 110001 \cdot 111111 = 110001$.

Άσκηση αυτοαξιολόγησης 4.3

Υπολογίστε τα βάρη των λέξεων $x_1 = 111000$, $x_2 = 001110$, $x_3 = x_1 + x_2$ και $x_4 = x_1 \cdot x_2$, καθώς και τις αποστάσεις μεταξύ των λέξεων κάθε ζεύγους αυτών.

Υποθέτουμε ότι σε ένα δυαδικό συμμετρικό κανάλι (BSC) αξιοπιστίας p μεταδόθηκε η λέξη x και ο παραλήπτης έλαβε τη λέξη y, μήκους n ψηφίων. Συμβολίζουμε με $\pi(x, y)$ την πιθανότητα να μεταδόθηκε η λέξη x και να ελήφθη από τον παραλήπτη η λέξη y. Αφού έχουμε κάνει την παραδοχή ότι ο θόρυβος κατανέμεται τυχαία, μπορούμε να αντιμετωπίσουμε τη μετάδοση κάθε δυαδικού ψηφίου ως ανεξάρτητο γεγονός. Έτσι, αν οι λέξεις x και y εμφανίζουν διαφορές σε d δυαδικά ψηφία, τότε $n - d$ ψηφία μεταδόθηκαν σωστά και d ψηφία μεταδόθηκαν εσφαλμένα. Επομένως, $\pi(x,y)=p^{n-d}(1-p)^d$.

Παράδειγμα 4.4

Δίνεται ο κώδικας $C = \{0000, 1011, 0110, 1110\}$, αξιοπιστίας $p = 0{,}8$. Ζητούνται οι $\pi(0000, 0000)$, $\pi(1110, 1110)$ και $\pi(1110, 1111)$.

Απάντηση

Για κάθε $x \varepsilon C$, η πιθανότητα ορθής μετάδοσης μιας κωδικής λέξης είναι $\pi(x,x) = p^4$, αφού $n = 4$. Έτσι, $\pi(0000, 0000) = \pi(1110, 1110) = 0{,}4096$. Οι λέξεις 1110 και 1111διαφέρουν μόνο σε μία θέση και επομένως $\pi(1110, 1111) = p^3(1 - p) = 0{,}1024$.

ΘΕΩΡΗΜΑ 4.1

Θεωρούμε ένα BSC κανάλι με $½ < p < 1$, δύο κωδικές λέξεις x_1 και x_2 και μία λέξη y, όλες μήκους n ψηφίων, καθώς και ότι οι x_1 και y διαφέρουν σε d_1 ψηφία και οι x_2 και y *σε* d_2 ψηφία. Τότε $\pi(x_1, y) \leq \pi(x_2, y)$ αν και μόνο αν $d_1 \geq d_2$.

Απόδειξη

Για να ισχύει η ανισότητα $\pi(x_1, y) \leq \pi(x_2, y)$ αρκεί να ισχύει $p^{n-d1}(1 - p)^{d1} \leq p^{n-d2}(1 - p)^{d2}$ ή $(p/(1 - p))^{d2-d1} \leq 1$ ή $d_2 \leq d_1$, η οποία ισχύει αφού $(p/(1 - p))>1$.

4.1.2 Το πρόβλημα της κωδικοποίησης και της αποκωδικοποίησης

Τα δεδομένα των σχεδιαστών επικοινωνιακών καναλιών είναι η αξιοπιστία του καναλιού, δηλαδή η πιθανότητα ένα δυαδικό ψηφίο να μεταδίδεται χωρίς σφάλμα και το πλήθος των δυνατών διαφορετικών μηνυμάτων που μπορεί να μεταδοθούν.

Τα δύο βασικά προβλήματα που απασχολούν τους σχεδιαστές στη Θεωρία Κωδικοποίησης είναι η κωδικοποίηση και η αποκωδικοποίηση. Η κωδικοποίηση συνίσταται στον προσδιορισμό ενός κώδικα, ο οποίος θα χρησιμοποιηθεί για την αποστολή των μηνυμάτων. Πρώτα επιλέγεται ένας θετικός ακέραιος k, το μήκος κάθε δυαδικής λέξης που αντιστοιχεί σε ένα μήνυμα. Το μήκος των λέξεων επιλέγεται κατά τέτοιον τρόπο ώστε το πλήθος των δυνατών λέξεων να είναι μεγαλύτερο ή ίσο του πλήθους των δυνατών μηνυμάτων, δηλαδή $2^k \geq |M|$, όπου $|M|$ είναι το πλήθος των δυνατών μηνυμάτων. Στη συνέχεια, επιλέγεται το πλήθος των δυαδικών ψηφίων που θα προστεθούν σε κάθε λέξη (πλεονασμός) έτσι ώστε να μπορεί να ανιχνεύεται ή και να διορθώνεται το επιθυμητό πλήθος σφαλμάτων. Έτσι προκύπτουν οι κωδικές λέξεις που αντιστοιχούν στα δυνατά μηνύματα, μήκους n ψηφίων, εκ των οποίων τα $n - k$ bits είναι ο πλεονασμός. Επομένως, για τη μετάδοση ενός συγκεκριμένου μηνύματος, ο μεταδότης βρίσκει την κωδική λέξη που αντιστοιχεί σε αυτό το μήνυμα.

Αναφορικά με το δεύτερο πρόβλημα, την αποκωδικοποίηση, αν ο αποδέκτης (παρα-

λήπτης) λάβει μία λέξη y, μήκους n ψηφίων, η οποία είναι κωδική λέξη, τότε εξάγει το αντίστοιχο μήνυμα. Αν όμως η λέξη y δεν είναι κωδική λέξη (ανίχνευση σφαλμάτων), ο παραλήπτης μπορεί να χρησιμοποιήσει μια διαδικασία, η οποία ονομάζεται **αποκωδικοποίηση μέγιστης πιθανότητας**, για την επιλογή της κωδικής λέξης που μεταδόθηκε (διόρθωση σφαλμάτων). Η διαδικασία αυτή διακρίνεται σε δύο εκδοχές:

1. Πλήρης αποκωδικοποίηση μέγιστης πιθανότητας (ΠΑΜΠ)

Αν υπάρχει μόνο μία κωδική λέξη x, η οποία εμφανίζει τη μικρότερη απόσταση από τη λέξη y, σε σύγκριση με τις αποστάσεις όλων των άλλων κωδικών λέξεων από τη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί την y ως x. Αν όμως υπάρχουν περισσότερες κωδικές λέξεις που εμφανίζουν την ίδια απόσταση από τη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί αυθαίρετα τη ληφθείσα λέξη ως μία από αυτές τις κωδικές λέξεις.

2. Ατελής αποκωδικοποίηση μέγιστης πιθανότητας (ΑΑΜΠ)

Όπως προηγουμένως, αν υπάρχει μία μοναδική κωδική λέξη x πλησιέστερη στη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί την y ως x. Αν όμως υπάρχουν περισσότερες κωδικές λέξεις με την ίδια απόσταση στη λέξη y, τότε ο αποδέκτης ζητά από τον αποστολέα επανάληψη της μετάδοσης. Επανάληψη της μετάδοσης μπορεί να ζητηθεί και στις περιπτώσεις που, ενώ υπάρχει μια μόνο κωδική λέξη εγγύτερη στη ληφθείσα λέξη, η απόστασή τους είναι πολύ μεγάλη.

Παράδειγμα 4.5

Θεωρούμε ένα πλήθος μηνυμάτων $|M| = 2$, $k = 1$, $n = 3$ και $C = \{000, 111\}$. Ο μεταδότης μεταδίδει την κωδική λέξη «111» ή «000» και ζητούνται οι περιπτώσεις που ο αποδέκτης συμπεραίνει τη σωστή κωδική λέξη στη βάση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας.

Απάντηση

Ο αποδέκτης συμπεραίνει την κωδική λέξη «111», εφόσον λάβει αυτή την κωδική λέξη ή λάβει μία από τις λέξεις «011», «101 ή «110», οι οποίες εμφανίζουν μικρότερη απόσταση προς την «111» από ό,τι προς την «000». Αν λάβει οποιαδήποτε από τις υπόλοιπες τέσσερις δυαδικές ακολουθίες, ο αποδέκτης συμπεραίνει την κωδική λέξη «000». Η περίπτωση της ίσης απόστασης της ληφθείσας λέξης και από τις δύο κωδικές λέξεις δεν είναι δυνατή με τον κώδικα αυτό και επομένως και η απαίτηση για επανάληψη της μετάδοσης.

Άσκηση αυτοαξιολόγησης 4.4

Θεωρούμε ένα πλήθος μηνυμάτων $|M| = 3$, $k = 2$, $n = 4$ και $C = \{0000, 1010, 1111\}$. Ζητούνται οι περιπτώσεις κατά τη μετάδοση που ο αποδέκτης συμπεραίνει τη σωστή κωδική λέξη, στη βάση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας.

Άσκηση αυτοαξιολόγησης 4.5

Θεωρούμε έναν κώδικα με τα δεδομένα του Παραδείγματος 5, καθώς και την αξιοπιστία του καναλιού $p = 0{,}9$. Να υπολογιστεί η πιθανότητα, ο αποδέκτης να συμπεράνει ορθά μετά από μετάδοση της κωδικής λέξης «000», στη βάση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας.

4.1.3 Κώδικες ανίχνευσης σφαλμάτων

Στην υποενότητα αυτή θα ασχοληθούμε με το ερώτημα του πότε ένας κώδικας ανιχνεύει σφάλματα κατά τη μετάδοση. Αλλά πριν προχωρήσουμε, ας ορίσουμε το **πρότυπο σφάλματος**, ε. Έτσι, ονομάζουμε το άθροισμα της κωδικής λέξης x που μεταδόθηκε με τη λέξη y που ελήφθη στον αποδέκτη, δηλαδή $\varepsilon = x + y$. Επίσης, ας ορίσουμε και την **απόσταση κώδικα** C (δείτε και Ορισμό 4.2). Η απόσταση ενός κώδικα C είναι η μικρότερη από τις αποστάσεις όλων των δυνατών ζευγών κωδικών λέξεων του κώδικα. Επειδή $d(x, y) = wt(x + y)$, η απόσταση του κώδικα C είναι ίση με την ελάχιστη τιμή του βάρους $wt(x + y)$, όπου $x, y \in C$ και $x \neq y$.

Όπως ήδη είπαμε, ο αποδέκτης μπορεί να ανιχνεύσει σφάλματα κατά τη μετάδοση, αν λάβει λέξεις που δεν ανήκουν στον κώδικα που χρησιμοποιείται, δεν είναι δηλαδή και κωδικές λέξεις. Έτσι, λέμε ότι ο κώδικας ανιχνεύει το πρότυπο σφάλματος ε,*αν* και μόνο αν $x + \varepsilon = y$ δεν είναι κωδική λέξη, (για κάθε) $\forall\, x \in C$.

Παράδειγμα 4.6

Θεωρούμε τον κώδικα $C = \{0000, 1010, 1111\}$. Η κωδική λέξη 1010 μεταδόθηκε τρεις φορές και ο δέκτης έλαβε με τη σειρά τις λέξεις 0100, 1001 και 1010. Ζητούνται τα αντίστοιχα πρότυπα σφάλματος καθώς και η απόσταση του κώδικα C.

Απάντηση

Τα αντίστοιχα πρότυπα σφάλματος είναι $1010 + 0100 = 1110$, $1010 + 1001 = 0011$ και $1010 + 1010 = 0000$. Η απόσταση του κώδικα είναι ίση με $d(0000, 1010) = d(1010, 1111) = 2$.

ΘΕΩΡΗΜΑ 4.2

Ένας κώδικας C απόστασης d ανιχνεύει όλα τα μη μηδενικά πρότυπα σφάλματος βάρους μικρότερου ή ίσου του $d - 1$. Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους d που δεν ανιχνεύει ο κώδικας C.

Απόδειξη

Θεωρούμε ένα μη μηδενικό πρότυπο σφάλματος ε βάρους $wt(\varepsilon) \leq d - 1$ και την κωδική λέξη x. Τότε

$$d(x, x + \varepsilon) = wt(x + x + \varepsilon) = wt(\varepsilon) \leq d - 1 < d.$$

Αφού πρόκειται για κώδικα απόστασης d, η λέξη $x + \varepsilon = y$ που ελήφθη από τον αποδέκτη δεν ανήκει στον κώδικα C και επομένως ο κώδικας ανιχνεύει το πρότυπο σφάλματος ε. Αν τώρα εξετάσουμε το πρότυπο σφάλματος $\varepsilon = x + y$ βάρους d με $y = x + \varepsilon \in C$, τότε ο κώδικας C δεν ανιχνεύει το πρότυπο σφάλματος ε βάρους d. (Εφιστάται η προσοχή στο ότι ο κώδικας C μπορεί να ανιχνεύει κάποια πρότυπα σφάλματος απόστασης d. Αυτό συμβαίνει στις περιπτώσεις που $y = x + \varepsilon \notin C$, όπου x η κωδική λέξη που μεταδόθηκε και y η λέξη που ελήφθη.)

Παράδειγμα 4.7

Δίνεται ο κώδικας $C = \{000, 111\}$ του Παραδείγματος 5. Ποια πρότυπα σφάλματος ανιχνεύονται από τον κώδικα;

Απάντηση

Σύμφωνα με το θεώρημα 4.2, αφού η απόσταση του κώδικα είναι ίση με 3, ο κώδικας ανιχνεύει κάθε πρότυπο σφάλματος βάρους 1 ή 2. Ο κώδικας δεν ανιχνεύει το πρότυπο σφάλματος «111» βάρους 3.

Άσκηση αυτοαξιολόγησης 4.6

Δίνεται ο κώδικας της Άσκησης Αυτοαξιολόγησης 4. Υπάρχουν πρότυπα σφάλματος, τα οποία ανιχνεύονται από τον κώδικα;

4.1.4 Κώδικες διόρθωσης σφαλμάτων

Όπως ήδη έχουμε πει, αν μεταδίδεται η κωδική λέξη x ενός κώδικα C και λαμβάνεται η λέξη y (με πρότυπο σφάλματος $\varepsilon = x + y$), τότε συμπεραίνεται από τον αποδέκτη, στη βάση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας, ότι μεταδό-

θηκε η x εφόσον η ληφθείσα λέξη y είναι πλησιέστερα στη x από ό,τι σε οποιαδήποτε άλλη κωδική λέξη του κώδικα C. Αν αυτό συμβαίνει κάθε φορά που εμφανίζεται το πρότυπο σφάλματος ε ανεξαρτήτως της κωδικής λέξης που μεταδόθηκε, τότε λέμε ότι ο κώδικας C διορθώνει το πρότυπο σφάλματος ε. Δηλαδή, ένας κώδικας C διορθώνει το πρότυπο σφάλματος ε αν $\forall\, x \in C$, τότε $x + \varepsilon = y$ είναι εγγύτερα στη x από ό,τι σε οποιαδήποτε άλλη κωδική λέξη του κώδικα C. Επίσης, χαρακτηρίζουμε έναν κώδικα C ως κώδικα β – διόρθωσης, αν διορθώνει όλα τα πρότυπα σφάλματος βάρους μικρότερου ή ίσου του β και δεν διορθώνει τουλάχιστον ένα πρότυπο σφάλματος βάρους $\beta + 1$.

ΘΕΩΡΗΜΑ 4.3

Ένας κώδικας C απόστασης d διορθώνει όλα τα πρότυπα σφάλματος βάρους μικρότερου ή ίσου του $\lfloor (d-1)/2 \rfloor$. (Υπενθυμίζεται ότι $\lfloor z \rfloor$ συμβολίζει το μεγαλύτερο ακέραιο αριθμό i που ικανοποιεί τη σχέση $i \le z$.) Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους $1 + \lfloor (d-1)/2 \rfloor$ που δε διορθώνει ο κώδικας C.

Απόδειξη

Θεωρούμε ένα μη μηδενικό πρότυπο σφάλματος ε βάρους $wt(\varepsilon) \le d-1$ και τις κωδικές λέξεις x και $y \in C$, $x \neq y$. Επιθυμούμε να δείξουμε ότι η απόσταση της λέξης που μεταδόθηκε από αυτή που ελήφθη είναι μικρότερη από την απόσταση οποιασδήποτε άλλης κωδικής λέξης από τη λέξη που ελήφθη, δηλαδή $d(x, x+\varepsilon) < d(y, x+\varepsilon)$. (Υπενθυμίζεται ότι το άθροισμα της λέξης x που μεταδόθηκε και του πρότυπου σφάλματος είναι ίσο με τη λέξη που ελήφθη.) Γενικά μεταξύ των αποστάσεων τριών λέξεων ίσου μήκους, και επομένως και στην περίπτωσή μας ισχύει:

$$d(y, x+\varepsilon) + d(x+\varepsilon, x) \ge d(y, x) \ge d.$$

Λαμβάνοντας υπόψη ότι

$$d(x+\varepsilon, x) = wt(x+\varepsilon+x) = wt(\varepsilon) \text{ και } wt(\varepsilon) \le (d-1)/2 \text{ ή } 2wt(\varepsilon) + 1 \le d,$$

ισχύει

$$d(y, x+\varepsilon) + wt(\varepsilon) \ge 2wt(\varepsilon) + 1$$

και επομένως

$$d(y, x+\varepsilon) \ge wt(\varepsilon) + 1 \ge d(x, x+\varepsilon) + 1.$$

Επομένως, αφού $d(x, x+\varepsilon) < d(y, x+\varepsilon)$, ο κώδικας διορθώνει το πρότυπο σφάλματος ε.

Τώρα θεωρούμε τις κωδικές λέξεις x και $y \in C$ και την απόστασή τους $d(x, y) = d$.

Σχηματίζουμε ένα πρότυπο σφάλματος ε αλλάζοντας $d - 1 - \lfloor (d-1)/2 \rfloor$ από τα d '1' της $(x + y)$ σε '0'. Τότε ισχύει:

$$d(x, x + \varepsilon) = wt(\varepsilon) = 1 + \lfloor (d-1)/2 \rfloor \text{ και}$$

$$d(y, x + \varepsilon) = wt(y + x + \varepsilon) = d(x + y, \varepsilon) = d - 1 - \lfloor (d-1)/2 \rfloor.$$

Αν d είναι περιττός, δηλαδή $d = 2t + 1$, τότε

$$d(x, x + \varepsilon) = wt(\varepsilon) = 1 + \lfloor (2t + 1 - 1)/2 \rfloor = 1 + t$$

και

$$d(y, x + \varepsilon) = 2t + 1 - 1 - \lfloor (2t + 1 - 1)/2 \rfloor = t$$

και επομένως

$$d(x, x + \varepsilon) > d(y, x + \varepsilon).$$

Αν d είναι άρτιος, δηλαδή $d = 2t$, τότε

$$d(x, x + \varepsilon) = wt(\varepsilon) = 1 + \lfloor (2t - 1)/2 \rfloor = 1 + t$$

και

$$d(y, x + \varepsilon) = 2t - 1 - \lfloor (2t - 1)/2 \rfloor = 2t - 1 - t = t - 1$$

και επομένως

$$d(x, x + \varepsilon) > d(y, x + \varepsilon).$$

Επομένως, ο κώδικας δε διορθώνει το πρότυπο σφάλματος ε, αφού $d(x, x + \varepsilon) > d(y, x + \varepsilon)$, δηλαδή υπάρχει η κωδική λέξη y με απόσταση μικρότερη από τη ληφθείσα λέξη $x + \varepsilon$ από ό,τι η κωδική λέξη x που πράγματι μεταδόθηκε.

Παράδειγμα 4.8

Θεωρούμε και πάλι τον κώδικα $C = \{000, 111\}$ του Παραδείγματος 5. Ποια πρότυπα σφάλματος διορθώνονται από τον κώδικα σύμφωνα με το θεώρημα 4.3;

Απάντηση

Σύμφωνα με το θεώρημα 4.3, αφού η απόσταση του κώδικα είναι ίση με 3, ο κώδικας διορθώνει κάθε πρότυπο σφάλματος βάρους 1. Πράγματι, όπως είδαμε στο Παράδειγμα 5, ο αποδέκτης συμπεραίνει την κωδική λέξη «111», εφόσον λάβει αυτή την κωδική λέξη ή λάβει μία από τις λέξεις «011», «101 ή «110», δηλαδή διορθώνει τα πρότυπα σφάλματος 111 + 011 = 100, 111 + 101 = 010 και 111 + 110 = 001 στην περίπτωση μετάδοσης της κωδικής λέξης «111». Κατά τον ίδιο τρόπο, βλέπουμε ότι

αποδέκτης συμπεραίνει την κωδική λέξη «000», εφόσον λάβει αυτή την κωδική λέξη ή λάβει μία από τις λέξεις «001», «010» ή «100», δηλαδή διορθώνει τα πρότυπα σφάλματος 000 + 100 = 100, 000 + 010 = 010 και 000 + 001 = 001. Επομένως, λέμε ότι ο κώδικας C διορθώνει τα πρότυπα σφάλματος 100, 010 και 001, αφού ισχύει και για τις δύο κωδικές λέξεις του κώδικα C. Όμως, ο κώδικας δε διορθώνει πρότυπα σφάλματος βάρους μεγαλύτερου του 1. Παραδείγματος χάριν, κατά τη μετάδοση της λέξης «111», αν εμφανιστεί το πρότυπο σφάλματος «110», δηλαδή ληφθεί η λέξη «001», ο κώδικας τη διορθώνει εσφαλμένα σε «000».

Άσκηση αυτοαξιολόγησης 4.7

Για κάθε έναν από τους κώδικες $C_1 = \{101, 011, 111\}$, $C_2 = \{00000, 11111\}$, $C_3 = \{00000, 01111, 10001, 11110\}$ και $C_4 = \{000000, 101010, 010101, 111111\}$ βρείτε ένα πρότυπο σφάλματος βάρους $1 + \lfloor (d - 1)/2 \rfloor$ που δε διορθώνει ο κώδικας, όπου d η απόσταση του κώδικα.

4.2 Γραμμικοί κώδικες

Σκοπός

Η ενότητα αυτή έχει ως στόχο την εισαγωγή μιας ευρείας κατηγορίας κωδίκων, των γραμμικών κωδίκων.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει αυτή την ενότητα, θα είστε σε θέση να:

- *εξηγήσετε την έννοια των γραμμικών κωδίκων και να αναφέρετε τρία πλεονεκτήματα των γραμμικών κωδίκων σε σύγκριση με μη γραμμικούς,*
- *περιγράψετε έναν αλγόριθμο σχηματισμού βάσεων ενός κώδικα και του δυϊκού του κώδικα,*
- *περιγράψετε έναν τρόπο αξιοποίησης του γεννήτορα πίνακα για την κωδικοποίηση μηνυμάτων καθώς και δύο διαδικασίες αποκωδικοποίησης: μία διαδικασία που βασίζεται μόνο στις 'συνομάδες' και μια δεύτερη διαδικασία που βασίζεται στην τυπική διάταξη αποκωδικοποίησης,*
- *διατυπώσετε τέσσερα θεωρήματα για τις σχέσεις μεταξύ του μήκους, της απόστασης και της διάστασης ή του πλήθους των λέξεων γραμμικών κωδίκων,*
- *ορίσετε τους τέλειους κώδικες,*
- *περιγράψετε τους κώδικες Hamming.*

Έννοιες κλειδιά

- *γραμμικός κώδικας* (*Linear Code*),
- *βάση Κώδικα* (*Basis for a Code*),
- *διάσταση κώδικα* (*Dimension of Code*),
- *μορφή* (*περιορισμένης*) *κλιμακωτής διάταξης γραμμών* (*Row Echelon Form*),
- *γεννήτορας πίνακας* (*Generator Matrix*),
- *πίνακας ελέγχου ισοτιμίας* (*Parity – Check Matrix*),
- *συστηματικός κώδικας,*
- *συνομάδα* (*Coset*),

- *μήνυμα ή ψηφία πληροφορίας και πλεονασμός ή ψηφία ελέγχου ισοτιμίας*,
- *σύνδρομο* (*Syndrome*),
- *τέλειοι κώδικες* (*Perfect Codes*),
- *κώδικες Hamming*.

Ένας κώδικας C ονομάζεται γραμμικός αν $\forall\ x, y \in C$, τότε $(x + y) \in C$. Παραδείγματος χάριν, ο κώδικας $C = \{00, 11\}$ είναι γραμμικός, αφού $00 + 00 = 00$, $00 + 11 = 11$, $11 + 00 = 11$ και $11 + 11 = 00$ είναι κωδικές λέξεις. Όμως, ο κώδικας $C = \{00, 10, 11\}$ δεν είναι γραμμικός, αφού η $11 + 10 = 01$ δεν είναι κωδική λέξη. Κάθε γραμμικός κώδικας πρέπει να περιέχει τη μηδενική λέξη, αφού το άθροισμα μιας οποιασδήποτε κωδικής λέξης με τον εαυτό της δίνει τη μηδενική λέξη.

Ένα σημαντικό πλεονέκτημα των γραμμικών κωδίκων είναι το ότι η απόσταση του κώδικα είναι ίση με το ελάχιστο των βαρών των μη μηδενικών κωδικών λέξεων.

Οι γραμμικοί κώδικες εμφανίζουν και άλλα πλεονεκτήματα σε σύγκριση με τους μη γραμμικούς. Σε αυτά συμπεριλαμβάνονται και τα ακόλουθα:

Η κωδικοποίηση ενός γραμμικού κώδικα είναι πιο απλή και έχει μικρότερες αποθηκευτικές απαιτήσεις.

Για γραμμικούς κώδικες υπάρχει μια πιο απλή διαδικασία πλήρους ή ατελούς αποκωδικοποίησης μέγιστης πιθανότητας από ό,τι αυτή που είδαμε στην Υποενότητα 4.1.2.

Η περιγραφή των συνόλων των προτύπων σφάλματος που ανιχνεύει ή διορθώνει ένας κώδικας είναι πιο εύκολη στην περίπτωση των γραμμικών από ό,τι στη γενική περίπτωση.

Άσκηση αυτοαξιολόγησης 4.8

Ποιοι από τους κώδικες $C_1 = \{101, 111, 011\}$, $C_2 = \{0000, 1001, 0110, 1111\}$, $C_3 = \{00000, 11100, 00111, 11011\}$ και $C_4 = \{000000, 101010, 010101, 111111\}$ είναι γραμμικοί και ποιες είναι οι αποστάσεις των γραμμικών κωδίκων;

Η ενότητα αυτή χωρίζεται σε πέντε υποενότητες. Η πρώτη υποενότητα αναφέρεται σε ορισμένες, χρήσιμες για τη συνέχεια, έννοιες και τεχνικές της γραμμικής άλγεβρας, η δεύτερη ενότητα στους γεννήτορες πίνακες και την κωδικοποίηση, η τρίτη στους πίνακες ελέγχου ισοτιμίας και την αποκωδικοποίηση, η τέταρτη στους τέλειους κώδικες και, τέλος, η πέμπτη στους κώδικες Hamming.

4.2.1 Μαθηματικό υπόβαθρο

Οι πιο σημαντικές μαθηματικές τεχνικές και εργαλεία για τη μελέτη των γραμμικών κωδίκων προέρχονται από τη γραμμική άλγεβρα. Για το λόγο αυτό θα επαναφέρουμε στη μνήμη μας ορισμένες έννοιες και τεχνικές της γραμμικής άλγεβρας, σε συνδυασμό με τις αντίστοιχες έννοιες της θεωρίας κωδικοποίησης, που θα μας χρησιμεύσουν στις επόμενες υποενότητες. Ειδικότερα, θα επαναφέρουμε στη μνήμη μας τις έννοιες του διανυσματικού χώρου, του γραμμικού αναπτύγματος, του ορθογωνίου συμπληρώματος, της βάσης και της διάστασης ενός υποσυνόλου διανυσματικού χώρου και αντίστοιχα τις έννοιες του δυϊκού κώδικα, της βάσης και της διάστασης ενός κώδικα. Στον Πίνακα 4.1 συνοψίζεται η αντιστοιχία των εννοιών της γραμμικής άλγεβρας και εννοιών γραμμικών κωδίκων. Επίσης, θα μας απασχολήσουν και τεχνικές υπολογισμού ισοδύναμων πινάκων.

Πίνακας 4.1

Αντιστοιχία εννοιών της γραμμικής άλγεβρας και εννοιών της θεωρίας κωδικοποίησης

Έννοιες Γραμμικής Άλγεβρας	Έννοιες Θεωρίας Κωδικοποίησης
Διανυσματικός υποχώρος	Γραμμικός Κώδικας
Διάνυσμα	Λέξη
Γραμμικό ανάπτυγμα υποσυνόλου S του διανυσματικού χώρου, $<S>$ (Διανυσματικός υποχώρος)	Γραμμικός κώδικας $C = <S>$
Διάνυσμα του $<S>$	Κωδική λέξη του $C = <S>$
Ορθογώνιο συμπλήρωμα υποσυνόλου S	Δυϊκός κώδικας
Βάση διανυσματικού υποχώρου	Βάση γραμμικού κώδικα
Διάσταση διανυσματικού υποχώρου	Διάσταση γραμμικού κώδικα

Σύμφωνα με τον ορισμό του διανυσματικού χώρου K^n ($K = \{0, 1\}$), αυτός απαρτίζεται από τις βαθμωτές ποσότητες (scalars) 0 και 1 και το σύνολο των διανυσμάτων (ή λέξεων) μήκους n, καθώς και από τις πράξεις της πρόσθεσης διανυσμάτων (λέξεων) και του πολλαπλασιασμού βαθμωτών ποσοτήτων. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού ικανοποιούν τις ιδιότητες που περιέχονται στον Πίνακα 4.2, όπου x, y, z διανύσματα (ή λέξεις του ιδίου μήκους n), α και β οι βαθμωτές ποσότητες του διανυσματικού χώρου K^n και 0 η μηδενική λέξη.

Πίνακας 4.2

Ιδιότητες των πράξεων της πρόσθεσης και του πολλαπλασιασμού σε ένα διανυσματικό χώρο K^n

1. $(y + z) \in K^n$,
2. $\alpha \cdot y \in K^n$,
3. $x + y = y + x$,
4. $(x + y) + z = x + (y + z)$,
5. $(\alpha \cdot \beta) \cdot y = \alpha \cdot (\beta \cdot y)$,
6. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot y$,
7. $a \cdot (x + y) = a \cdot x + a \cdot y$,
8. $(x + 0) = x$,
9. $1 \cdot x = x$,
10. υπάρχει λέξη $x' \in K^n$, τέτοια ώστε $x + x' = x' + x = 0$.

Ένα μη κενό υποσύνολο S του διανυσματικού χώρου K^n είναι ένας υποχώρος αυτού, αν για κάθε ζεύγος διανυσμάτων (λέξεων) $y, z \in S$, ισχύει $(y + z) \in S$ και $\alpha \cdot y \in S$ για κάθε βαθμωτή ποσότητα α. Έτσι, C είναι ένας γραμμικός κώδικας αν και μόνο αν C είναι υποχώρος του K^n.

Ας δούμε τώρα δύο σημαντικούς υποχώρους του διανυσματικού χώρου K^n, το **γραμμικό ανάπτυγμα** ενός υποσυνόλου του S και το ορθογώνιο συμπλήρωμά του $S^{\perp}$.

Το σύνολο όλων των γραμμικών συνδυασμών των διανυσμάτων (ή λέξεων) ενός συνόλου $S = \{z_1, z_2, \ldots, z_k\}$ ονομάζεται το **γραμμικό ανάπτυγμα** (ή **γραμμικό άνοιγμα**) του S και συμβολίζεται με $<S>$. (Υπόμνηση: Μια λέξη (ή διάνυσμα) y λέγεται γραμμικός συνδυασμός των διανυσμάτων $z_1, z_2, \ldots, z_k$ αν υπάρχουν βαθμωτές ποσότητες $\alpha_1, \alpha_2, \ldots, \alpha_k$ τέτοιες ώστε: $y = a_1 \cdot z_1 + \alpha_2 \cdot z_2 + \ldots + \alpha_k \cdot z_k$.) Έχει δειχθεί ότι, για κάθε υποσύνολο S ενός διανυσματικού χώρου K^n, το γραμμικό του ανάπτυγμα $<S>$ είναι υποχώρος του K^n . Για το λόγο αυτό, το $<S>$ καλείται και γραμμικός κώδικας που δημιουργείται από το S, αφού ως υποχώρος πληροί τις προϋποθέσεις του ορισμού των γραμμικών κωδίκων. Το γραμμικό ανάπτυγμα $<S>$ του υποσυνόλου S του διανυσματικού χώρου K^n περιέχει τα εξής διανύσματα (λέξεις): τη μηδενική λέξη, όλες τις λέξεις του S και όλα τα αθροίσματα δύο ή περισσότερων λέξεων του S.

Παράδειγμα 4.9

Το γραμμικό ανάπτυγμα του υποσυνόλου $S = \{00011, 11100\}$ αποτελείται από τις ακόλουθες λέξεις: 00000, 00011, 11100, 00011 + 11100 = 11111. Επομένως, $<S> = \{00000, 00011, 11100, 11111\}$.

Το **βαθμωτό γινόμενο** δύο διανυσμάτων (ή λέξεων) $x = (\alpha_1, \alpha_2, ..., \alpha_n)$ και $y = (\beta_1, \beta_2, ..., \beta_n)$ στο K^n ορίζεται ως ακολούθως:

$x \cdot y = \alpha_1 \cdot \beta_1 + \alpha_2 \cdot \beta_2 + ... + \alpha_n \cdot \beta_n$.

Το αποτέλεσμα του βαθμωτού γινομένου δύο διανυσμάτων είναι βαθμωτή ποσότητα, στην περίπτωσή μας το 0 ή το 1.

Παράδειγμα 4.10

Ο βαθμωτός πολλαπλασιασμός των διανυσμάτων (λέξεων) $x = 00011$ και $y = 11100$ στο K^5 οδηγεί στο ακόλουθο αποτέλεσμα: $00011 \cdot 11100 = 0 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 = 0 + 0 + 0 + 0 + 0 = 0$.

Δύο διανύσματα (λέξεις) x και y χαρακτηρίζονται **ορθογώνια** αν $x \cdot y = 0$ (δείτε Παράδειγμα 10). Ένα διάνυσμα (λέξη) x χαρακτηρίζεται ορθογώνιο σε ένα σύνολο S, αν το x είναι ορθογώνιο σε κάθε διάνυσμα (λέξη) $y \in S$. Το σύνολο όλων των διανυσμάτων (λέξεων), που είναι ορθογώνια ενός συνόλου S, συμβολίζεται με $S^{\wedge}$ και ονομάζεται το **ορθογώνιο συμπλήρωμα** του S. Για κάθε υποσύνολο S του διανυσματικού χώρου K^n, το ορθογώνιο συμπλήρωμά του, $S^{\perp}$, είναι επίσης υποχώρος του K^n. Επίσης, για κάθε διανυσματικό χώρο K^n, αν $C = <S>$, τότε $C^{\perp} = S^{\perp}$. (Με άλλα λόγια, το ορθογώνιο συμπλήρωμα του γραμμικού αναπτύγματος $<S>$ ισούται με το ορθογώνιο συμπλήρωμα του S, $S^{\perp}$.) Το ορθογώνιο συμπλήρωμα $C^{\perp}$ καλείται **δυϊκός κώδικας** του κώδικα C, όπου S υποσύνολο του διανυσματικού χώρου K^n, $C = <S>$ και $C^{\perp} = S^{\perp}$.

Παράδειγμα 4.11

Υποθέτουμε το υποσύνολο $S = \{0001, 1100\}$ του K^n και θέλουμε να υπολογίσουμε το ορθογώνιο συμπλήρωμά του $C^{\perp} = S^{\perp}$. Επομένως, πρέπει να βρούμε όλες τις λέξεις $x = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, μήκους 4 ψηφίων, οι οποίες είναι ορθογώνιες στις λέξεις του S. Δηλαδή, $x \cdot 0001 = 0$ και $x \cdot 1100 = 0$. Από το πρώτο βαθμωτό γινόμενο έχουμε $0 \cdot \alpha_1 + 0 \cdot \alpha_2 + 0 \cdot \alpha_3 + 1 \cdot \alpha_4 = 0$. Επομένως, $\alpha_4 = 0$. Από το δεύτερο βαθμωτό γινόμενο έχουμε $1 \cdot \alpha_1 + 1 \cdot \alpha_2 + 0 \cdot \alpha_3 + 0 \cdot \alpha_4 = 0$. Επομένως, $\alpha_1 + \alpha_2 = 0$, δηλαδή $\alpha_1 = \alpha_2 = 0$ ή $\alpha_1 = \alpha_2 = 1$. Το α_3 μπορεί να είναι 0 ή 1. Συνεπώς, $\alpha_1 = \alpha_2 = 0$ είτε $\alpha_1 = \alpha_2 = 1$, $\alpha_3 = 0$ είτε $\alpha_3 = 1$ και $\alpha_4 = 0$. Οι συνδυασμοί των δυνατών επιλογών λοιπόν οδηγούν στο ορθογώ-

νιο συμπλήρωμα $C^{\perp} = S^{\perp} = \{0000, 0010, 1100, 1110\}$.

Ένα σύνολο διανυσμάτων $S = \{z_1, z_2,..., z_k\}$ είναι **γραμμικώς ανεξάρτητο** αν δεν υπάρχουν βαθμωτές ποσότητες $\alpha_1, \alpha_2,..., \alpha_k$, με τουλάχιστον μία εξ αυτών διάφορη του 0, τέτοιες ώστε: $\alpha_1 \cdot z_1 + \alpha_2 \cdot z_2 + ... + \alpha_k \cdot z_k. = 0$. Διαφορετικά, το σύνολο S είναι **γραμμικώς εξαρτημένο**. Ένα σύνολο, που περιέχει τη μηδενική λέξη, είναι γραμμικώς εξαρτημένο. Κάθε σύνολο $S \neq \{0\}$ περιέχει ένα, μέγιστης διάστασης, γραμμικώς ανεξάρτητο, υποσύνολο.

Παράδειγμα 4.12

Υποθέτουμε το σύνολο $S = \{110, 011, 101, 111\}$ και θέλουμε να εξετάσουμε αν είναι γραμμικώς εξαρτημένο ή ανεξάρτητο. Επίσης, αν το *S είναι* γραμμικώς εξαρτημένο, ζητείται ένα, από τα μέγιστης διάστασης, γραμμικώς ανεξάρτητο υποσύνολό του.

Απάντηση

Εξετάζουμε τη σχέση $\alpha_1 \cdot 110 + \alpha_2 \cdot 011 + \alpha_3 \cdot 101 + \alpha_4 \cdot 111 = 000$ ή $\alpha_1\alpha_1 0 + 0\alpha_2\alpha_2 + \alpha_3 0\alpha_3 + \alpha_4\alpha_4\alpha_4 = 000$, η οποία ισχύει αν $\alpha_1 + \alpha_3 + \alpha_4 = 0$, $\alpha_1 + \alpha_2 + \alpha_4 = 0$ και $\alpha_2 + \alpha_3 + \alpha_4 = 0$. Προσθέτοντας και τις τρεις εξισώσεις λαμβάνουμε $\alpha_4 = 0$. Έτσι, έχουμε τις εξισώσεις $\alpha_1 + \alpha_3 = 0$, $\alpha_1 + \alpha_2 = 0$ και $\alpha_2 + \alpha_3 = 0$, από τις οποίες προκύπτει $\alpha_1 = \alpha_2 = \alpha_3$. Μπορούμε να επιλέξουμε λοιπόν $\alpha_1 = \alpha_2 = \alpha_3 = 1$ και επομένως το S είναι γραμμικώς εξαρτημένο. Για την εύρεση ενός από τα μέγιστης διάστασης, γραμμικώς ανεξάρτητου, υποσυνόλου του S, αφαιρούμε από το S το πρώτο διάνυσμα (λέξη) που βρίσκουμε να είναι γραμμικός συνδυασμός των άλλων. Παρατηρούμε ότι το διάνυσμα (λέξη) 110 είναι γραμμικός συνδυασμός των υπολοίπων, αφού προκύπτει από την πρόσθεση 011 + 101. Το αφαιρούμε από το S και εξετάζουμε αν το $S' = \{011, 101, 111\}$ είναι γραμμικώς ανεξάρτητο. Δηλαδή, εξετάζουμε την εξίσωση $0\alpha_1\alpha_1 + \alpha_2 0\alpha_2 + \alpha_3\alpha_3\alpha_3 = 000$, η οποία ισχύει αν $\alpha_2 + \alpha_3 = 0$, $\alpha_1 + \alpha_3 = 0$ και $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Από την πρώτη και την τελευταία εξίσωση έχουμε $\alpha_1 = 0$ και επομένως $\alpha_3 = 0$ και $\alpha_2 = 0$. Δηλαδή, δεν υπάρχουν βαθμωτές ποσότητες, με τουλάχιστον μία εξ αυτών διάφορη του 0, τέτοιες ώστε $0\alpha_1\alpha_1 + \alpha_2 0\alpha_2 + \alpha_3\alpha_3\alpha_3 = 000$. Συνεπώς, το S' είναι ένα, από τα μέγιστης διάστασης, γραμμικώς ανεξάρτητο υποσύνολο του S.

Ένα μη κενό υποσύνολο διανυσμάτων B ενός διανυσματικού υποχώρου V είναι μία **βάση** για τον υποχώρο V, αν $<B> = V$ και το B είναι γραμμικώς ανεξάρτητο σύνολο. Επομένως, ένα γραμμικώς ανεξάρτητο υποσύνολο διανυσμάτων S είναι μία βάση για τον διανυσματικό υποχώρο $<S>$. Στην περίπτωση ενός γραμμικώς εξαρτημένου συνόλου S, κάθε ένα από τα μέγιστης διάστασης γραμμικώς ανεξάρτητα υποσύνολά του είναι βάση του υποχώρου $<S>$. Αν $S = \{0\}$, τότε η βάση του $<S>$ είναι το κενό σύνολο.

Παράδειγμα 4.13

Υποθέτουμε και πάλι, όπως στο Παράδειγμα 12, το υποσύνολο $S = \{110, 011, 101, 111\}$, το οποίο είναι γραμμικώς εξαρτημένο. Όπως είδαμε, ένα από, τα μέγιστης διάστασης, γραμμικώς ανεξάρτητα υποσύνολά του, είναι το $B = \{011, 101, 111\}$, το οποίο είναι, επομένως, μία βάση του $<S> = \{000, 011, 101, 111, 110, 100, 010, 001\}$.

Κατά κανόνα, ένας διανυσματικός χώρος έχει πολλές βάσεις. Όμως, όλες οι βάσεις έχουν το ίδιο πλήθος διανυσμάτων (λέξεων). Το πλήθος των διανυσμάτων (λέξεων) μιας βάσης ενός διανυσματικού (υπο)χώρου ονομάζεται **διάσταση του διανυσματικού (υπο)χώρου**. Παραδείγματος χάριν, ο διανυσματικός χώρος $<S>$ του Παραδείγματος 13 έχει διάσταση 3. Η διάσταση του διανυσματικού χώρου K^n είναι n, επειδή το σύνολο των λέξεων μήκους n και βάρους 1, δηλαδή το σύνολο $\{0...01, 0...10, ..., 1...00\}$, είναι μια βάση του διανυσματικού χώρου (της οποίας το γραμμικό ανάπτυγμα είναι ο διανυσματικός χώρος K^n).

Αν η διάσταση ενός γραμμικού κώδικα (ή διανυσματικού χώρου) C είναι k και μια βάση του είναι το σύνολο $X = \{x_1, x_2,..., x_k\}$, τότε οποιαδήποτε λέξη $c \in C$ μπορεί να γραφτεί ως

$$c = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + ... + \alpha_k \cdot x_k$$

για κάποια μοναδική επιλογή των ψηφίων $\alpha_1, \alpha_2,..., \alpha_k$. Επειδή κάθε βαθμωτή ποσότητα α_i παίρνει την τιμή 0 ή 1, οι δυνατοί συνδυασμοί όλων των $\alpha_1, \alpha_2,..., \alpha_k$ είναι 2^k και επομένως και οι κωδικές λέξεις του C.

Ακόμα, θα πρέπει να φρεσκάρουμε τις γνώσεις μας από τη θεωρία πινάκων που θα χρειαστούμε στη συνέχεια , όπου θα σχηματίζουμε πίνακες με γραμμές (ή στήλες) τις λέξεις κωδίκων για την εύρεση βάσεων των κωδίκων αυτών. Υπάρχουν οι ακόλουθοι δύο τύποι στοιχειωδών πράξεων που μπορούν να εφαρμοστούν στις γραμμές ενός πίνακα για να πάρουμε έναν ισοδύναμό του πίνακα:

- η ανταλλαγή δύο γραμμών και
- η αντικατάσταση μιας γραμμής από το άθροισμα του εαυτού της με κάποια άλλη.

Έτσι, δύο πίνακες είναι **ισοδύναμοι** ως προς τις γραμμές, αν ο ένας μπορεί να ληφθεί από τον άλλο με μια σειρά των ανωτέρω στοιχειωδών πράξεων γραμμών.

Ένας πίνακας βρίσκεται σε **μορφή κλιμακωτής διάταξης γραμμών** (ΚΔΓ, row echelon form), αν όλες οι μηδενικές γραμμές είναι στο κάτω μέρος και το πρώτο ψηφίο «1» («οδηγός») μιας γραμμής είναι σε στήλη πιο δεξιά σε σχέση με το πρώτο (τον οδηγό) «1» των προηγούμενων γραμμών. Μια στήλη που περιέχει έναν «οδηγό»

«1» ονομάζεται στήλη «οδηγός». Αν, επιπλέον, σε κάθε στήλη οδηγό του πίνακα (δηλαδή στήλη που περιέχεται ο οδηγός «1» μιας γραμμής) δεν περιέχονται άλλα ψηφία «1» αλλά μόνο ψηφία «0», τότε ο πίνακας είναι σε **μορφή περιορισμένης κλιμακωτής διάταξης γραμμών** (ΠΚΔΓ, reduced row echelon form). Κάθε πίνακας με στοιχεία «0» και «1» μπορεί να τεθεί σε μορφή ΚΔΓ και ΠΚΔΓ. Για έναν πίνακα, η μορφή ΠΚΔΓ είναι μοναδική. Αντίθετα, ο πίνακας μπορεί να έχει πολλές μορφές ΚΔΓ.

Η μεταφορά ενός πίνακα, του οποίου οι γραμμές αποτελούνται από τις λέξεις του κώδικα C, σε μορφή ΚΔΓ ή ΠΚΔΓ μας είναι ιδιαίτερα χρήσιμη, διότι οι μη μηδενικές γραμμές του πίνακα στη μορφή ΚΔΓ και ΠΚΔΓ απαρτίζουν ένα μέγιστης διάστασης γραμμικώς ανεξάρτητο υποσύνολο του C.

Παράδειγμα 4.14

Δίνεται ο κώδικας $C = \{0000, 1110, 0111, 1001\}$, του οποίου οι λέξεις αποτελούν τις γραμμές του πίνακα P. Το ζητούμενο είναι να φέρουμε τον πίνακα P σε μορφή ΚΔΓ και ΠΚΔΓ.

Απάντηση. Εφαρμόζοντας, σύμφωνα με τα ανωτέρω, τις δύο στοιχειώδεις πράξεις γραμμών λαμβάνουμε καταρχήν τη ζητούμενη μορφή ΚΔΓ του πίνακα.

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Από τον αρχικό πίνακα P οδηγούμαστε στο 2ο πίνακα μόνο με ανταλλαγή της θέσης των γραμμών. Από το 2ο πίνακα στον 3ο με την αντικατάσταση της 3ης γραμμής με το άθροισμα του εαυτού της και της 1ης γραμμής. Τέλος, αντικαθιστώντας την 3η γραμμή του 3ου πίνακα με το άθροισμα του εαυτού της και της 2ης γραμμής καταλήγουμε στον 4ο πίνακα, ο οποίος αποτελεί τη μορφή ΚΔΓ του πίνακα P. Τώρα για να φέρουμε τον πίνακα P στη μορφή ΠΚΔΓ, πρέπει να λάβουμε υπόψη τον επιπρόσθετο περιορισμό, η στήλη που περιέχει τον οδηγό «1» μιας γραμμής να μην περιέχει άλλα ψηφία «1».

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Πράγματι, ο 4ος πίνακας είναι σε μορφή ΠΚΔΓ, αφού οι δύο πρώτες του στήλες που περιέχουν τους οδηγούς «1» των δύο μη μηδενικών γραμμών δεν περιέχουν άλλα ψηφία «1» αλλά μόνο «0».

Ας εστιάσουμε τώρα στον τρόπο εύρεσης βάσεων των δύο κωδίκων (διανυσματικών χώρων) που μας ενδιαφέρουν, του κώδικα $C = <S>$ (γραμμικού αναπτύγματος $<S>$) και του δυϊκού του κώδικα $C^{\perp}$ (ορθογωνίου συμπληρώματος $S^{\perp}$). Σύμφωνα με τον ορισμό της βάσης ενός διανυσματικού χώρου, οποιοδήποτε από τα μέγιστης διάστασης γραμμικώς ανεξάρτητα υποσύνολα του διανυσματικού χώρου C (ή του συνόλου S, όπου $C = <S>$) είναι βάση του. Επίσης, όπως προαναφέραμε, οι μη μηδενικές γραμμές ενός πίνακα σε μορφή ΚΔΓ ή ΠΚΔΓ που σχηματίζεται από τις λέξεις του συνόλου S (ή από τις λέξεις του C, όπου $C = <S>$), είναι οι λέξεις ενός μέγιστης διάστασης γραμμικώς ανεξάρτητου υποσυνόλου του C και, επομένως, μια βάση του.

Επομένως, για να βρούμε μια βάση του κώδικα C αρκεί να μεταφέρουμε σε μορφή ΚΔΓ ή ΠΚΔΓ τον πίνακα που σχηματίζεται από τις λέξεις του συνόλου S (ή και από όλες τις λέξεις του C, $C = <S>$). Στο Παράδειγμα 14, το υποσύνολο {1110, 0111} είναι μια βάση του κώδικα $C = \{0000, 1110, 0111, 1001\}$, από την οποία προκύπτουν, με γραμμικούς συνδυασμούς, όλες οι λέξεις του C.

Με τον ίδιο τρόπο θα μπορούσαμε να βρούμε και μια βάση του δυϊκού κώδικα $C^{\perp}$, αν είχαμε στη διάθεσή μας τις λέξεις που τον απαρτίζουν. Αντί αυτού του τρόπου, μπορούμε όμως να εφαρμόσουμε μια πιο απλή διαδικασία, η οποία περιγράφεται στη συνέχεια.

Αλγόριθμος 4.1 (Εύρεση μιας βάσης του δυϊκού κώδικα $C^{\perp}$)

Η διαδικασία εύρεση μιας βάσης του δυϊκού κώδικα $C^{\perp}$ ($C = <S>$) διακρίνεται στα ακόλουθα βήματα:

1. Σχηματισμός του πίνακα P, του οποίου οι γραμμές είναι οι λέξεις του S (ή του C) και μεταφορά του P σε μορφή ΠΚΔΓ.
2. Σχηματισμός του πίνακα G, ο οποίος αποτελείται από τις μη μηδενικές γραμμές του πίνακα P σε μορφή ΠΚΔΓ και αποτελεί μια βάση του C. Ο πίνακας G είναι διάστασης $l \times m$.
3. Σχηματισμός του πίνακα M, ο οποίος αποτελείται μόνον από εκείνες τις στήλες του πίνακα G που δεν είναι οδηγοί, δηλαδή από τις στήλες που δεν περιέχουν οδηγούς «1». Αφού το πλήθος των στηλών οδηγών του πίνακα G είναι ίσο με το πλήθος των γραμμών του, η διάσταση του πίνακα M είναι $l \times (m - l)$.

4. Σχηματισμός του πίνακα $H = \begin{bmatrix} M \\ I \end{bmatrix}$, διάστασης mx($m - l$), από τον πίνακα M(lx($m - l$)) και τον πίνακα ταυτότητας I (($m - l$)x($m - l$)). (Υπόμνηση: Ο πίνακας ταυτότητας I είναι αυτός που έχει τα στοιχεία της διαγωνίου του ίσα με 1 και όλα τα υπόλοιπα ίσα με 0.) Με άλλα λόγια, ο πίνακας H (mx($m - l$)) σχηματίζεται ως εξής:
   - Στις πρώτες l γραμμές του H τοποθετούνται με τη σειρά οι γραμμές του M.
   - Στις υπόλοιπες ($m - l$) γραμμές του H τοποθετούνται οι γραμμές του πίνακα ταυτότητας I διάστασης ($m - l$)×($m - l$).
5. Μια βάση του δυϊκού κώδικα $C^{\perp}$ αποτελείται από τις στήλες του πίνακα H (ή τις γραμμές του ανάστροφου πίνακα H^T).

Παράδειγμα 4.15

Δίνεται το σύνολο S = {11101, 10110, 01011, 11010} και ο κώδικας C = <S>. Ζητείται μία βάση του $C^{\perp}$.

Απάντηση

Σύμφωνα με τον Αλγόριθμο 1, σχηματίζουμε τον πίνακα P, ο οποίος έχει ως γραμμές τις λέξεις του S. Τον πίνακα P μεταφέρουμε στη μορφή ΠΚΔΓ ως ακολούθως:

$$P = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow$$

$$\rightarrow \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Ο πίνακας G, διαστάσεων (3×5), σχηματίζεται από τις μη μηδενικές γραμμές του P σε μορφή ΠΚΔΓ και ο πίνακας M, (3×2), από τον πίνακα G με την αφαίρεση των τριών πρώτων στηλών που περιέχουν οδηγούς (πρώτα) «1». Από το M και τον πίνακα ταυτότητας I, (2×2), παίρνουμε το ζητούμενο πίνακα H, διαστάσεων (5×2).

$$G=\begin{bmatrix}1&0&0&0&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix},\ M=\begin{bmatrix}0&1\\1&1\\1&1\end{bmatrix},\ H=\begin{bmatrix}M\\I\end{bmatrix}=\begin{bmatrix}0&1\\1&1\\1&1\\1&0\\0&1\end{bmatrix}$$

Επομένως, μια βάση του δυϊκού κώδικα $C^{\perp}$ είναι το σύνολο {01110, 11101}.

Άσκηση αυτοαξιολόγησης 4.9

Ζητείται η εύρεση, με τη βοήθεια του Αλγόριθμου 1, μιας βάσης του κώδικα C και μιας βάσης του $C^{\perp}$, όπου $C = <S>$ και S = {001101, 001000, 001111, 000101, 000001}.

4.2.2 Γεννήτορες πίνακες και κωδικοποίηση

Κάθε πίνακας, του οποίου οι γραμμές αποτελούν μια βάση του κώδικα C, ονομάζεται **γεννήτορας πίνακας** για τον C. Το πλήθος των γραμμών του γεννήτορα πίνακα είναι ίσο με τη διάσταση του C, δηλαδή το πλήθος των λέξεων που απαρτίζουν μια βάση του. Αν η διάσταση ενός κώδικα C συμβολίζεται με k, το μήκος των κωδικών λέξεων είναι n και η απόστασή του d, τότε χαρακτηρίζουμε τον C και ως (n, k, d) γραμμικό κώδικα.

Αν G είναι ένας γεννήτορας πίνακας για έναν κώδικα C, τότε κάθε πίνακας ισοδύναμος του G, ως προς τις γραμμές, είναι γεννήτορας πίνακας για τον C. Για την εύρεση, βεβαίως, ενός γεννήτορα πίνακα για κάποιον κώδικα C, αρκεί να βρούμε μια βάση του. Όπως είδαμε στην Υποενότητα 4.2.1, οι μη μηδενικές λέξεις του πίνακα σε μορφή ΠΚΔΓ, που σχηματίζεται από τις λέξεις του C (ή του S, όπου $C = <S>$), αποτελούν μια βάση του C.

Ένας γεννήτορας πίνακας G για ένα γραμμικό κώδικα (n, k, d), C, μπορεί να αξιοποιηθεί για την κωδικοποίηση λέξεων (μηνυμάτων) u μήκους k ψηφίων ως εξής:

$$c = u.G = \begin{bmatrix}a_1 & a_2 & \dots & a_k\end{bmatrix}\begin{bmatrix}g_1\\g_2\\\cdot\\\cdot\\\cdot\\g_k\end{bmatrix} = a_1g_1 + a_2g_2 + \dots + a_kg_k = \begin{bmatrix}b_1 & b_2 & \dots & b_n\end{bmatrix}$$

όπου $u = [\alpha_1\ \alpha_2 \ldots\ \alpha_k]$ η λέξη (διάνυσμα – γραμμή) του μηνύματος και $c = [b_1\ b_2 \ldots\ b_n]$ η κωδική λέξη (διάνυσμα – γραμμή) μήκους n ψηφίων. Το αποτέλεσμα c είναι κωδική λέξη του C, αφού το γινόμενο $u \cdot G$ είναι γραμμικός συνδυασμός των γραμμών του G, που σχηματίζεται από τις λέξεις g_i που απαρτίζουν μια βάση του κώδικα C.

Παράδειγμα 4.16

Θεωρούμε ένα γραμμικό κώδικα (5, 3, d) και το γεννήτορα πίνακα που προκύπτει από το Παράδειγμα 15, G, καθώς και τα μηνύματα A, B, Γ, Δ, E, Z, H και Θ, στα οποία έχουμε αποδώσει τις λέξεις (στο K^3) «000», «001», «010», «011», «100», «101», «110» και «111», αντίστοιχα. Ζητείται η κωδικοποίηση των μηνυμάτων A, B, Δ και Θ.

Απάντηση

Σύμφωνα με τα ανωτέρω, για την κωδικοποίηση ενός μηνύματος, η αντίστοιχη λέξη στο K^3 πολλαπλασιάζεται με τον γεννήτορα πίνακα του κώδικα.

$$A \to c_1 = \begin{bmatrix}0 & 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\end{bmatrix} = 0.(10001) + 0.(01011) + 0.(00111) = 00000.$$

$$B \to c_2 = \begin{bmatrix}0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\end{bmatrix} = 0.(10001) + 0.(01011) + 1.(00111) = 00111.$$

$$\Delta \to c_4 = \begin{bmatrix}0 & 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\end{bmatrix} = 0.(10001) + 1.(01011) + 1.(00111) = 01100.$$

$$\Theta \to c_8 = \begin{bmatrix}1 & 1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\end{bmatrix} = 1.(10001) + 1.(01011) + 1.(00111) = 11101.$$

Άσκηση αυτοαξιολόγησης 4.10

Με δεδομένα αυτά του Παραδείγματος 16, ζητείται η κωδικοποίηση των μηνυμάτων Z και H.

Άσκηση αυτοαξιολόγησης 4.11

Θεωρούμε ένα γραμμικό κώδικα (7, 4, d) και τον κατωτέρω γεννήτορα πίνακα G, καθώς και τα μηνύματα A, E, Z, H, Θ, I, K, Λ, M, N, Ξ, O, Π, P, Σ και T, στα οποία έχουμε αποδώσει τις λέξεις στο K^4 «0000», «0001», «0010», «0011», «0100», «0101», «0110», «0111», «1000», «1001», «1010», «1011», «1100», «1101», «1110» και «1111», αντίστοιχα. Ζητείται η κωδικοποίηση του μηνύματος *ΚΑΙΡΟΣ*.

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

4.2.3 Πίνακες ελέγχου ισοτιμίας και αποκωδικοποίηση

Ο πίνακας ελέγχου ισοτιμίας σχετίζεται με ένα γραμμικό κώδικα C και συνδέεται με το γεννήτορα πίνακα. Ο πίνακας ελέγχου ισοτιμίας μπορεί να χρησιμοποιηθεί για την αποκωδικοποίηση κωδικοποιημένων μηνυμάτων.

Όπως είδαμε στην Υποενότητα 4.2.1, με τον Αλγόριθμο 1 μπορούμε να προσδιορίσουμε έναν πίνακα H, του οποίου οι στήλες είναι οι λέξεις μιας βάσης του δυϊκού κώδικα $C^{\perp}$. Ένας τέτοιος πίνακας H, του οποίου οι στήλες σχηματίζουν μια βάση του δυϊκού κώδικα $C^{\perp}$, ονομάζεται πίνακας ελέγχου ισοτιμίας του κώδικα C.

Αν η διάσταση του C είναι k, τότε η διάσταση του $C^{\perp}$ είναι $n - k$ και επομένως και το πλήθος των στηλών του πίνακα ισοτιμίας H, ενώ το πλήθος των γραμμών του είναι n, αφού το άθροισμα των διαστάσεων των κωδίκων C και $C^{\perp}$ είναι n, δηλαδή ίσο με το μήκος των κωδικών λέξεων του κώδικα C.

Σύμφωνα με όσα ήδη έχουμε εξετάσει, ο γεννήτορας πίνακας G και ο πίνακας ισοτιμίας H ενός κώδικα C είναι γραμμικώς ανεξάρτητοι ως προς τις γραμμές και τις στήλες, αντίστοιχα, αφού είναι βάσεις των κωδίκων C και $C^{\perp}$. Το άθροισμα του πλήθους των γραμμών του G και των στηλών του H είναι ίσο με το πλήθος των στηλών του G και ίσο με το πλήθος των γραμμών του H, τα οποία είναι ίσα με το μήκος των λέξεων του κώδικα C. Τέλος, το γινόμενο των πινάκων G και H ισούται με 0, δηλαδή $G \cdot H = 0$.

Ένας γεννήτορας πίνακας G, $(k \times n)$, του οποίου οι πρώτες k στήλες σχηματίζουν τον πίνακα ταυτότητας I_k, $(k \times k)$, δηλαδή $G = [I_k, M]$, λέγεται ότι βρίσκεται σε τυπική μορφή (standard form). Ο γεννήτορας πίνακας G, ο οποίος προκύπτει στο βήμα 2

του Αλγόριθμου 1 είναι σε τυπική μορφή. *Ο* κώδικας *C*, ο οποίος έχει γεννήτορα πίνακα *G* σε τυπική μορφή, χαρακτηρίζεται **συστηματικός κώδικας**. Όμως δεν έχουν όλοι οι γραμμικοί κώδικες γεννήτορες πίνακες σε τυπική μορφή.

Οι συστηματικοί κώδικες εμφανίζουν ένα πλεονέκτημα πολύ σημαντικό για την αποκωδικοποίηση. Πιο συγκεκριμένα, κάθε κωδική λέξη *c* ενός κώδικα *C*, μήκους *n* και διάστασης *k*, είναι ίση με $u \cdot G$ για μία μόνο λέξη, δηλαδή το προς κωδικοποίηση μήνυμα, $u \in K^k$. (Υπόμνηση: K^k είναι το σύνολο όλων των λέξεων μήκους *k* bits.) Αν θεωρήσουμε τώρα ότι ο λήπτης του κωδικοποιημένου μηνύματος είναι σε θέση να συμπεράνει, με τη βοήθεια της αποκωδικοποίησης μέγιστης πιθανότητας (ΑΜΠ), τη μετάδοση της κωδικής λέξης *c*, τότε ο δέκτης μπορεί εύκολα να ανακτήσει το μήνυμα *u* από το ληφθέν $c = u \cdot G$. Αυτό οφείλεται στο ότι το μήνυμα *u* αποτελείται από τα πρώτα *k* ψηφία του *c*, αφού $c = u \cdot G = u \cdot [I, M] = [uI, uM] = [u, uM]$. Για το λόγο αυτό, τα πρώτα *k* ψηφία των κωδικών λέξεων λέγονται **ψηφία πληροφορίας** και τα υπόλοιπα $n - k$ **πλεονασμός** ή **ψηφία ελέγχου ισοτιμίας**.

Παράδειγμα 4.17

Δίνεται ο γεννήτορας πίνακας *G* ενός συστηματικού κώδικα *C* και ζητείται η κωδικοποίηση των μηνυμάτων $a = 0000$, $b = 0101$ και $h = 1111$.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Ποια είναι τα ψηφία πληροφορίας και ποια τα ψηφία ελέγχου ισοτιμίας κάθε μιας από τις αντίστοιχες κωδικές λέξεις;

Απάντηση

Αν $u = \alpha = 0000$, τότε $u \cdot G = 0000 \cdot G = 0000000$, δηλαδή *τα* bits πληροφορίας είναι τα $0000 = \alpha$ και τα ψηφία ισοτιμίας τα υπόλοιπα 000. Αντίστοιχα, αν $u = b = 0101$, τότε $u \cdot G = 0101 \cdot G = 0101101$, δηλαδή *τα* bits πληροφορίας είναι τα $0101 = \beta$ και τα ψηφία ισοτιμίας τα υπόλοιπα 101. Κατά τον ίδιο τρόπο, αν $u = h = 1111$, τότε $u \cdot G = 1111 \cdot G = 1111111$, δηλαδή τα bits πληροφορίας είναι τα $1111 = h$ και τα ψηφία ισοτιμίας τα υπόλοιπα 111.

Το κύριο ερώτημα ωστόσο είναι το πώς θα συμπεράνει ο δέκτης τη μετάδοση κάποιας κωδικής λέξης *c*, όταν λάβει μια λέξη *y*, η οποία δεν ανήκει στον κώδικα *C*. Πριν μας απασχολήσει όμως αυτό το ερώτημα, ας ορίσουμε μια χρήσιμη για τη συνέχεια

έννοια, αυτή των **συνομάδων** (cosets). Μια συνομάδα του C προσδιορισμένη από τη λέξη x συμβολίζεται ως $C + x$ και ορίζεται ως το σύνολο όλων των λέξεων της μορφής $c + x$, όπου $c \in C$ (το x είναι σταθερό και το c κυμαίνεται σε όλο το εύρος του C). Δηλαδή, $C + x = \{c + x | \ c \in C\}$.

Παράδειγμα 4.18

Ζητούνται όλες οι συνομάδες του κώδικα $C = \{000, 111\}$.

Απάντηση

Για $x = 001$ έχουμε $C + 001 = \{000 + 001 = 001, 111 + 001 = 110\}$. Ανάλογα, $C + 010 = \{010, 101\}$, $C + 100 = \{100, 011\}$, $C + 011 = \{011, 100\}$, $C + 101 = \{101, 010\}$, $C + 110 = \{110, 001\}$, $C + 111 = C + 000 = \{000, 111\}$.

Ίσως να σκεφτούμε, πως υπάρχουν 2^n διαφορετικές συνομάδες όσες και οι κωδικές λέξεις κάποιου κώδικα C μήκους λέξεων n. Δεν είναι όμως σε καμιά περίπτωση έτσι. Είναι δυνατό δύο συνομάδες να ταυτίζονται $C + x = C + y$, ακόμα και αν $x \neq y$. Αυτό μπορούμε να το δούμε και στο Παράδειγμα 18. Στη συνέχεια, θα παραθέσουμε ορισμένα χαρακτηριστικά των συνομάδων, χωρίς ωστόσο να επιχειρήσουμε αποδείξεις αυτών.

Αν C είναι ένας συστηματικός γραμμικός κώδικας μήκους n και x και y δύο λέξεις επίσης μήκους n ψηφίων, τότε ισχύουν αναφορικά με τις συνομάδες τα ακόλουθα:

- Κάθε λέξη x περιέχεται στη συνομάδα $C + x$.
- Αν το άθροισμα $x + y$ περιέχεται στον κώδικα C, τότε οι x και y περιέχονται στην ίδια συνομάδα. Αν το άθροισμα $x + y$ δεν περιέχεται στον κώδικα C, τότε οι x και y περιέχονται σε διαφορετικές συνομάδες.
- Αν μια λέξη x περιέχεται στη συνομάδα $C + y$, τότε ισχύει $C + x = C + y$, δηλαδή κάθε λέξη της συνομάδας την προσδιορίζει.
- Κάθε λέξη $x \in K^n$ περιέχεται μόνο σε μία συνομάδα του C, δηλαδή δύο συνομάδες $C + x$ και $C + y$ είτε ταυτίζονται είτε δεν έχουν κανένα στοιχείο κοινό.
- Το πλήθος των λέξεων σε μια συνομάδα είναι ίσο με το πλήθος των λέξεων του κώδικα C, δηλαδή $|C + x| = |C|$.
- Το πλήθος των διαφορετικών συνομάδων του κώδικα C, διάστασης k, ισούται με 2^{n-k} και κάθε συνομάδα περιέχει 2^k λέξεις, όπως άλλωστε και ο κώδικας C που και αυτός αποτελεί μια συνομάδα του εαυτού του.

Έχοντας ορίσει τον πίνακα ελέγχου ισοτιμίας και τις έννοιες του συστηματικού κώδικα και των συνομάδων, ας στρέψουμε πλέον την προσοχή μας στο βασικό ερώτημα που μας απασχολεί, αυτό της αποκωδικοποίησης. Θεωρούμε τον συστηματικό γραμμικό κώδικα C και τη μετάδοση της κωδικής λέξης x. Επίσης, υποθέτουμε ότι η μετάδοση της λέξης x οδηγεί στη λήψη της λέξης y. Επομένως, έχουμε το πρότυπο σφάλματος $\varepsilon = x + y$. Αφού ισχύει $\varepsilon = x + y$, ισχύει και $x = \varepsilon + y$ και επομένως οι λέξεις ε (πρότυπο σφάλματος) και y (ληφθείσα λέξη) περιέχονται στο ίδιο ομοσύνολο του C ($x \in C$). Όπως ήδη γνωρίζουμε, πρότυπα σφάλματος μικρού βάρους λαμβάνουν χώρα με τη μεγαλύτερη πιθανότητα. Αυτό ακριβώς αποτελεί τη βάση της αποκωδικοποίησης μέγιστης πιθανότητας (ΑΜΠ). Στη συνέχεια παρατίθεται η διαδικασία αποκωδικοποίησης με τη βοήθεια των συνομάδων.

Αλγόριθμος 4.2 (Αποκωδικοποίηση με τη βοήθεια των συνομάδων)

Η διαδικασία αποκωδικοποίησης με τη βοήθεια των συνομάδων διακρίνεται στα ακόλουθα βήματα:

1. Λήψη της λέξης y και υπολογισμός της συνομάδας $C + y$.
2. Επιλογή από το δέκτη της λέξης ε, ελάχιστου βάρους, που περιέχεται στη συνομάδα $C + y$. Αν υπάρχουν περισσότερες λέξεις της συνομάδας $C + y$, οι οποίες έχουν το ελάχιστο βάρος, τότε στην περίπτωση της πλήρους αποκωδικοποίησης μέγιστης πιθανότητας (ΠΑΜΠ) επιλέγεται αυθαίρετα μία εξ αυτών, ενώ στην περίπτωση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας (ΑΑΜΠ) ζητείται από το μεταδότη επανάληψη της μετάδοσης.
3. Υπολογισμός από το δέκτη της κωδικής λέξης x που έχει μεταδοθεί προσθέτοντας τη ληφθείσα λέξη y με το πρότυπο σφάλματος ελάχιστου βάρους ε, δηλαδή $x = y + \varepsilon$.

Παράδειγμα 4.19

Δίνεται ο συστηματικός γραμμικός κώδικας $C = \{0000, 1010, 1101, 0111\}$ και οι τέσσερις συνομάδες του $\{0000, 1010, 1101, 0111\}$, $\{0001, 1011, 1100, 0110\}$, $\{0010, 1000, 1111, 0101\}$ και $\{0011, 1001, 1110, 0100\}$. Θεωρούμε ότι ο δέκτης έλαβε τις λέξεις 1110 και 1111, οι οποίες δεν είναι κωδικές λέξεις. Σε ποιο συμπέρασμα οδηγείται σύμφωνα με τις ΠΑΜΠ και ΑΑΜΠ.

Απάντηση

Αν ο δέκτης λάβει τη λέξη 1110, τότε αφού εντοπίσει τη συνομάδα στην οποία περιέ-

χεται, δηλαδή την τέταρτη, επιλέγει από αυτή το πρότυπο βάρους με το μικρότερο βάρος, δηλαδή το 0100. Επομένως, σύμφωνα με τη διαδικασία αποκωδικοποίησης συμπεραίνει ότι μεταδόθηκε η κωδική λέξη 1110 + 0100 = 1010. Στην περίπτωση λήψης όμως της λέξης 1111, ο δέκτης, αφού διαπιστώσει ότι αυτή περιέχεται στην 3η συνομάδα του C, παρατηρεί ότι σε αυτή υπάρχουν δύο πρότυπα σφάλματος με το ελάχιστο βάρος, τα 0010 και 1000. Ο επιλογή του εξαρτάται από το αν βασίζεται στην ΠΑΜΠ ή την ΑΑΜΠ. Αν έχουμε εφαρμογή της ΑΑΜΠ, ο δέκτης ζητά από το μεταδότη την επαναμετάδοση του μηνύματος. Αν εφαρμόζεται όμως η ΠΑΜΠ, ο δέκτης επιλέγει αυθαίρετα ένα από τα πρότυπα σφάλματος με το ελάχιστο βάρος, έστω το 1000 και συμπεραίνει επομένως ότι μεταδόθηκε η κωδική λέξη 1111 + 1000 = 0111.

Άσκηση αυτοαξιολόγησης 4.12

Δίνεται ο συστηματικός γραμμικός κώδικας C = {000000, 001111, 010011, 011100, 100110, 101001, 110101, 111010}. Ζητούνται οι οκτώ συνομάδες του. Ακόμα, υποθέτοντας ότι ο δέκτης έλαβε τις λέξεις 111011 και 111111, ζητούνται τα σχετικά συμπεράσματά του στη βάση των ΠΑΜΠ και ΑΑΜΠ.

Αν έχουμε να κάνουμε με κώδικες με πολλές λέξεις, η εφαρμογή του Αλγόριθμου 2 εμφανίζει δύο δυσκολίες, την αναζήτηση της συνομάδας στην οποία περιέχεται η ληφθείσα λέξη και την αναζήτηση στη συνέχεια του πρότυπου σφάλματος με το ελάχιστο βάρος. Για την αντιμετώπιση αυτών των προβλημάτων, μπορούμε να αξιοποιήσουμε τον πίνακα ελέγχου ισοτιμίας. Πριν όμως προχωρήσουμε για να δούμε πώς απλοποιείται περαιτέρω η διαδικασία της αποκωδικοποίησης με τη βοήθεια του πίνακα ελέγχου ισοτιμίας, πρέπει να γνωρίσουμε μια έννοια που μας χρειάζεται για την περιγραφή της, την έννοια του συνδρόμου μιας ληφθείσας λέξης.

Ορίζουμε ως **σύνδρομο μιας λέξης *y*** τη λέξη $y \cdot H$, η οποία περιέχεται στο K^{n-k}, όπου H είναι ο πίνακας ελέγχου ισοτιμίας για έναν κώδικα C μήκους n και διάστασης k και y η ληφθείσα λέξη. Αν x, y και ε είναι λέξεις του συνόλου K^n, τότε σχετικά με τον πίνακα ελέγχου ισοτιμίας H και το σύνδρομο των λέξεων x και y ισχύουν τα ακόλουθα:

1. Αν και μόνο αν $x \in C$, τότε $x \cdot H = 0$.
2. Αν και μόνο αν x και y περιέχονται στην ίδια συνομάδα, τότε $x \cdot H = y \cdot H$.
3. Αν ε είναι το πρότυπο σφάλματος σε σχέση με μια ληφθείσα λέξη y, τότε $\varepsilon \cdot H$ ισούται με το άθροισμα των γραμμών του πίνακα H που αντιστοιχούν στις θέσεις στις οποίες προκλήθηκαν σφάλματα κατά τη μετάδοση.

Αν δεν υπεισέλθουν σφάλματα κατά τη μετάδοση, η ληφθείσα λέξη y θα ανήκει στον κώδικα C και τότε $y \cdot H = 0$. Βέβαια, αν $y \cdot H = 0$ τότε το y είναι κωδική λέξη και θεωρούμε ότι δεν εμφανίστηκαν σφάλματα στη μετάδοση. Ωστόσο, δεν αποκλείεται ο δέκτης να λάβει μια λέξη y, διαφορετική από τη λέξη x που έστειλε ο αποστολέας, δηλαδή να υπεισέλθουν σφάλματα που οδηγούν στη λήψη μιας διαφορετικής κωδικής όμως λέξης $x \neq y$.

Επειδή όλες οι λέξεις μιας συνομάδας έχουν το ίδιο σύνδρομο, το σύνδρομο μπορεί να χρησιμοποιηθεί αντί της συνομάδας για τον προσδιορισμό της. Έτσι, αρκεί να έχουμε από κάθε συνομάδα μόνο το σύνδρομό της και τη λέξη με το ελάχιστο βάρος για να πετύχουμε την αποκωδικοποίηση μιας ληφθείσας λέξης. Τη λέξη μιας συνομάδας με το ελάχιστο βάρος την ονομάζουμε και **οδηγό της συνομάδας**. Ο πίνακας που περιέχει τα σύνδρομα και τους οδηγούς (τις λέξεις ελάχιστου βάρους) όλων των συνομάδων καλείται **τυπική διάταξη αποκωδικοποίησης** (ΤΔΑ, standard decoding array). Αν μια συνομάδα έχει περισσότερες λέξεις ελάχιστου βάρους, τότε είτε επιλέγεται μία από αυτές αυθαίρετα αν εφαρμόζεται ΠΑΜΠ είτε δεν επιλέγεται καμία αν εφαρμόζεται ΑΑΜΠ. Όταν η ληφθείσα λέξη έχει σύνδρομο συνομάδας, της οποίας δεν περιέχεται οδηγός ή λέξη ελάχιστου βάρους στην ΤΔΑ, τότε ζητείται επανάληψη της μετάδοσης.

Παράδειγμα 4.20

Δίνεται ο συστηματικός γραμμικός κώδικας C του Παραδείγματος 19 και οι τέσσερις συνομάδες του {0000, 1010, 1101, 0111}, {0001, 1011, 1100, 0110}, {0010, 1000, 1111, 0101} και {0011, 1001, 1110, 0100}. Ζητούνται οι ΤΔΑ στις περιπτώσεις εφαρμογής των ΠΑΜΠ και ΑΑΜΠ.

Απάντηση

Για τον υπολογισμό του συνδρόμου μιας συνομάδας, αρκεί να επιλέξουμε μια οποιαδήποτε λέξη της, y και να υπολογίσουμε το γινόμενο $y \cdot H$. Επομένως, αφού υπολογίσουμε τον πίνακα ελέγχου ισοτιμίας και επιλέξουμε τον οδηγό κάθε συνομάδας, δηλαδή τη λέξη με το μικρότερο βάρος και υπολογίσουμε το σύνδρομο κάθε συνομάδας, μπορούμε να σχηματίσουμε τις ΤΔΑ για τις περιπτώσεις εφαρμογής των ΠΑΜΠ και ΑΑΜΠ.

$$P=\begin{bmatrix}1&1&0&1\\1&0&1&0\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&0&1\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&0&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}\Rightarrow$$

$$M=\begin{bmatrix}1&0\\1&1\end{bmatrix},\ H=\begin{bmatrix}M\\I\end{bmatrix}=\begin{bmatrix}1&0\\1&1\\1&0\\0&1\end{bmatrix}$$

ΤΔΑ για ΠΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	$y\cdot H = 00$
0001	$(0001)\cdot H = 01$
0010	$(0010)\cdot H = 10$
0100	$(0100)\cdot H = 11$

ΤΔΑ για ΑΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	00
0001	01
———	10
0100	11

Αλγόριθμος 4.3 (Αποκωδικοποίηση στη βάση της ΤΔΑ)

Η διαδικασία αποκωδικοποίησης που βασίζεται στην ΤΔΑ διακρίνεται στα ακόλουθα βήματα:

1. Λήψη της λέξης y και υπολογισμός του συνδρόμου $y\cdot H$.
2. Εύρεση από την ΤΔΑ του οδηγού ε που αντιστοιχεί στη συνομάδα με σύνδρομο $y\cdot H$. Αν δεν υπάρχει αντίστοιχος οδηγός της συνομάδας, τότε ζητείται αναμετάδοση.
3. Υπολογισμός από το δέκτη της κωδικής λέξης x που μεταδόθηκε, προσθέτοντας τη ληφθείσα λέξη y με τον οδηγό της συνομάδας (το πρότυπο σφάλματος) ε, δηλαδή $x = y + \varepsilon$.

Παράδειγμα 4.21

Δίνεται η ΤΔΑ του κώδικα του Παραδείγματος 20 για την περίπτωση της ΠΑΜΠ και της ΑΑΜΠ. Θεωρούμε ότι ο δέκτης λαμβάνει τις λέξεις 0110 και 1111. Ποιο

είναι το συμπέρασμα του δέκτη σχετικά με τις λέξεις που μεταδόθηκαν στην περίπτωση της ΠΑΜΠ και ποιο στην περίπτωση της ΑΑΜΠ;

Απάντηση.

Υπολογίζουμε τα σύνδρομα των λέξεων που έλαβε ο δέκτης και ελέγχουμε στην ΤΔΑ τους αντίστοιχους οδηγούς των συνομάδων. Έτσι, τα σύνδρομα των λέξεων που έλαβε ο δέκτης είναι $0110 \cdot H = 01$ και $1111 \cdot H = 10$. Επομένως, στην περίπτωση της ΠΑΜΠ, ο δέκτης συμπεραίνει τις λέξεις $0110 + 0001 = 0111$και $1111 + 0010 = 1101$, αντίστοιχα. Στην περίπτωση της ΑΑΜΠ, ο δέκτης συμπεραίνει από τη ληφθείσα λέξη 0110 την κωδική λέξη 0111, ενώ από τη ληφθείσα λέξη 1111 δεν οδηγείται σε κάποιο συμπέρασμα, αφού δεν υπάρχει αντίστοιχος οδηγός αλλά ζητά αναμετάδοση.

Άσκηση αυτοαξιολόγησης 4.13

Δίνεται ο συστηματικός γραμμικός κώδικας της Άσκησης Αυτοαξιολόγησης 12, $C = \{000000, 001111, 010011, 011100, 100110, 101001, 110101, 111010\}$ και οι οκτώ συνομάδες του. Ζητείται η ΤΔΑ για τις περιπτώσεις της ΠΑΜΠ και της ΑΑΜΠ. Επίσης, τα συμπεράσματα του δέκτη μετά τη λήψη των λέξεων 011111 και 101111, σύμφωνα με τη διαδικασία αποκωδικοποίησης που βασίζεται στην ΤΔΑ.

Είναι σύνηθες, στην πράξη, το πλήθος των συνομάδων και επομένως και των οδηγών και των συνδρόμων τους να είναι της τάξης του 2^{50}, κάτι που καθιστά και τη διαχείριση της ΤΔΑ ιδιαίτερα δύσκολη. Έτσι λοιπόν και η εισαγωγή της ΤΔΑ δεν επιτρέπει την ευρεία πρακτική εφαρμογή της αποκωδικοποίησης μέγιστης πιθανότητας. Όμως, όπως θα δούμε στην Ενότητα 4.3, η αποκωδικοποίηση μέγιστης πιθανότητας είναι, από υπολογιστικής άποψης, εφικτή, εφόσον τηρούνται ορισμένες προϋποθέσεις.

4.2.4 Τέλειοι κώδικες

Πριν προχωρήσουμε στον ορισμό των τέλειων κωδίκων, ας προσπαθήσουμε να απαντήσουμε σε ορισμένα ερωτήματα σχετικά με το πλήθος των λέξεων που περιέχονται σε γραμμικούς κώδικες δεδομένου μήκους n και απόστασης d. Τα ερωτήματα αυτά δεν έχουν ακόμα απαντηθεί στη γενική τους μορφή, αλλά μόνο για κάποιες συγκεκριμένες τιμές των n και d. Ωστόσο, μπορούμε να βρούμε κάποιες σχέσεις που ισχύουν αναφορικά με τα μεγέθη κωδίκων και τις παραμέτρους n και d.

ΘΕΩΡΗΜΑ 4.4

Αν $0 \le t \le n$ και αν x είναι μια λέξη μήκους n, τότε το πλήθος των λέξεων μήκους n που εμφανίζουν απόσταση το πολύ t από τη x είναι ίσο με

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}.$$ [1]

Απόδειξη

Παρατηρούμε πρώτα ότι το πλήθος των λέξεων μήκους n και βάρους t είναι ίσο με $\binom{n}{t}$, δηλαδή ίσο με το πλήθος των λέξεων με t '1' που επιλέγονται από το σύνολο των 2^n λέξεων (δείτε και Υποσημείωση 1). Επίσης, παρατηρούμε ότι το πλήθος των λέξεων μήκους n, οι οποίες έχουν μια δεδομένη απόσταση t από μια λέξη x του ιδίου μήκους, είναι ίσο με το πλήθος των λέξεων βάρους t, δηλαδή $\binom{n}{t}$. (Στην κατανόηση της τελευταίας πρότασης θα βοηθούσε ίσως, αν λάβουμε υπόψη ότι για να βρούμε όλες τις λέξεις y απόστασης t από μια δεδομένη λέξη x, αρκεί να προσθέσουμε στη x όλες τις λέξεις z βάρους t. Πράγματι, αφού $x + y = z$, είναι και $x + z = y$.) Επομένως, το άθροισμα $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}$ δίνει το πλήθος των λέξεων μήκους n και απόστασης το πολύ t από μια δεδομένη λέξη.

Θεώρημα 4.5 (Το όριο του Hamming)

Αν C ένας κώδικας μήκους n και απόστασης $d = 2t + 1$ ή $d = 2t + 2$, τότε ισχύει αναφορικά με το πλήθος των κωδικών λέξεων $|C|$ και τις παραμέτρους n και t η σχέση:

$$|C|\left(\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}\right)\le 2^n.$$

Απόδειξη

Αν x_1 και x_2 είναι δύο διαφορετικές κωδικές λέξεις, δηλαδή $x_1 \neq x_2$, τότε δεν υπάρχει λέξη y, τέτοια ώστε $d(y, x_1) \le t$ και $d(y, x_2) \le t$. Διότι αν ίσχυε $d(y, x_1) \le t$ και $d(y, x_2)$

1. Αν $0 \le i \le n$, τότε $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ είναι το πλήθος των διαφορετικών μη διατεταγμένων υποσυνόλων με i στοιχεία, τα οποία μπορούν να επιλεγούν από το σύνολο των n στοιχείων.

$\leq t$, τότε $d(x_1, x_2) \leq d(y, x_1) + d(y, x_2) \leq 2t < d$, που δεν μπορεί να ισχύει αφού $d = 2t + 1$ ή $d = 2t + 2$. Επομένως, το υποσύνολο των λέξεων απόστασης t από μια κωδική λέξη δεν έχει κανένα κοινό στοιχείο με όλα τα άλλα υποσύνολα που σχηματίζονται για τις υπόλοιπες κωδικές λέξεις. Αφού λοιπόν το πλήθος των λέξεων σε κάθε υποσύνολο είναι $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}$, το πλήθος των κωδικών λέξεων είναι $|C|$ και το πλήθος των λέξεων μήκους n (κωδικών λέξεων και μη) είναι 2^n, ισχύει

$$|C|\left(\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}\right) \leq 2^n.$$

Το όριο του Hamming είναι ένα άνω όριο και ισχύει ανεξαρτήτως του αν ο κώδικας είναι γραμμικός ή όχι.

Θεώρημα 4.6 (Το όριο του Singleton)

Αν C είναι ένας γραμμικός κώδικας (n, k, d), τότε $d - 1 \leq n - k$.

Απόδειξη

Γνωρίζουμε ήδη ότι ο πίνακας ισοτιμίας H ενός (n, k, d) γραμμικού κώδικα είναι πίνακας διαστάσεων $(n)\times(n–k)$, τέτοιος ώστε κάθε $d–1$ γραμμές του είναι ανεξάρτητες. Επειδή από την άλλη, το μήκος των γραμμών (πλήθος στηλών) είναι $n–k$, δεν μπορούμε να έχουμε περισσότερες ανεξάρτητες γραμμές από $n - k$. Επομένως, $d–1 \leq n–k$ ή $d \leq n–k + 1$.

Παράδειγμα 4.22

Θεωρούμε το γραμμικό κώδικα $(7, k, 3)$, C. Ζητείται το όριο του Hamming και το όριο του Singleton.

Απάντηση

Σχετικά με το όριο του Hamming, έχουμε $|C| \leq \dfrac{2^7}{\left(\binom{7}{0}+\binom{7}{1}\right)} = \dfrac{128}{1+7} = \dfrac{128}{8} = 16$,

δηλαδή $|C| \leq 16$ και επομένως $k \leq 4$ (αφού πρέπει να είναι δύναμη του 2). Από την άλλη, σχετικά με το όριο του Singleton, έχουμε $3 – 1 \leq 7 – k$ ή $k \leq 7 – 3 + 1 = 5$.

Παρατηρούμε στο Παράδειγμα 22 ότι το όριο του Hamming είναι πιο ισχυρό σε σύγκριση με αυτό του Singleton. Ωστόσο, το όριο του Singleton χρησιμοποιείται για τον ορισμό μιας χρήσιμης κατηγορίας κωδίκων. Οι κώδικες αυτοί ορίζονται στη συνέχεια.

Ορισμός 4.4 Κώδικας Μέγιστης Διαχωρίσιμης Απόστασης

Ένας γραμμικός κώδικας (n, k, d) χαρακτηρίζεται **κώδικας μέγιστης διαχωρίσιμης απόστασης (ΜΔΑ)** αν $d = n - k + 1$.

Ορισμός 4.5 Τέλειοι Κώδικες

Ένας γραμμικός κώδικας C μήκους n και περιττής απόστασης $d = 2t + 1$ χαρακτηρίζεται τέλειος κώδικας αν $|C| = \dfrac{2^n}{\left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t}\right)}$.

Δεν υπάρχουν πολλοί τέλειοι κώδικες. Η δυσκολία έγκειται στο ότι ο παρανομαστής της ανωτέρω ισότητας πρέπει να είναι δύναμη του 2, αφού και ο αριθμός |C| είναι δύναμη του 2. Στο Παράδειγμα 22 είδαμε ότι $|C| \le 16 = 2^4$. Επομένως, θα μπορούσε να υπάρξει τέλειος κώδικας μήκους $n = 7$ και απόστασης $d = 3$. Πράγματι, όπως θα δούμε στην Υποενότητα 4.2.5, υπάρχει ο κώδικας Hamming.

Άσκηση αυτοαξιολόγησης 4.14

Θεωρούμε το γραμμικό κώδικα $C = \{00000, 11111\}$, μήκους $n = 5$ και απόστασης $d = 2t + 1 = 5$. Ζητείται να εξεταστεί αν ο κώδικας αυτός είναι τέλειος.

Έχει διατυπωθεί ένα ενδιαφέρον θεώρημα (Θεώρημα 4.7), το οποίο προσδιορίζει τα δυνατά μήκη και τις αποστάσεις τέλειων κωδίκων. Η απόδειξή του είναι αρκετά σύνθετη και για το λόγο αυτό θα παραληφθεί.

ΘΕΩΡΗΜΑ 4.7

Αν C είναι ένας τέλειος κώδικας (μη τετριμμένος, non – trivial) μήκους n και απόστασης $d = 2t + 1$, τότε είτε $n = 23$ και $d = 7$ είτε $n = 2^r - 1$ για κάποιο $r \ge 2$ και $d = 3$.

4.2.5 Κώδικες Hamming

Ας ασχοληθούμε τώρα με μια οικογένεια κωδίκων, οι οποίοι επιτρέπουν εύκολη κωδικοποίηση και αποκωδικοποίηση και τη διόρθωση κάθε μεμονωμένου σφάλμα-

τος (απλού σφάλματος). Οι κώδικες αυτοί προτάθηκαν το 1950 από τον R.W. Hamming.

Ορισμός 4.6 (Κώδικας Hamming)

Ένας κώδικας μήκους $n = 2^r - 1$ ($r \geq 2$) και πίνακα ελέγχου ισοτιμίας H, ο οποίος (H) απαρτίζεται από όλες τις δυνατές μη μηδενικές λέξεις μήκους r, ονομάζεται **κώδικας Hamming μήκους** $2^r - 1$.

Παράδειγμα 4.23

Σύμφωνα με τον ορισμό 4.6, ένας πίνακας ελέγχου ισοτιμίας ενός κώδικα Hamming, μήκους 7 ($r = 3$) θα μπορούσε να είναι ο ακόλουθος:

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Από τον πίνακα H μπορούμε, ακολουθώντας με αντίστροφη σειρά τα βήματα της διαδικασίας σχηματισμού του H από το γεννήτορα πίνακα G σε μορφή ΠΚΔΓ (Αλγόριθμος 1), να σχηματίσουμε ένα γεννήτορα πίνακα G του κώδικα. Έτσι λοιπόν, από τον H μπορούμε να σχηματίσουμε τον ακόλουθο G:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Επομένως, ο κώδικας έχει διάσταση $k = 4$.

Άσκηση αυτοαξιολόγησης 4.15

Θεωρούμε τον κώδικα Hamming μήκους 7 του Παραδείγματος 23. Ζητείται να δειχθεί ότι ο κώδικας αυτός είναι τέλειος και να βρεθεί η απόστασή του και ο ρυθμός πληροφορίας του.

Ο πίνακας ελέγχου ισοτιμίας H ενός κώδικα Hamming έχει όλες τις r γραμμές βάρους 1 (σύμφωνα με τον ορισμό) και επομένως τις r στήλες του γραμμικώς ανεξάρτητες. Συνεπώς, η διάσταση του κώδικα είναι $n - r = 2^r - 1 - r$ και το πλήθος των κωδικών λέξεων 2^{2^r-1-r}. Μπορεί ακόμα να δειχθεί ότι η απόσταση των κωδίκων Hamming είναι $d = 3$ και ότι είναι τέλειοι κώδικες.

Ο σχηματισμός της ΤΔΑ ενός κώδικα Hamming είναι πολύ εύκολος. Αφού ο κώδικας διορθώνει κάθε απλό σφάλμα, όλα τα δυνατά πρότυπα σφάλματος βάρους 1 θα περιέχονται ως οδηγοί των συνομάδων (δηλαδή ο πίνακας ταυτότητας I_{2^r-1}). Το αντίστοιχο σύνδρομο είναι η γραμμή του H που πολλαπλασιάζεται με το μοναδικό «1» του οδηγού (ή πρότυπου σφάλματος).

ΤΔΑ για Κώδικα Hamming	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
00…0	00…0
I_{2^r-1}	H

4.3 Κυκλικοί κώδικες

Σκοπός

Η ενότητα αυτή έχει ως στόχο την εξέταση μιας ειδικής κατηγορίας γραμμικών κωδίκων, των κυκλικών κωδίκων.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει αυτή την ενότητα, θα είστε σε θέση να:

- *ορίσετε τους κυκλικούς κώδικες,*
- *διατυπώσετε δύο θεωρήματα σχετικά με το πολυώνυμο – γεννήτορα κυκλικών κωδίκων,*
- *περιγράψετε την πολυωνυμική κωδικοποίηση,*
- *περιγράψετε την πολυωνυμική αποκωδικοποίηση,*
- *περιγράψετε τη διαδικασία αποκωδικοποίησης των BCH κωδίκων.*

Έννοιες κλειδιά

- *κυκλικοί κώδικες* (*Cyclic Codes*),
- *πολυώνυμο – γεννήτορας* (*Generator Polynomial*),
- *BCH κώδικες.*

Τώρα θα στρέψουμε την προσοχή μας σε μια ειδική κατηγορία γραμμικών κωδίκων, τους κυκλικούς κώδικες. Επειδή στη μελέτη των κυκλικών κωδίκων θα μας διευκολύνει η παράσταση των λέξεων με πολυώνυμα, πριν προχωρήσουμε θα φρεσκάρουμε κάποιες γνώσεις μας για τα πολυώνυμα μιας μεταβλητής. Επίσης, τις γνώσεις μας για τα πεπερασμένα πεδία που θα μας χρησιμεύσουν στη μελέτη των κωδίκων BCH.

Η ενότητα αυτή χωρίζεται σε τέσσερις υποενότητες. Η πρώτη αναφέρεται στην παράσταση λέξεων με πολυώνυμα και στα πεπερασμένα πεδία, η δεύτερη περιέχει εισαγωγικά στοιχεία για τους κυκλικούς κώδικες, η τρίτη είναι αφιερωμένη στην πολυωνυμική κωδικοποίηση και αποκωδικοποίηση και η τέταρτη στους κώδικες BCH.

4.3.1 Παράσταση λέξεων με πολυώνυμα, πεπερασμένα πεδία

Μία λέξη a μήκους n, αποτελούμενη από τα bits $a_0\, a_1\, a_2 \ldots a_{n-1}$, παριστάνεται ως ένα πολυώνυμο βαθμού $(n-1)$ με συντελεστές στο σύνολο $K = \{0, 1\}$: $a_0 + a_1 x + a_2 x^2 +$

$\ldots + a_{n-1}x^{n-1}$. Το σύνολο όλων των πολυωνύμων με συντελεστές στο K συμβολίζεται με $K[x]$. Πολυώνυμα, στοιχεία του $K[x]$, συμβολίζονται με $f(x)$, $p(x)$, $q(x)$,$r(x)$, κ.ο.κ.

Οι πράξεις του πολλαπλασιασμού και της πρόσθεσης μεταξύ πολυωνύμων του $K[x]$ εμφανίζουν μια διαφορά από τις αντίστοιχες πράξεις μεταξύ πολυωνύμων με συντελεστές στο σύνολο των ακεραίων ή πραγματικών αριθμών, αφού οι δυνατοί συντελεστές είναι μόνο το 0 και 1. Η διαφορά έγκειται στο ότι το άθροισμα δύο συντελεστών ίσων με 1 δίνει 0, δηλαδή $1 + 1 = 0$ και επομένως $x^n + x^n = (1 + 1)x^n = 0$.

Αν $f(x), g(x) \in K[x]$, με $g(x) \neq 0$, τότε υπάρχουν τα μοναδικά πολυώνυμα $q(x), r(x) \in K[x]$, τέτοια ώστε $f(x) = q(x) \cdot g(x) + r(x)$, όπου $r(x) = 0$ ή ο βαθμός του είναι μικρότερος του βαθμού του $g(x)$. Το $q(x)$ είναι το πηλίκο και το $r(x)$ είναι το υπόλοιπο. Η διαίρεση πολυωνύμων στο $K[x]$ γίνεται ως συνήθως, εκτός από την ανωτέρω διαφορά στην πρόσθεση των συντελεστών.

Αν $f(x) = q(x) \cdot g(x) + r(x)$, τότε $f(x) \bmod g(x) = r(x)$ ή $f(x) \equiv r(x) \pmod{g(x)}$, δηλαδή το πολυώνυμο $f(x)$ είναι ισότιμο (ή ισοδύναμο) με *το* $r(x) \pmod{g(x)}$. (Στη βιβλιογραφία μπορείτε να βρείτε και το συμβολισμό $f(x) = r(x) \pmod{g(x)}$.) Δύο πολυώνυμα $f(x)$, $h(x)$, τα οποία διαιρούμενα με το ίδιο πολυώνυμο $g(x)$ έχουν το ίδιο υπόλοιπο $r(x)$, χαρακτηρίζονται ισοδύναμα $\bmod g(x)$ και η σχέση ισοτιμίας ή ισοδυναμίας συμβολίζεται με $f(x) \equiv h(x) \pmod{g(x)}$. Η σχέση ισοτιμίας μεταξύ δύο πολυωνύμων διατηρείται και μετά την πρόσθεση ή τον πολλαπλασιασμό με ένα τρίτο πολυώνυμο, δηλαδή αν $f(x) \equiv h(x) \pmod{g(x)}$ τότε $f(x) + p(x) \equiv h(x) + p(x) \pmod{g(x)}$ και $f(x) \cdot p(x) \equiv h(x) \cdot p(x) \pmod{g(x)}$.

Παράδειγμα 4.24

Δίνεται ο κώδικας $C = \{000000, 100100, 010010, 001001, 110110, 101101, 011011, 111111\}$. Ζητείται η παράστασή του με πολυώνυμα.

Απάντηση

Η παράσταση των κωδικών λέξεων με πολυώνυμα περιέχεται στον ακόλουθο πίνακα:

Κωδική λέξη	Πολυώνυμο
000000	0
100100	$1 + x^3$
010010	$x + x^4$
001001	$x^2 + x^5$

110110	$1 + x + x^3 + x^4$
101101	$1 + x^2 + x^3 + x^5$
011011	$x + x^2 + x^4 + x^5$
111111	$1 + x + x^2 + x^3 + x^4 + x^5$

Ένα πολυώνυμο χαρακτηρίζεται μη αναγόμενο(*irreducible*) αν δεν έχει άλλους διαιρέτες εκτός από το 1 και τον εαυτό του. Ένα πολυώνυμο $f(x) \in K[x]$ χαρακτηρίζεται μη αναγόμενο (*irreducible*) στο K, αν δεν έχει άλλους διαιρέτες που να ανήκουν στο $K[x]$ εκτός του εαυτού του και του 1. Διαφορετικά, χαρακτηρίζεται αναγόμενο ή παραγοντοποιήσιμο (*reducible* ή *factorable*). Για παράδειγμα, τα πολυώνυμα x, $1 + x$ και $1 + x + x^2$ είναι μη αναγόμενα, ενώ τα πολυώνυμα x^2, $1 + x^2$ είναι αναγόμενα. (Αναφορικά με το πολυώνυμο $1 + x^2$, προσέχουμε ότι $1 + x^2 = (1 + x)^2 = (1 + x)\cdot(1 + x)$.) Το πολυώνυμο $(1 + x)$ είναι διαιρέτης ενός πολυωνύμου $f(x)$, αν ισχύει $f(1) = 0$, δηλαδή αν το 1 είναι ρίζα του.

Ένα πολυώνυμο βαθμού n, το οποίο είναι μη αναγόμενο (*irreducible*), χαρακτηρίζεται πρωτογενές (*primitive*), αν δεν είναι διαιρέτης του πολυωνύμου $1 + x^m$ για οποιοδήποτε $m < 2^n - 1$. Για παράδειγμα, το πολυώνυμο $1 + x + x^2$ είναι πρωτογενές, αφού είναι μη αναγόμενο και δεν είναι διαιρέτης του $1 + x^m$, όπου $m < 2^n - 1 = 3$.

Πεπερασμένα Πεδία (Finite Fields)

Πολυωνυμικές ισοτιμίες με μέτρο ένα πολυώνυμο $g(x)$ μπορούν να αξιοποιηθούν στην κατασκευή κωδίκων, την κωδικοποίηση και αποκωδικοποίηση. Πιο συγκεκριμένα, η πρόσθεση και ο πολλαπλασιασμός πολυωνύμων mod*ulo* ένα πολυώνυμο $g(x)$ βαθμού n μπορεί να αξιοποιηθεί για την εκτέλεση των αντίστοιχων πράξεων μεταξύ λέξεων μήκους n, δηλαδή λέξεων στο K^n.

Ιδιαίτερα, επιλέγοντας κατάλληλο μέτρο ισοτιμίας, δηλαδή το πολυώνυμο $g(x)$ μη αναγόμενο (*irreducible*) στο $K = \{0,1\}$ και βαθμού n, δημιουργούμε ένα πεπερασμένο πεδίο $GF(2^n)$. Αν δε το μέτρο ισοτιμίας είναι ένα πρωτογενές (*primitive*) πολυώνυμο, τότε οι υπολογισμοί στο $GF(2^n)$ γίνονται πιο εύκολοι. Ας δούμε με τη βοήθεια του ακόλουθου παραδείγματος, πώς οι υπολογισμοί στο πεπερασμένο πεδίο $GF(2^n)$ αντιστοιχούν σε υπολογισμούς μεταξύ λέξεων που απαιτούνται στην κωδικοποίηση και αποκωδικοποίηση.

Παράδειγμα 4.25

Δίνεται ένα πεπερασμένο πεδίο $GF(2^3)$ με μέτρο ισοτιμίας το πολυώνυμο

$g(x)=1+x+x^3$. Να δειχτεί ότι, αν συμβολίσουμε με λ ($\lambda \in K^n$) τη λέξη που παριστάνεται από το πολυώνυμο x, δηλαδή τη λέξη (010), τότε κάθε δύναμη του λ αντιστοιχεί με την ίδια δύναμη του x mod $g(x)$, δηλαδή $\lambda^i \leftrightarrow x^i \pmod{g(x)}$.

Απάντηση

Η παράσταση των λέξεων μήκους 3 ψηφίων, καθώς και η αντιστοιχία των δυνάμεων της λέξης (010) και του x περιέχονται στον ακόλουθο πίνακα.

Κωδική λέξη	Πολυώνυμο mod $1 + x + x^3$	Δύναμη της $\lambda = 010$
000	0	————
100	1	λ^0
010	x	λ^1
001	x^2	λ^2
110	$1 + x \equiv x^3 \bmod (g(x))$	λ^3
011	$x + x^2 \equiv x^4 \bmod (g(x))$	λ^4
111	$1 + x + x^2 \equiv x^5 \bmod(g(x))$	λ^5
101	$1 + x^2 \equiv x^6 \bmod(g(x))$	λ^6

Είδαμε λοιπόν με τη βοήθεια του Παραδείγματος 25, ότι κάθε μη μηδενική λέξη του K^3 μπορεί να παρασταθεί ως δύναμη της λέξης λ. Αυτή η ιδιότητα καθιστά την πράξη του πολλαπλασιασμού στο πεδίο εύκολη. Μια λέξη λ χαρακτηρίζεται πρωτογενής (*primitive*) στο $GF(2^n)$, αν κάθε άλλη μη μηδενική λέξη μπορεί να παρασταθεί ως δύναμη του λ. Σύμφωνα με τα προηγούμενα, εφόσον το μέτρο ισοτιμίας είναι ένα πρωτογενές πολυώνυμο, η λέξη λ μήκους n που αντιστοιχεί στο πολυώνυμο x, δηλαδή η λέξη 010…0 είναι πρωτογενής στο $GF(2^n)$.

4.3.2 Εισαγωγή στους κυκλικούς κώδικες

Η κυκλική μετατόπιση $\kappa(x)$ μιας λέξης x είναι η λέξη y που έχει ως πρώτο ψηφίο της το τελευταίο ψηφίο της x και τα υπόλοιπα ψηφία της προκύπτουν με απλή μετατόπιση κατά μία θέση προς τα δεξιά όλων των ψηφίων της x. Για παράδειγμα, $\kappa(010011) = 101001$ και $\kappa(101001) = 110100$. Με τη βοήθεια της συνάρτησης της κυκλικής μετατόπισης μπορούμε να ορίσουμε τους κυκλικούς κώδικες.

Ορισμός 4.7 Κυκλικοί Κώδικες

Ένας γραμμικός κώδικας C καλείται **κυκλικός** αν η κυκλική μετατόπιση κάθε κωδικής λέξης είναι και αυτή κωδική λέξη.

Παράδειγμα 4.26

Θεωρούμε τον κώδικα $C = \{000, 110, 101, 011\}$ και ζητείται να εξεταστεί αν είναι κυκλικός κώδικας.

Απάντηση

Πρώτα ελέγχουμε αν είναι γραμμικός κώδικας, δηλαδή αν το άθροισμα οποιωνδήποτε δύο ή περισσότερων κωδικών λέξεων του C είναι επίσης κωδική λέξη του C, που στην περίπτωσή μας ισχύει και κατόπιν εξετάζουμε τις κυκλικές μετατοπίσεις όλων των κωδικών λέξεων. Οι κυκλικές μετατοπίσεις είναι οι εξής: $\kappa(000) = 000$, $\kappa(110) = 011$, $\kappa(101) = 110$, $\kappa(011) = 101$. Αφού όλες είναι κωδικές λέξεις, ο κώδικας είναι κυκλικός.

Αναφορικά με τη συνάρτηση κυκλικής μετατόπισης $\kappa(.)$, ισχύει $\kappa(x + y) = \kappa(x) + \kappa(y)$ και $\kappa(\alpha x) = \alpha\kappa(x)$, όπου x, y λέξεις και $a \in K = \{0,1\}$. Επομένως, για να δείξουμε ότι ένας γραμμικός κώδικας C είναι κυκλικός, αρκεί να δείξουμε ότι $\kappa(x) \in C$ για κάθε x που περιέχεται σε μία βάση του C. Έτσι, αν θέλουμε να κατασκευάσουμε έναν κυκλικό κώδικα C μήκους n, αρκεί να σχηματίσουμε το υποσύνολο S αποτελούμενο από μία λέξη x μήκους n και τις $(n – 1)$ κυκλικές της μετατοπίσεις, $S = \{x, \kappa(x), \kappa(\kappa(x)), ...\}$. Αν ο κώδικας C είναι το γραμμικό ανάπτυγμα του S, δηλαδή $C = <S>$, τότε αφού το S περιέχει μια βάση του C, ο C είναι σύμφωνα με τα προηγούμενα κυκλικός κώδικας. Στο Παράδειγμα 26, θα μπορούσαμε να ξεκινήσουμε από τη λέξη $x = 110$ και να σχηματίσουμε το $S = \{110, \kappa(110) = 011, \kappa(011) = 101\}$, του οποίου το γραμμικώς ανεξάρτητο υποσύνολο $\{110, 011\}$ είναι μια βάση του $C = \{000, 110, 101, 011\}$. Η λέξη x που απαρτίζει μαζί με τις $(n – 1)$ κυκλικές της μετατοπίσεις το S, γραμμικό ανάπτυγμα του οποίου είναι ο κώδικας C, ονομάζεται **γεννήτορας** του κυκλικού κώδικα C. Κάθε κώδικας μπορεί να έχει πολλούς γεννήτορες.

Όπως είδαμε στην Υποενότητα 4.3.1, οι κωδικές λέξεις μπορούν να παρασταθούν με πολυώνυμα. Ιδιαίτερα στην περίπτωση των κυκλικών κωδίκων, παρατηρούμε ότι, αν μια λέξη υ παριστάνεται από το πολυώνυμο $\upsilon(x)$, τότε η κυκλική μετατόπιση $\kappa(\upsilon)$ αναπαριστάται από το πολυώνυμο $x \cdot \upsilon(x) \bmod(1 + x^n)$.

Παράδειγμα 4.27

Θεωρούμε την κωδική λέξη $\upsilon = 1101000$ μήκους $n = 7$. Τότε $\upsilon(x) = 1 + x + x^3$ και $x \cdot \upsilon(x) = x + x^2 + x^4$ αναπαριστά τη λέξη 0110100,

$x^2 \cdot \upsilon(x) = x^2 + x^3 + x^5$ αναπαριστά τη λέξη 0011010,

$x^3 \cdot \upsilon(x) = x^3 + x^4 + x^6$ αναπαριστά τη λέξη 0001101,

$x^4 \cdot v(x) = x^4 + x^5 + x^7 \equiv 1 + x^4 + x^5 \bmod (1 + x^7)$ αναπαριστά τη λέξη 1000110,

$x^5 \cdot v(x) = x^5 + x^6 + x^8 \equiv x + x^5 + x^6 \bmod (1 + x^7)$ αναπαριστά τη λέξη 0100011,

$x^6 \cdot v(x) = x^6 + x^7 + x^9 \equiv 1 + x^2 + x^6 \bmod (1 + x^7)$ αναπαριστά τη λέξη 1010001.

Λαμβάνοντας υπόψη τη γενική ισχύ της ισοδυναμίας $1K\ x^n \bmod (1 + x^n)$ και ότι αν $f(x) \equiv h(x) \pmod{g(x)}$ και $s(x) \equiv t(x) \pmod{g(x)}$ τότε $f(x) + p(x) \equiv h(x) + p(x) \pmod{g(x)}$, $f(x) + s(x) \equiv h(x) + t(x) \pmod{g(x)}$ και $f(x) \cdot p(x) \equiv h(x) \cdot p(x) \pmod{g(x)}$, μπορούμε με ευκολία να υπολογίσουμε τις σχέσεις ισοδυναμίας $\bmod(1 + x^n)$. Έτσι, στο Παράδειγμα 27, η σχέση ισοδυναμίας $x^4 + x^5 + x^7 \equiv 1 + x^4 + x^5 \bmod (1 + x^7)$ προκύπτει ξεκινώντας από την ισοδυναμία $1 \equiv x^7 \bmod (1 + x^7)$ και πολλαπλασιάζοντας ή προσθέτοντας κατάλληλα πολυώνυμα, δηλαδή στην περίπτωσή μας προσθέτοντας $x^4 + x^5$ λαμβάνουμε $1 + x^4 + x^5 \equiv x^4 + x^5 + x^7 \bmod (1 + x^7)$.

Πρόταση 4.1

Αν C είναι ένας κυκλικός κώδικας και $v \in C$, τότε για κάθε πολυώνυμο $a(x)$, η λέξη c που αντιστοιχεί στο πολυώνυμο $c(x) = a(x)v(x) \bmod(1 + x^n)$ ανήκει στον κώδικα C.

Απόδειξη

Αν $a(x) = (a_0 + a_1x + a_2\,x^2 + \ldots + a_3\,x^{n-1})$, τότε $c(x) = a(x)v(x) \bmod(1 + x^n) = (a_0 + a_1x + a_2\,x^2 + \ldots + a_{n-1}\,x^{n-1})v(x) \bmod(1 + x^n) = (a_0v(x) + a_1xv(x) + a_2x^2v(x) + \ldots + a_{n-1}\,x^{n-1}\,v(x)) \bmod(1 + x^n)$. Αφού λοιπόν το πολυώνυμο $c(x)$ είναι ένας γραμμικός συνδυασμός του $v(x)$ και των $(n - 1)$ γραμμικών μετατοπίσεών του, δηλαδή περιέχεται στο γραμμικό ανάπτυγμα $< \{v(x), xv(x), x^2v(x), \ldots, x^{n-1}v(x)\} >$, $\bmod(1 + x^n)$, η αντίστοιχη λέξη c περιέχεται στον κώδικα C.

Σε ένα γραμμικό κυκλικό κώδικα C υπάρχει μία μοναδική λέξη γ, της οποίας το αντίστοιχο πολυώνυμο $\gamma(x)$ έχει το μικρότερο βαθμό σε σύγκριση με τα αντίστοιχα πολυώνυμα όλων των άλλων μη μηδενικών λέξεων. Το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε αυτή τη μοναδική, μη μηδενική, λέξη του C καλείται **πολυώνυμο – γεννήτορας**. Ονομάζεται γεννήτορας γιατί για κάθε πολυώνυμο (λέξη) $c(x) \in C$, υπάρχει πολυώνυμο $a(x)$, τέτοιο ώστε $c(x) = a(x)\gamma(x) \bmod(1 + x^n)$, δηλαδή το πολυώνυμο – γεννήτορας διαιρεί όλες τις κωδικές λέξεις $c(x) \in C$.

ΘΕΩΡΗΜΑ 4.8

Αν C είναι ένας κυκλικός κώδικας μήκους n, $\gamma(x)$ το **πολυώνυμο – γεννήτορας** και $n - k$ ο βαθμός του, τότε ισχύουν τα ακόλουθα:

1. Ο κώδικας C είναι διάστασης k,
2. Οι λέξεις που αντιστοιχούν στα πολυώνυμα $\gamma(x)$, $x\gamma(x)$, $x^2\gamma(x)$, ..., $x^{k-1}\gamma(x)$ αποτελούν μια βάση του C και
3. Μία λέξη c ανήκει στον C, αν και μόνον αν το αντίστοιχο πολυώνυμο $c(x)$ είναι το γινόμενο του γεννήτορα $\gamma(x)$ με κάποιο πολυώνυμο $a(x)$, δηλαδή αν $c(x) = a(x)\gamma(x) \bmod(1 + x^n)$.

Παράδειγμα 4.28

Έστω $n = 4$ και $\gamma(x) = 1 + x^2$ το πολυώνυμο γεννήτορας ενός κώδικα C. Ζητείται η διάσταση και μία βάση του C.

Απάντηση

Σύμφωνα με το θεώρημα 4.8, αφού ο βαθμός του $\gamma(x)$ είναι 2, η διάσταση του κώδικα C είναι $k = n - (n - k) = 4 - 2 = 2$ και μια βάση του είναι {1010, 0101}, αφού $\gamma(x) \leftrightarrow 1010$ και $x\gamma(x) = x + x^3 \leftrightarrow 0101$. Το γραμμικό ανάπτυγμα της βάσης είναι ο κώδικας $C = <\{1010, 0101\}> = \{0000, 1010, 0101, 1111\}$.

ΘΕΩΡΗΜΑ 4.9

Το πολυώνυμο $\gamma(x)$ είναι το **πολυώνυμο – γεννήτορας** ενός κυκλικού κώδικα C μήκους n, αν και μόνον αν διαιρεί το μέτρο ισοτιμίας $(1 + x^n)$, δηλαδή αν $(1 + x^n) = q(x)\gamma(x)$.

Πρόταση 4.2

Το πολυώνυμο γεννήτορας $\gamma(x)$ του πιο μικρού (ελάχιστης διάστασης k) κυκλικού κώδικα C μήκους n που περιέχει τη λέξη υ, της οποίας το αντίστοιχο πολυώνυμο είναι το $\upsilon(x)$, είναι ο μέγιστος κοινός διαιρέτης των $\upsilon(x)$ και $(1 + x^n)$, δηλαδή $\gamma(x) = \mu\kappa\delta(\upsilon(x), (1 + x^n))$.

Απόδειξη

Το πολυώνυμο γεννήτορας $\gamma(x)$ διαιρεί τόσο το $\upsilon(x)$ όσο και το $(1 + x^n)$. Επίσης, *το* $\gamma(x)$ περιέχεται στο γραμμικό ανάπτυγμα $< \{\upsilon(x), x\upsilon(x), x^2\upsilon(x), ..., x^{n-1}\upsilon(x)\} >$ και επομένως $\gamma(x) = a(x)\upsilon(x) \bmod(1 + x^n)$ ή $\gamma(x) = a(x)\upsilon(x) + p(x)(1 + x^n)$. Συνεπώς, κάθε κοινός διαιρέτης των $\upsilon(x)$ και $(1 + x^n)$ διαιρεί και το γεννήτορα $\gamma(x)$ και άρα ο $\gamma(x)$ μέγιστου βαθμού (για να προκύψει η ελάχιστη διάσταση k, αφού ο βαθμός του $\gamma(x)$ είναι ίσος με $n - k$) είναι ο μέγιστος κοινός διαιρέτης των $\upsilon(x)$ και $(1 + x^n)$, δηλαδή

$\gamma(x) = \mu\kappa\delta(\upsilon(x), (1 + x^n))$.

Ο Ευκλείδειος Αλγόριθμος χρησιμοποιείται για τον υπολογισμό του μέγιστου κοινού διαιρέτη (μκδ) δύο πολυωνύμων. Εναλλακτικά, το πολυώνυμο – γεννήτορας ενός κυκλικού κώδικα C μήκους n και διάστασης k μπορεί να ευρεθεί με τη βοήθεια ενός γεννήτορα πίνακα του κώδικα C. Πιο συγκεκριμένα, αν πάρουμε ένα γεννήτορα πίνακα (μια βάση) του κώδικα C και τον θέσουμε σε μορφή ΠΚΔΓ, έχοντας όμως ως τελευταίες k στήλες τις στήλες με οδηγούς ή «πρώτα» «1», τότε το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε λέξη (γραμμή) είναι το πολυώνυμο γεννήτορας.

4.3.3 Κωδικοποίηση και αποκωδικοποίηση

Όπως είδαμε στην Ενότητα 4.2, για ένα γραμμικό κώδικα μπορούμε να βρούμε διάφορους γεννήτορες πίνακες. Στην περίπτωση των κυκλικών κωδίκων, ο πιο απλός γεννήτορας πίνακας είναι εκείνος που έχει ως γραμμές τις λέξεις που αντιστοιχούν στο πολυώνυμο – γεννήτορα του κώδικα και τις πρώτες $k - 1$ κυκλικές μετατοπίσεις του.

Παράδειγμα 4.29

Θεωρούμε τον κώδικα $C = \{0000, 1010, 0101, 1111\}$. Ζητείται ένας γεννήτορας πίνακας του C.

Απάντηση

Το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε μη μηδενική λέξη του και επομένως το πολυώνυμο γεννήτορας του C είναι $\gamma(x) = 1 + x^2$. Αφού $k = n - \beta\alpha\theta\mu\acute{o}\varsigma(\gamma(x)) = 4 - 2 = 2$, ο γεννήτορας πίνακας του C έχει ως γραμμές τις λέξεις που αντιστοιχούν στα πολυώνυμα $\gamma(x)$ και $x \cdot \gamma(x)$, δηλαδή $P = \begin{bmatrix} \gamma(x) \\ x\gamma(x) \end{bmatrix} = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$.

Αλγόριθμος 4.4 (Διαδικασία πολυωνυμικής κωδικοποίησης)

Θεωρούμε έναν κυκλικό κώδικα C μήκους n και διάστασης k και το πολυώνυμο – γεννήτορα του C, $\gamma(x)$, του οποίου ο βαθμός είναι $n - k$. Αν τα k δυαδικά ψηφία πληροφορίας $a_0a_1...a_{k-1}$, τα οποία πρόκειται να κωδικοποιηθούν, παριστάνονται με το πολυώνυμο κωδικοποίησης $(a_0 + a_1x + ... + a_{k-1}x^{k-1})$, τότε η κωδικοποίηση συνίσταται στο ακόλουθο βήμα:

Τα ψηφία πληροφορίας $a_0a_1...a_{k-1}$ κωδικοποιούνται ως η λέξη $c_0c_1...c_{n-1}$ που αντιστοιχεί στο πολυώνυμο $c(x) = a(x) \cdot \gamma(x)$.

Παράδειγμα 4.30

Θεωρούμε και πάλι τον κώδικα του Παραδείγματος 29. Ζητείται η κωδικοποίηση των ψηφίων πληροφορίας 01 και 10.

Απάντηση

Οι ακολουθίες των ψηφίων πληροφορίας αντιστοιχούν στα πολυώνυμα 1 και x και το γινόμενό τους με το πολυώνυμο – γεννήτορα $\gamma(x) = 1 + x^2$ είναι $1 + x^2$ και $x + x^3$, αντίστοιχα. Επομένως, οι αντίστοιχες κωδικές λέξεις είναι 1010 και 0101.

Άσκηση αυτοαξιολόγησης 4.16

Θεωρούμε ένα κώδικα C μήκους $n = 7$ με πολυώνυμο – γεννήτορα $\gamma(x) = 1 + x^2 + x^3$. Ζητείται ένας γεννήτορας πίνακας του C, καθώς και η κωδικοποίηση των μηνυμάτων 1110 και 0110.

Ας δούμε τώρα πώς επιτυγχάνεται η αποκωδικοποίηση. Θα μπορούσαμε να ορίσουμε τον πίνακα ελέγχου ισοτιμίας H, του οποίου η γραμμή r_j μήκους $n – k$ αντιστοιχεί στο πολυώνυμο $r_j(x) = x^j \bmod \gamma(x)$, καθώς επίσης και την ΤΔΑ. Έτσι, η αποκωδικοποίηση θα συνίστατο κάθε φορά στον υπολογισμό του συνδρόμου της ληφθείσας λέξης, στην εύρεση του αντίστοιχου προτύπου σφάλματος από την ΤΔΑ και στον υπολογισμό της κωδικής λέξης που μεταδόθηκε (άθροισμα της ληφθείσας λέξης με το πρότυπο σφάλματος).

Όμως, στους κυκλικούς κώδικες μπορούν να αξιοποιηθούν ορισμένες συμμετρίες, οι οποίες επιτρέπουν μια πιο απλή διαδικασία αποκωδικοποίησης που δε βασίζεται στην ΤΔΑ. Πιο συγκεκριμένα, θεωρούμε το πολυώνυμο – γεννήτορα $\gamma(x)$, τη μετάδοση της κωδικής λέξης $c(x)$ μήκους n, τη λήψη της λέξης $l(x)$ και το αντίστοιχο πολυώνυμο σφάλματος $\varepsilon(x) = c(x) + l(x)$. Το σύνδρομο πολυώνυμο $\sigma(x)$, που αντιστοιχεί στο σύνδρομο της ληφθείσας λέξης $l(x)$, ορίζεται ως εξής: $\sigma(x) = l(x) \bmod \gamma(x)$. Αν ο βαθμός του $\gamma(x)$ είναι $n – k$, τότε ο βαθμός του $\sigma(x)$ είναι μικρότερος του $n – k$. Το $\sigma(x)$ αντιστοιχεί σε μία δυαδική λέξη μήκους $n – k$. Το σύνδρομο εξαρτάται μόνο από το σφάλμα, αφού $\sigma(x) = l(x) \bmod \gamma(x) = (c(x) + \varepsilon(x)) \bmod \gamma(x) = a(x)\gamma(x) \bmod \gamma(x) + \varepsilon(x) \bmod \gamma(x) = 0 + \varepsilon(x) \bmod \gamma(x)$. Επομένως, αφού $x^i\,\sigma(x) \equiv x^i\,\varepsilon(x) \bmod \gamma(x)$, είναι προτιμότερο να αξιοποιηθεί αυτή η σχέση ισοδυναμίας από το να αποθηκευτεί η ΤΔΑ.

Αλγόριθμος 4.5 (Διαδικασία πολυωνυμικής αποκωδικοποίησης)

Θεωρούμε έναν κυκλικό κώδικα C μήκους n και διάστασης k και το πολυώνυμο – γεννήτορα του C, $\gamma(x)$, του οποίου ο βαθμός είναι $n - k$. Επίσης, τη ληφθείσα λέξη $l(x)$. Η αποκωδικοποίηση συνίσταται στα ακόλουθα τρία βήματα:

1. Υπολογισμός του συνδρόμου $\sigma(x) = l(x) \bmod \gamma(x)$.
2. Υπολογισμός του $\sigma_i \leftrightarrow \sigma_i(x) = x^i \sigma(x) \bmod \gamma(x)$, για κάθε $i \geq 0$, μέχρι να βρεθεί ένα σ_j του οποίου το βάρος είναι μικρότερο ή ίσο του t, δηλαδή $wt(\sigma_j) \leq t$. (Υπόμνηση: Αν $d = 2t + 1$ είναι η απόσταση του κώδικα, τότε $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.) Τότε το πρότυπο σφάλματος είναι $\varepsilon \leftrightarrow \varepsilon(x) = x^{n-j} \sigma_j(x) \bmod (1 + x^n)$.
3. Υπολογισμός της κωδικής λέξης που μεταδόθηκε $c \leftrightarrow c(x) = l(x) + \varepsilon(x)$.

Παράδειγμα 4.31

Θεωρούμε έναν κώδικα C μήκους $n = 7$ με πολυώνυμο – γεννήτορα $\gamma(x) = 1 + x^2 + x^3$. Επίσης, τη λήψη της λέξης 1111000. Ζητείται η κωδική λέξη που μεταδόθηκε.

Απάντηση

Η διάσταση του κώδικα είναι $k = 4 = n - 3$, η απόσταση είναι $d = n - k = 3$ και $t = 1$. Η ληφθείσα λέξη αντιστοιχεί στο πολυώνυμο $l(x) = 1 + x + x^2 + x^3$ και επομένως $\sigma(x) = l(x) \bmod \gamma(x) = 1 + x + x^2 + x^3 \bmod (1 + x^2 + x^3) = x$, του οποίου ο βαθμός είναι 1, ίσος με t. Επομένως, το πρότυπο σφάλματος είναι $\varepsilon = 0100000$ και η κωδική λέξη που μεταδόθηκε $c = l + \varepsilon = 1111000 + 0100000 = 1011000$.

Άσκηση Αυτοαξιολόγησης 4.17

Θεωρούμε έναν κώδικα C, μήκους $n = 7$, με πολυώνυμο – γεννήτορα $\gamma(x) = 1 + x + x^3$ και τη λήψη των λέξεων 1111000 και 1100101. Ζητούνται οι κωδικές λέξεις που μεταδόθηκαν.

Σύμφωνα με τα προηγούμενα, για την κατασκευή ενός κυκλικού κώδικα C μήκους n και διάστασης k απαιτείται η εύρεση ενός πολυωνύμου – γεννήτορα βαθμού $n - k$, το οποίο πρέπει να διαιρεί το πολυώνυμο $(1 + x^n)$. Επομένως, για να βρούμε όλους τους κυκλικούς κώδικες C μήκους n, αρκεί να βρούμε τους παράγοντες του $(1 + x^n)$ που είναι μη αναγόμενοι (*irreducible*), αφού εξ αυτών μπορούμε να υπολογίσουμε όλα τα πολυώνυμα που διαιρούν το $(1 + x^n)$.

4.3.4 BCH κώδικες

Όπως είδαμε στην Ενότητα 4.3.1, μια λέξη λ χαρακτηρίζεται πρωτογενής (*primitive*) στο $GF(2^r)$, αν κάθε άλλη μη μηδενική λέξη μπορεί να παρασταθεί ως δύναμη του λ (ή ισοδύναμα αν $\lambda^m \neq 1$ για $1 \leq m < 2^r - 1$). Από την άλλη πλευρά, ένα στοιχείο (λέξη) ρ του πεπερασμένου πεδίου χαρακτηρίζεται ρίζα του πολυωνύμου $p(x)$, αν $p(\rho) = 0$. (Με 0 υποδηλώνουμε τη λέξη 00...0 και με 1 τη λέξη 10...0.) Ονομάζουμε **τάξη** ενός μη μηδενικού στοιχείου $\eta \in GF(2^r)$ τον πιο μικρό αριθμό m έτσι ώστε $\eta^m = 1$, δηλαδή το η είναι ρίζα του $(x^m + 1)$. Γνωρίζουμε ότι για κάθε μη μηδενικό $\eta \in GF(2^r)$, η τάξη του η είναι $m \leq 2^r - 1$. Αν η είναι πρωτογενής (*primitive*), τότε $m = 2^r - 1$.

Για κάθε $\eta \in GF(2^r)$ ορίζουμε το ελάχιστο πολυώνυμο του η, το πολυώνυμο με το μικρότερο βαθμό $m_\eta(x) \in K[x]$, το οποίο έχει ως ρίζα το η, δηλαδή $m_\eta(\eta) = 0$. Το ακόλουθο θεώρημα μπορεί να μας βοηθήσει στην προσπάθεια εύρεσης του ελάχιστου πολυωνύμου ενός στοιχείου (λέξης) του $GF(2^r)$.

ΘΕΩΡΗΜΑ 4.10

Αν $\eta \in GF(2^r)$, $\eta \neq 0$ και $m_\eta(x) \in K[x]$ το ελάχιστο πολυώνυμο του η, τότε

1. Το $m_\eta(x)$ είναι μη αναγόμενο (*irreducible*) στο K,
2. Το ελάχιστο πολυώνυμο $m_\eta(x)$ είναι μοναδικό (*unique*),
3. Το $m_\eta(x)$ διαιρεί ένα πολυώνυμο $f(x)$ (είναι παράγων του), αν η είναι ρίζα του $f(x)$, δηλαδή $f(\eta) = 0$,
4. Το $m_\eta(x)$ διαιρεί το $1 + x^{2^r - 1}$ (είναι παράγων του).

Η εύρεση του ελάχιστου πολυωνύμου ενός στοιχείου $\eta \in GF(2^r)$ περιορίζεται στην εύρεση ενός γραμμικού συνδυασμού των διανυσμάτων $\{1, \eta, \eta^2, ..., \eta^r\}$, του οποίου το άθροισμα είναι 0. Γνωρίζουμε ότι υπάρχει ένας τέτοιος συνδυασμός, αφού κάθε σύνολο $r + 1$ διανυσμάτων στο K^r είναι εξαρτημένο.

Αν έχουμε κατασκευάσει ένα πεπερασμένο πεδίο $GF(2^r)$ με τη βοήθεια ενός πρωτογενούς (*primitive*) πολυωνύμου $g(x)$ (δείτε Ενότητα 4.3.1) και αν λ είναι η αντίστοιχη πρωτογενής (*primitive*) λέξη (η λέξη που αντιστοιχεί στο πολυώνυμο x, δηλαδή η λέξη 01...0), τότε το ελάχιστο πολυώνυμο $m_\eta(x)$ συμβολίζεται, συνήθως, με $m_i(x)$, όπου $\eta = \lambda^i$.

Όπως ήδη γνωρίζουμε, $(\eta + \theta)^2 = \eta^2 + \theta^2$ και έτσι αν $f(\eta) = 0$, τότε $f(\eta^2) = (f(\eta)^2) = 0$. Επομένως, αν η είναι ρίζα του πολυωνύμου $f(x)$, τότε και οι άρτιες δυνάμεις του η, δηλαδή $\eta^2, \eta^4, \ldots$, είναι ρίζες του $f(x)$.

ΘΕΩΡΗΜΑ 4.11

Αν $\eta \in GF(2^r)$, $\eta \neq 0$ και $m_\eta(x) \in K[x]$ το ελάχιστο πολυώνυμο του η, τότε $\{\eta, \eta^2, \eta^4, \ldots, \eta^{2^{r-1}}\}$ είναι το σύνολο των ριζών του $m_\eta(x)$. Ο βαθμός του $m_\eta(x)$ είναι $2^r - 1$.

Παράδειγμα 4.32

Θεωρούμε το πεπερασμένο πεδίο $GF(2^3)$ του Παραδείγματος 25, με μέτρο ισοτιμίας το πολυώνυμο $g(x) = 1 + x + x^3$. Να ευρεθεί το ελάχιστο πολυώνυμο του $\eta = \lambda^3$, $\eta \in GF(2^3)$, καθώς και οι ρίζες του ελάχιστου πολυωνύμου $m_\eta(x) = m_3(x)$.

Απάντηση

Για την εύρεση του ελάχιστου πολυωνύμου, αρκεί να βρεθεί ένας γραμμικός συνδυασμός των διανυσμάτων $\{1, \eta, \eta^2, \eta^3\}$, $m_\eta(x) = m_3(x) = (a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3)$, a_0, a_1, a_2, $a_3 \in K = \{0,1\}$, του οποίου το άθροισμα είναι 0.

Επομένως, $m_\eta(x) = m_3(x) = (a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3) = (a_0 + a_1\lambda^3 + a_2\lambda^6 + a_3\lambda^9) = 0$. Αν λάβουμε υπόψη τον πίνακα του Παραδείγματος 25 και το ότι $\lambda^7 = 1$, έχουμε $(a_0 + a_1\,110 + a_2\,101 + a_3\lambda^2) = a_0\,100 + a_1 110 + a_2 101 + a_3 001 = 000$. Δηλαδή, $a_0 + a_1 + a_2 = 0$, $a_1 = 0$ και $a_2 + a_3 = 0$. Συνεπώς, $a_0 = a_2 = a_3 = 1$ και $m_3(x) = 1 + x^2 + x^3$.

Σύμφωνα με το θεώρημα 4.11, το σύνολο των ριζών του $m_3(x)$ είναι το $\{\eta, \eta^2, \eta^4, \ldots, \eta^{2^{r-1}}\} = \{\lambda^3, \lambda^6, \lambda^{12}\} = \{\lambda^3, \lambda^5, \lambda^6\}$. (Προσέχουμε ότι αφού $\lambda^7 = 1$, είναι $\lambda^{12} = \lambda^5$. Επίσης, μπορούμε να επαληθεύσουμε ότι $m_3(\lambda^3) = 1 + (\lambda^3)^2 + (\lambda^3)^3 = 1 + \lambda^6 + \lambda^9 = 1 + \lambda^6 + \lambda^2 = 100 + 101 + 001 = 000$, $m_3(\lambda^5) = 1 + (\lambda^5)^2 + (\lambda^5)^3 = 1 + \lambda^{10} + \lambda^{15} = 1 + \lambda^3 + \lambda^1 = 100 + 110 + 010 = 000$ και $m_3(\lambda^6) = 1 + (\lambda^6)^2 + (\lambda^6)^3 = 1 + \lambda^{12} + \lambda^{18} = 1 + \lambda^5 + \lambda^4 = 100 + 011 + 111 = 000$.)

Οι κώδικες BCH (Bose – Chaudhuri – Hocquengham) συγκροτούν μια σημαντική κατηγορία κυκλικών κωδίκων διόρθωσης πολλαπλών σφαλμάτων. Η σημαντικότητα των κωδίκων αυτών έγκειται στο ότι απλοποιούν κατά πολύ τη διαδικασία αποκωδικοποίησης. Ακόμα, στο ότι αποτελούν μια εκτενή κατηγορία, αφού για κάθε ζεύγος θετικών ακέραιων r και t, $t \leq 2^{r-1} - 1$, υπάρχει ένας κώδικας BCH μήκους $n = 2^r - 1$, ο οποίος διορθώνει t σφάλματα και έχει απόσταση $k \geq n - rt$.

Ο κώδικας BCH μήκους $n = 2^r - 1$ είναι ο κυκλικός κώδικας που δημιουργείται από το πολυώνυμο – γεννήτορα $\gamma(x) = m_\lambda(x) m_{\lambda^3}(x)$, όπου λ είναι πρωτογενές (*primitive*) στοιχείο στο $GF(2^r)$ και $r \geq 4$.

Πρόταση 4.3

Ο κυκλικός κώδικας BCH, μήκους $n = 2^r - 1$ που δημιουργείται από το πολυώνυμο – γεννήτορα $\gamma(x) = m_\lambda(x)m_{\lambda^3}(x)$, όπου λ είναι πρωτογενές (*primitive*) στοιχείο στο $GF(2^r)$, έχει τον ακόλουθο πίνακα ελέγχου ισοτιμίας H:

$$H = \begin{bmatrix} \lambda^0 & \lambda^0 \\ \lambda^1 & \lambda^3 \\ \lambda^2 & \lambda^6 \\ \vdots & \vdots \\ \lambda^i & \lambda^{3i} \\ \vdots & \vdots \\ \lambda^{2^r-2} & \lambda^{3(2^r-2)} \end{bmatrix}.$$

Αφού $\lambda^i \in GF(2^r)$, το λ^i αναπαριστά μια λέξη μήκους r. Επομένως, ο πίνακας H είναι διαστάσεων $(2^r - 1)\times(2r)$. Επίσης, επειδή ο βαθμός του πολυωνύμου – γεννήτορα είναι $2r$, η διάσταση του κώδικα είναι $k = n - 2r = 2^r - 1 - 2r$.

Θεώρημα 4.12

Για κάθε ακέραιο $r \geq 4$ υπάρχει κώδικας BCH, διόρθωσης 2 σφαλμάτων, μήκους $n = 2^r - 1$, διάστασης $k = 2^r - 1 - 2r$ και απόστασης $d = 5$, ο οποίος έχει πολυώνυμο – γεννήτορα το $\gamma(x) = m_\lambda(x)m_{\lambda^3}(x)$.

Αλγόριθμος 4.6 (Διαδικασία αποκωδικοποίησης BCH κωδίκων)

Η διαδικασία αποκωδικοποίησης, στην περίπτωση ΑΑΜΠ και κωδίκων διόρθωσης 2 σφαλμάτων με πολυώνυμο – γεννήτορα $\gamma(x) = m_\lambda(x)m_{\lambda^3}(x)$, διακρίνεται στα ακόλουθα βήματα:

1. Υπολογισμός του συνδρόμου $lH = [\sigma_1, \sigma_3] = [l(\lambda), l(\lambda^3)]$, όπου λ το πρωτογενές (*primitive*) στοιχείο, $\lambda \in GF(2^r)$, H ο πίνακας ελέγχου ισοτιμίας (Πρόταση 4.3) και l η ληφθείσα λέξη.
2. Αν $\sigma_1 = \sigma_3 = 0$, τότε η κωδική λέξη c που μεταδόθηκε είναι η ληφθείσα λέξη l, δηλαδή $c = l$.
3. Αν $\sigma_1 = 0$ και $\sigma_3 \neq 0$, τότε ζητείται επανάληψη της μετάδοσης.
4. Αν $\sigma_1^3 = \sigma_3 = 0$, τότε διορθώνεται ένα απλό σφάλμα στη θέση i, όπου $\sigma_1 = \lambda^i$.

5. Σχηματισμός της εξίσωσης $x^2 + \sigma_1 x + \frac{\sigma_3}{\sigma_1} + \sigma_1^2 = 0$ και εξέταση των ριζών της. Αν η εξίσωση έχει δύο ξεχωριστές ρίζες λ^i και λ^j, τότε διορθώνονται τα λάθη στις θέσεις i και j.
6. Αν η εξίσωση του σημείου 5 δεν έχει δύο ξεχωριστές λύσεις, τότε συμπεραίνεται ότι τα σφάλματα είναι περισσότερα των δύο και ζητείται επανάληψη της μετάδοσης.

Παράδειγμα 4.33

Ζητείται η κατασκευή του πεπερασμένου πεδίου $GF(2^4)$ με μέτρο ισοτιμίας το (πρωτογενές) πολυώνυμο $g(x) = 1 + x + x^4$, τα ελάχιστα πολυώνυμα $m_1(x)$ και $m_3(x)$, ο πίνακας ελέγχου ισοτιμίας H του BCH κώδικα μήκους $n = 2^4 - 1 = 15$ καθώς και η αποκωδικοποίηση της ληφθείσας λέξης l, της οποίας το σύνδρομο είναι $lH = 11010011$.

Απάντηση

Η παράσταση των λέξεων μήκους 4 ψηφίων καθώς και η αντιστοιχία των δυνάμεων της λέξης $\lambda = 0100$ και του x στο $GF(2^4)$ (με πρωτογενές πολυώνυμο $g(x) = 1 + x + x^4$) περιέχονται στον ακόλουθο πίνακα.

Κωδική λέξη	Πολυώνυμο mod $1 + x + x^4$	Δύναμη της $\lambda = 010$
0000	0	——————— –
1000	1	λ^0
0100	x	λ^1
0010	x^2	λ^2
0001	$x^3 \bmod (g(x))$	λ^3
1100	$1 + x \equiv x^4 \bmod (g(x))$	λ^4
0110	$x + x^2 \equiv x^5 \bmod(g(x))$	λ^5
0011	$x^2 + x^3 \equiv x^6 \bmod(g(x))$	λ^6
1101	$1 + x + x^3 \equiv x^7 \bmod(g(x))$	λ^7
1010	$1 + x^2 \equiv x^8 \bmod(g(x))$	λ^8
0101	$x + x^3 \equiv x^9 \bmod(g(x))$	λ^9
1110	$1 + x + x^2 \equiv x^{10} \bmod(g(x))$	λ^{10}
0111	$x + x^2 + x^3 \equiv x^{11} \bmod(g(x))$	λ^{11}
1111	$1 + x + x^2 + x^3 \equiv x^{12} \bmod(g(x))$	λ^{12}
1011	$1 + x^2 + x^3 \equiv x^{13} \bmod(g(x))$	λ^{13}
1001	$1 + x^3 \equiv x^{14} \bmod(g(x))$	λ^{14}

Για να βρούμε το ελάχιστο πολυώνυμο $m_\eta(x) = m_1(x)$, αρκεί να βρούμε ένα γραμμικό συνδυασμό των διανυσμάτων $\{1, \eta, \eta^2, \eta^3, \eta^4\}$, $m_\eta(x) = m_1(x) = (a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3 + a_4\eta^4)$, $a_0, a_1, a_2, a_3, a_4 \in K = \{0,1\}$, του οποίου το άθροισμα είναι 0. Επομένως, για $\eta = \lambda$ έχουμε $(a_0 + a_1\lambda + a_2\lambda^2 + a_3\lambda^3 + a_4\lambda^4) = (a_0 1000 + a_1 0001 + a_2 0010 + a_3 0001 + a_4 1100) = 0000$. Δηλαδή, $a_0 + a_4 = 0$, $a_1 + a_4 = 0$ και $a_2 = a_3 = 0$. Συνεπώς, $a_0 = a_1 = a_4 = 1$ και $m_1(x) = 1 + x + x^4$.

Κατά τον ίδιο τρόπο βρίσκουμε και το ελάχιστο πολυώνυμο $m_\eta(x) = m_3(x)$. Για $\eta = \lambda^3$ έχουμε $(a_0 + a_1\lambda^3 + a_2\lambda^6 + a_3\lambda^9 + a_4\lambda^{12}) = (a_0 1000 + a_1 0001 + a_2 0011 + a_3 0101 + a_4 1111) = 0000$. Δηλαδή, $a_0 + a_4 = 0$, $a_2 + a_4 = 0$, $a_3 + a_4 = 0$, και $a_1 + a_2 + a_3 + a_4 = 0$. Συνεπώς, $a_0 = a_1 = a_2 = a_3 = a_4 = 1$ και $m_3(x) = 1 + x + x^3 + x^3 + x^4$.

Για το σχηματισμό του πίνακα ελέγχου ισοτιμίας, που περιέχεται στον ακόλουθο πίνακα, αξιοποιούμε την Πρόταση 4.3. (Λαμβάνουμε υπόψη ότι $\lambda^{15} = 1$.)

$$H = \begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix} \leftrightarrow \begin{bmatrix} 1 & 1 \\ \lambda & \lambda^3 \\ \lambda^2 & \lambda^6 \\ \lambda^3 & \lambda^9 \\ \lambda^4 & \lambda^{12} \\ \lambda^5 & 1 \\ \lambda^6 & \lambda^3 \\ \lambda^7 & \lambda^6 \\ \lambda^8 & \lambda^9 \\ \lambda^9 & \lambda^{12} \\ \lambda^{10} & 1 \\ \lambda^{11} & \lambda^3 \\ \lambda^{12} & \lambda^6 \\ \lambda^{13} & \lambda^9 \\ \lambda^{14} & \lambda^{12} \end{bmatrix}.$$

Τέλος, για την αποκωδικοποίηση της ληφθείσας λέξης l της οποίας το σύνδρομο είναι $lH = 11010011$, σύμφωνα με τον Αλγόριθμο 6, εξετάζουμε πρώτα τη σχέση μεταξύ των $\sigma_1 = 1101 = \lambda^7$ και $\sigma_3 = 0011 = \lambda^6$. Επειδή ${\sigma_1}^3 = (\lambda^7)^3 = \lambda^{21} = \lambda^6 = \sigma_3$, συμπεραίνουμε την εμφάνιση ενός απλού σφάλματος στη θέση $i = 7$ (αφού $\sigma_1 = \lambda^7$). Δηλαδή το πρότυπο σφάλματος είναι $\varepsilon = 000000100000000$ και η κωδική λέξη που μεταδόθηκε είναι $c = \varepsilon + l$.

Άσκηση αυτοαξιολόγησης 4.18

Δίνεται ο BCH κώδικας του Παραδείγματος 33 και ζητείται η αποκωδικοποίηση της ληφθείσας λέξης l = 110100111010000.

4.4 Άλλοι κώδικες

Στην ενότητα αυτή θα αναφερθούμε μόνο πολύ συνοπτικά στους Reed – Solomon κώδικες, στους κώδικες διόρθωσης καταιγιστικών σφαλμάτων και στους συνελικτικούς κώδικες. Μια πιο εκτενής αναφορά δεν είναι δυνατή εξαιτίας της περιορισμένης έκτασης του κειμένου.

4.4.1 Reed – Solomon κώδικες

Οι Reed – Solomon κώδικες βρίσκουν ευρεία εφαρμογή στην πράξη. Χρησιμοποιήθηκαν τόσο από τη NASA όσο και από την European Space Agency.

Ο δυαδικός Reed – Solomon κώδικας $RS(2^r, \delta)$ είναι ένας κυκλικός κώδικας στο $GF(2^r)$ (ενώ οι BCH κώδικες είναι στο $K = \{0, 1\}$), με πολυώνυμο – γεννήτορα $\gamma(x) = (\lambda^{m+1} + x)(\lambda^{m+2} + x)...(\lambda^{m+\delta-1} + x)$, όπου m κάποιος ακέραιος και λ πρωτογενές (*primitive*) στοιχείο του $GF(2^r)$. Οι BCH κώδικες περιέχονται ως υποκώδικες στους Reed – Solomon κώδικες.

4.4.2 Κώδικες διόρθωσης καταιγιστικών σφαλμάτων

Όπως είδαμε στην Υποενότητα 4.1.1, η δεύτερη παραδοχή στη θεωρία κωδικοποίησης αναφέρεται σε τυχαία, ομοιόμορφα κατανεμημένα, σφάλματα. Στην περίπτωση των κωδίκων διόρθωσης καταιγιστικών σφαλμάτων (ή σφαλμάτων κατά συστάδες), η παραδοχή μας αυτή της ανεξαρτησίας μεταξύ των σφαλμάτων δεν έχει πλέον ισχύ.

Στη βάση της αποκωδικοποίησης μέγιστης πιθανότητας (ΑΜΠ), κατά το σχηματισμό της ΤΔΑ (δείτε Ενότητα 4.2), ο οδηγός μιας συνομάδας είναι η λέξη με το ελάχιστο βάρος. Για τη διόρθωση όμως καταιγισμών σφαλμάτων, παίρνουμε ως οδηγούς των συνομάδων και επομένως ως πρότυπα σφάλματος τις λέξεις ελάχιστου μήκους συστάδας (ή καταιγισμού, δηλαδή πλήθους συνεχόμενων «1» στον οδηγό της συνομάδας). Έτσι, για να έχουμε έναν κώδικα που διορθώνει καταιγισμό (ή συστάδα) h σφαλμάτων, πρέπει όλες οι λέξεις με μήκος καταιγισμού το πολύ h να βρίσκονται σε διαφορετικές συνομάδες.

Μία μέθοδος για τη βελτίωση της ικανότητας διόρθωσης καταιγισμών σφαλμάτων από έναν κώδικα είναι η κατάλληλη διευθέτηση της σειράς με την οποία μεταδίδο-

νται τα ψηφία του κώδικα. Δε μεταδίδονται ολόκληρες κωδικές λέξεις με κάποια σειρά, αλλά ψηφία από διαφορετικές κωδικές λέξεις. Για παράδειγμα, καταρχήν μεταδίδεται το πρώτο ψηφίο από τ κωδικές λέξεις, στη συνέχεια το δεύτερο ψηφίο από τις τ κωδικές λέξεις, κοκ.

Οι κώδικες διόρθωσης καταιγισμού σφαλμάτων βρίσκουν εφαρμογή στους compact disks, για την αντιμετώπιση κυρίως σφαλμάτων που δημιουργούνται από αμυχές (γρατσουνιές).

4.4.3 Συνελικτικοί κώδικες

Οι συνελικτικοί κώδικες[2] (convolutional codes) είναι και αυτοί γραμμικοί. Σε αντίθεση όμως με τους κώδικες που εξετάσαμε στις προηγούμενες ενότητες, τα ψηφία εξόδου του κωδικοποιητή σε μια χρονική στιγμή δεν εξαρτώνται μόνο από τα ψηφία εισόδου αυτής της χρονικής στιγμής αλλά και από προηγούμενα.

Η κωδικοποίηση και η αποκωδικοποίηση στους συνελικτικούς κώδικες μπορεί να πραγματοποιηθεί με τη χρήση απλών ολισθητών καταχωρητών, όπως άλλωστε και η πολυωνυμική κωδικοποίηση και αποκωδικοποίηση (κυκλικοί κώδικες).

[2] Αναφέρονται στη βιβλιογραφία και ως «συγκεραστικοί» ή «αναδρομικοί».

Σύνοψη

Το κεφάλαιο αυτό το αφιερώσαμε στην κωδικοποίηση καναλιού, δηλαδή στη μελέτη μεθόδων για την ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό. Το κύριο αντικείμενο της μελέτης μας αποτέλεσαν οι γραμμικοί κώδικες, καθώς και μία κατηγορία αυτών, οι κυκλικοί κώδικες και ειδικότερα οι BCH κώδικες.

Η αξιοπιστία του καναλιού και το πλήθος των δυνατών διαφορετικών μηνυμάτων, που μπορεί να μεταδοθούν μέσω ενός καναλιού, αποτελούν τα δύο δεδομένα για τη σχεδίαση κωδίκων και πιο συγκεκριμένα για την αντιμετώπιση του προβλήματος της κωδικοποίησης και της αποκωδικοποίησης. Οι λέξεις των κωδίκων αντιστοιχούν στα δυνατά μηνύματα που μεταφέρονται μέσω του καναλιού. Η αποκωδικοποίηση συνίσταται στον προσδιορισμό της κωδικής λέξης (και επομένως και του μηνύματος) που μεταδόθηκε, αφού ενδεχομένως ανιχνευτούν και διορθωθούν σφάλματα στη ληφθείσα λέξη. Συνήθως χρησιμοποιείται η διαδικασία αποκωδικοποίησης μέγιστης πιθανότητας.

Οι γραμμικοί κώδικες είναι μια ευρεία κατηγορία κωδίκων, στην οποία ανήκουν όλοι οι κώδικες που εξετάσαμε στο παρόν κεφάλαιο. Οι γραμμικοί κώδικες έχουν να επιδείξουν σημαντικά πλεονεκτήματα σε σύγκριση με μη γραμμικούς κώδικες. Στους γραμμικούς κώδικες, η κωδικοποίηση βασίζεται στους γεννήτορες πίνακες και η αποκωδικοποίηση στους πίνακες ελέγχου ισοτιμίας. Η τυπική διάταξη αποκωδικοποίησης καθιστά πιο εύκολη τη διαδικασία αποκωδικοποίησης, χωρίς ωστόσο να μειώνει στον επιθυμητό βαθμό τα πρακτικά προβλήματα εφαρμογής στην περίπτωση κωδίκων πολύ μεγάλης διάστασης.

Μεταξύ του μήκους, της απόστασης και της διάστασης κωδίκων ισχύουν ορισμένες σχέσεις. Η ισχύς μιας τέτοιας σχέσης χαρακτηρίζει τους τέλειους κώδικες. Οι κώδικες Hamming αποτελούν ένα παράδειγμα τέλειων κωδίκων.

Οι κυκλικοί κώδικες είναι μια ειδική κατηγορία γραμμικών κωδίκων, που ονομάζονται κυκλικοί, επειδή η μετατόπιση κάθε κωδικής τους λέξης είναι επίσης κωδική λέξη. Οι κυκλικοί κώδικες δεν απαιτούν την αποθήκευση της τυπικής διάταξης αποκωδικοποίησης αλλά μόνον του πολυωνύμου – γεννήτορα, απλοποιώντας έτσι τη διαδικασία αποκωδικοποίησης. Οι κυκλικοί κώδικες BCH συγκροτούν μια σημαντική κατηγορία κωδίκων διόρθωσης πολλαπλών σφαλμάτων, επειδή απλοποιούν ακόμα περισσότερο τη διαδικασία αποκωδικοποίησης.

Βιβλιογραφία

ΠΡΟΤΑΣΕΙΣ ΜΕΛΕΤΗΣ

Στο βιβλίο των G. A. Jones, J. M. Jones, «Information and Coding Theory», Springer Verlag, 2000, στο 2ο μέρος του, μπορείτε να βρείτε παραδείγματα κατασκευής διαφόρων κωδίκων ελέγχου σφάλματος, όπως των κωδίκων Hamming, Hadamard, Golay και Reed – Muller. Το βιβλίο αυτό απευθύνεται σε φοιτητές μαθηματικής κατεύθυνσης, της επιστήμης των ηλεκτρονικών και της επιστήμης των υπολογιστών ή πληροφορικής και προϋποθέτει μόνο βασικές γνώσεις Θεωρίας Πιθανοτήτων και Γραμμικής Άλγεβρας.

Στο βιβλίο των D. Hoffman, D. Leonard, C. Lindner, K. Phelps, C. Rodger, J. Wall «Coding Theory», Marcel Dekker, Inc., 1991, περιγράφονται πολλοί κώδικες, στους οποίους συμπεριλαμβάνονται οι κώδικες Hamming, κυκλικοί, BCH, Golay, Reed – Solomon, συνελικτικοί, και Reed – Muller.

Στο βιβλίο του V. Snaith «Groups, Rings and Galois Theory», World Scientific, 1998, μπορείτε να βρείτε περιγραφές των πεπερασμένων πεδίων και ειδικότερα των πεδίων Galois, που αποτελούν τη μαθηματική βάση διαφόρων κωδίκων. Απευθύνεται όμως περισσότερο σε φοιτητές μαθηματικής κατεύθυνσης και λιγότερο πληροφορικής ή μηχανικής.

Στο μεταφρασμένο στα ελληνικά βιβλίο του K. Sam Shanmugam «Ψηφιακά & Αναλογικά Συστήματα Επικοινωνίας» μπορείτε να βρείτε το Κεφάλαιο 9 αφιερωμένο κυρίως στους γραμμικούς κώδικες μπλοκ, τους κυκλικούς κώδικες και τους συνελικτικούς (συγκεραστικούς) κώδικες. Ελληνική Έκδοση Γ. Πνευματικού, Αθήνα, Μετάφραση – Επιμέλεια Κ. Καρούμπαλου. Αγγλόφωνη Έκδοση, John Wiley & Sons, Inc., 1979.

Ξενόγλωσση βιβλιογραφία

[1] [BAY1997] J. Baylis, «Error Correcting Codes: A Mathematical Introduction», CRC Press, 1997.

[2] [HAM1950] R. W. Hamming, «Error Detecting and Error Correcting Codes», The Bell System Technical Journal, Vol. XXVI, April, 1950, pp. 147 – 160.

[3] [HIL1986] R. Hill, «A First Course in Coding Theory», Oxford University Press, 1986.

[4] [LID1984] R. Lidl and H. Niederreiter, «Finite Fields», Cambridge University PressBasic Me, 1984.

[5] [LIN1983] S. Lin and D. J. Costello, «Error Control Coding: Fundametntals and Applications», Prentice – Hall, 1983.

[6] [McE1987] R. J. McEliece, «Finite Fields for Computer Scientists and Engineers» Kluwer Academic Publishers, 1987.

[7] [PLE1982] V. Pless, «Introduction to the Theory of Error – Correcting Codes», John Wiley & Sons, 1982.

[8] [ROM1996] S. Roman, «Introduction to Coding and Information Theory», Springer Verlag, 1996.

ΚΕΦΑΛΑΙΟ 5

Κρυπτογραφία και Θεωρία Πληροφορίας

Σκοπός

Το κεφάλαιο αυτό έχει ως σκοπό την εξέταση θεμάτων Κρυπτογραφίας και ιδιαίτερα θεμάτων ασφαλείας κρυπτογραφικών συστημάτων από τη σκοπιά της Θεωρίας Πληροφορίας και της Θεωρίας Πολυπλοκότητας.

Προσδοκώμενα αποτελέσματα

Όταν θα έχετε μελετήσει το κεφάλαιο αυτό, θα είστε σε θέση να:

- *διακρίνετε μεταξύ Κρυπτογραφίας και Κρυπτανάλυσης,*
- *διακρίνετε μεταξύ συμμετρικών και ασύμμετρων κρυπτογραφικών συστημάτων,*
- *αναφέρετε τύπους κρυπταναλυτικών επιθέσεων,*
- *περιγράψετε τις τεχνικές της μονοαλφαβητικής και της πολυαλφαβητικής αντικατάστασης,*
- *περιγράψετε τον κωδικοποιητή του Vernam (one – time pad),*
- *περιγράψετε το ασύμμετρο κρυπτογραφικό σύστημα RSA,*
- *εξηγήσετε την έννοια των απόλυτα ασφαλών κρυπτογραφικών συστημάτων από τη σκοπιά της Θεωρίας Πληροφορίας,*
- *υπολογίσετε το μήκος του κρυπτογραφημένου κειμένου, το οποίο είναι απαραίτητο, για να οδηγεί η αποκρυπτογράφηση σε ένα και μοναδικό εύλογο καθαρό κείμενο,*
- *αποδείξετε την απόλυτη ασφάλεια του κρυπτογραφικού συστήματος 'one – time pad',*
- *εξηγήσετε την έννοια των υπολογιστικά ασφαλών κρυπτογραφικών συστημάτων από τη σκοπιά της Θεωρίας Πολυπλοκότητας,*
- *αναφέρετε δύο δύσκολα προβλήματα, τα οποία αποτελούν τη βάση μονόδρομων συναρτήσεων και κατ' επέκταση και κρυπτογραφικών συστημάτων,*
- *περιγράψετε το ασύμμετρο κρυπτογραφικό σύστημα ElGamal.*

Έννοιες κλειδιά

- *Κρυπτογραφία, Κρυπτανάλυση, Κρυπτολογία,*
- *συμμετρικά και ασύμμετρα κρυπτογραφικά σύστημα,*
- *τύποι κρυπταναλυτικών επιθέσεων,*
- *σύστημα 'μπλοκ μιας χρήσης' (one –*

time pad),

- *ασφάλεια κρυπτογραφικών συστημάτων*,
- *απόλυτα ασφαλή κρυπτογραφικά συστήματα*,
- *εντροπία μηνύματος, κρυπτογράμματος και κλειδιού*,
- *αμοιβαία πληροφορία μεταξύ καθαρού και κρυπτογραφημένου μηνύματος*,
- *μοναδιαία απόσταση κρυπτογραφημένου μηνύματος*,
- *αβεβαιότητα του κλειδιού και του μηνύματος*,
- *υπολογιστικά ασφαλή κρυπτογραφικά συστήματα*,
- *μονόδρομοι συναρτήσεις* (*one – way functions*),
- *συναρτήσεις κρυφής διόδου* (*trapdoor functions*),
- *γεννήτριες ψευδοτυχαίων ακολουθιών*

Εισαγωγικές παρατηρήσεις

Το κεφάλαιο αυτό έχει κυρίως ως στόχο την ανάδειξη της έννοιας της ασφαλείας κρυπτογραφικών συστημάτων, στην οποία βρίσκουν εφαρμογή έννοιες της Θεωρίας Πληροφορίας και της Θεωρίας Πολυπλοκότητας. Μια εμπεριστατωμένη εισαγωγή στο αντικείμενο της Κρυπτογραφίας θα απαιτούσε πολύ μεγαλύτερη έκταση κειμένου, η οποία όμως δεν είναι διαθέσιμη στο παρόν βιβλίο. Η επιλογή της ύλης λοιπόν που παρατίθεται σε αυτό το κεφάλαιο έγινε με γνώμονα την καλύτερη περιγραφή του χαρακτηριστικού της ασφαλείας κρυπτογραφικών συστημάτων. Αν και ο βασικός λόγος για τη συμπερίληψη του κεφαλαίου ήταν η εφαρμογή εννοιών της Θεωρίας Πληροφορίας στην Κρυπτογραφία, κρίθηκε αναγκαία και η αναφορά στη Θεωρία Πολυπλοκότητας, αφού σχεδόν το σύνολο των σύγχρονων κρυπτογραφικών συστημάτων βασίζεται σε υπολογιστικά δύσκολα προβλήματα.

Πιο συγκεκριμένα, το κεφάλαιο αυτό αποτελείται από δύο ενότητες. Στην πρώτη ενότητα θα μας απασχολήσουν έννοιες κρυπτογραφίας και κρυπτανάλυσης, τύποι κρυπταναλυτικών επιθέσεων, καθώς και ορισμένες κλασικές κρυπτογραφικές τεχνικές και το σύγχρονο ασύμμετρο κρυπτογραφικό σύστημα RSA. Στη δεύτερη ενότητα θα εξετάσουμε ζητήματα ασφαλείας κρυπτογραφικών συστημάτων πρώτα από τη σκοπιά της Θεωρίας Πληροφορίας και στη συνέχεια από τη σκοπιά της Θεωρίας Πολυπλοκότητας.

5.1 Εισαγωγή στην Κρυπτογραφία

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων. Μαζί με τον κλάδο της **Κρυπτανάλυσης**, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της **Κρυπτολογίας**. Κρυπτολογία είναι, επομένως, η επιστήμη της απόκρυψης από τη μία πλευρά και, από την άλλη, της αποκάλυψης του περιεχομένου κωδικοποιημένων μηνυμάτων ή δεδομένων.

Στις ακόλουθες τρεις υποενότητες θα αναφερθούμε πολύ συνοπτικά σε θέματα κρυπτογραφίας, κρυπτανάλυσης και κρυπτογραφικών αλγορίθμων.

5.1.1 Κρυπτογραφία

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων, τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιο τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται **κρυπτογράφηση** και η αντίστροφή της **αποκρυπτογράφηση**.

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται **κρυπτογραφικός αλγόριθμος** ή **κρυπτογραφικό σύστημα.** (Σε μερικές περιπτώσεις, στη βιβλιογραφία, διαφοροποιείται μεταξύ αλγόριθμου και συστήματος, όπου ως σύστημα εννοείται η πραγματοποίηση του αλγόριθμου.) Ο κρυπτογραφικός αλγόριθμος καλείται και **κωδικοποιητής** (cipher). Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται **κρυπτογραφικά πρωτόκολλα**. Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, κρυπτογραφικά **κλειδιά (keys),** η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση.

Υπάρχουν δύο κατηγορίες κρυπτογραφικών αλγορίθμων και επομένως και συστημάτων: **οι συμμετρικοί και οι ασύμμετροι** αλγόριθμοι. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση και για το λόγο αυτό καλούνται, επίσης, **αλγόριθμοι μυστικού κλειδιού** ή **αλγόριθμοι μονού κλειδιού**. Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν ένα ζεύγος κρυπτογραφικών κλειδιών, το **δημόσιο κλειδί** για την κρυπτογράφηση και το **ιδιωτικό κλειδί** για την αποκρυπτογράφηση. Έτσι, ο κάθε χρήστης ενός ασύμμετρου συστήματος έχει δύο κλειδιά, το δημόσιο και το ιδιωτικό. Το πρώτο το κοινοποιεί σε όλους που επιθυμούν να επικοινωνήσουν μαζί του. Όμως, δεν είναι δυνατό από το δημό-

σιο να υπολογίσουμε το ιδιωτικό κλειδί ενός χρήστη. Οι ασύμμετροι αλγόριθμοι ονομάζονται και **αλγόριθμοι δημόσιου κλειδιού**.

Οι συμμετρικοί αλγόριθμοι χωρίζονται, με τη σειρά τους, σε δύο κατηγορίες: στους κωδικοποιητές ροής (**stream ciphers)** και στους κωδικοποιητές τμημάτων (**block ciphers**). Οι πρώτοι εφαρμόζονται σε κάθε bit ή χαρακτήρα ενός μηνύματος, ενώ οι δεύτεροι σε τμήματα (blocks) του μηνύματος σταθερού μήκους. Συνήθως, το μήκος αυτό ανέρχεται σε 64 ή 128 bits.

Στο κεφάλαιο αυτό, θα συμβολίζουμε το καθαρό (ή μη κρυπτογραφημένο) μήνυμα ή κείμενο (plaintext) με M, το κρυπτογραφημένο μήνυμα ή κείμενο (ciphertext) με C και το κλειδί με K.

5.1.2 Κρυπτανάλυση

Η Κρυπτανάλυση έχει ως σκοπό την ανάπτυξη τεχνικών και μεθόδων για την παραβίαση κρυπτογραφημένων μηνυμάτων ή κρυπτογραφικών συστημάτων. Μία επιτυχής κρυπτανάλυση μπορεί να αποκαλύψει το καθαρό από το κρυπτογραφημένο μήνυμα. Μπορεί, ακόμα, να εντοπίσει αδυναμίες σε ένα κρυπτογραφικό σύστημα, οι οποίες οδηγούν τελικά στα παραπάνω αποτελέσματα. Αντίθετα, η Κρυπτογραφία επιδιώκει την ανάπτυξη ισχυρών κρυπτογραφικών συστημάτων, τα οποία να είναι σε θέση να ανταπεξέλθουν σε απόπειρες παραβίασης από τους κρυπταναλυτές.

Μία επιχειρούμενη κρυπτανάλυση χαρακτηρίζεται και **επίθεση (attack)**. Οι κρυπταναλυτές μπορεί να έχουν στη διάθεσή τους κρυπτογραφημένα μηνύματα, τα αντίστοιχα καθαρά μηνύματα, τους αλγόριθμους κρυπτογράφησης που χρησιμοποιήθηκαν, στατιστικά εργαλεία και τεχνικές, κτλ. Επίσης, υποθέτουμε ότι ο κρυπταναλυτής γνωρίζει τις λεπτομέρειες του κρυπτογραφικού αλγόριθμου, αν και αυτό δε συμβαίνει πάντα στην πράξη. Η υπόθεση αυτή είναι εύλογη, γιατί, όπως αναφέρεται συχνά στη βιβλιογραφία, αν η ασφάλεια των κρυπτογραφικών συστημάτων στηρίζεται στη μυστικότητά τους, τότε αυτή δεν μπορεί να είναι επαρκής. Αν στηρίζεται εκτός των άλλων και στη μυστικότητα των αλγορίθμων, κάτι το οποίο δεν συνιστάται, τότε πρόκειται κατά κανόνα για συστήματα με περιορισμένο πεδίο εφαρμογής.

Οι τύποι κρυπταναλυτικών επιθέσεων διαφοροποιούνται σύμφωνα με το τι έχει στη διάθεσή του ο επιτιθέμενος. Όλοι οι τύποι επιθέσεων προϋποθέτουν ότι ο κρυπταναλυτής γνωρίζει πλήρως τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Στη συνέχεια, παρατίθενται βασικοί τύποι επιθέσεων, οι οποίοι αποτελούν τη βάση αξιολόγησης κρυπτογραφικών συστημάτων.

- Επίθεση κρυπτογραφημένου κειμένου (Ciphertext – only attack). Ο κρυπταναλυ-

τής έχει στη διάθεσή του αρκετά κρυπτογραφημένα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, μηνύματα και επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει το καθαρό από το κρυπτογραφημένο μήνυμα.

- Επίθεση γνωστού καθαρού κειμένου (Known – plaintext attack). Ο κρυπταναλυτής έχει στη διάθεσή του όχι μόνο κρυπτογραφημένα μηνύματα αλλά και τα αντίστοιχα καθαρά μηνύματα και επιδιώκει να προσδιορίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων ή κάποιον αλγόριθμο που θα του επιτρέπει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο καθαρό που πλέον δεν γνωρίζει.
- Επίθεση επιλεγμένων καθαρών κειμένων (Chosen – plaintext attack). Οι κρυπταναλυτές έχουν στη διάθεσή τους τα κρυπτογράμματα επιλεγμένων από τους ίδιους καθαρών μηνυμάτων. Ο στόχος είναι να βρεθεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων, ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, τα οποία κρυπτογραφούνται με το ίδιο κλειδί.
- Επίθεση επιλεγμένων κρυπτογραφημένων κειμένων (Chosen – ciphertext attack). Οι κρυπταναλυτές μπορούν να επιλέξουν διάφορα κρυπτογραφημένα μηνύματα και διαθέτουν ακόμα τα αντίστοιχα καθαρά μηνύματα, επιδιώκουν δε τον προσδιορισμό του κλειδιού που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση.

5.1.3 Κρυπτογραφικοί αλγόριθμοι

Όπως αναφέρθηκε προηγουμένως, τα κρυπτογραφικά συστήματα που χρησιμοποιούνται για την προστασία του περιεχομένου μηνυμάτων διακρίνονται στα συμμετρικά και τα ασύμμετρα. Στους κρυπτογραφικούς αλγόριθμους συγκαταλέγονται ωστόσο και αλγόριθμοι που χρησιμοποιούνται σε σχήματα ψηφιακών υπογραφών (digital signature schemes), σε συναρτήσεις κατακερματισμού (one – way hash functions), για την ανταλλαγή κλειδιών (key exchange mechanisms) κ.ά. Στην υποενότητα αυτή θα αναφερθούμε πολύ συνοπτικά σε ορισμένους κλασικούς αλγόριθμους, στο μοναδικό απόλυτα ασφαλές σύστημα «one – time pad» καθώς και στο σύγχρονο ασύμμετρο σύστημα RSA, έτσι ώστε να είναι δυνατή, στην επόμενη ενότητα, η εξέταση του χαρακτηριστικού της ασφαλείας κρυπτογραφικών συστημάτων.

Αν και οι περισσότερες «κλασικές» κρυπτογραφικές τεχνικές και μέθοδοι θεωρούνται πολύ αδύνατες για να εφαρμοστούν στην πράξη, εντούτοις οι βασικές τους αρχές

μπορούν να αναγνωριστούν ως συστατικά στοιχεία των πλέον εξελιγμένων συμμετρικών και ασύμμετρων κρυπτογραφικών αλγορίθμων. Η κλασική κρυπτογραφία διακρίνει τις τεχνικές της αντικατάστασης και της μετάθεσης.

Η μέθοδος του Καίσαρα αποτελεί μια από τις πιο παλιές τεχνικές μονοαλφαβητικής αντικατάστασης. Σύμφωνα με τη μέθοδο αυτή, κάθε γράμμα του απλού μηνύματος αντικαθίσταται από το γράμμα που βρίσκεται τρεις θέσεις δεξιά του στο αλφάβητο. Δηλαδή το «Α» αντικαθίσταται από το «Δ», το «Β» από το «Ε», το «Γ» από το «Ζ», κοκ. Η μέθοδος του Καίσαρα μπορεί να γενικευθεί, αν στη θέση του 3 (κλειδιού) χρησιμοποιήσουμε έναν οποιοδήποτε αριθμό k, μικρότερο του 24 και μεγαλύτερο του μηδενός. Με τη βοήθεια μιας αντιστοιχίας των γραμμάτων του αλφαβήτου με αριθμούς από το 1 έως το 24, μπορούμε να εκφράσουμε την κρυπτογράφηση και την αποκρυπτογράφηση της μονοαλφαβητικής αντικατάστασης με τις ακόλουθες σχέσεις (όπου M συμβολίζει ένα οποιοδήποτε γράμμα του μηνύματος και C το σύμβολο – γράμμα από το οποίο αντικαθίσταται):

Κρυπτογράφηση: $C = (M + k) \bmod 24$ (για το ελληνικό αλφάβητο)

Αποκρυπτογράφηση: $M = (C - k) \bmod 24$

Αν το αποτέλεσμα της αφαίρεσης $(C - k)$ είναι αρνητικός αριθμός, προσθέτουμε σε αυτόν το 24 και έτσι παίρνουμε τον επιθυμητό μη αρνητικό αριθμό. Στην περίπτωση του αγγλικού αλφαβήτου αντί του mod 24 χρησιμοποιούμε mod 26. Αν χρησιμοποιήσουμε για την κρυπτογράφηση τη σχέση $C = (aM + k) \bmod 26$ (αγγλικό αλφάβητο), όπου a μεγαλύτερος ή ίσος του 1 και σχετικά πρώτος του 26, έχουμε τον επονομαζόμενο Affine Κωδικοποιητή. Η αποκρυπτογράφηση επιτυγχάνεται με τη σχέση $M = b(C - k) \bmod 26$, όπου b είναι ο αντίστροφος του a mod26, δηλαδή $ab = m26 + 1$ (m οποιοσδήποτε ακέραιος).

Στην πολυαλφαβητική αντικατάσταση, το κλειδί δεν είναι μόνο ένας αριθμός k, αλλά μια ακολουθία αριθμών $k_1k_2...k_n$. Ο αριθμός k_1 χρησιμοποιείται για την αντικατάσταση του 1ου, του $(n + 1)$ – οστού, του $(2n + 1)$ – οστού γράμματος του μηνύματος κοκ., ο αριθμός k_2 χρησιμοποιείται για την αντικατάσταση του 2ου, του $(n + 2)$ – οστού, του $(2n + 2)$ – οστού γράμματος του μηνύματος κοκ. και ο αριθμός k_n για την αντικατάσταση του n – οστού, του $2n$ – οστού γράμματος του μηνύματος κοκ.

Ο κωδικοποιητής του Vernam

Ο κωδικοποιητής του Vernam βασίζεται στην πολυαλφαβητική αντικατάσταση και προβλέπει μήκος κλειδιού ίσο με αυτό του μηνύματος καθώς και τυχαία δημιουργία των αριθμών (ή αντίστοιχων γραμμάτων ή συμβόλων) του κλειδιού. Η μέθοδος αυτή

κρυπτογράφησης λέγεται **μπλοκ μιας χρήσης (one – time pad)**. Η ανακάλυψη του Vernam χρησιμοποιούσε διάτρητες ταινίες χαρτιού με τυχαίους αριθμούς, τους οποίους συνδύαζε με τα γράμματα του καθαρού μηνύματος που τροφοδοτούσε σε συσκευή τηλετύπου. Η ακολουθία των τυχαίων αριθμών ήταν μη επαναλαμβανόμενη και κάθε ταινία χρησιμοποιείτο μία φορά.

Ο δυαδικός κωδικοποιητής του Vernam χρησιμοποιεί, αντί γραμμάτων και αριθμών, δυαδικά ψηφία. Δηλαδή τόσο οι τυχαίοι αριθμοί που απαρτίζουν το κλειδί όσο και το μήνυμα είναι σε δυαδική μορφή. Για τον υπολογισμό του κρυπτογραφημένου, δυαδικού, μηνύματος, κάθε bit αυτού συσχετίζεται με το αντίστοιχο bit του κλειδιού μέσω της πράξης XOR, το αποτέλεσμα δε αυτής είναι το bit του κρυπτογραφημένου μηνύματος. Στη συνέχεια μπορούμε να δούμε ένα σχετικό παράδειγμα. Τόσο ο αποστολέας όσο και ο παραλήπτης έχουν την ίδια τυχαία ακολουθία δυαδικών ψηφίων. Ο αποστολέας υπολογίζει το κρυπτογραφημένο μήνυμα και το αποστέλλει στον παραλήπτη. Ο παραλήπτης, από την πλευρά του, από την τυχαία ακολουθία και το κρυπτογραφημένο μήνυμα υπολογίζει το καθαρό μήνυμα (το αποτέλεσμα της πράξης XOR).

Παράδειγμα 5.1

$\oplus$ = πράξη *XOR*

Αποστολέας (κλειδί $\oplus$ μήνυμα = κρυπτόγραμμα)	
Κλειδί:	1 1 0 1 0 0 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 0 1
Μήνυμα:	0 0 1 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0
Κρυπτόγραμμα:	1 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 1 1 1 0 0 1 1
Παραλήπτης (κλειδί $\oplus$ κρυπτόγραμμα = μήνυμα)	
Κλειδί:	1 1 0 1 0 0 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 0 1
Κρυπτόγραμμα:	1 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 1 1 1 0 0 1 1
Μήνυμα:	0 0 1 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0

Το ασύμμετρο κρυπτογραφικό σύστημα RSA

Ας δούμε τώρα και το ευρέως χρησιμοποιούμενο, σύγχρονο κρυπτογραφικό σύστημα, το RSA, το οποίο βασίζεται στο δύσκολο πρόβλημα της ανάλυσης πολύ μεγάλων αριθμών σε γινόμενο πρώτων παραγόντων και το οποίο εντάσσεται στην κατηγορία των ασύμμετρων συστημάτων. Πιο συγκεκριμένα, στον αλγόριθμο RSA χρη-

σιμοποιούνται υπολογισμοί μεγάλων δυνάμεων ως προς μέτρο ισοτιμίας ένα φυσικό αριθμό n, ο οποίος είναι το γινόμενο δύο πολύ μεγάλων πρώτων αριθμών. Για τον λόγο αυτό, πρώτα επιλέγονται δύο πολύ μεγάλοι πρώτοι αριθμοί p και q και στη συνέχεια υπολογίζεται το γινόμενό τους, $n = p\,q$. Στη συνέχεια επιλέγονται το δημόσιο e και το μυστικό κλειδί d. Ο αριθμός e επιλέγεται έτσι ώστε να είναι σχετικά πρώτος ως προς το $\varphi(n)$ και να ικανοποιεί την ακόλουθη σχέση: $3 < e < \varphi(n) = (p - 1)\,(q - 1)$. (Υπόμνηση: $\varphi(n)$ είναι η συνάρτηση του Euler, η οποία υποδηλώνει το πλήθος των φυσικών, μικρότερων ή ίσων του n, οι οποίοι είναι σχετικά πρώτοι με αυτόν.) Αναφορικά με το φυσικό αριθμό d, αυτός είναι αντίστροφος του e, δηλαδή προσδιορίζεται έτσι ώστε να πληροί την ακόλουθη σχέση ισοτιμίας: $d\,e \equiv 1 \bmod \varphi(n)$ *ή* $d \equiv e^{-1} \bmod \varphi(n)$.

Η κρυπτογράφηση ενός μηνύματος M, το οποίο χωρίζεται σε τμήματα $M_1, M_2, \ldots, M_k$ που αναπαριστώνται από αριθμούς μικρότερους του n καθώς και η αποκρυπτογράφηση επιτυγχάνονται ως εξής:

$$C_1 = M_1^{\,e} \bmod n,\ C_2 = M_2^{\,e} \bmod n,\ \ldots,\ C_k = M_k^{\,e} \bmod n,$$

$$M_1 = C_1^{\,d} \bmod n = M_1^{\,ed} \bmod n,\ M_2 = C_2^{\,d} \bmod n,\ \ldots,\ M_k = C_k^{\,d} \bmod n.$$

Ο αποστολέας του μηνύματος χρησιμοποιεί για την κρυπτογράφηση το δημόσιο κλειδί του παραλήπτη, το οποίο αποτελείται από τους αριθμούς e και n, δηλαδή $\{e, n\}$. Ο παραλήπτης αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα με το ιδιωτικό του κλειδί, το οποίο αποτελείται από τους αριθμούς d και n, δηλαδή $\{d, n\}$.

Η ασφάλεια του RSA στηρίζεται στο ότι είναι μη εφικτό να υπολογιστεί το ιδιωτικό από το δημόσιο κλειδί. Για την εύρεση του d, από τα δημοσιοποιημένα e και n, απαιτείται η ανάλυση του n σε γινόμενο πρώτων παραγόντων, δηλαδή στα p και q. Η ανάλυση πολύ μεγάλων αριθμών, μήκους μεγαλύτερου των 1024 bits, σε γινόμενο πρώτων παραγόντων είναι ανέφικτη σε πρακτικά χρήσιμους χρόνους με τις τωρινές δυνατότητες υπολογιστικών πόρων (δείτε Ενότητα 5.2.3).

Παράδειγμα 5.2

Επιλέγουμε δύο πρώτους αριθμούς $p = 5$ και $q = 11$ και υπολογίζουμε το γινόμενό τους $n = p\,q = 55$. (Η επιλογή των μικρών αριθμών έγινε για λόγους απλοποίησης του παραδείγματος. Στην πράξη, οι αριθμοί αυτοί είναι, όπως ήδη είπαμε, πάρα πολύ μεγάλοι.) Επίσης, υπολογίζουμε το γινόμενο $(p - 1)(q - 1) = 40$. Επιλέγοντας $e = 7$, υπολογίζουμε τον αντίστροφό του, $d = 23$ (ως προς τον αριθμό 40). Υποθέτουμε τώρα ότι θέλουμε να κρυπτογραφήσουμε το $M = 2$. Το κρυπτογραφημένο μήνυμα υπολογίζεται ως εξής: $C = 2^7 \pmod{55} = 128 \pmod{55} = 18$. Από το κρυπτογρα-

φημένο μήνυμα και το ιδιωτικό κλειδί {23, 55} υπολογίζεται το καθαρό μήνυμα: $M = 18^{23} \pmod{55} = (((18^2 \bmod 55)^2 \bmod 55)^2 \bmod 55)^2 ((18^2 \bmod 55)^2 \bmod 55) (18^2 \bmod 55) (18 \bmod 55) = (26) (36) (49) (18) \bmod 55 = 2$.

5.2 Ασφάλεια κρυπτογραφικών συστημάτων

Η ασφάλεια των κρυπτογραφικών συστημάτων, δηλαδή η ανθεκτικότητά τους σε απόπειρες παραβίασης, είναι ένα από τα πρώτα ερωτήματα που θέτουμε πριν αποφασίσουμε να τα χρησιμοποιήσουμε σε πρακτικές εφαρμογές. Τα κρυπτογραφικά συστήματα εμφανίζουν διάφορα επίπεδα ασφαλείας, ανάλογα με το πόσο δύσκολα παραβιάζονται. Όλοι οι αλγόριθμοι – πλην του one – time – pad που είδαμε στην Υποενότητα 5.1.3 – είναι θεωρητικά **παραβιάσιμοι**, δεδομένης επαρκούς υπολογιστικής ισχύος και αποθηκευτικής χωρητικότητας. Μερικοί όμως αλγόριθμοι απαιτούν εκατομμύρια χρόνια ή απεριόριστους υπολογιστικούς πόρους για να παραβιαστούν.

Αυτοί οι αλγόριθμοι είναι θεωρητικά παραβιάσιμοι, αλλά όχι πρακτικά. Ένας αλγόριθμος που δεν παραβιάζεται στην πράξη θεωρείται **ασφαλής (secure)**.

Ένας αλγόριθμος είναι **απόλυτα ασφαλής (unconditionally secure)**, αν, ανεξαρτήτως του μεγέθους του κρυπτογραφημένου μηνύματος, των υπολογιστικών πόρων και του χρόνου που μπορεί να διαθέτει ο κρυπταναλυτής, δεν υπάρχει δυνατότητα να παραβιαστεί, δηλαδή να αποκαλυφθεί το καθαρό μήνυμα. Τα **one – time pads**, όπως θα αποδείξουμε στην Υποενότητα 5.2.1, δεν μπορούν να παραβιασθούν, ακόμα και αν ο κρυπταναλυτής έχει στη διάθεσή του άπειρους υπολογιστικούς και αποθηκευτικούς πόρους.

Ωστόσο, η μοντέρνα κρυπτογραφία ασχολείται κυρίως με κρυπτογραφικά συστήματα, τα οποία δεν μπορούν να παραβιαστούν με τις δεδομένες υπολογιστικές δυνατότητες. Ένας αλγόριθμος λέγεται **υπολογιστικά ασφαλής (computationally secure)**, ή **δυνατός (strong)**, αν είναι αδύνατη η παραβίασή του με τους διαθέσιμους (τωρινούς ή μελλοντικούς) πόρους.

Με τη βοήθεια της Θεωρίας Πληροφορίας, μπορούμε να δώσουμε κάποιες απαντήσεις στο ερώτημα της ασφαλείας κρυπτογραφικών συστημάτων, καθώς επίσης και στο ερώτημα του «πόσο σημαντικό είναι το μήκος του κρυπτογραφημένου μηνύματος» το οποίο έχει στη διάθεσή του ένας κρυπταναλυτής για την παραβίασή του, θεωρώντας ωστόσο ότι ο κρυπταναλυτής έχει στη διάθεσή του απεριόριστους υπολογιστικούς και αποθηκευτικούς πόρους.

Από την άλλη πλευρά, στη σύγχρονη Κρυπτογραφία θεωρούμε κατά κανόνα ότι ο κρυπταναλυτής έχει στη διάθεσή του μόνο περιορισμένους πόρους και ανατρέχουμε πλέον στη Θεωρία Πολυπλοκότητας για να απαντήσουμε στο ερώτημα της ασφα-

λείας κρυπτογραφικών συστημάτων, αφού αυτά βασίζονται κυρίως σε υπολογιστικά δύσκολα προβλήματα.

Η ενότητα χωρίζεται σε τέσσερις υποενότητες. Στις δύο πρώτες υποενότητες θα εξετάσουμε θέματα ασφαλείας κρυπτογραφικών συστημάτων από τη σκοπιά της Θεωρίας Πληροφορίας, εστιάζοντας στη δεύτερη υποενότητα και στην έννοια της μοναδιαίας απόστασης κρυπτογραφημένων μηνυμάτων. Στην τρίτη και την τέταρτη υποενότητα, θα μας απασχολήσουν θέματα ασφαλείας κρυπτογραφικών συστημάτων από την οπτική της Θεωρίας Πολυπλοκότητας, όπου θα ναφερθούμε συνοπτικά και στο ασύμμετρο κρυπτογραφικό σύστημα του ElGamal.

5.2.1 Μέτρα πληροφορίας και ασφάλεια κρυπτογραφικών συστημάτων

Ας αναφερθούμε πρώτα στις παραδοχές που κάνουμε σ' αυτή την υποενότητα. Θεωρούμε τη χρήση διαφορετικού κλειδιού για κάθε μήνυμα που κρυπτογραφείται. Το κλειδί (K), το καθαρό μήνυμα (M), καθώς και το κρυπτογραφημένο μήνυμα (ή κρυπτόγραμμα, C) θεωρούνται τυχαίες ποσότητες. Αυτά επιλέγονται ή δημιουργούνται και αποστέλλονται από τον αποστολέα με κάποια πιθανότητα. Η μέση ποσότητα πληροφορίας (μέση πληροφορία ή εντροπία ή μέσο πληροφορικό περιεχόμενο) του καθαρού, του κρυπτογραφημένου μηνύματος και του κλειδιού δίνονται από τις σχέσεις (5.1), όπου m_i, c_i και k_j είναι τα δυνατά μηνύματα, τα δυνατά κρυπτογράμματα και τα δυνατά κλειδιά, αντίστοιχα.

$$
\begin{aligned}
H(M) &= -\sum_{i=1}^{n} p(m_i)\log p(m_i),\\
H(C) &= -\sum_{i=1}^{n} p(c_i)\log p(c_i),\\
H(K) &= -\sum_{j=1}^{m} p(k_j)\log p(k_j).
\end{aligned}
\tag{5.1}
$$

Η πιθανότητα αποστολής του μηνύματος m_i είναι η $p(m_i)$, *του* κρυπτογράμματος c_i η $p(c_i)$ και η πιθανότητα επιλογής και χρησιμοποίησης του κλειδιού k_j είναι η $p(k_j)$. Το πλήθος των δυνατών μηνυμάτων και των κρυπτογραμμάτων είναι n και το πλήθος των δυνατών κλειδιών είναι m. Εδώ υποθέτουμε ότι τα κρυπτογραφικά συστήματα οδηγούν σε κρυπτογραφημένα μηνύματα του ιδίου μήκους με τα καθαρά μηνύματα. Για παράδειγμα, αν υποθέσουμε ότι τα καθαρά και τα κρυπτογραφημένα μηνύματα σχηματίζονται από 56 γράμματα του αγγλικού αλφάβητου, τότε το πλήθος των δυνατών μηνυμάτων και των κρυπτογραμμάτων είναι $n = 26^{56}$. Τέλος, υποθέτουμε

πως η δημιουργία ενός μηνύματος από τον αποστολέα δεν εξαρτάται από άλλα προηγούμενα μηνύματα.

Εκτός των μέτρων πληροφορίας της σχέσης (5.1), τα οποία αναφέρονται ξεχωριστά στα μηνύματα, κρυπτογράμματα και τα κλειδιά, μπορούμε να υπολογίσουμε και μέτρα πληροφορίας, τα οποία συσχετίζουν δύο εξ αυτών ή και όλα. Πιο συγκεκριμένα, μπορούμε να υπολογίσουμε την υπό συνθήκη ποσότητα πληροφορίας του κλειδιού, με δεδομένο το κρυπτογραφημένο μήνυμα και την υπό συνθήκη ποσότητα πληροφορίας του κλειδιού με δεδομένο και το καθαρό και το κρυπτογραφημένο μήνυμα, καθώς επίσης και την υπό συνθήκη ποσότητα πληροφορίας του καθαρού μηνύματος δεδομένου του κρυπτογραφημένου μηνύματος. Αυτές οι υπό συνθήκη ποσότητες πληροφορίας δίνονται από τις ακόλουθες σχέσεις:

$$
\begin{aligned}
H(K/C) &= -\sum_{j=1}^{m}\sum_{i=1}^{n} p(k_j,c_i)\log p(k_j/c_i),\\
H(K/M,C) &= -\sum_{\mathrm{l}=1}^{\mathrm{m}}\sum_{j=1}^{n}\sum_{i=1}^{n} p(k_l,m_j,c_i)\log p(k_l/m_j,c_i),\\
H(M/C) &= -\sum_{j=1}^{n}\sum_{i=1}^{n} p(m_j,c_i)\log p(m_j/c_i).
\end{aligned}
\tag{5.2}
$$

Κατά τον ίδιο τρόπο, $H(M/C,K)$ είναι η ποσότητα πληροφορίας του καθαρού μηνύματος δεδομένου του αντίστοιχου κρυπτογράμματος και του κλειδιού, δηλαδή με γνωστό το κρυπτογραφημένο μήνυμα και το κλειδί. Ωστόσο, αφού από το κρυπτογραφημένο μήνυμα και το κλειδί μπορούμε να υπολογίσουμε το καθαρό μήνυμα (με τη βοήθεια του κρυπτογραφικού αλγορίθμου που θεωρούμε γνωστό), δηλαδή δεν υφίσταται αβεβαιότητα ως προς το καθαρό μήνυμα, ισχύει η σχέση $H(M/C,K) = 0$.

Η αμοιβαία πληροφορία μεταξύ του καθαρού και του κρυπτογραφημένου μηνύματος δίνεται από τη σχέση:

$$I(M;C) = H(M) - H(M/C) = H(C) - H(C/M). \tag{5.3}$$

Μεταξύ των $H(K/C)$, $H(M/C)$ *και* $H(K/M,C)$ που ορίζονται στην (5.2), ισχύει η ακόλουθη σχέση:

$$H(K/M,C) = H(K/C) - H(M/C). \tag{5.4}$$

Για την απόδειξη αυτής της σχέσης μπορούμε να χρησιμοποιήσουμε τις συνδυασμένες ποσότητες πληροφορίας του καθαρού και του κρυπτογραφημένου μηνύματος, του κρυπτογραφημένου μηνύματος και του κλειδιού και του καθαρού, του κρυ-

πτογραφημένου μηνύματος και του κλειδιού, οι οποίες παρατίθενται στη συνέχεια.

$$\begin{aligned} &H(M,C) = H(M/C) + H(C), \\ &H(C,K) = H(C/K) + H(K), \\ &H(M,C,K) = H(M/C,K) + H(C,K) = H(K/M,C) + H(M,C). \end{aligned} \tag{5.5}$$

Από τις σχέσεις (5.5) οδηγούμαστε στη σχέση (5.6), από την οποία λαμβάνουμε την (5.4) αφού $H(M/C,K) = 0$.

$$H(M/C,K) + H(K/C) = H(K/M,C) + H(M/C). \tag{5.6}$$

Ακόμα, αναφορικά με την αμοιβαία πληροφορία μεταξύ του καθαρού και του κρυπτογραφημένου μηνύματος ισχύει:

$$I(M;C) \geq H(M) - H(K). \tag{5.7}$$

Η (5.7) αποδεικνύεται με τον ακόλουθο τρόπο. Από την (5.4) έχουμε την ανισότητα $H(K/C) \geq H(M/C)$, αφού η ποσότητα πληροφορίας $H(K/M,C)$ είναι μη αρνητική. Επίσης, ισχύει $H(K) \geq H(K/C)$ και επομένως $H(K) \geq H(M/C)$. Αντικαθιστώντας την τελευταία ανισότητα στην (5.3) λαμβάνουμε την (5.7).

Παρατηρούμε από τη σχέση (5.4) ότι η ποσότητα πληροφορίας $H(K/M,C)$ αυξάνεται όταν αυξάνεται η $H(K/C)$ και μειώνεται η $H(M/C)$. Η αύξηση της $H(K/M,C)$, δηλαδή η αύξηση της αβεβαιότητας ως προς το κλειδί, είναι ιδιαίτερα επιθυμητή, αφού συνεπάγεται αύξηση της δυσκολίας εξαγωγής του κλειδιού από τον κρυπταναλυτή, αν έχει στη διάθεσή του τόσο το καθαρό όσο και το κρυπτογραφημένο μήνυμα. Από την άλλη πλευρά, χαμηλές τιμές της $H(M/C)$ *δεν* είναι επιθυμητές, αφού υποδηλώνουν μικρή δυσκολία εξαγωγής του καθαρού μηνύματος από το κρυπτογραφημένο μήνυμα, κάτι που θέλουμε να αποφύγουμε. Επομένως, όσο πιο μεγάλη είναι η ποσότητα πληροφορίας του κλειδιού με δεδομένο το καθαρό και το κρυπτογραφημένο μήνυμα, τόσο πιο μικρή είναι η ποσότητα πληροφορίας του καθαρού μηνύματος με δεδομένο το κρυπτογραφημένο μήνυμα και αντίστροφα.

Από τη σχέση (5.7) συνάγεται πως, όταν το πληροφορικό περιεχόμενο του κλειδιού είναι μικρό, τότε η αμοιβαία πληροφορία μεταξύ του καθαρού και του κρυπτογραφημένου μηνύματος είναι μεγάλη, κάτι που πρέπει να αποφεύγεται. Υπενθυμίζουμε ότι η αμοιβαία πληροφορία δύο τυχαίων μεταβλητών ερμηνεύεται ως ένα μέτρο της εξάρτησης μεταξύ τους. Αν το πληροφορικό περιεχόμενο του κλειδιού είναι μικρότερο από το πληροφορικό περιεχόμενο του μηνύματος, η αμοιβαία πληροφορία είναι μεγαλύτερη του μηδενός. Από την άλλη πλευρά, μηδενική αμοιβαία πληροφορία μπορεί να επιτευχθεί μόνο αν η ποσότητα πληροφορίας του κλειδιού είναι μεγαλύ-

τερη ή ίση αυτής του καθαρού μηνύματος. Τότε από το κρυπτογραφημένο μήνυμα δεν μπορεί να εξαχθεί οποιαδήποτε πληροφορία για το καθαρό μήνυμα. Ωστόσο, η απαίτηση για πληροφορικό περιεχόμενο του κλειδιού τουλάχιστον ίσο με αυτό του καθαρού μηνύματος συνεπάγεται ισότητα των μηκών τους, θεωρώντας τις πιθανότητες επιλογής τους, επίσης, ίσες. Ο κωδικοποιητής (αλγόριθμος) one – time pad, ο οποίος πληροί αυτήν την απαίτηση, θα μελετηθεί στο Παράδειγμα 3 και από τη σκοπιά της Θεωρίας Πληροφορίας.

Επιδιώκεται, λοιπόν, η ελαχιστοποίηση της αμοιβαίας πληροφορίας μεταξύ του καθαρού και του κρυπτογραφημένου μηνύματος, η οποία ορίζεται από την (5.3). Εφόσον το κρυπτογραφημένο μήνυμα δεν αποκαλύπτει καμιά πληροφορία για το καθαρό μήνυμα, η $H(M/C)$ είναι ίση με $H(M)$. Αλλά τότε, $I(M;C) = 0$. Ένα **κρυπτογραφικό σύστημα**, το οποίο χαρακτηρίζεται από αυτήν την τελευταία σχέση, καλείται **απόλυτα ασφαλές**.

Παράδειγμα 5.3

Ο κωδικοποιητής του Vernam (one – time pad) που είδαμε στην Υποενότητα 5.1.3 χαρακτηρίζεται ως απόλυτα ασφαλής. Ας προσπαθήσουμε στη συνέχεια να το δείξουμε με τη βοήθεια της Θεωρίας Πληροφορίας.

Απάντηση

Αρκεί να αποδείξουμε γι' αυτό το κρυπτογραφικό σύστημα την ισχύ της σχέσης $I(M;C) = 0$. Υποθέτουμε πως τα μηνύματα είναι στην αγγλική γλώσσα και ότι χρησιμοποιούμε μόνο τα 26 γράμματα του αγγλικού αλφάβητου, χωρίς το κόμμα ή το διάστημα ή τα σημεία στίξης κτλ. Επίσης, υποθέτουμε πως κάθε μήνυμα αποτελείται από N γράμματα. Για την κρυπτογράφηση ενός μηνύματος χρησιμοποιείται μία τυχαία ακολουθία γραμμάτων του ιδίου μήκους με το μήνυμα, το κλειδί, από το ίδιο αλφάβητο.

Η πιθανότητα για την επιλογή κάθε γράμματος, κατά το σχηματισμό του κλειδιού, είναι 1/26 και, ακόμα, η επιλογή κάθε γράμματος είναι ανεξάρτητη από τις άλλες επιλογές.

Είναι φανερό ότι υπάρχουν 26^N διαφορετικά δυνατά κλειδιά και επομένως η ποσότητα πληροφορίας του κλειδιού (πληροφορικό περιεχόμενο) είναι $H(K) = N\log 26$.

Αφού η πιθανότητα επιλογής ενός κλειδιού είναι ίση με $1/26^N$ και το κλειδί καθορίζει το αποτέλεσμα της κρυπτογράφησης, η πιθανότητα ενός οποιουδήποτε συνδυασμού καθαρού και κρυπτογραφημένου μηνύματος, C και M, είναι ίση με $1/26^N$ και επομένως ισχύει $p(C/M) = 1/26^N$. Επίσης, η πιθανότητα κάθε κρυπτογράμματος, $p(C)$, είναι ίση με $1/26^N$, αφού το πλήθος των δυνατών κρυπτογραφημένων μηνυμάτων είναι 26^N.

Από την ισότητα των πιθανοτήτων έχουμε την ισότητα των ποσοτήτων πληροφορίας $H(C)$ και $H(C/M)$. Έτσι, $I(M;C) = H(C) - H(C/M) = 0$ και, επομένως, το κρυπτογραφικό σύστημα είναι απόλυτα ασφαλές.

Άσκηση Αυτοαξιολόγησης 5.1

Θεωρούμε ένα τηλεφωνικό δίκτυο αποτελούμενο από M τηλεφωνικές παροχές με αριθμούς μήκους m bits. Θεωρούμε ότι το πλήθος των τηλεφωνικών παροχών είναι ίσο με το πλήθος των δυνατών τηλεφωνικών αριθμών, δηλαδή $M = 2^m$. Επίσης, θεωρούμε ότι κάθε ζεύγος τηλεφωνικών παροχών που επιθυμεί απόρρητη επικοινωνία έχει συμφωνήσει στη χρήση κάποιου κλειδιού K, το οποίο έχει μήκος n bits. Το κλειδί K είναι επίσης γνωστό σε έναν εξυπηρετητή ασφαλείας του τηλεφωνικού δικτύου, ο οποίος δημιουργεί και διανέμει, όταν του ζητηθεί, στους ενδιαφερόμενους συνδρομητές τυχαίες δυαδικές ακολουθίες που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των μηνυμάτων. Όταν το κλειδί K σχηματισθεί από τον αποστολέα ενός μηνύματος M_i και από τον παραλήπτη ενός κρυπτογραφημένου μηνύματος C_i, τότε ο εξυπηρετητής στέλνει σ' αυτούς κάθε φορά μια μοναδική τυχαία ακολουθία R_i. Ο αποστολέας συσχετίζει το μήνυμα και την τυχαία ακολουθία με την πράξη της αποκλειστικής διάζευξης $C_i = M_i \oplus R_i$ και αποστέλλει το κρυπτογραφημένο μήνυμα C_i. Ο παραλήπτης από την πλευρά του, αφού λάβει το κρυπτογραφημένο μήνυμα και την ίδια τυχαία ακολουθία R_i από τον εξυπηρετητή, έχοντας καλέσει τον αριθμό K (δηλαδή το κλειδί του ζεύγους αποστολέα – παραλήπτη που επιθυμεί απόρρητη επικοινωνία), αποκρυπτογραφεί εφαρμόζοντας και πάλι την πράξη της αποκλειστικής διάζευξης $M_i = C_i \oplus R_i$.

Για το τηλεφωνικό αυτό δίκτυο ζητείται να εξετάσουμε το ακόλουθο πρόβλημα: Υποθέτοντας ότι ένας εισβολέας κατόρθωσε να υποκλέψει το κρυπτογραφημένο μήνυμα C_i, μπορεί να χαρακτηρισθεί το σύστημά μας απόλυτα ασφαλές εφόσον ο εισβολέας δεν έχει υποκλέψει και την τυχαία ακολουθία που χρησιμοποιήθηκε για την κρυπτογράφηση; (Υπόδειξη: Αφού ο εισβολέας δεν γνωρίζει το κλειδί K, δεν μπορεί να ζητήσει από τον εξυπηρετητή την τυχαία ακολουθία. Ωστόσο, μπορεί να στείλει στον εξυπηρετητή διάφορα κλειδιά ελπίζοντας να κάνει τη σωστή επιλογή.)

5.2.2 Η έννοια της μοναδιαίας απόστασης

Ας ασχοληθούμε τώρα με το ερώτημα του «πόσο σημαντικό είναι το μήκος του κρυπτογράμματος» το οποίο έχει στη διάθεσή του ο κρυπταναλυτής κατά την προσπάθειά του να ανακτήσει το καθαρό από το κρυπτογραφημένο μήνυμα. Το κρυπτογραφημένο μήνυμα εμφανίζει κατά τη μονοαλφαβητική ή και την πολυαλφαβητική

αντικατάσταση στατιστικά χαρακτηριστικά, τα οποία επιτρέπουν στον κρυπταναλυτή να επιχειρήσει στατιστική κρυπτανάλυση. Ασφαλώς, όσο πιο μεγάλο το μήκος του κρυπτογραφημένου μηνύματος τόσο πιο ακριβή είναι τα στατιστικά μεγέθη που υπολογίζει ο κρυπταναλυτής.

Με άλλα λόγια, όσο πιο μεγάλο το μήκος του κρυπτογραφημένου μηνύματος που έχει στη διάθεσή του τόσο πιο πολλές και οι πιθανότητες του κρυπταναλυτή να ανακτήσει το καθαρό από το κρυπτογραφημένο μήνυμα. Αυτό ισχύει γενικότερα για κάθε αλγόριθμο κρυπτογράφησης και μπορούμε να το δούμε με τη βοήθεια εννοιών της Θεωρίας Πληροφορίας. Την υπό συνθήκη ποσότητα πληροφορίας του κλειδιού με δεδομένο το κρυπτογραφημένο μήνυμα, $H(K/C_L)$, την ονομάζουμε **αβεβαιότητα του κλειδιού**. Η αβεβαιότητα του κλειδιού είναι αντιστρόφως ανάλογη του μήκους του κρυπτογραφημένου μηνύματος L και μπορεί ακόμα να γίνει και μηδέν αν μπορεί το κλειδί να προσδιορισθεί από το κρυπτογραφημένο μήνυμα. Αν η αμοιβαία ποσότητα πληροφορίας μεταξύ του κλειδιού και του κρυπτογραφημένου μηνύματος είναι μηδέν τότε η αβεβαιότητα του κλειδιού παίρνει τη μέγιστη τιμή της, η οποία ισούται με την εντροπία του κλειδιού, $H(K)$.

Αντίστοιχα, η υπό συνθήκη ποσότητα πληροφορίας του μηνύματος με δεδομένο το κρυπτόγραμμα, $H(M_L/C_L)$, που ονομάζουμε **αβεβαιότητα του μηνύματος**, μειώνεται όταν αυξάνεται το μήκος L (για μήκος $L > L_0$). Ωστόσο, αν το μήκος του μηνύματος είναι μικρό, τότε μικρή είναι και η αβεβαιότητα του μηνύματος, αφού το πλήθος των δυνατών μηνυμάτων είναι μικρό. Στην τελευταία περίπτωση, αυξανομένου του μήκους αυξάνεται και η αβεβαιότητα του μηνύματος, όσο ισχύει $L_0 > L$.

Επίσης, η υπό συνθήκη ποσότητα πληροφορίας του κλειδιού με δεδομένα τόσο το καθαρό όσο και το κρυπτογραφημένο μήνυμα, $H(K/M_L,C_L)$, είναι αντιστρόφως ανάλογη του μήκους του μηνύματος. Η μείωση αυτής της ποσότητας πληροφορίας είναι ταχύτερη σε σύγκριση με τη μείωση της αβεβαιότητας του κλειδιού, αυξανομένου του μήκους L.

ΘΕΩΡΗΜΑ 5.1

Η αβεβαιότητα του κλειδιού είναι μεγαλύτερη ή ίση της εντροπίας του κλειδιού μειωμένης κατά τον πλεονασμό του καθαρού μηνύματος

$$H(K/C_L) \geq H(K) - R_L. \tag{5.8}$$

Απόδειξη

Μεταξύ της συνδυασμένης ποσότητας πληροφορίας, των μέσων πληροφοριών και των υπό συνθήκη ποσοτήτων πληροφορίας δύο τυχαίων μεταβλητών και επομένως

του κλειδιού και του κρυπτογραφημένου κειμένου ισχύει η ακόλουθη σχέση:

$$H(K,C_L) = H(C_L/K) + H(K) = H(K/C_L) + H(C_L).$$

Λαμβάνοντας ακόμα υπόψη πως κάθε κρυπτογραφημένο αντιστοιχεί σ' ένα καθαρό μήνυμα, οι πιθανότητες εμφάνισής τους είναι ίσες και επομένως $H(K,C_L) = H(K,M_L)$. Έτσι έχουμε την ακόλουθη σχέση, υποθέτοντας στατιστική ανεξαρτησία μεταξύ του κλειδιού και του μηνύματος (δηλαδή $H(M_L/K) = H(M_L)$):

$$H(K/C_L) = H(K,C_L) - H(C_L) = H(K, M_L) - H(C_L) = H(K) + H(M_L) - H(C_L). \quad (5.9)$$

Αν θεωρήσουμε ότι τα καθαρά ή κρυπτογραφημένα μηνύματα συνίστανται από ακολουθίες q διαφορετικών συμβόλων (το αλφάβητο πηγής έχει q σύμβολα), τότε το πλήθος των δυνατών μηνυμάτων μήκους L συμβόλων ανέρχεται σε q^L. Η εντροπία των καθαρών ή κρυπτογραφημένων μηνυμάτων παίρνει τη μέγιστη τιμή της, αν τα μηνύματα είναι ισοπίθανα. Τότε ισχύει $H(C_L) = H(M_L) = L\log q$. Επομένως, στη γενική περίπτωση (όταν δηλαδή τα μηνύματα δεν είναι ισοπίθανα) ισχύει

$$H(M_L) = H(C_L) \leq L\log q.$$

Με τη βοήθεια της προηγούμενης σχέσης, η (5.9) μπορεί να γραφεί ως ανισότητα, όπου η ποσότητα $R_L = L\log q - H(M_L)$ καλείται πλεονασμός και εκφράζει την απόκλιση της εντροπίας των μηνυμάτων (με τις δεδομένες πιθανότητες εμφάνισής τους) από τη μέγιστη τιμή της (αν οι εμφανίσεις όλων των μηνυμάτων ήταν ισοπίθανα γεγονότα).

$$H(K/C_L) \geq H(K) + H(M_L) - L\log q = H(K) - R_L. \quad (5.10)$$

Έτσι καταλήξαμε στη ζητούμενη σχέση.

Προφανώς, όσο πιο μεγάλη η τιμή της αβεβαιότητας του κλειδιού τόσο πιο ασφαλές είναι το κρυπτογραφικό σύστημα. Παρατηρούμε από τη σχέση (5.8) ότι η αύξηση του πλεονασμού οδηγεί σε μείωση της αβεβαιότητας του κλειδιού. Έτσι για τη βελτίωση της ασφάλειας των κρυπτογραφικών συστημάτων συνιστάται η μείωση του πλεονασμού των μηνυμάτων με τη βοήθεια αλγορίθμων συμπίεσης (ή αλγορίθμων κωδικοποίησης πηγής).

Στη συνέχεια, με το επόμενο θεώρημα, θα αναζητήσουμε το μήκος του κρυπτογραφημένου μηνύματος L για το οποίο η αβεβαιότητα του κλειδιού μπορεί να γίνει ίση με μηδέν.

ΘΕΩΡΗΜΑ 5.2

Στην περίπτωση πηγής πληροφορίας χωρίς μνήμη, η αβεβαιότητα του κλειδιού μπορεί να γίνει μηδέν αν ισχύει η ακόλουθη σχέση, όπου q είναι το πλήθος των διαφορετικών συμβόλων που χρησιμοποιούνται και $H(S)$ η εντροπία ανά σύμβολο:

$$L \geq H(K) / [\log q - H(S)]. \qquad (5.11)$$

Απόδειξη

Αφού η πηγή πληροφορίας είναι χωρίς μνήμη, δηλαδή πηγή που παράγει μηνύματα αποτελούμενα από σύμβολα στατιστικά ανεξάρτητα μεταξύ τους, η εντροπία ενός μηνύματος αποτελούμενου από L σύμβολα είναι ίση με το γινόμενο της εντροπίας ανά σύμβολο επί το μήκος L. Έτσι, η (5.10) γράφεται

$$H(K/C_L) \geq H(K) + LH(S) - L\log q = H(K) + L[H(S) - \log q].$$

Αν $L \geq H(K)/[\log q - H(S)]$, *τότε* $0 \geq H(K) + L[H(S) - \log q]$. Επομένως, $H(K/C_L) \geq 0$. Σε άλλη περίπτωση, αν $L < H(K)/[\log q - H(S)]$, τότε $H(K/C_L) > 0$, δηλαδή η $H(K/C_L)$ δεν μπορεί να γίνει 0, αφού $H'(K) + L[H(S) - \log q] > 0$. Άρα η αβεβαιότητα του κλειδιού, που είναι μη αρνητική ποσότητα, μπορεί να γίνει 0 αν ισχύει η ανισότητα (3.11), δηλαδή $L \geq H(K) / [\log q - H(S)]$.

Η τιμή του L για την οποία η (5.11) γίνεται ισότητα ονομάζεται **μοναδιαία απόσταση** και υποδηλώνει το ελάχιστο απαιτούμενο μήκος του κρυπτογραφημένου μηνύματος για τον προσδιορισμό του κλειδιού. Η μοναδιαία απόσταση είναι αντιστρόφως ανάλογη του πλεονασμού. Επομένως ακόμα και απλά κρυπτογραφικά συστήματα για την κρυπτογράφηση μηνυμάτων με σχεδόν μηδενικό πλεονασμό επιτρέπουν πολύ καλή προστασία.

Άσκηση Αυτοαξιολόγησης 5.2

Εξετάζουμε ένα κείμενο στην ελληνική γλώσσα, το οποίο κωδικοποιείται σύμφωνα με τη μονοαλφαβητική αντικατάσταση. Να προσδιορισθεί το ελάχιστο μήκος του κρυπτογραφημένου μηνύματος για το οποίο η αβεβαιότητα του κλειδιού μπορεί να γίνει ίση με μηδέν. (Θεωρούμε ότι η εντροπία της ελληνικής γλώσσας είναι 4 bits ανά γράμμα και η μέγιστη τιμή της 4,6 bits, αν και δεν ανταποκρίνεται στην πραγματικότητα. Η πραγματική τιμή της εντροπίας ανά γράμμα ελληνικού κειμένου είναι πολύ μικρότερη και μπορεί να υπολογισθεί από το μέσο πληροφορικό περιεχόμενο μηνυμάτων, λαμβανομένης υπόψη της εξάρτησης, το οποίο διαιρείται με το μέσο πλήθος των γραμμάτων των μηνυμάτων. Για παράδειγμα, η τιμή που προκύπτει κατ' αυτόν τον τρόπο για αγγλικά κείμενα είναι περίπου ίση με 1,2 bit/γράμμα σε αντίθεση με την τιμή των 3,8 bits/γράμμα που θα προέκυπτε κατά ανάλογο τρόπο με την τιμή των 4 bits/ γράμμα για την ελληνική.)

5.2.3 Θεωρία πολυπλοκότητας και Ασφάλεια Κρυπτογραφικών Συστημάτων

Όπως γνωρίζουμε από τη Θεωρία Πολυπλοκότητας υπάρχουν οι κλάσεις των **P** και **NP προβλημάτων**. Η πρώτη κλάση περιλαμβάνει όλα τα προβλήματα των οποίων η λύση (αλγόριθμος) εκτελείται σε χρόνο φραγμένο από πολυωνυμική συνάρτηση μεγέθους αυτού του προβλήματος. Για παράδειγμα, το πρόβλημα της αναζήτησης ενός συγκεκριμένου αντικειμένου σε μια λίστα n αντικειμένων ή η ταξινόμηση n αντικειμένων κατά φθίνουσα τάξη μπορεί να επιλυθεί σε χρόνο ανάλογο του n ή n^2, αντίστοιχα. Τα προβλήματα αυτά ανήκουν στην P κλάση. Ωστόσο και τα προβλήματα της κλάσης αυτής για πολύ μεγάλες τιμές του n, καθώς και του εκθέτη (έως $n^{1000000000}$ περιλαμβάνονται στην κλάση αυτή) απαιτούν τόσο πολύ χρόνο που ενδεχομένως καθιστούν την πρακτική τους εφαρμογή ανέφικτη.

Από την άλλη πλευρά, το σύνολο των προβλημάτων, των οποίων η λύση μπορεί να εκτελεσθεί σε χρόνο φραγμένο από πολυωνυμική συνάρτηση μεγέθους αυτού του προβλήματος, εφόσον υποθέσουμε δεδομένη την ικανότητα να εικάζουμε (nondeterministic Turing machine) με απόλυτη ακρίβεια, απαρτίζουν την NP κλάση. Για παράδειγμα, το πρόβλημα της κρυπτανάλυσης κρυπτογραφημένου μηνύματος με το σύστημα DES που βασίζεται στη δοκιμή όλων των δυνατών κλειδιών, που στην περίπτωση αυτή είναι 2^{56}, ανήκει στην κλάση αυτή. Αν κάποιος μπορούσε να εικάσει με απόλυτη ακρίβεια το κλειδί, τότε η αποκρυπτογράφηση είναι βεβαίως εφικτή σε πολυωνυμικό χρόνο. Όμως, η ορθή εικασία δεν είναι δυνατή. Τέλος, υπάρχει και η κλάση **EXP**, που περιλαμβάνει όλα τα προβλήματα για τα οποία υπάρχει ντετερμινιστική λύση (αλγόριθμος) που εκτελείται σε εκθετικό χρόνο (κ^n, όπου κ = *σταθερά*). Η κλάση P είναι υποσύνολο της NP και η NP της EXP.

Ερευνητές έχουν αναγνωρίσει διάφορα NP προβλήματα (αρκετές εκατοντάδες προβλήματα), στα οποία συγκαταλέγεται και το πρόβλημα του σακιδίου ή «knapsack» (όπως και του περιοδεύοντος πωλητή), που συνδέονται με την ακόλουθη ιδιότητα και χαρακτηρίζονται **NP – πλήρη (NP – Complete)**. Αν κάποιο απ' αυτά τα προβλήματα έχει ως λύση έναν πολυωνυμικό αλγόριθμο, τότε και τα υπόλοιπα προβλήματα της κλάσης NP ανήκουν στην κλάση P. Ακόμα, αν δειχθεί για κάποιο απ' αυτά τα προβλήματα ότι δεν υπάρχει ντετερμινιστικός πολυωνυμικός αλγόριθμος που το επιλύει, τότε αυτό ισχύει και για όλα τα προβλήματα της κλάσης NP.

Στη σύγχρονη Κρυπτογραφία, θεωρώντας πλέον ότι ο κρυπταναλυτής δεν διαθέτει άπειρους αλλά πεπερασμένους υπολογιστικούς πόρους, επιδιώκεται η σχεδίαση κρυπτογραφικών συστημάτων, τα οποία επιτρέπουν μεν αποτελεσματική κρυπτογράφηση και αποκρυπτογράφηση για τους νόμιμους χρήστες, καθιστούν όμως υπολο-

γιστικά ανέφικτη την αποκρυπτογράφηση για τους κρυπταναλυτές. Απαιτούνται για το λόγο αυτό προβλήματα ή πρωτογενή στοιχεία (primitives), τα οποία χαρακτηρίζονται από συγκεκριμένες ιδιότητες υπολογιστικής δυσκολίας. Τέτοια πρωτογενή στοιχεία είναι οι μονόδρομοι συναρτήσεις (one – way functions) και οι γεννήτριες ψευδοτυχαίων αριθμών (pseudo – random number generators), εκ των οποίων μπορούν να δημιουργηθούν υπολογιστικά ασφαλή κρυπτογραφικά συστήματα.

Οι μονόδρομοι συναρτήσεις υπολογίζονται εύκολα, αντιστρέφονται όμως δύσκολα. Ωστόσο, αν και πιθανολογείται (πιστεύεται) δεν έχει ακόμα αποδειχθεί μαθηματικά ότι υπάρχουν μονόδρομοι συναρτήσεις. Για να αποτελέσουν τη βάση ασύμμετρων κρυπτογραφικών συστημάτων, οι μονόδρομοι συναρτήσεις θα πρέπει να επιτρέπουν την εύκολη αντιστροφή τους στους νόμιμους χρήστες που διαθέτουν κάποια μυστική πληροφορία (trapdoor information ή μυστικό κλειδί). Οι συναρτήσεις που έχουν και την ιδιότητα αυτή καλούνται και μονόδρομοι συναρτήσεις κρυφής διόδου (trapdoor functions). Η αξιοποίηση μονόδρομων συναρτήσεων κρυφής διόδου ως βάσεων ασύμμετρων κρυπτογραφικών συστημάτων προτάθηκε από τους Diffie και Hellman το 1976, αποτέλεσε δε το έναυσμα για τη ραγδαία ανάπτυξη της σύγχρονης Κρυπτογραφίας.

Το ασύμμετρο κρυπτογραφικό σύστημα RSA (δείτε Υποενότητα 5.1.3) έχει ως βάση τη μονόδρομο συνάρτηση $f(M) = C = M^e \bmod n$, της οποίας η αντίστροφος $f^{-1}(M)$ οδηγεί στην αποκρυπτογράφηση. Ο υπολογισμός της $f(M)$ είναι εύκολος (το δημόσιο κλειδί που δημοσιοποιείται απαρτίζεται από το μέτρο ισοτιμίας n και τον εκθέτη e), της $f^{-1}(M)$ όμως δύσκολος, εκτός και αν είναι γνωστή η μυστική πληροφορία ή κρυφή δίοδος (trapdoor information) p και q (υπόμνηση: $n = pq$), δηλαδή το μυστικό κλειδί που οφείλει να γνωρίζει μόνον ο νόμιμος χρήστης. Η ανωτέρω συνάρτηση f πιθανολογείται ότι είναι μονόδρομος. Σήμερα, πιστεύεται ότι ο καλύτερος τρόπος παραβίασης της μονόδρομου συνάρτησης και επομένως και του RSA είναι η ανάλυση του n σε γινόμενο πρώτων παραγόντων, δηλαδή στους p και q, που όμως θεωρείται υπολογιστικά δύσκολη ή ανέφικτη. Ωστόσο, δεν έχει δειχθεί ότι δεν υπάρχει άλλος αποτελεσματικός τρόπος παραβίασης του RSA.

Τα υπολογιστικά δύσκολα προβλήματα (NP), λοιπόν, τα οποία αποτελούν τη βάση μονόδρομων συναρτήσεων και κατ' επέκταση και κρυπτογραφικών συστημάτων είναι θεμελιώδη στην Κρυπτογραφία. Όμως, η επιλογή ενός NP – προβλήματος ως βάσης δεν είναι, γενικά, αρκετή για τη σχεδίαση ασφαλών κρυπτογραφικών συστημάτων. Στη συνέχεια θα συζητήσουμε ορισμένες σχετικές πτυχές.

Τα προβλήματα που ανήκουν στην NP κλάση, έχουν όπως είπαμε μη – ντετερμινιστική πολυωνυμική χρονική πολυπλοκότητα και ασφαλώς ντετερμινιστική εκθετι-

κή χρονική πολυπλοκότητα, δηλαδή ανάλογη του 2^n. Ας παρατηρήσουμε, ως παράδειγμα, το πρόβλημα της κρυπτανάλυσης κρυπτογραφημένου μηνύματος με κλειδί πολύ μικρού μήκους, n. Τότε το 2^n, δηλαδή το πλήθος των δυνατών κλειδιών, δεν είναι μεγάλο και συνεπώς η κρυπτανάλυση είναι εφικτή δοκιμάζοντας όλα τα δυνατά κλειδιά (brute force attack). Επομένως, δεν είναι αρκετό να στηριζόμαστε σε ένα πρόβλημα με εκθετική πολυπλοκότητα αν το μέγεθος της εισόδου είναι μικρό. Αντίθετα, μόνο αν το n είναι επαρκώς μεγάλο, τότε και το 2^n είναι τόσο μεγάλο που καθιστά μη εφικτή τη δοκιμή όλων των δυνατών κλειδιών. Στον Πίνακα 5.1 βλέπουμε τα μεγέθη των εισόδων που μπορούν να εκτελεσθούν στη μονάδα του χρόνου με δεδομένη τη διαθέσιμη υπολογιστική ισχύ και την πολυπλοκότητα του αλγορίθμου.

Το να στηριχθούμε για τη δημιουργία ενός κρυπτογραφικού συστήματος σε ένα NP – πλήρες πρόβλημα δε συνεπάγεται την ύπαρξη μόνο λύσης με εκθετική πολυπλοκότητα. Δεν αποκλείεται, δηλαδή, η ύπαρξη μιας πιο εύκολης λύσης, αν και κάτι τέτοιο εκτιμάται ως άκρως απίθανο (όχι όμως αδύνατο). Στο σημείο αυτό αναφερόμαστε στην περίπτωση να δειχθεί ότι οι κλάσεις P και NP ταυτίζονται, δηλαδή P = NP. Ακόμα, το ότι ένα κρυπτογραφικό σύστημα βασίζεται σε ένα δύσκολο πρόβλημα δε σημαίνει ότι και ο κρυπταναλυτής θα πρέπει να λύσει το δύσκολο πρόβλημα για την παραβίασή του. Για παράδειγμα, ένα δύσκολο πρόβλημα, στο οποίο βασίσθηκε μια κατηγορία «μη ασφαλών» κρυπτογραφικών συστημάτων, είναι το επονομαζόμενο πρόβλημα του «σακιδίου» («knapsack»). Το πρόβλημα αυτό προτάθηκε ως βάση κρυπτογραφικών συστημάτων, χωρίς όμως επιτυχία, αφού μερικά χρόνια αργότερα βρέθηκε τρόπος για την παραβίασή τους, με αξιοποίηση κάποιας ακόμα εύκολης λύσης, εκτός αυτής (κρυφής διόδου ή μυστικού κλειδιού) που αξιοποιούσε ο νόμιμος χρήστης.

Πίνακας 5.1

Μεγέθη εισόδου που εκτελούνται στη μονάδα του χρόνου (sec) από υπολογιστή ισχύος ενός εκατομμυρίου πράξεων ανά μονάδα χρόνου

Πολυπλοκότητα	**Μέγεθος εισόδου που εκτελείται στο 1 sec (υπολογιστική ισχύς 10^6 πράξεων/sec)**
$\log n$	$2^{1000000}$
n	1000000
n^2	1000
n^3	100
2^n	περίπου 20
$n!$	περίπου 9

Η υπολογιστική ισχύς και η αποθηκευτική ικανότητα αυξάνεται ραγδαία με την ανάπτυξη νέων υπολογιστικών συστημάτων. Η αύξηση της υπολογιστικής ισχύος καθιστά προβλήματα κρυπτανάλυσης αντιμετωπίσιμα. Η χρήση πολυεπεξεργαστών ή και πολυυπολογιστών στην κρυπτανάλυση αποτελούν μία πραγματικότητα που πρέπει να λαμβάνεται υπόψη από τους σχεδιαστές κρυπτογραφικών συστημάτων. Είναι ευρέως γνωστή η περίπτωση της παραβίασης κρυπτογραφημένου μηνύματος με τον DES (με κλειδί μήκους 40 bits), από τη συνεργασία χιλιάδων υπολογιστών συνδεδεμένων στο Internet, αλλά και η παραβίαση κρυπτογραφημένου μηνύματος με κλειδί μήκους 56 bits με τη βοήθεια ειδικών επεξεργαστών, όπως επίσης και η ανάλυση πολύ μεγάλων ακεραίων σε γινόμενο πρώτων παραγόντων (150 δεκαδικών ψηφίων). Επομένως, η επιλογή των μεγεθών εισόδου θα πρέπει να λαμβάνει υπόψη τόσο τις τωρινές τεχνολογικές δυνατότητες όσο και τις αναμενόμενες μελλοντικές εξελίξεις. Ιδιαίτερα, η ανάπτυξη των κβαντικών υπολογιστικών και επικοινωνιακών συστημάτων αναμένεται να ακυρώσει την πρακτική αξία πολλών κρυπτογραφικών συστημάτων που χαρακτηρίζονται ως υπολογιστικά ασφαλή.

Άσκηση Αυτοαξιολόγησης 5.3

Δίνεται ένα κρυπτογραφικό σύστημα με κλειδί μήκους 40 ή 56 ή 128 bits και δύο υπολογιστικά συστήματα ισχύος 2^{40} πράξεων / sec και 2^{56} πράξεων / sec, αντίστοιχα. Να υπολογισθεί ο χρόνος που απαιτείται σε κάθε υπολογιστικό σύστημα για την παραβίαση του κρυπτογραφικού συστήματος για όλα τα διαφορετικά μήκη κλειδιών. Η παραβίαση επιχειρείται με δοκιμή όλων των δυνατών κλειδιών (brute force attack).

5.2.4 Μονόδρομοι συνάρτησης ως βάσεις κρυπτογραφικών συστημάτων

Οι μονόδρομοι συναρτήσεις θεωρούνται ως το πιο βασικό πρωτογενές στοιχείο για τη δημιουργία κρυπτογραφικών εφαρμογών. Όπως προαναφέραμε, ο υπολογισμός τους είναι εύκολος, η αντιστροφή τους όμως δύσκολη. Όπως επίσης προαναφέραμε, οι μονόδρομοι συναρτήσεις για να αποτελέσουν τη βάση ασύμμετρων κρυπτογραφικών συστημάτων θα πρέπει να διαθέτουν και μία κρυφή δίοδο, η οποία θα επιτρέπει στους νόμιμους χρήστες και την εύκολη αντιστροφή, δηλαδή την αποκρυπτογράφηση. Η έννοια της ευκολίας υπολογισμού υποδηλώνει την ύπαρξη αλγορίθμου που εκτελείται σε χρόνο φραγμένο από πολυωνυμική συνάρτηση μεγέθους αυτού του προβλήματος (N – πρόβλημα), ενώ η έννοια της υπολογιστικής δυσκο-

λίας υποδηλώνει ότι κάθε αλγόριθμος πολυωνυμικής χρονικής πολυπλοκότητας έχει αμελητέα πιθανότητα επιτυχούς αντιστροφής (NP – πρόβλημα). Επομένως, η δυσκολία αντιστροφής των κατάλληλων για κρυπτογραφικές εφαρμογές μονόδρομων συναρτήσεων πρέπει να αφορά σε όλες τις δυνατές και όχι μόνο σε ορισμένες εισόδους. Στη συνέχεια, θα μας απασχολήσουν υποψήφιες μονόδρομοι συναρτήσεις, οι οποίες βασίζονται στα δύσκολα προβλήματα της ανάλυσης μεγάλων φυσικών σε γινόμενο πρώτων παραγόντων και των διακριτών λογαρίθμων, καθώς και σε μια οικογένεια ψευδοτυχαίων συναρτήσεων. (Δείτε τις σημειώσεις των S. Golwasser και M. Bellare για μια εκτενή εισαγωγή στη θεωρητική αυτή οπτική εξέτασης της Κρυπτογραφίας.) Ακολούθως, θα μας απασχολήσει εν συντομία και το ασύμμετρο κρυπτογραφικό σύστημα του ELGamal, το οποίο έχει ως βάση του το δύσκολο πρόβλημα των διακριτών λογαρίθμων, σε αντίθεση με τον RSA που βασίζεται στο πρόβλημα της ανάλυσης ακεραίων σε γινόμενο πρώτων παραγόντων.

1. Ανάλυση σε γινόμενο πρώτων παραγόντων

Ας θεωρήσουμε τους πρώτους αριθμούς p και q, το γινόμενό τους $n = pq$ και τη συνάρτηση $f:(p,q) \rightarrow pq$. Η f πιθανολογείται ότι είναι μονόδρομος συνάρτηση. Παραλλαγές του αλγορίθμου τυχαίων τετραγώνων του Dixon είναι σήμερα οι πιο ταχείς αλγόριθμοι ανάλυσης αριθμών σε γινόμενο πρώτων παραγόντων με χρονική πολυπλοκότητα $\left(e^{\sqrt{\log n \log n \log n}}\right)^{\sqrt{2}}$.

2. Το πρόβλημα των διακριτών λογαρίθμων

Θεωρούμε τον πρώτο αριθμό p και την πολλαπλασιαστική ομάδα $Z_p^*=(\{x < p \mid (x, p) = 1\}, \text{mod p})$, η οποία είναι κυκλική, έτσι ώστε $Z_p^*=\{g^i \bmod p \mid 1 \le i \le p-1\}$ για κάποιον γεννήτορα (πρωτογενές στοιχείο) $g \in Z_p^*$. Επίσης, θεωρούμε τη συνάρτηση $f:(p, g, x) \rightarrow (g^x \bmod p, p, g)$. Η f πιθανολογείται ότι είναι μονόδρομος συνάρτηση. Σήμερα, ο καλύτερος, πλήρως αποδεδειγμένος, αλγόριθμος υπολογισμού διακριτών λογαρίθμων είναι ο Index – Calculus, χρονικής πολυπλοκότητας $e^{\sqrt{k \log k}}$, όπου k το πλήθος των δυαδικών ψηφίων του μέτρου ισοτιμίας p. Μια πρόσφατη παραλλαγή του αλγορίθμου Number Filed Sieve για τον υπολογισμό διακριτών λογαρίθμων φαίνεται να είναι ταχύτερη, της τάξης του $e^{(k \log k)^{\frac{1}{3}}}$. Ο υπολογισμός διακριτών λογαρίθμων και η ανάλυση ακεραίων σε γινόμενο πρώτων παραγόντων φαίνεται να είναι, κατ΄ ουσία,

της ίδιας υπολογιστικής δυσκολίας, τουλάχιστον σύμφωνα με τους σημερινούς αλγόριθμους επίλυσης των προβλημάτων αυτών.

3. DES με σταθερό μήνυμα

Θεωρούμε ένα μήνυμα M, μήκους 64 bits, και ορίζουμε τη συνάρτηση $f(K) = DES_K(M)$ με έξοδο μήκους 64 bits, όπου K το κλειδί μήκους 56 bits. Η συνάρτηση αυτή μπορεί να δειχθεί ότι είναι μονόδρομος θεωρώντας τον DES ως μία οικογένεια ψευδοτυχαίων ακολουθιών.

Έχοντας ωστόσο υπόψη ότι ο απλός DES δε θεωρείται ασφαλής (σε αντίθεση με τον τριπλό DES), αφού έχει ήδη παραβιαστεί, συνειδητοποιούμε και πάλι ότι δεν είναι αρκετή η ύπαρξη μιας μονόδρομου συνάρτησης ή, αντίστοιχα, ενός δύσκολου προβλήματος ως βάσης για τη δημιουργία υπολογιστικά ασφαλών κρυπτογραφικών εφαρμογών. Θα πρέπει να συνδυάζεται με την κατάλληλη επιλογή των καθοριστικών παραμέτρων, όπως του μήκους του κλειδιού, λαμβάνοντας επίσης υπόψη τωρινές και μελλοντικές υπολογιστικές δυνατότητες.

Το ασύμμετρο κρυπτογραφικό σύστημα του ElGamal

Πρώτα επιλέγεται και δημοσιοποιείται ένας κατάλληλος πρώτος αριθμός p καθώς και ένας γεννήτορας (ή πρωτογενής ρίζα) a του πεδίου Z_p. Ο a είναι ένας ακέραιος μικρότερος του p και $a^{p-1} = 1 \bmod p$, αλλά $a^{b-1} \neq 1 \bmod p$, για κάθε b, όπου $1 < b < p$. Το ιδιωτικό (μυστικό) κλειδί ενός χρήστη Α είναι ένας ακέραιος S_A, ο οποίος επιλέγεται τυχαία από τον A, έτσι ώστε $1 \leq S_A \leq p - 1$. Το δημόσιο κλειδί του A είναι ο ακέραιος P_A, ο οποίος προκύπτει ως εξής: $P_A = a^{SA} \bmod p$.

Για την κρυπτογράφηση ενός μηνύματος M, ένας άλλος χρήστης, έστω ο B, επιλέγει πρώτα έναν τυχαίο αριθμό r, τέτοιον ώστε $1 \leq r \leq p - 1$ και υπολογίζει το «κλειδί» K ως εξής: $K = {P_A}^k \bmod p$. Κατόπιν κρυπτογραφεί το μήνυμα M, $C_1 = a^r \bmod p$ και $C_2 = KxM \bmod p$. Το ζεύγος των ακεραίων (C_1, C_2) αποτελεί την κρυπτογραφημένη μορφή του μηνύματος M.

Για την αποκρυπτογράφηση, ο παραλήπτης, δηλαδή ο χρήστης A, ανακτά το «κλειδί» K ως εξής: $K = {P_A}^r = (a^r)^{SA} \bmod p = (C_1)^{SA} \bmod p$. (Ο Α μπορεί να εκτελέσει αυτούς τους υπολογισμούς, αφού αυτός γνωρίζει το μυστικό του κλειδί, S_A.) Η αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος C_2, επιτυγχάνεται με τη διαίρεση του C_2 δια του K (mod p).

Παράδειγμα 5.4

Επιλέγουμε τον πρώτο αριθμό $p = 71$ και τη γεννήτρια του πεδίου Z_{71}, $\alpha = 7$. Ο χρή-

στης Α επιλέγει το ιδιωτικό κλειδί $S_A = 11$ και υπολογίζει το δημόσιο κλειδί του $P_A = 7^{11} \bmod 71 = 31$, το οποίο δημοσιοποιεί. Ο χρήστης Β επιθυμεί να στείλει στον Α το μήνυμα $M = 64$. Πρώτα όμως επιλέγει τον τυχαίο $r = 3$ και υπολογίζει το «κρυπτογραφικό κλειδί» $K = 31^3 \bmod 71 = 42$. Ο χρήστης Β υπολογίζει $C_1 = 7^3 \bmod 71 = 59$ και $C_2 = 42x64 \bmod 71 = 61$, τα οποία αποστέλλει στον Α. Ο παραλήπτης Α ανακτά πρώτα το κρυπτογραφικό κλειδί $K = (C_1)^{SA} \bmod p = (59)^{11} \bmod 11 = 42$ και στη συνέχεια ανακτά το καθαρό από το κρυπτογραφημένο μήνυμα, $M = (C_2/K) \bmod p = (61/42) \bmod 71 = 64$.

Άσκηση αυτοαξιολόγησης 5.4

Δίνεται ο πρώτος αριθμός $p = 71$ και η γεννήτρια του πεδίου Z_{71}, $a = 7$. Ο χρήστης Α επιλέγει το ιδιωτικό κλειδί $S_A = 13$ και υπολογίζει το αντίστοιχο δημόσιο κλειδί του P_A, το οποίο δημοσιοποιεί. Ζητείται η κρυπτογραφημένη μορφή του μηνύματος $M = 47$, το οποίο αποστέλλει ο χρήστης Β στο χρήστη Α. Ο χρήστης Β επιλέγει τον τυχαίο αριθμό $r = 3$ για την κρυπτογράφηση του μηνύματος Μ. Επίσης, ζητείται το «κρυπτογραφικό κλειδί» K και να δείξετε πώς ανακτάται το καθαρό από το κρυπτογραφημένο μήνυμα.

Σύνοψη

Στο κεφάλαιο αυτό εξετάσαμε κρυπτογραφικά θέματα από τη σκοπιά κυρίως της Θεωρίας Πληροφορίας, αλλά και από τη σκοπιά της Θεωρίας Πολυπλοκότητας. Μετά από μία σύντομη αναφορά στην Κρυπτογραφία, παραθέσαμε βασικούς τύπους κρυπταναλυτικών επιθέσεων και μας απασχόλησαν η μονοαλφαβητική και η πολυαλφαβητική αντικατάσταση, ο δυαδικός κωδικοποιητής του Vernam (one – time pad) και το ασύμμετρο κρυπτογραφικό σύστημα RSA.

Η Θεωρία Πληροφορίας μας επιτρέπει να εξάγουμε ορισμένα χρήσιμα συμπεράσματα αναφορικά με την ασφάλεια κρυπτογραφικών συστημάτων. Ασφαλώς, οι σχεδιαστές κρυπτογραφικών συστημάτων επιδιώκουν το κρυπτογραφημένο μήνυμα να αποκαλύπτει την ελάχιστη δυνατή πληροφορία για το κλειδί. Επίσης, επιδιώκουν το κρυπτογραφημένο μήνυμα να αποκαλύπτει την ελάχιστη δυνατή πληροφορία για το καθαρό μήνυμα. Η αμοιβαία πληροφορία μεταξύ του καθαρού και του κρυπτογραφημένου μηνύματος, η οποία αποτελεί ένα μέτρο της εξάρτησης μεταξύ τους, είναι μηδέν στις περιπτώσεις απόλυτα ασφαλών κρυπτογραφικών συστημάτων, όπως του one – time pad. Τότε το μήκος του κλειδιού είναι ίσο με αυτό του μηνύματος. Ωστόσο, η εισαγωγή της έννοιας του γεγονότος ασφάλειας επιτρέπει την επίτευξη απόλυτα ασφαλών κρυπτογραφικών συστημάτων στις περιπτώσεις που τα γεγονότα αυτά λαμβάνουν χώρα, ακόμα και αν το κλειδί είναι μήκους μικρότερου απ' αυτό του μηνύματος.

Η αβεβαιότητα του κλειδιού, είναι μεγαλύτερη ή ίση της εντροπίας του κλειδιού αφαιρουμένου του πλεονασμού του μηνύματος. Το μήκος του κρυπτογραφημένου μηνύματος για το οποίο η αβεβαιότητα του κλειδιού μπορεί να γίνει μηδέν, είναι η μοναδιαία, απόστασή του. Αυτή υποδηλώνει το ελάχιστο απαιτούμενο μήκος του κρυπτογραφημένου μηνύματος για τον προσδιορισμό του κλειδιού και επομένως την εξαγωγή ενός μοναδικού εύλογου καθαρού μηνύματος.

Τα υπολογιστικά δύσκολα προβλήματα (NP) και οι μονόδρομοι συναρτήσεις είναι θεμελιώδη στην Κρυπτογραφία, αφού επιλέγονται ως βάσεις κρυπτογραφικών συστημάτων. Ωστόσο, η επιλογή ενός NP – προβλήματος ως βάσης δεν είναι αρκετή για τη σχεδίαση ασφαλών κρυπτογραφικών συστημάτων, αλλά πρέπει να συνδυαστεί με κατάλληλη επιλογή των διαφόρων παραμέτρων και να αποκλειστεί η αξιοποίηση εύκολων λύσεων από την πλευρά των κρυπταναλυτών.

Οι μονόδρομοι συναρτήσεις, των οποίων ο υπολογισμός είναι εύκολος, η αντιστροφή όμως δύσκολη, θεωρούνται ως το πλέον βασικό πρωτογενές στοιχείο για τη δημιουργία κρυπτογραφικών εφαρμογών. Στα δύσκολα προβλήματα, τα οποία αποτελούν τις βάσεις μονόδρομων συναρτήσεων και κατ' επέκταση και κρυπτογραφικών συστη-

μάτων, συγκαταλέγονται η ανάλυση πολύ μεγάλων φυσικών αριθμών σε γινόμενο πρώτων παραγόντων και οι διακριτοί λογάριθμοι. Όπως το RSA βασίζεται στο δύσκολο πρόβλημα της ανάλυσης ακεραίων σε γινόμενο πρώτων παραγόντων, το επίσης ασύμμετρο κρυπτογραφικό σύστημα του ElGamal βασίζεται στο δύσκολο πρόβλημα των διακριτών λογαρίθμων.

Βιβλιογραφία

ΠΡΟΤΑΣΕΙΣ ΜΕΛΕΤΗΣ

Στον τόμο «Κρυπτογραφία», του Β. Ζορκάδη, ΕΑΠ, 2002, περιγράφονται αναλυτικά οι έννοιες της Κρυπτογραφίας και της Κρυπτανάλυσης καθώς και κλασικές και σύγχρονες κρυπτογραφικές τεχνικές, όπως συμμετρικοί και ασύμμετροι κρυπτογραφικοί αλγόριθμοι, σχήματα ψηφιακών υπογραφών και συναρτήσεις κατακερματισμού. Μεγάλο μέρος του κεφαλαίου αυτού, συμπεριλαμβανομένων των παραδειγμάτων και των ασκήσεων, προέρχεται από το βιβλίο ΄Κρυπτογραφία».

Στο βιβλίο του D. R. Stinson, «Cryptography, Theory and Praxis», CRC Press, 1995, μπορείτε να βρείτε μια εκτενή κάλυψη των βασικών κρυπτογραφικών θεμάτων, όπως της κλασικής κρυπτογραφίας, της θεωρίας του Shannon και πολλών συμμετρικών και ασύμμετρων κρυπτογραφικών συστημάτων, τα οποία βασίζονται στα δύσκολα προβλήματα της ανάλυσης μεγάλων αριθμών σε γινόμενο πρώτων παραγόντων, των διακριτών λογαρίθμων και των ελλειπτικών καμπυλών (RSA, ElGamal κά.).

Στο «Lecture Notes on Cryptography» των S. Goldwasser και M. Bellare, http://theory.lcs.mit.edu/shafi ή http://www – cse.ucsd.edu/users/mihir, 2001, μπορείτε να βρείτε μια αρκετά ενδιαφέρουσα, κυρίως θεωρητική προσέγγιση της Κρυπτογραφίας. Στις σημειώσεις αυτές αναπτύσσεται και ερμηνεύεται, ιδιαίτερα, η έννοια της ευαπόδεικτης ασφαλείας καθώς και της αξιοποίησής της στη σχεδίαση ασφαλών κρυπτογραφικών εφαρμογών.

Επίσης, το βιβλίο «Foundations of Cryptography: Basic Tools» του O. Goldreich, Cambridge University Press, 2001, εστιάζει κυρίως στη θεωρητική θεμελίωση της Κρυπτογραφίας, δηλαδή στα βασικά μαθηματικά θέματα, συμπεριλαμβανομένης της υπολογιστικής πολυπλοκότητας, της ψευδοτυχαιότητας και των αποδείξεων μηδενικής γνώσης. Απευθύνεται, όπως και οι σημειώσεις των S. Goldwasser και M. Bellare, περισσότερο σε ερευνητές ή μεταπτυχιακούς φοιτητές και λιγότερο σε προπτυχιακούς.

Στο βιβλίο του B. Schneier με τον τίτλο Applied Cryptography ([SCH1994], Willey & Sons, first edition, 1994) μπορείτε να βρείτε περιγραφές κρυπτογραφικών τεχνικών και των θεμάτων που μας απασχόλησαν στο Κεφάλαιο αυτό. Η δεύτερη έκδοση αυτού του βιβλίου είναι αρκετά βελτιωμένη και ιδιαίτερα εκτενής ([SCH1996], Willey & Sons, 2nd edition, 1996).

Ξενόγλωσση βιβλιογραφία

[1] [DIF1976] W. Diffie, M. E.. Hellman, «New Directions in Cryptography», IEEE Transactions on Information Theory, Vol. 22, n. 6, 1976, pp. 644 – 654),

[2] [LUB1998] J. C. A. Van der Lubbe, Basic Methods of Cryptography, Cambridge University Press, 1998.

[3] [SHA1948] C. E. Shannon, «A Mathematical Theory of Communication», Bell System Technical Journal, v. 27, n. 4, 1948, pp. 379 – 423, 623 – 656.

[4] [SHA1949] C. E. Shannon, «Communication Theory of Secret Systems», Bell System Technical Journal, v. 28, n. 4, 1949, pp. 656 – 715.

[5] [SHA1951] C. E. Shannon, «Predication and Entropy in Printed English», Bell System Technical Journal, v. 30, n. 1, 1951, pp. 50 – 64.

[6] [SHA1993] C. E. Shannon, «Collected Papers», N.J.A. Sloane and A.D. Wyner, editors, IEEE Press, NewYork, 1993.

[7] [SPI1996] T. P. Spiller, «Quantum Information Processing: Cryptography, Computation, and Teleportation», Proc. Of the IEEE, Vol. 84, No. 12, December 1996.

[8] [STA1995] W. Stallings, Network and Internetwork Security, Principles and Practice, Prentice Hall, 1995.

Απαντήσεις Ασκήσεων Αυτοαξιολόγησης

1.1

Η ποσότητα πληροφορίας σε decit και bit δίνεται από τις ακόλουθες σχέσεις, αντίστοιχα:

$$H\left(32^2\right) = \log_{10}\left(32^2\right) = \log_{10}\left(2^{10}\right) = 3{,}01 \text{ decit},$$

$$H\left(32^2\right) = \log_2\left(32^2\right) = \log_2\left(2^{10}\right) = 10 \text{ bits}.$$

Αν τα καταφέρατε, πολύ ωραία! Αν όχι, τότε πρέπει να επαναλάβετε τη μελέτη της πρώτης ενότητας και να προσπαθήσετε και πάλι. Απαιτεί απλή εφαρμογή των τύπων που γνωρίσαμε στην πρώτη ενότητα.

1.2

Οι οριακές (ακραίες) συναρτήσεις πυκνότητας πιθανότητας υπολογίζονται ως εξής:

$$f(x) = \int_0^{1-x} 4xydy = 2xy^2\Big|_0^{1-x} = 2x(1-x)^2, \text{ για } 0 \le y \le 1,$$

$$f(y) = \int_0^{1-y} 4xydx = 2x^2y\Big|_0^{1-y} = 2y(1-y)^2, \text{ για } 0 \le x \le 1.$$

Αν τα καταφέρατε, ωραία! Χρειαζόμαστε παρόμοιους υπολογισμούς σε ασκήσεις αργότερα. Αν διαπιστώσατε δυσκολίες, προσπαθήστε να εξασκηθείτε και με τη βοήθεια βιβλίων Θεωρίας Πιθανοτήτων που έχετε στη διάθεσή σας.

1.3

Η μέση ποσότητα πληροφορίας της ρίψης (ή συνδυασμού) υπολογίζεται ως εξής:

$$H(X) = -\sum p_i \log p_i = -36\frac{1}{36}\log\frac{1}{36} = \log 36 = 5{,}17 \text{ bits/ρίψη}$$

Αν τα καταφέρατε, μπράβο! Αν όχι, τότε πριν από την επόμενη προσπάθεια λάβετε υπόψη ότι οι δυνατοί συνδυασμοί είναι συνολικά 36 και συνεπώς τα ενδεχόμενα κατά τη ρίψη δύο ζαριών. Ο κάθε συνδυασμός έχει την ίδια πιθανότητα να λάβει χώρα, που ισούται με 1/36. Επομένως, η μέση ποσότητα πληροφορίας της ρίψης ή συνδυασμού υπολογίζεται όπως ανωτέρω.

1.4

Η μέγιστη μέση πληροφορία προκύπτει από την ακόλουθη κατανομή πιθανοτήτων:

$$p(x_1) = p(x_2) = p(x_3) = p(x_4) = 1/4.$$

Από την άλλη πλευρά, η ελάχιστη μέση πληροφορία είναι ίση με 0 και προκύπτει για κατανομή πιθανοτήτων με τιμή 1 για οποιοδήποτε των τεσσάρων ενδεχομένων και τιμή 0 για τα υπόλοιπα 3 ενδεχόμενα, αφού τότε όλα τα γινόμενα $p_i \log p_i$ είναι ίσα με μηδέν και επομένως και το άθροισμά τους.

Αν τα καταφέρατε, μπράβο! Αν όχι, τότε μελετήστε εκ νέου την Πρόταση 1 και την Πρόταση 2 της Υποενότητας 1.4.2 και συγκρίνετε αυτές με την ανωτέρω απάντηση.

1.5

Η συνδυασμένη πληροφορία της ταυτόχρονης ρίψης των τεσσάρων κερμάτων είναι 4 bits.

Αν τα καταφέρατε, μπράβο! Αν όχι, τότε μελετήστε και πάλι το αντίστοιχο τμήμα της Ενότητας 1.4 και το Παράδειγμα 4 και συγκρίνετε την απάντησή σας με αυτή που ακολουθεί.

Η συνδυασμένη πληροφορία της ταυτόχρονης ρίψης των τεσσάρων κερμάτων μπορεί να υπολογιστεί από την ακόλουθη σχέση, αφού οι δυνατοί συνδυασμοί είναι 16 και η πιθανότητα να λάβει χώρα κάθε συνδυασμός είναι 1/16. Επομένως, η συνδυασμένη ποσότητα πληροφορίας είναι ίση με

$$H(X,Y,Z,U) = -\sum_{i=1}^{klmn} p(v_i) \log p(v_i) = -\sum_{1}^{16} \frac{1}{16} \log \frac{1}{16} = 4 \text{ bits.}$$

1.6

1. $H(X) = 0{,}81$ bits, $H(Y) = 0{,}95$ bits,
2. $H(X, Y) = 1{,}75$ bits,
3. $H(Y/X) = H(X, Y) - H(X) = 1{,}75 - 0{,}81 = 0{,}94$ bits,
4. $H(X/Y) = H(X, Y) - H(Y) = 1{,}75 - 0{,}95 = 0{,}8$ bits.

Αν τα καταφέρατε, συγχαρητήρια! Αν όχι, μην ανησυχείτε. Ας δούμε τα σημεία που πρέπει να προσέξετε ιδιαίτερα στην επόμενη προσπάθειά σας.

Από τις δεδομένες συνδυασμένες πιθανότητες μπορούμε να υπολογίσουμε τις ακραίες πιθανότητες:

$$p(x_1) = \sum_{j=1}^{2} p(x_1, y_j) = \frac{1}{8} + \frac{1}{8} = \frac{1}{4},$$

$$p(x_2)=\sum_{j=1}^{2}p(x_2,y_j)=\frac{1}{2}+\frac{1}{4}=\frac{3}{4},$$

$$p(y_1)=\sum_{i=1}^{2}p(x_i,y_1)=\frac{1}{8}+\frac{1}{2}=\frac{5}{8},$$

$$p(y_2)=1-p(y_1)=\frac{3}{8},$$

Τα ζητούμενα μέτρα ποσότητας πληροφορίας υπολογίζονται ως εξής:

$$H(Y/X) = H(X,Y) - H(X),\ H(X/Y) = H(X,Y) - H(Y).$$

1.7

Για την απόδειξη της σχέσης $H(X/Y)\le H(X)$ πρέπει να χρησιμοποιήσουμε την ανισότητα $\ln x \le x-1$, που είδαμε στην Υποενότητα 1.4.2. Πρέπει, ακόμα, να θυμηθούμε ότι $\sum_{i=1}^{n}p(x_i/y_j)=\sum_{j=1}^{m}p(y_j/x_i)=1$. Ισχύει η ακόλουθη σχέση:

$$\begin{aligned}
H(X/Y)-H(X) &= -\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log p(x_i/y_j)+\\
&\quad+\sum_{i=1}^{n}p(x_i)\log p(x_i)\\
&= -\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log p(x_i/y_j)+\\
&\quad+\sum_{j=1}^{m}p(y_j/x_i)\sum_{i=1}^{n}p(x_i)\log p(x_i)\\
&= \sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log\frac{p(x_i)}{p(x_i/y_j)}\\
&\le \sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\left[\frac{p(x_i)}{p(x_i/y_j)}-1\right]\log e\\
&= \sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\left[\frac{p(x_i)}{p(x_i/y_j)}\right]\log e-\\
&\quad-\sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i,y_j)\log e\\
&= \sum_{i=1}^{n}\sum_{j=1}^{m}p(x_i/y_j)p(y_j)\left[\frac{p(x_i)}{p(x_i/y_j)}\right]\log e-\log e=0.
\end{aligned}$$

Επομένως, $H(X/Y) - H(X) \leq 0$.

Αν τα καταφέρατε, συγχαρητήρια, γιατί ήταν όντως πολύ δύσκολο! Αν δεν τα καταφέρατε, προσπαθήστε να κατανοήσετε την απόδειξη που δίνεται στην απάντηση.

1.8

Έστω οι τυχαίες μεταβλητές *X*, *Y* και *Z*, που αναφέρονται στο χρώμα, στην κατηγορία και τον αριθμό ενός χαρτιού, αντίστοιχα. Χρησιμοποιώντας αυτούς τους συμβολισμούς, έχουμε τα ακόλουθα αποτελέσματα:

1. $H(X) = -0{,}5\log 0{,}5 - 0{,}5\log 0{,}5 = 1$ bit

   $H(Y) = -0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 = 2$ bits

   $H(Z) = 13(-(1/13)\log(1/13)) = 3{,}7$ bits

2. $H(X, Y) = -0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 - 0{,}25\log 0{,}25 = 2$ bits

   $H(X, Z) = 26(-(1/26)\log(1/26)) = 4{,}7$ bits

3. $H(X, Y, Z) = 52(-(1/52)\log(1/52)) = 5$ bits

4. $H(Z/X) = H(X, Z) - H(X) = 4{,}7 - 1 = 3{,}7$ bits

5. $H(Y/X) = H(X, Y) - H(X) = 2 - 1 = 1$ bit

Αν απαντήσατε σωστά, έχετε πιάσει το νόημα! Αν όχι, ας δούμε στη συνέχεια πώς ακριβώς οδηγούμαστε στα αποτελέσματα αυτά.

Οι δυνατές τιμές της *X* είναι το μαύρο και το κόκκινο, της *Y* είναι μπαστούνια, σπαθιά, καρό και κούπες και της *Z* είναι οι αριθμοί από το ένα έως το 10 και βαλές, ντάμα και ρήγας, συνολικά δεκατρείς αριθμοί. Αφού το κάθε χαρτί μπορεί να τραβηχτεί με την ίδια πιθανότητα, η πιθανότητα να είναι αυτό μαύρο ή κόκκινο είναι 0,5 και η πιθανότητα να είναι αυτό μπαστούνι, σπαθί, καρό ή κούπα είναι 0,25. Αντίστοιχα, η πιθανότητα να είναι το «τρία» ή ο «ρήγας» ή οποιοδήποτε άλλο είναι 1/13. Από αυτές τις πιθανότητες μπορούμε να υπολογίσουμε την εντροπία της *X*, της *Y* και της *Z*, όπως στο σημείο 1.

Οι δυνατοί συνδυασμοί των *X* και *Y* για τους οποίους οι πιθανότητες είναι διάφορες του μηδενός είναι (μαύρο, μπαστούνι), (μαύρο, σπαθί), (κόκκινο, καρό) και (κόκκινο, κούπα). Η πιθανότητα αυτών των συνδυασμών είναι ίση με 0,25. Οι υπόλοιποι συνδυασμοί (μαύρο, καρό), (μαύρο, κούπα), (κόκκινο, μπαστούνι) και (κόκκινο, σπαθί) δεν μπορούν να λάβουν χώρα, δηλαδή η πιθανότητά τους είναι μηδενική. Έτσι, η συνδυασμένη πληροφορία των (*X*, *Y*) υπολογίζεται όπως ανωτέρω στο σημείο 2.

Επειδή μπορούμε, σε επόμενο ερώτημα, να χρησιμοποιήσουμε και τη συνδυασμένη πληροφορία των (X, Z), υπολογίζουμε και αυτή. Παρατηρούμε ότι υπάρχουν συνολικά 26 συνδυασμοί (1, μαύρο), (1, κόκκινο), (2, μαύρο), (2, κόκκινο) κ.ο.κ., των οποίων η πιθανότητα να λάβουν χώρα είναι (1/26). Έτσι, μπορούμε να υπολογίσουμε τη συνδυασμένη πληροφορία των (X, Z) όπως ανωτέρω στο σημείο 2.

Τώρα μας ενδιαφέρει η συνδυασμένη πληροφορία των (X, Y, Z). Οι δυνατοί συνδυασμοί είναι 52, δηλαδή (μαύρο, μπαστούνι, 1), (μαύρο, μπαστούνι, 2), …, (κόκκινο, κούπα, ρήγας) και η πιθανότητα για κάθε συνδυασμό να λάβει χώρα (1/52). Έτσι, η συνδυασμένη πληροφορία μπορεί να υπολογιστεί όπως ανωτέρω στο σημείο 3.

Για τον υπολογισμό τής υπό συνθήκης πληροφορίας της Z με δεδομένη τη X παρατηρούμε ότι η Z είναι ανεξάρτητη της X. Έτσι, η υπό συνθήκη πληροφορία της Z με δεδομένη την τιμή της X είναι ίση με την εντροπία της Z, δηλαδή ίση με 3,7 bits. Το αποτέλεσμα αυτό το υπολογίσαμε ανωτέρω, στο σημείο 4, με ένα δεύτερο τρόπο (Πίνακας 1.1), αφαιρώντας από τη συνδυασμένη πληροφορία $H(X, Z)$ την εντροπία της X, $H(X)$.

Τέλος, για τον υπολογισμό τής υπό συνθήκης πληροφορίας της Y με δεδομένη την τιμή της X παρατηρούμε ότι οι δυνατοί συνδυασμοί με πιθανότητα μεγαλύτερη του μηδενός είναι δύο: μπαστούνι ή σπαθί αν το χρώμα είναι μαύρο και καρό ή κούπα αν είναι κόκκινο. Η πιθανότητα για κάθε συνδυασμό είναι ίση με 0,5. Έτσι, η υπό συνθήκη πληροφορία είναι ίση με 1 bit, που υπολογίσαμε ανωτέρω, στο σημείο 5, αφαιρώντας από τη συνδυασμένη πληροφορία $H(X, Y)$ την εντροπία της X, $H(X)$.

1.9

Η αμοιβαία πληροφορία δίνεται από τη σχέση

$$I(X;Y) = H(Y) - H(Y/X) = 0,91 - 0,90 = 0,01 \text{ bits}$$

Αν τα καταφέρατε, ωραία! Αν όχι, μελετήστε και πάλι την Υποενότητα 1.5.3. Ο υπολογισμός της αμοιβαίας πληροφορίας είναι απλή εφαρμογή του αντίστοιχου τύπου.

1.10

Τα ζητούμενα μέτρα ποσότητας πληροφορίας δίνονται κατωτέρω στα σημεία 1, 2 και 3.

Αν τα καταφέρατε, συγχαρητήρια! Αν όχι, μελετήστε με προσοχή τα ακόλουθα:

Η πιθανότητα κάποιος που υποβάλλεται σε ιατρικές εξετάσεις να έχει υψηλή χοληστερίνη είναι $p(x_1) = 0,8$ και να έχει χαμηλή χοληστερίνη είναι $p(x_2) = 0,2$. Ένας

ασθενής με υψηλή χοληστερίνη, με πιθανότητα $p(y_1 / x_1) = 0,75$ κάνει δουλειά γραφείου και με πιθανότητα $p(y_2 / x_1) = 0,25$ δεν κάνει δουλειά γραφείου και ένας με χαμηλό επίπεδο χοληστερίνης με πιθανότητα $p(y_1 / x_2) = 0,5$ κάνει δουλειά γραφείου και, επίσης, με πιθανότητα $p(y_2 / x_2) = 0,5$ δεν κάνει δουλειά γραφείου.

1. Η μέση ποσότητα πληροφορίας που παρέχεται κατά τη γνωστοποίηση του αποτελέσματος μιας ιατρικής εξέτασης ως προς το επίπεδο χοληστερίνης δίνεται από τη σχέση

$$H(X) = -0,8 \log 0,8 - 0,2 \log 0,2 = 0,73 \text{ bits.}$$

2. Η πιθανότητα κάποιος με υψηλή χοληστερίνη να κάνει δουλειά γραφείου είναι 0,75 και να μην κάνει δουλειά γραφείου είναι 0,25. Η γνωστοποίηση του αν κάποιος με υψηλή χοληστερίνη κάνει δουλειά γραφείου ή όχι προσφέρει την ακόλουθη ποσότητα πληροφορίας:

$$H(\mathrm{Y} / \mathrm{x}_1) = -0,75 \log 0,75 - 0,25 \log 0,25 = 0,81 \text{ bits.}$$

3. Από τις υπό συνθήκη πιθανότητες $P(Y/X)$ και τις πιθανότητες $P(X)$ υπολογίζουμε τις συνδυασμένες πιθανότητες $P(X,Y) = \{0,6, 0,2, 0,1, 0,1\}$. Στη συνέχεια υπολογίζουμε

$$H(X,Y) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j) \log p(x_i, y_j) = 1,57 \text{ bits και}$$

$$H(Y / X) = H(Y,X) - H(X) = 1,57 - 0,73 = 0,84 \text{ bits.}$$

1.11

Τα ζητούμενα μέτρα της πληροφορίας είναι τα ακόλουθα:

1. $H(Y/x_2) = 0,81$ bits,
2. $H(Y/X) = 0,91$ bits,
3. $H(X, Y) = H(X) + H(Y/X) = 1 + 0,91 = 1,91$ bits,
4. $H(X/Y) = H(X, Y) - H(Y) = 1,91 - 0,96 = 0,95$ bits.

Αν τα καταφέρατε, συγχαρητήρια! Αν όχι, προσέξτε τα ακόλουθα σημεία στη νέα σας προσπάθεια:

Από τις δεδομένες πιθανότητες, μπορούμε να συνάγουμε τα ακόλουθα:

$$p(x_2) = \frac{1}{2},$$

$$p(y_2 / x) = \frac{1}{4},$$

$$p(y_1 / x_2) = \frac{1}{2}.$$

Επίσης, μπορούμε να υπολογίσουμε τις συνδυασμένες πιθανότητες, που δίνονται από

$$p(x_1, y_2) = p(y_1 / x_2)p(x_2) = \frac{1}{8},$$

$$p(x_2, y_1) = p(y_1 / x_2)p(x_2) = \frac{1}{4},$$

$$p(x_1, y_1) = p(y_1 / x_1)p(x_1) = \frac{3}{8},$$

$$p(x_2, y_2) = p(y_2 / x_2)p(x_2) = \frac{1}{4}.$$

Επομένως, μπορούμε να υπολογίσουμε τα ζητούμενα μέτρα ως ακολούθως:

$$\begin{aligned} H(Y / x_2) &= -p(y_1 / x_2)\log p(y_1 / x_2) - p(y_2 / x_2)\log p(y_2 / x_2) \\ &= -\frac{1}{4}\log\frac{1}{4} - \frac{3}{4}\log\frac{3}{4} = 0{,}81 \text{ bits}, \end{aligned}$$

$$H(Y / X) = -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i, y_j)\log p(y_j / x_i) = 0{,}91 \text{ bits},$$

$$H(X,Y) = H(X) + H(Y / X) = 1 + 0{,}91 = 1{,}91 \text{ bits},$$

$$H(Y) = -\frac{5}{8}\log\frac{5}{8} - \frac{3}{8}\log\frac{3}{8} = 0{,}96 \text{ bits},$$

$$H(X / Y) = H(X,Y) - H(Y).$$

2.1

Η εντροπία των συμβόλων, η μέγιστη εντροπία, ο πλεονασμός και ο μέσος ρυθμός πληροφορίας της πηγής είναι 1,5 bits/symbol, 1,59 bits/symbol, 0,0566 και 1500

bits/sec, αντίστοιχα.

Αν τα καταφέρατε, μπράβο! Είστε σε θέση να εφαρμόζετε τους αντίστοιχους τύπους με επιτυχία. Αν όχι, καλό είναι να προσπαθήσετε και πάλι, αφού μελετήσετε εκ νέου την Υποενότητα 2.1.1. Για σύγκριση παρατίθεται η ακόλουθη απάντηση:

Το αλφάβητο της πηγής είναι S = {X, Ψ, Ω} και η συνάρτηση πιθανότητας μάζας P = {0,25, 0,5, 0,25}. Εφαρμόζοντας τις εξισώσεις (2.1), (2.2), (2.3.) και (2.4), μπορούμε να υπολογίσουμε την εντροπία, τη μέγιστη μέση ποσότητα πληροφορίας, τον πλεονασμό και το μέσο ρυθμό πληροφορίας της πηγής:

$$H(S) = -\sum_{i=1}^{3} p_i \log p_i = -\frac{1}{4}\log\frac{1}{4} - \frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} = 1{,}5 \text{ bits / symbol},$$

$$\max H(S) = \log 3 = 1{,}59 \text{ bits / symbol},$$

$$red = 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{1{,}5}{1{,}59} = 0{,}0566,$$

$$R = r_S H(S) = 1500 \text{ H bits / sec}.$$

2.2

Το μέσο πληροφορικό περιεχόμενο των μηνυμάτων της πηγής είναι 2,44 bits/message. Αν τα καταφέρατε, πολύ ωραία! Αν όχι, προσπαθήστε και πάλι. Ο τρόπος υπολογισμού του ζητούμενου μέσου πληροφορικού περιεχομένου των μηνυμάτων ακολουθεί.

Το σύνολο των δυνατών μηνυμάτων είναι M = {(000), (001), (010), (011), (100), (101), (110), (111)} με συνάρτηση πιθανότητας μάζας P = {(27/64), (9/64), (9/64), (3/64), (9/64), (3/64), (3/64), (1/64)}. Με την εξίσωση (2.5) υπολογίζουμε το μέσο πληροφορικό περιεχόμενο της πηγής σε επίπεδο μηνυμάτων:

$$H(M) = -\sum_{i=1}^{8} p(m_i)\log p(m_i)$$

$$= -\frac{27}{64}\log\frac{27}{64} - 3\frac{3}{64}\log\frac{3}{64} - 3\frac{9}{64}\log\frac{9}{64} - \frac{1}{64}\log\frac{1}{64} = 2{,}44 \text{ bits / message}.$$

2.3

Αν οι πιθανότητες των κωδικών λέξεων είναι 1/2, 1/4, 1/8 και 1/8, τότε το μέσο πληροφορικό περιεχόμενο της πηγής είναι 1,75 bits. Επομένως, η επίδοση του κώδικα του Παραδείγματος 5 είναι α = 0,875 (2.9).

Στην περίπτωση των δεδομένων κωδικών λέξεων «1», «10», «100» και «1000» το μέσο πληροφορικό περιεχόμενο της πηγής, $H(S)$, είναι επίσης ίσο με 1,75 bits (2.1), το πλήθος των κωδικών συμβόλων είναι 2 και το μέσο μήκος των κωδικών λέξεων ίσο με 1,75. Επομένως, η επίδοση, a, είναι ίση με 1 (2.9).

Αν δεν τα καταφέρατε, θα πρέπει να μελετήσετε εκ νέου τις Υποενότητες 2.1.1 και 2.1.2, και ιδιαίτερα τους τύπους (2.1) και (2.9), αφού πρόκειται για απλή εφαρμογή τους, και να προσπαθήσετε και πάλι.

2.4

Για τη δεδομένη πηγή μπορούμε να σχηματίσουμε με τη βοήθεια του αλγόριθμου του Fano τις κωδικές λέξεις, οι οποίες παρατίθενται στην τρίτη στήλη του ακόλουθου πίνακα. Στην πρώτη στήλη περιέχονται τα σύμβολα και στη δεύτερη οι αντίστοιχες πιθανότητες εκπομπής τους. Σε παρένθεση, στην τρίτη στήλη του πίνακα, περιέχονται οι κωδικές λέξεις που θα προέκυπταν αν κατά τον εκάστοτε χωρισμό των συμβόλων σε δύο ομάδες αντιστοιχούσαμε στην πρώτη το κωδικό σύμβολο «0» και στη δεύτερη το «1», και όχι αντίστροφα.

Σύμβολα Πηγής	Πιθανότητες	Κωδικές Λέξεις
S_1	1/4	11 (00)
S_2	1/4	10 (01)
S_3	1/8	011 (100)
S_4	1/8	010 (101)
S_5	1/16	0011 (1100)
S_6	1/16	0010 (1101)
S_7	1/32	00011 (11100)
S_8	1/32	00010 (11101)
S_9	1/32	00001 (11110)
S_{10}	1/32	00000 (11111)

Αν τα καταφέρατε, μπράβο! Είστε σε θέση να εφαρμόζετε τον αλγόριθμο του Fano. Αν είχατε δυσκολίες στην απάντηση, θα πρέπει να επαναλάβετε τη μελέτη του αλγόριθμου και να προσπαθήσετε πάλι. Η άσκηση αυτή αποτελεί απλή σχετικά εφαρμογή του αλγόριθμου κωδικοποίησης του Fano.

2.5

Σύμβολα Πηγής	Πιθανότητες Συμβόλων	P_i	Μήκος l_i	Ανάπτυγμα του P_i	Κώδικας Shannon	Κώδικας Fano
S_1	27/128	$P_1 = 0$	$l_1 = 3$	.0000000	000	00
S_2	27/128	$P_2 = 27/128$	$l_2 = 3$	.0011011	001	010
S_3	9/128	$P_3 = 54/128$	$l_3 = 4$	.0110110	0110	011
S_4	9/128	$P_4 = 63/128$	$l_4 = 4$	.0111111	0111	1000
S_5	9/128	$P_5 = 72/128$	$l_5 = 4$	.1001000	1001	1001
S_6	9/128	$P_6 = 81/128$	$l_6 = 4$	.1010001	1010	1010
S_7	9/128	$P_7 = 90/128$	$l_7 = 4$	.1011010	1011	1011
S_8	9/128	$P_8 = 99/128$	$l_8 = 4$	.1100011	1100	1100
S_9	3/128	$P_9 = 108/128$	$l_9 = 6$	.1101100	110110	110110
S_{10}	3/128	$P_{10} = 111/128$	$l_{10} = 6$	.1101111	110111	110011
S_{11}	3/128	$P_{11} = 114/128$	$l_{11} = 6$	.1110010	111001	111001
S_{12}	3/128	$P_{12} = 117/128$	$l_{12} = 6$	.1110101	111010	111010
S_{13}	3/128	$P_{13} = 120/128$	$l_{13} = 6$	.1111000	111100	111100
S_{14}	3/128	$P_{14} = 123/128$	$l_{14} = 6$	.1111011	111101	111101
S_{15}	2/128	$P_{15} = 126/128$	$l_{15} = 6$	.1111110	111111	111111

Αν τα καταφέρατε, μπράβο! Αν όχι, μελετήστε εκ νέου τους αλγόριθμους κωδικοποίησης του Fano και του Shannon, καθώς και τα Παραδείγματα 6, 7 και 8 και προσπαθήστε και πάλι.

2.6

1. Η εντροπία της πηγής υπολογίζεται από την εξίσωση (2.1):

$$\begin{aligned} H(S) &= -\sum_{i=1}^{8} p(s_i)\log p(s_i) \\ &= -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{16}\log\frac{1}{16} - \\ &\quad -\frac{1}{32}\log\frac{1}{32} - \frac{1}{64}\log\frac{1}{64} - 2\frac{1}{128}\log\frac{1}{128} \\ &= 1{,}98 \text{ bits / symbol.} \end{aligned}$$

2. Με τη βοήθεια του τύπου (2.9) μπορούμε να υπολογίσουμε την επίδοση του δεδομένου κώδικα:

$$a = \frac{H(S)}{\sum_{i=1}^{8} l_i p_i \log 2} = \frac{1,98}{3} = 0,66$$

3. Ο αλγόριθμος κωδικοποίησης του Huffman μάς οδηγεί στον ακόλουθο κώδικα:

Σύμβολα	Πιθανότητες							Κώδικας
S_1	1/2	1/2	1/2	1/2	1/2	1/2	1/2 (0)	0
S_2	1/4	1/4	1/4	1/4	1/4	1/4 (0)	1/2 (1)	10
S_3	1/8	1/8	1/8	1/8	1/8 (0)	1/4 (1)		110
S_4	1/16	1/16	1/16	1/16 (0)	1/8 (1)			1110
S_5	1/32	1/32	1/32 (0)	1/16 (1)				11110
S_6	1/64	1/64 (0)	1/32 (1)					111110
S_7	1/128 (0)	1/64 (1)						1111110
S_8	1/128 (1)							1111111

4. Το μέσο μήκος των κωδικών λέξεων του κώδικα Huffman και η επίδοσή του υπολογίζονται ως εξής:

$$\sum_{i=1}^{8} l_i p_i = \frac{1}{2} + 2\frac{1}{4} + 3\frac{1}{8} + 4\frac{1}{16} + 5\frac{1}{32} + 6\frac{1}{64} + 7\frac{1}{128} + 7\frac{1}{128} = 1,98 \text{ bits / symbol}$$

$$a_H = \frac{H(S)}{\sum_{i=1}^{8} l_i p_i \log 2} = \frac{1,98}{1,98} = 1$$

Ο αλγόριθμος του Huffman οδηγεί, λοιπόν, σε άριστο δυαδικό κώδικα, αφού η επίδοσή του είναι ίση με 1, δηλαδή το μέσο μήκος των κωδικών του λέξεων είναι ίσο με την εντροπία των συμβόλων της πηγής.

Αν τα καταφέρατε, μπράβο! Σίγουρα έχετε την ικανότητα να εφαρμόζετε τον αλγόριθμο του Huffman. Αν όμως δεν τα καταφέρατε, προσπαθήστε και πάλι, αφού μελετήσετε προσεκτικά ακόμα μια φορά τον αλγόριθμο, καθώς και το Παράδειγμα 9. Επίσης, μια καλή ιδέα είναι να προχωρήσετε πιο πέρα και να κατασκευάσετε και

κωδικούς για τη δεδομένη πηγή σύμφωνα με τους αλγόριθμους κωδικοποίησης του Fano και του Shannon και να υπολογίσετε τις επιδόσεις τους.

2.7

Σύμβολα	Πιθανότητες	Κώδικας ($q = 2$)	Κώδικας ($q = 3$)	Κώδικας ($q = 4$)
S_1	0,32	00	0	0
S_2	0,24	01	1	1
S_3	0,20	10	20	2
S_4	0,09	1100	210	30
S_5	0,05	1101	211	31
S_6	0,04	1110	220	32
S_7	0,04	11110	221	330
S_8	0,02	11111	222	331

Αν τα καταφέρατε, συγχαρητήρια! Σίγουρα έχετε κατανοήσει τους αλγόριθμους κωδικοποίησης. Αν όχι, μελετήστε και πάλι την περιγραφή του αλγόριθμου και προσέξτε ιδιαίτερα, στην επόμενη προσπάθειά σας, κατά το χωρισμό των συμβόλων σε ισοπίθανες ομάδες τα σύμβολα που περιέχονται σε κάθε ομάδα να είναι συνεχόμενα στη διάταξη που προκύπτει κατά φθίνουσα πιθανότητα εμφάνισης. Στη δυαδική κωδικοποίηση τα σύμβολα χωρίζονται σε δύο ομάδες, (S_1, S_2) και (S_3, S_4, S_5, S_6, S_7, S_8) και τους αποδίδονται το «0» και το «1», αντίστοιχα. Τα σύμβολα της πρώτης ομάδας χωρίζονται σε δύο υποομάδες που περιέχουν από ένα σύμβολο πηγής, το S_1 και το S_2, στις οποίες αποδίδονται το «0» και το «1» και επομένως οι κωδικές τους λέξεις είναι «00» και «01», αντίστοιχα. Η δεύτερη ομάδα χωρίζεται στις υποομάδες (S_3) και (S_4, S_5, S_6, S_7, S_8), αφού έτσι προσεγγίζεται καλύτερα η απαίτηση για ισοπίθανες ομάδες, δηλαδή έχουμε πιθανότητες 0,20 και 0,24, αντίστοιχα. Αν είχαμε σχηματίσει τις υποομάδες (S_3, S_4) και (S_5, S_6, S_7, S_8), οι πιθανότητες θα ήταν 0,29 και 0,15, δηλαδή θα διέφεραν πολύ περισσότερο μεταξύ τους. Συνεχίζοντας κατά τον ίδιο τρόπο, λαμβάνουμε το δυαδικό κώδικα που περιέχεται στον πίνακα.

Κατά την κατασκευή του κώδικα με τρία κωδικά σύμβολα, το «0», «1» και «2», ο αρχικός χωρισμός οδηγεί στις ομάδες (S_1), (S_2) και (S_3, S_4, S_5, S_6, S_7, S_8), αφού έτσι προκύπτει η μικρότερη δυνατή διαφορά στις (αθροιστικές) πιθανότητές τους. (Η μικρότερη δυνατή διαφορά πιθανοτήτων προκύπτει και για τις ομάδες (S_1), (S_2, S_3)

και (S_4, S_5, S_6, S_7, S_8). Θα μπορούσαμε επομένως να διαλέξουμε και αυτές τις ομάδες). Οι πιθανότητες αυτών των ομάδων είναι 0,32, 0,24 και 0,44, αντίστοιχα. Αν είχαμε χωρίσει τα σύμβολα στις ομάδες (S_1), (S_2, S_3, S_4) και (S_5, S_6, S_7, S_8), οι πιθανότητές τους θα ήταν 0,32, 0,53 και 0,15, δηλαδή θα διέφεραν μεταξύ τους πολύ περισσότερο. Αφού, λοιπόν, επιλέξουμε κατάλληλα τις ομάδες στις οποίες χωρίζονται τα σύμβολα, αποδίδουμε σ' αυτές τα κωδικά σύμβολα «0», «1» και «2», αντίστοιχα. Επομένως, το S_1 κωδικοποιείται με τη λέξη «0» και το S_2 με τη λέξη «1». Η τρίτη ομάδα χωρίζεται στις υποομάδες (S_3), (S_4, S_5) και (S_6, S_7, S_8), στις οποίες αποδίδουμε τα κωδικά σύμβολα «0», «1» και «2». Συνεχίζοντας όπως προηγουμένως, καταλήγουμε στον κώδικα που περιέχεται στον πίνακα.

Κατά την κατασκευή του κώδικα με τέσσερα κωδικά σύμβολα, τα «0», «1», «2» και «3», ο αρχικός χωρισμός οδηγεί στις ομάδες (S_1), (S_2), (S_3) και (S_4, S_5, S_6, S_7, S_8), αφού έτσι προκύπτει η μικρότερη δυνατή διαφορά στις (αθροιστικές) πιθανότητές τους. Στις ομάδες αυτές αποδίδουμε τα κωδικά σύμβολα «0», «1», «2» και «3», αντίστοιχα. Επομένως, το S_1 κωδικοποιείται με τη λέξη «0», το S_2 με τη λέξη «1» και το S_3 με τη λέξη «2». Η τέταρτη ομάδα χωρίζεται στις υποομάδες (S_4), (S_5), (S_6) και (S_7, S_8), στις οποίες αποδίδονται τα κωδικά σύμβολα «0», «1», «2» και «3», αντίστοιχα. Συνεχίζοντας κατά τον ίδιο τρόπο, οδηγούμαστε στον κώδικα που περιέχεται στον πίνακα.

2.8

Τα ζητούμενα αποτελέσματα της άσκησης είναι τα εξής:

1. $p(\varphi) = 9/27$, $p(x) = 2/27$ και $p(\psi) = 16/27$,
2. 0,93 bits/symbol,
3. 2,18 bits/message.

Αν τα καταφέρατε, συγχαρητήρια! Αν όχι, ας δούμε στη συνέχεια τα πιο βασικά σημεία. Το πλήθος των καταστάσεων της πηγής είναι ίσο με το πλήθος των συμβόλων, αφού πρόκειται για Μαρκοβιανή αλυσίδα πρώτης τάξης (Υποενότητα 2.2.1). Επομένως, η κατάσταση της πηγής περιγράφει το τελευταίο σύμβολο που αυτή παρήγαγε και έτσι η πιθανότητα παραγωγής ενός συμβόλου είναι ίση με την πιθανότητα της αντίστοιχης κατάστασης της πηγής. Η σχέση $\pi P = \pi$ (Υποενότητα 2.2.1) περιγράφει τη σχέση που υφίσταται μεταξύ των πιθανοτήτων μετάβασης και των πιθανοτήτων των καταστάσεων της πηγής. Από τη σχέση αυτή λαμβάνουμε το ακόλουθο σύστημα εξισώσεων, όπου $p(\varphi)$ είναι η πιθανότητα παραγωγής του φ ή της αντίστοιχης κατάστασης της πηγής, $p(\chi)$ η πιθανότητα παραγωγής του συμβόλου χ και $p(\psi)$ η πιθανότητα παραγωγής του ψ:

$$p(\varphi) = p(\varphi)P(\varphi/\varphi) + p(x)P(\varphi/x) + p(\psi)P(\varphi/\psi)$$

$$p(\chi) = p(\varphi)P(\chi/\varphi) + p(x)P(\chi/x) + p(\psi)P(\chi/\psi)$$

$$p(\psi) = p(\varphi)P(\psi/\varphi) + p(x)P(\psi/x) + p(\psi)P(\psi/\psi)$$

Επίσης, το άθροισμα των πιθανοτήτων όλων των καταστάσεων είναι ίσο με τη μονάδα:

$$p(\varphi) + p(x) + p(\psi) = 1$$

Η επίλυση του συστήματος των τεσσάρων εξισώσεων με τους τρεις αγνώστους οδηγεί στην ακόλουθη λύση:

$$p(\varphi) = 9/27,\ p(x) = 2/27 \text{ και } p(\psi) = 16/27$$

Οι (2.12) και (2.13) επιτρέπουν τον υπολογισμό της εντροπίας της πηγής:

$$H(S) = -\sum_{i=1}^{3} p_i \sum_{j+1}^{3} P_{ij} \log P_{ij} = 0{,}93 \text{ bit / symbol}$$

Τέλος, το μέσο πληροφορικό περιεχόμενο μηνυμάτων αποτελούμενων από δύο σύμβολα μπορεί να υπολογιστεί από την εξίσωση (2.14). Το πλήθος των διαφορετικών μηνυμάτων που αποτελούνται από δύο σύμβολα είναι ίσο με το τετράγωνο του πλήθους των συμβόλων της πηγής, δηλαδή ίσο με 9. Οι πιθανότητες εκπομπής αυτών των μηνυμάτων μπορούν να υπολογιστούν από τον πίνακα μετάβασης και τις υπολογισμένες πιθανότητες εκπομπής των συμβόλων. Έτσι, η πιθανότητα εκπομπής του μηνύματος m_k που σχηματίζεται από τα σύμβολα s_i *και* s_j δίνεται από την ακόλουθη σχέση:

$$P(m_k = s_i\, s_j) = p(s_i, s_j) = p(s_i)P(s_j / s_i)$$

Επομένως, οι πιθανότητες όλων των δυνατών μηνυμάτων είναι

$$p(\varphi\varphi) = p(\varphi)P(\varphi/\varphi) = (9/27)(0) = 0,$$

$$p(\varphi\chi) = p(\varphi)P(\chi/\varphi) = 1/15,$$

$$p(\varphi\psi) = p(\varphi)P(\psi/\varphi) = 4/15$$

$$p(\chi\varphi) = p(\chi)P(\varphi/\chi) = (2/27)(1/2) = 2/54,$$

$$p(\chi\chi) = p(\chi)P(\chi/x) = 2/270,$$

$$p(\chi\psi) = p(\chi)P(\psi/\chi) = 4/135$$

$$p(\psi\varphi) = p(\psi)P(\varphi/\psi) = 16/54,$$

$$p(\psi\chi) = p(\psi)P(\chi/\psi) = 0,$$

$$p(\psi\psi) = p(\psi)P(\psi/\psi) = 16/54.$$

Απλή εφαρμογή του τύπου (2.14) οδηγεί στον υπολογισμό του μέσου πληροφορι-

κού περιεχομένου των μηνυμάτων που αποτελούνται από δύο σύμβολα. Το αποτέλεσμα είναι $H(M) = 2{,}18$ bits/symbol.

Ωστόσο, υπάρχει ακόμα ένας τρόπος να υπολογίσουμε το μέσο πληροφορικό περιεχόμενο των μηνυμάτων, που θα συζητήσουμε στη συνέχεια. Όπως είδαμε στην Υποενότητα 1.4, η συνδυασμένη ποσότητα πληροφορίας δύο τυχαίων μεταβλητών, X και Y, ισούται με το άθροισμα της ποσότητας πληροφορίας $H(X)$ με την υπό συνθήκη ποσότητα πληροφορίας $H(Y/X)$. Θεωρώντας ότι οι τυχαίες μεταβλητές X και Y αναπαριστούν την εκπομπή ενός συμβόλου από την πηγή, η μέση ποσότητα πληροφορίας μηνυμάτων αποτελούμενων από δύο σύμβολα είναι ίση με τη συνδυασμένη ποσότητα πληροφορίας των X και Y.

Η $H(X)$ είναι ίση με την ποσότητα πληροφορίας πηγής χωρίς μνήμη που εκπέμπει τα σύμβολα φ, χ και ψ με τις πιθανότητες που υπολογίσαμε:

$$H(X) = -\sum_{i=1}^{3} p(x_i)\log p(x_i) = -p(\varphi)\log p(\varphi) - p(x)\log p(x) - p(\psi)\log p(a)$$
$$= -\frac{9}{27}\log\frac{9}{27} - \frac{2}{27}\log\frac{2}{27} - \frac{16}{27}\log\frac{16}{27} = 1{,}25 \text{ bits / symbol.}$$

Από την άλλη πλευρά, η $H(Y/X)$ είναι ίση με την εντροπία της πηγής που υπολογίσαμε πιο πάνω, αφού η εντροπία της πηγής ορίστηκε ως το πληροφορικό περιεχόμενο μιας τυχαίας μετάβασης κατάστασης της πηγής [δείτε τύπους (2.12) και (2.13)]. Επομένως, το μέσο πληροφορικό περιεχόμενο μηνυμάτων αποτελούμενων από δύο σύμβολα είναι

$$H(M) = H(X,Y) = H(X) + H(Y/X) = 1{,}25 + 0{,}93 = 2{,}18 \text{ bits / message.}$$

Το μέσο πληροφορικό περιεχόμενο ανά σύμβολο που προκύπτει αν διαιρέσουμε το $H(M)$ με το πλήθος των συμβόλων του μηνύματος, δηλαδή με το 2, είναι σημαντικά μεγαλύτερο από την εντροπία της πηγής. Όπως ήδη γνωρίζουμε από την Πρόταση 2.3, όταν το πλήθος των συμβόλων των μηνυμάτων τείνει στο άπειρο, τότε το μέσο πληροφορικό περιεχόμενο των συμβόλων, που προκύπτει από τη διαίρεση του πληροφορικού περιεχομένου των μηνυμάτων δια του πλήθους των συμβόλων, τείνει στην εντροπία της πηγής.

2.9

Τα ζητούμενα αποτελέσματα είναι τα εξής:

$$red = 1 - \frac{H_{\text{χωρίς μνήμη}}(S)}{\max H(S)} = 1 - \frac{1,25}{\log 3} = 0,21$$

$$red_{\varepsilon\xi} = 1 - \frac{H_{\text{με μνήμη}}(S)}{H_{\text{χωρίς μνήμη}}(S)} = 1 - \frac{0,93}{1,25} = 0,26$$

$$red_{o\lambda} = 1 - \frac{H_{\text{με μνήμη}}(S)}{\max H(S)} = 1 - \frac{H_{\text{με μνήμη}}(S)}{\log q} = 1 - \frac{0,93}{1,58} = 0,41.$$

Αν τα καταφέρατε, πολύ ωραία! Αν όχι, τότε, αφού μελετήσετε εκ νέου την Υποενότητα 2.2.3, προσπαθήστε και πάλι.

Η απλή εφαρμογή των τύπων (2.3), (2.17) και (2.18) μάς επιτρέπει τον υπολογισμό του πλεονασμού, του πλεονασμού εξάρτησης και του ολικού πλεονασμού. Όσο για το μέτρο του πλεονασμού, αυτό αναφέρεται σε πηγές χωρίς μνήμη. Παρ' όλα αυτά, ζητήθηκε να υπολογιστεί και για τη δεδομένη πηγή με μνήμη, θεωρώντας τη για τον υπολογισμό αυτό ως πηγή χωρίς μνήμη.

2.10

Από τη συνδυασμένη συνάρτηση πυκνότητας πιθανότητας, $f(x,y)$, μπορούμε να υπολογίσουμε τις ακραίες συναρτήσεις πυκνότητας πιθανότητας $f(x)$ και $f(y)$ και στη συνέχεια και τις υπό συνθήκη συναρτήσεις πυκνότητας πιθανότητας, $f(x/y)$ και $f(y/x)$, ως ακολούθως. Τέλος, από τις συναρτήσεις πυκνότητας πιθανότητας μπορούμε να υπολογίσουμε τις ζητούμενες ποσότητες πληροφορίας.

$$f(x) = \int_0^{4-2x} f(x,y)dy = \frac{1}{4}y\Big|_0^{4-2x} = 1 - \frac{1}{2}x,\ 0 \le x \le 2$$

$$f(y) = \int_0^{2-\frac{y}{2}} f(x,y)dx = \frac{1}{4}x\Big|_0^{2-\frac{y}{2}} = \frac{1}{2} - \frac{1}{8}y,\ 0 \le y \le 4$$

$$f(x/y) = \frac{f(x,y)}{f(y)} = \frac{2}{4-y},\ 0 \le x \le 2 - \frac{1}{2}y$$

$$f(x/y) = \frac{f(x,y)}{f(x)} = \frac{1}{4-2x},\ 0 \le y \le 4 - 2x$$

$$H(X)=-\int_0^2\left(1-\frac{1}{2}x\right)\log\left(1-\frac{1}{2}x\right)dx,$$

$$=2\int_1^0 z\log z\,dz=2\log e\int_1^0 z\ln z\,dz,$$

$$=2\log e\left[\frac{1}{2}z^2\ln z-\frac{1}{4}z^2\right]_1^0=\log\sqrt{e}\approx 0,72,$$

$$H(Y)=-\int_0^4\left(\frac{1}{2}-\frac{1}{8}y\right)\log\left(\frac{1}{2}-\frac{1}{8}y\right)dy=\log 2\sqrt{e}\approx 1,72,$$

$$H(X/Y)=H(X,Y)-H(Y)=2-\log 2\sqrt{e}=\log\frac{2}{\sqrt{e}}\approx 0,28,$$

$$H(Y/X)=H(X,Y)-H(X)=2-\log\sqrt{e}=\log\frac{4}{\sqrt{e}}\approx 1,28,$$

$$H(X,Y)=-\int_0^2\int_0^{4-2x}f(x,y)\log f(x,y)\,dxdy=-\int_0^2\int_0^{4-2x}\frac{1}{4}\log\frac{1}{4}\,dxdy,$$

$$=\frac{1}{2}\int_0^2(4-2x)dx=\frac{1}{2}(4x-x^2)\Big|_0^2=2,$$

$$I(X;Y)=H(X)+H(Y)-H(X,Y)=0,44.$$

Αν τα καταφέρατε, μπράβο! Είστε σε θέση να εφαρμόζετε με επιτυχία τους τύπους της Ενότητας 2.3. Αν δεν τα καταφέρατε με την πρώτη, μην απογοητεύεστε. Προσπαθήστε και πάλι.

3.1

Η χωρητικότητα του διακριτού καναλιού είναι ίση με

$$C=\max_{p(x)}I(X;Y)r=1+p\log p+(1-p)\log(1-p)\text{ bits / sec.}$$

Αν τα καταφέρατε, μπράβο! Αν όχι, ας επιχειρήσουμε μαζί την επίλυση της άσκησης.

Όπως είδαμε στο Παράδειγμα 1, από τα δεδομένα $p(x_1 = 0) = a$, $p(x_2 = 1) = 1 - a$ και $p(0/0) = p(1/1) = (1 - p)$ μπορούμε να υπολογίσουμε τις πιθανότητες εμφάνισης σφάλματος $p(1/0) = p(0/1) = 1 - p$. Επίσης, έχουμε την πιθανότητα $p(y_1 = 0) = b$ και επομένως $p(y_2 = 1) = 1 - b$. Ισχύει, βεβαίως, η σχέση $b = a(1 - p) + (1 - a)p$, αφού $p(y_1) = p(x_1)\,p(0/0) + p(x_2)\,p(1/0)$. Εφαρμόζοντας τις σχέσεις της Ενότητας 3.1, υπολογίζουμε την αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου

του καναλιού.

$$I(X;Y) = H(Y) - H(Y/X)$$
$$= -b\log b - (1-b)\log(1-b) + p\log p + (1-p)\log(1-p).$$

Η χωρητικότητα του διακριτού καναλιού υπολογίζεται επιλέγοντας τις τιμές των $p(x_i)$ που οδηγούν στη μέγιστη τιμή της αμοιβαίας εντροπίας μεταξύ της εισόδου και της εξόδου του καναλιού (3.1). Αφού p είναι ανεξάρτητο του b (ή του a), η μέγιστη τιμή προκύπτει για την πιθανότητα b που μεγιστοποιεί την ποσότητα $-b\log b - (1-b)\log(1-b)$. Γνωρίζουμε από τις ιδιότητες της ποσότητας πληροφορίας, που είδαμε στο Κεφάλαιο 1, ότι η ποσότητα αυτή μεγιστοποιείται για $b = 1-b$. Επομένως, $b = 1/2$. Έτσι, η χωρητικότητα του καναλιού, που δίνεται από τη σχέση (3.2), γράφεται:

$$C = \max_{p(x)} I(X;Y)r = 1 + p\log p + (1-p)\log(1-p) \text{ bits/sec.}$$

Παρατηρούμε ότι για $p = 1/2$ είναι $C = 0$ και για $p = 1$ (ή $p = 0$) είναι $C = 1$ bit/sec.

3.2

Η ποσότητα πληροφορίας της εξόδου, η αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου και η χωρητικότητα του καναλιού δίνονται από τις ακόλουθες σχέσεις:

$$H(Y) = -(1-a+ap)\log(1-a+ap) - a(1-p)\log a(1-p)$$

$$I(X;Y) = -(1-a+ap)\log(1-a+ap) - a(1-p)\log a + ap\log p$$

$$C = -\log \frac{p^{\frac{p}{p-1}}}{1-p+p^{\frac{p}{p-1}}} \text{ bits/sec}$$

Αν τα καταφέρατε, μπράβο! Απαιτούσε αρκετή προσπάθεια. Αν όχι, ας προσπαθήσουμε μαζί.

Πρώτα υπολογίζουμε τις πιθανότητες εξόδου:

$$p(y_1) = p(x_1)\,p(y_1|x_1) + p(x_2)\,p(y_1|x_2) = (1-a) + ap,$$

$$p(y_2) = p(x_2)\,p(y_2|x_2) = a(1-p).$$

Τώρα μπορούμε να υπολογίσουμε την εντροπία της εξόδου του καναλιού ως ακολούθως:

$$H(Y) = -\sum_{i=1}^{2} p(y_i) \log p(y_i) = -(1-a+ap)\log(1-a+ap) - a(1-p)\log a(1-p).$$

Για τον υπολογισμό της αμοιβαίας πληροφορίας μεταξύ της εισόδου και της εξόδου απαιτείται η υπό συνθήκη ποσότητα πληροφορίας $H(Y/X)$, η οποία υπολογίζεται στη συνέχεια (δείτε την Ενότητα 3.1).

$$\begin{aligned} H(Y/X) &= -\sum_{i=1}^{2}\sum_{j=1}^{2} p(x_i)\, p(y_j / x_i) \log p(y_j / x_i) \\ &= -(1-a).1\log 1 - ap\log p - a(1-p)\log(1-p). \end{aligned}$$

Από την εντροπία της εξόδου του καναλιού $H(Y)$ και την υπό συνθήκη ποσότητα πληροφορίας $H(Y/X)$ μπορούμε να υπολογίσουμε τη ζητούμενη αμοιβαία πληροφορία:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y/X) \\ &= -(1-a+ap)\log(1-a+ap) - a(1-p)\log a + ap\log p. \end{aligned}$$

Τέλος, για τον υπολογισμό της χωρητικότητας του καναλιού πρέπει να υπολογίσουμε την τιμή της πιθανότητας εισόδου a που μεγιστοποιεί την αμοιβαία ποσότητα πληροφορίας $I(X;Y)$. Για το λόγο αυτό πρώτα σχηματίζουμε την πρώτη παράγωγο της $I(X;Y)$ ως προς a:

$$\begin{aligned} I'(X;Y) = \frac{dI(X;Y)}{da} &= (1-p)\log(1-a+ap) - (1-a+ap)\frac{p-1}{1-a+ap}\log e \\ &\quad -(1-p)\log a - a(1-p)\frac{1}{a}\log e + p\log p \\ &= (1-p)\log(1-a+ap) - (1-p)\log a + p\log p. \end{aligned}$$

Θέτοντας την πρώτη παράγωγο ως προς a ίση με 0, λαμβάνουμε:

$$\begin{aligned} &(1-p)\log(1-a+ap) - (1-p)\log a + p\log p = 0 \\ &\log\frac{1-a+ap}{a} = -\frac{p}{1-p}\log p = -\log p^{\frac{p}{1-p}} \\ &1-a+ap = ap^{\frac{p}{p-1}} \Rightarrow a = \frac{1}{1-p+p^{\frac{p}{p-1}}}. \end{aligned}$$

Θέτοντας αυτή την τιμή της πιθανότητας a στην ανωτέρω έκφραση της αμοιβαίας πληροφορίας μεταξύ της εισόδου και της εξόδου, λαμβάνουμε τη ζητούμενη χωρητικότητα του διακριτού καναλιού Z ως προς p.

$$C = \max_{p(x)} I(X;Y)r = \left[-ap^{\frac{p}{p-1}} \log ap^{\frac{p}{p-1}} - a(1-p)\log a + ap \log p \right] 1$$

$$= -a\frac{1-a+ap}{a}\log a - a\frac{1-a+ap}{a}\frac{p}{p-1}\log p - a\log a + ap\log a + ap\log p$$

$$= \frac{-p\log a + \log a - p\log p}{p-1} = -\log a - \frac{p}{p-1}\log p = -\log a - \log p^{\frac{p}{p-1}}$$

$$= -\log \frac{p^{\frac{p}{p-1}}}{1-p+p^{\frac{p}{p-1}}} \text{ bits / sec.}$$

3.3

Η πιθανότητα q πρέπει να πληροί την ακόλουθη σχέση για να λάβει η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού τη μέγιστη τιμή της:

$$(1-q)^{2(1-q)} = q^{(1-2q)}.$$

Αν τα καταφέρατε, μπράβο! Απαιτούσε αρκετή προσπάθεια. Αν όχι, ας δούμε στη συνέχεια πώς μπορούμε να απαντήσουμε. Από τα δεδομένα της άσκησης έχουμε τα ακόλουθα:

$$p(X = x_0 = 0) = p(X = x_1 = 1) = \frac{p}{2},$$

$$p(X = x_2 = 2) = p(X = x_3 = 3) = \frac{q}{2},$$

$$p(x_0 / y_0) = p(x_1 / y_1) = 1,$$

$$p(x_2 / y_2) = p(x_3 / y_3) = p,$$

$$p(x_3 / y_2) = p(x_2 / y_3) = 1 - p = q,$$

$$p(y_0) = \sum_{i=0}^{3} p(x_i)p(x_i \mid y_0) = \frac{p}{2},$$

$$p(y_1) = \sum_{i=0}^{3} p(x_i)p(x_i \mid y_1) = \frac{p}{2},$$

$$p(y_2) = \sum_{i=0}^{3} p(x_i)p(x_i \mid y_2) = \frac{q}{2}p + \frac{q}{2}(1-p) = \frac{q}{2},$$

$$p(y_3) = \sum_{i=0}^{3} p(x_i)p(x_i \mid y_3) = \frac{q}{2}(1-p) + \frac{q}{2}p = \frac{q}{2},$$

$$
\begin{aligned}
H(X) &= -\sum_{i=0}^{3} p(x_i)\log p(x_i),\\
&= -\frac{p}{2}\log\frac{p}{2} - \frac{p}{2}\log\frac{p}{2} - \frac{q}{2}\log\frac{q}{2} - \frac{q}{2}\log\frac{q}{2},\\
&= -p(\log p - 1) - q(\log q - 1) a \underset{p+q=1}{=} 1 - p\log p - q\log q,
\end{aligned}
$$

$$
\begin{aligned}
H(X/Y) &= -\sum_{i=0}^{3}\sum_{j=0}^{3} p(y_j)p(x_i/y_j)\log(x_i/y_j),\\
&= -p(y_0)p(x_0/y_0)\log p(x_0/y_0) - p(y_1)p(x_1/y_1)\log p(x_1/y_1),\\
&\quad -p(y_2)p(x_2/y_2)\log p(x_2/y_2) - p(y_3)p(x_3/y_3)\log p(x_3/y_3),\\
&\quad -p(y_2)p(x_3/y_2)\log p(x_3/y_2) - p(y_3)p(x_2/y_3)\log p(x_2/y_3),\\
&= -\frac{p}{2}1\log 1 - \frac{p}{2}1\log 1 - \frac{q}{2}p\log p - \frac{q}{2}p\log p - \frac{q}{2}q\log q - \frac{q}{2}q\log q,\\
&= -0 - 0 - qp\log p - q^2\log q.
\end{aligned}
$$

Τώρα μπορούμε να σχηματίσουμε τη διαφορά της εντροπίας της εισόδου μειωμένης κατά την υπό συνθήκη εντροπία της εισόδου με δεδομένη την έξοδο:

$$
\begin{aligned}
I(X;Y) &= H(X) - H(X\,|\,Y)\\
&= 1 - p\log p - q\log q + pq\log p + q^2\log q\\
&\underset{p=1-q}{=} 1 - (1-q)^2\log(1-q) - q(1-q)\log q.
\end{aligned}
$$

Θέτοντας την πρώτη παράγωγο της $I(X;Y)$ ως προς q ίση με μηδέν, μπορούμε να προσδιορίσουμε τη ζητούμενη σχέση:

$$
\begin{aligned}
\frac{dI(X;Y)}{dq} &= -2(1-q)(-1)\log(1-q) - (1-q)^2\frac{(-1)}{1-q}\log e -\\
&\quad -(1-q)\log q - q(1-q)\frac{1}{q}\log e\\
&= 2(1-q)\log(1-q) - (1-2q)\log q = 0
\end{aligned}
$$

$$
\begin{aligned}
\frac{dI(X;Y)}{dq} = 0 &\Rightarrow 2(1-q)\log(1-q) = (1-2q)\log q\\
&\Rightarrow (1-q)^{2(1-q)} = q^{(1-2q)}.
\end{aligned}
$$

Η τελευταία είναι η ζητούμενη σχέση. (Αν υπολογίσουμε τιμή του q που πληροί τη σχέση αυτή, τότε μπορούμε να υπολογίσουμε τη χωρητικότητα του διακριτού καναλιού, θέτο-

ντας την τιμή αυτή στην ανωτέρω σχέση της αμοιβαίας πληροφορίας και πολλαπλασιάζοντας την αμοιβαία πληροφορία με το ρυθμό μετάδοσης κωδικών συμβόλων.)

3.4

	Σωστό	Λάθος
Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην είσοδο του καναλιού είναι ίσο με $M_x = 2^{lH(X)}$.	☑	❑
Το πλήθος των πιο πιθανών μηνυμάτων μήκους l στην έξοδο του καναλιού είναι ίσο με $M_y = 2^{lH(Y)}$.	☑	❑
Το πλήθος των πιο πιθανών μηνυμάτων εισόδου που οδηγούν στη λήψη του ίδιου μηνύματος εξόδου είναι ίσο με $M_{y/x} = 2^{lH(Y/X)}$.	❑	☑
Στην περίπτωση μη ιδανικής προσαρμογής της πηγής στο κανάλι, ισχύει $M_R = 2^{lR}$, όπου $rI(X;Y) = R$.	☑	❑
Αναφορικά με την πιθανότητα εμφάνισης σφάλματος κατά τη μετάδοση ενός τυχαίου μηνύματος, ισχύει η ανισότητα: $p_{error} > 2^{-l\varepsilon}$, όπου ε θετικός σταθερός αριθμός.	❑	☑

Αν τα καταφέρατε, πολύ ωραία! Αν όχι, μην απογοητεύεστε. Πρέπει να μελετήσετε και πάλι την Υποενότητα 2.1.4, καθώς και την απόδειξη του Θεωρήματος 3.1.

Ειδικότερα, για την απάντηση των δύο πρώτων ερωτημάτων κάνουμε χρήση της Πρότασης 2.2, καθώς και του τύπου (2.10).

Για την ορθή απάντηση της τρίτης ερώτησης πρέπει να προσέξουμε ότι ζητούμενο είναι το πλήθος των πιο πιθανών μηνυμάτων εισόδου που οδηγούν στη λήψη του ίδιου μηνύματος εξόδου και όχι το πλήθος των πιο πιθανών μηνυμάτων εξόδου που μπορούν να προέλθουν από το ίδιο μήνυμα εισόδου. Επομένως, το ζητούμενο πλήθος δίνεται προσεγγιστικά από $M_{x/y} = 2^{lH(X/Y)}$.

Αναφορικά με την τέταρτη ερώτηση, αφού η πηγή δεν προσαρμόζεται ιδανικά στο κανάλι, ο ρυθμός μετάδοσης που επιτυγχάνεται στο κανάλι είναι μικρότερος από το μέγιστο ρυθμό, που εκφράζει η χωρητικότητα.

Τέλος, αναφορικά με την πέμπτη ερώτηση, η πιθανότητα εμφάνισης σφάλματος πληροί την ανισότητα: $p_{error} \leq 2^{-l\varepsilon}$ (δείτε απόδειξη Θεωρήματος 3.1).

3.5

Οι ζητούμενες πιθανότητες είναι οι εξής:

$p(good) = 0{,}95238$, $p(bad) = 0{,}04762$,

$p(b\_error) = p_{error} = 0{,}004762$ και $p(b\_correct) = 0{,}042858$.

Αν τα καταφέρατε, συγχαρητήρια! Σίγουρα έχετε την ικανότητα να χρησιμοποιείτε και να αναλύετε το μαθηματικό υπόδειγμα του Σχήματος 3.7 και του Σχήματος 3.8. Αν δεν τα καταφέρατε, μην απογοητεύεστε, μελετήστε και πάλι την Υποενότητα 3.1.3 και επιχειρήστε την επίλυση της άσκησης με τη βοήθεια και των παρατηρήσεων που ακολουθούν.

Για το μοντέλο του Σχήματος 3.8 ισχύει, στην κατάσταση ισορροπίας, το ακόλουθο σύστημα εξισώσεων. Κάθε εξίσωση αφορά έναν κόμβο (κατάσταση) του μοντέλου και εκφράζει την ισότητα που ισχύει μεταξύ του αθροίσματος των γινομένων των πιθανοτήτων μετάπτωσης (από τον τρέχοντα κόμβο προς όλους τους άλλους) με την πιθανότητα του τρέχοντος κόμβου και του αθροίσματος των γινομένων των πιθανοτήτων μετάπτωσης (από όλους τους κόμβους προς τον τρέχοντα) με την πιθανότητα του εκάστοτε κόμβου από τον οποίο προέρχεται η ροή:

$$p_{(b\_correct)}\lambda(1-p) + p_{(good)}\lambda p = p_{(b\_error)}q + p_{(b\_error)}(1-\lambda)(1-p)$$

$$p_{(b\_correct)}\lambda(1-p) + p_{(b\_correct)}q = p_{(good)}(1-\lambda)p + p_{(b\_error)}(1-\lambda)(1-p)$$

$$p_{(b\_correct)}\lambda(1-p) + p_{(good)}\lambda p = p_{(b\_error)}q + p_{(b\_error)}(1-\lambda)(1-p)$$

Ακόμα, το άθροισμα των πιθανοτήτων όλων των κόμβων είναι ίσο με 1:

$$p_{(b\_correct)} + p_{(good)} + p_{(b\_error)} = 1.$$

Η επίλυση του συστήματος των εξισώσεων οδηγεί στα αποτελέσματα που παραθέσαμε ανωτέρω. Ο υπολογισμός των αποτελεσμάτων της άσκησης μπορεί ασφαλώς να βασιστεί μόνο στους τύπους της Υποενότητας 3.1.3, καθώς επίσης και στην παρατήρηση ότι $p(b\_error) = p_{error}$ και $p(bad) = p(b\_error) + p(b\_correct)$.

3.6

Οι ποσότητες πληροφορίας των σημάτων εισόδου, εξόδου και θορύβου, η συνδυασμένη ποσότητα του σήματος εισόδου και του σήματος εξόδου, η υπό συνθήκη ποσότητα πληροφορίας του σήματος εισόδου με γνωστό το σήμα εξόδου, η αμοιβαία ποσότητα πληροφορίας μεταξύ της εισόδου και της εξόδου και η χωρητικότητα του καναλιού έχουν ως εξής:

$$H(X) = 3,\ H(Y) = 3 + 0{,}125 \log e,\ H(N) = H(Y/X) = 1,$$

$$H(X,Y) = 4,\ H(X/Y) = -0{,}125 \log e,\ I(X;Y) = H(Y) - H(N) = 2 + 0{,}125 \log e,$$

$$C = \lim_{f(x)} H(Y) - 1.$$

Αν τα καταφέρατε, μπράβο! Απαιτούσε αρκετή προσπάθεια. Αν όχι, μην απογοητεύεστε που δεν τα καταφέρατε με την πρώτη. Ας δούμε μαζί στη συνέχεια πώς μπορούμε να επιλύσουμε την άσκηση.

Για τον υπολογισμό των διαφόρων ποσοτήτων πληροφορίας απαιτούνται οι αντίστοιχες συναρτήσεις πυκνότητας πιθανότητας. Αφού πρόκειται για αθροιστικό συνεχές κανάλι, το σήμα εξόδου είναι ίσο με το άθροισμα του σήματος εισόδου και του θορύβου, $Y = X + N$. Έτσι, μεταξύ της συνάρτησης πυκνότητας πιθανότητας του θορύβου, του σήματος εισόδου, της συνδυασμένης και της υπό συνθήκη συνάρτησης πυκνότητας της εισόδου και της εξόδου ισχύει η σχέση $f(n) = f(y/x) = f(x,y)/f(x)$. Επομένως, η συνδυασμένη συνάρτηση πυκνότητας πιθανότητας $f(x,y)$ δίνεται από την ακόλουθη σχέση:

$$f(x,y) = \begin{cases} \dfrac{1}{16}, & \text{αν } -4 \le x \le 4,\ -1 \le y - x \le 1 \\ 0, & \text{αν } x > 4,\ x < -4,\ y > 1,\ y < -1 \end{cases}$$

Από τις δεδομένες συναρτήσεις πυκνότητας πιθανότητας και τη $f(x,y)$ μπορούμε στη συνέχεια να προσδιορίσουμε τις $f(y)$ και $f(x/y)$. Πιο συγκεκριμένα, η $f(y)$ προσδιορίζεται από τη $f(x,y)$ και η $f(x/y)$ με τη βοήθεια της σχέσης $f(x/y) = f(x,y)/f(y)$.

$$f(y) = \begin{cases} \displaystyle\int_{-4}^{y+1} f(x,y)dx = \left|\frac{1}{16}x\right|_{-4}^{y+1} = \frac{1}{16}(y+5), & -5 \le y \le -3 \\ \displaystyle\int_{y-1}^{y+1} f(x,y)dx = \frac{1}{8}, & -3 \le y \le -3 \\ \displaystyle\int_{y-1}^{4} f(x,y)dx = \frac{1}{16}(5-y), & -5 \le y \le -3 \end{cases}$$

$$f(x/y) = \frac{f(x,y)}{f(x)} = \begin{cases} \dfrac{1}{y+5}, & -5 \le y \le -3, -4 \le x \le y+1 \\ \dfrac{1}{2}, & -3 \le y \le 3, y-1 \le x \le y+1 \\ \dfrac{1}{5-y}, & 3 \le y \le 5, y-1 \le x \le 4 \end{cases}$$

Έχοντας, λοιπόν, προσδιορίσει τις διάφορες συναρτήσεις πυκνότητας πιθανότητας,

μπορούμε να υπολογίσουμε τις ζητούμενες ποσότητες πληροφορίας με τη βοήθεια των γνωστών μας τύπων (2.20, 2.21, 2.22, 2.23) και να οδηγηθούμε επίσης στη ζητούμενη σχέση για τη χωρητικότητα του συνεχούς καναλιού.

$$C = \lim_{f(x)} H(Y) - H(N) = \lim_{f(x)} H(Y) - 1.$$

Η μέγιστη τιμή της εντροπίας της εξόδου μπορεί να υπολογιστεί μεταβάλλοντας τη συνάρτηση πυκνότητας πιθανότητας της εισόδου. Αλλά γι' αυτό απαιτείται κάποιος περιορισμός, όπως είδαμε στην Ενότητα 2.3, κατά την εξέταση των συνεχών πηγών πληροφορίας.

3.7

Η ποσότητα πληροφορίας του θορύβου είναι 0,57 bits/*δείγμα* και η χωρητικότητα του καναλιού είναι άνω φραγμένη από την ποσότητα που αντιστοιχεί στη χωρητικότητα του καναλιού που προκύπτει για τη μέγιστη τιμή της εντροπίας του σήματος εξόδου.

$$C \le W \log(13,84).$$

Αν τα καταφέρατε, συγχαρητήρια! Απαιτούσε αρκετή προσπάθεια. Αν δεν τα καταφέρατε, θα πρότεινα να μελετήσετε τις ακόλουθες οδηγίες για την επίλυση και να προσπαθήσετε και πάλι.

Πρώτα πρέπει να υπολογίσουμε το a, το οποίο είναι απαραίτητο για τον πλήρη προσδιορισμό της συνάρτησης πυκνότητας πιθανότητας του θορύβου. Γνωρίζουμε ότι το ολοκλήρωμα της συνάρτησης πυκνότητας πιθανότητας είναι ίσο με τη μονάδα και επομένως:

$$\int_{-a}^{a} f(n)dn = \int_{-a}^{a} n^2 dn = \frac{n^3}{3}\Big|_{-a}^{a} = \frac{2}{3}a^3 = 1 \Rightarrow a = \sqrt[3]{\frac{3}{2}}.$$

Τώρα μπορούμε να υπολογίσουμε την εντροπία του θορύβου:

$$H(N) = H(Y/X) = -\int_{-\sqrt[3]{\frac{3}{2}}}^{\sqrt[3]{\frac{3}{2}}} f(n)\log f(n)dn = 0,57 \text{ bit/sample}.$$

Η ποσότητα πληροφορίας του σήματος εξόδου έχει ως άνω φράγμα τη μέγιστη τιμή που προκύπτει για σταθερή διακύμανση και γκαουσιανή συνάρτηση πυκνότητας πιθανότητας. Η διακύμανση της εξόδου είναι ίση με το άθροισμα των διακυμάνσε-

ων της εισόδου και του θορύβου, αφού αυτά είναι στατιστικά ανεξάρτητα μεταξύ τους. Επομένως, λαμβάνοντας υπόψη το πλήθος των δειγμάτων στη μονάδα του χρόνου, $M = 2W$, έχουμε

$$H(Y) = 2W \log\left(\sqrt{\left(\sigma_x^2+\sigma_n^2\right)2\pi e}\right) = W \log\left(\sigma_x^2+\sigma_n^2\right)2\pi e.$$

Η διακύμανση του σήματος εισόδου δίνεται ίση με τη μονάδα και του θορύβου μπορεί να υπολογιστεί από τη συνάρτηση πυκνότητας πιθανότητας:

$$\sigma_n^2 = \int_{-\sqrt[3]{\frac{3}{2}}}^{\sqrt[3]{\frac{3}{2}}} n^2 f(n)dn = \int_{-\sqrt[3]{\frac{3}{2}}}^{\sqrt[3]{\frac{3}{2}}} n^4 dn = \frac{1}{5}n^5\Big|_{-\sqrt[3]{\frac{3}{2}}}^{\sqrt[3]{\frac{3}{2}}} = 0,786.$$

Η χωρητικότητα του καναλιού είναι ίση με τη μέγιστη τιμή της εντροπίας της εξόδου μειωμένης κατά την εντροπία του θορύβου. Επομένως, το άνω φράγμα της χωρητικότητας (σε bits/sec) μπορεί να υπολογιστεί λαμβάνοντας στη θέση της εντροπίας εξόδου το άνω φράγμα της, που υπολογίσαμε ανωτέρω.

$$\begin{aligned} C &\le W \log\left(\sigma_x^2+\sigma_n^2\right)2\pi e - 2WH(N) \\ &= W \log(30,5) - W1,14 = W\left[4,93 - 1,14\right] = 3,79W. \end{aligned}$$

Το άνω φράγμα της χωρητικότητας του καναλιού μπορεί να βρεθεί και με τη βοήθεια της έννοιας της πληροφορικής ισχύος. Η πληροφορική ισχύς ενός στοχαστικού σήματος, I_N, είναι ίση με την ισχύ ενός γκαουσιανού σήματος το οποίο έχει την ίδια ποσότητα πληροφορίας που έχει και το στοχαστικό αυτό σήμα. Έτσι, η ποσότητα πληροφορίας του θορύβου ως συνάρτηση της πληροφορικής του ισχύος δίνεται από την ακόλουθη σχέση:

$$H(N) = \log\sqrt{2\pi e I_N} = \frac{1}{2}\log\left(2\pi e I_N\right).$$

Από τη σχέση αυτή μπορούμε να υπολογίσουμε την πληροφορική ισχύ του θορύβου:

$$I_N = \frac{1}{2\pi e} 2^{2H(N)} = 0,129.$$

Έτσι, για το άνω φράγμα της χωρητικότητας του καναλιού ισχύει η ανισότητα αφού λάβουμε υπόψη τα $2W$ *δείγματα*/*sec*:

$$C \le W \log\left(\sigma_x^2+\sigma_n^2\right)2\pi e - W \log I_N 2\pi e = W \log\left(\frac{\sigma_x^2+\sigma_n^2}{I_N}\right) = W \log 13,84 = 3,79W.$$

3.8

Η χωρητικότητα του καναλιού και ο μέγιστος ρυθμός με τον οποίο μπορούν να μεταδοθούν δεδομένα με αμελητέα πιθανότητα εμφάνισης σφαλμάτων είναι:

C = 12000 bits/sec, r = 1500 characters/sec.

Αν τα καταφέρατε, μπράβο! Αν όχι, ας προσπαθήσουμε μαζί. Προηγουμένως, όμως, θα ήταν καλύτερα να επαναλάβετε τη μελέτη των Υποενοτήτων 3.2.1 και 3.2.2.

Η χωρητικότητα του συνεχούς καναλιού με αθροιστικό γκαουσιανό λευκό θόρυβο υπολογίζεται με τη βοήθεια της ακόλουθης σχέσης, όπως είδαμε στην Υποενότητα 3.2.1:

$$C = W \log\left\{1+\frac{\sigma_\chi^2}{\sigma_v^2}\right\} = 3000 \log 16 = 12000 \text{ bits / sec.}$$

Για την απάντηση του δεύτερου ερωτήματος βασιζόμαστε στο θεώρημα κωδικοποίησης του Shannon για συνεχή κανάλια (Θεώρημα 3.2). Σύμφωνα με αυτό, μια δεδομένη ποσότητα πληροφορίας H μπορεί να μεταδοθεί με ρυθμό r μέσω ενός συνεχούς καναλιού, με οσοδήποτε μικρή πιθανότητα σφάλματος επιθυμούμε, αν ισχύει $rH < C$. Επομένως, ο μέγιστος ρυθμός μετάδοσης του καναλιού, με αμελητέα πιθανότητα λάθους, υπολογίζεται ως εξής:

$$rH(X) < C \Rightarrow r \log 256 < 12000 \Rightarrow 8r < 12000 \Rightarrow r < 15000 \text{ bits / sec.}$$

3.9

Η χωρητικότητα του καναλιού είναι ίση με $1,45W$ και η μέγιστη χωρητικότητα είναι ίση $2,06W$.

Αν τα καταφέρατε, μπράβο! Αν όχι, μην απογοητεύεστε. Ας δούμε μαζί πώς μπορούμε να προσδιορίσουμε τη χωρητικότητα του καναλιού εφαρμόζοντας τους τύπους της Υποενότητας 3.2.3:

$$
\begin{aligned}
C &= \frac{1}{2\pi}\int_0^{2\pi W} \log\left\{1+\frac{\Phi_x(\omega_i)}{\Phi_n(\omega_i)}\right\}d\omega \\
&= \frac{1}{2\pi}\left\{\frac{2}{3}\pi W \log\left(1+\frac{4}{1}\right)+\frac{1}{3}\pi W \log\left(1+\frac{4}{2}\right)+\right. \\
&\left.+\frac{1}{3}\pi W \log\left(1+\frac{8}{2}\right)+\frac{2}{3}\pi W \log\left(1+\frac{8}{4}\right)\right\} \\
&= \frac{1}{2}\,\mathrm{W}\log 15 = 1,45 \text{ bits / sec.}
\end{aligned}
$$

Η μέση ισχύς του σήματος εισόδου καθώς και του θορύβου υπολογίζονται ως εξής:

$$
\sigma_x^2 = \frac{1}{2\pi}\int_0^{2\pi\omega} \Phi_x(\omega)d\omega = \frac{1}{4}\left(4\pi W + 8\pi W\right) = 12W,
$$

$$
\sigma_n^2 = \frac{1}{2\pi}\int_0^{2\pi\omega} \Phi_n(\omega)d\omega = \frac{1}{\pi}\left(\frac{2}{3}\pi W + \frac{4}{3}\pi W + \frac{8}{3}\pi W\right) = \frac{14}{3}W.
$$

Η χωρητικότητα παίρνει τη μέγιστη τιμή της για

$$
\Phi_x(\omega) + \Phi_n(\omega) = \frac{\sigma_x^2+\sigma_n^2}{2W} = \frac{25}{3},
$$

Τότε η μέγιστη χωρητικότητα του καναλιού είναι ίση

$$
C = W\log\left\{\frac{\sigma_x^2+\sigma_n^2}{2W}\right\} = 2,06W.
$$

4.1

Ένα κανάλι αξιοπιστίας $p = 0$ μπορεί να μετατραπεί σε ένα κανάλι με αξιοπιστία $p = 1$, δηλαδή σε ένα τέλειο κανάλι, αν αντικαταστήσουμε κάθε «1» με το «0» και κάθε «0» με το «1». Με τον ίδιο τρόπο, αντικαθιστώντας δηλαδή κάθε «1» με το «0» και κάθε «0» με το «1», μπορούμε να μετατρέψουμε ένα κανάλι με $0 < p \leq 1/2$ σε ένα κανάλι με $1/2 \leq p < 1$.

4.2

Σφάλματα κατά τη μετάδοση δεν μπορούν να ανιχνευτούν στις περιπτώσεις κατά τις οποίες οι κωδικές λέξεις που στάλθηκαν μετατρέπονται σε άλλες, επίσης, κωδικές λέξεις στον παραλήπτη.

Εφόσον στην έξοδο του καναλιού λαμβάνονται λέξεις που δεν είναι και κωδικές λέξεις, τότε ανιχνεύονται σφάλματα μετάδοσης. Αν όμως η λέξη που λαμβάνεται εμφανίζει το ίδιο πλήθος διαφορετικών ψηφίων με δύο ή περισσότερες κωδικές λέξεις, τότε δεν μπορεί να επιτευχθεί η διόρθωση χωρίς επανάληψη της μετάδοσης.

Οι πλησιέστερες (εγγύτερες) κωδικές λέξεις στις λέξεις «100000001», «111011111», «111101001» και «010110111» είναι οι «000000000», «011011011», «101101101» και «110110110» , αντίστοιχα.

Αν τα καταφέρατε, μπράβο! Αν όχι, μην απογοητεύεστε. Επαναλάβετε τη μελέτη της Ενότητας 4.1.1 και προσπαθήστε και πάλι.

4.3

Οι λέξεις είναι $x_1 = 111000$, $x_2 = 001110$, $x_3 = 111000 + 001110 = 110110$ και $x_4 = 111000. 001110 = 001000$.

Τα βάρη των λέξεων είναι $wt(111000) = 3$, $wt(001110) = 3$, $wt(110110) = 4$ και $wt(001000) = 1$. Οι αποστάσεις μεταξύ των λέξεων κάθε ζεύγους είναι $d(111000, 001110) = 4$, $d(111000, 110110) = 3$, $d(111000, 001000) = 2$, $d(001110, 110110) = 3$, $d(001110, 001000) = 2$ και $d(110110, 001000) = 5$.

Αν τα καταφέρατε, μπράβο! Σίγουρα μπορείτε να εφαρμόζετε τις πράξεις της πρόσθεσης και του πολλαπλασιασμού σε δυαδικές λέξεις, να υπολογίζετε τα βάρη τους, καθώς και τις αποστάσεις μεταξύ λέξεων.

Αν δεν τα καταφέρατε, προσπαθήστε και πάλι, αφού πρώτα επαναλάβετε τη μελέτη των Ορισμών 4.1, 4.2, των πράξεων της πρόσθεσης και του πολλαπλασιασμού και των Παραδειγμάτων 2 και 3.

4.4

Κατά τη μετάδοση της κωδικής λέξης «0000», ο αποδέκτης τη συμπεραίνει σωστά, αν λάβει μία από τις «0000» ή «0100» ή «0001». Κατά τη μετάδοση της κωδικής λέξης «1010», ο αποδέκτης τη συμπεραίνει σωστά μόνο στην περίπτωση λήψης αυτής «1010». Αντίστοιχα, ο αποδέκτης συμπεραίνει σωστά τη μετάδοση της κωδικής λέξης «1111», αν λάβει μία από τις «1111» ή «0111» ή «1101». Αν όμως λάβει μία από τις «0010», «0011», «0101», «0110», «1000», «1001», «1011», «1100», «1110», τότε ο αποδέκτης ζητά επανάληψη της μετάδοσης.

4.5

Κατά τη μετάδοση της κωδικής λέξης «000», ο αποδέκτης συμπεραίνει σωστά, αν

λάβει την κωδική αυτή λέξη ή μία από τις εγγύτερες προς αυτή λέξεις «001», «010» και «100». Επομένως, η ζητούμενη πιθανότητα είναι ίση με το ακόλουθο άθροισμα πιθανοτήτων

$\pi(000, 000) + \pi(000, 001) + \pi(000, 010) + \pi(000, 100) =$

$0{,}9^3 + 0{,}9^2(1 - 0{,}9) + 0{,}9^2(1 - 0{,}9) + 0{,}9^2(1 - 0{,}9) = 0{,}972.$

Αν τα καταφέρατε, μπράβο! Αν όχι, μην απογοητεύσετε! Προσπαθήστε και πάλι αφού επαναλάβετε τη μελέτη της Ενότητας 4.1.

4.6

Η απόσταση του κώδικα είναι 2 και σύμφωνα με το θεώρημα 4.2, ο κώδικας ανιχνεύει όλα τα πρότυπα σφάλματος βάρους 1, δηλαδή τα πρότυπα σφάλματος 0001, 0010, 0100 και 1000. Επίσης, ανιχνεύει και άλλα πρότυπα σφάλματος μεγαλύτερου βάρους, όπως τα 1100, 0011, 1110, 0111 κλπ. Όμως δεν ανιχνεύει τουλάχιστον ένα πρότυπο σφάλματος βάρους 2. Πράγματι, δεν ανιχνεύει για παράδειγμα το 0101.

4.7

Ο αποστάσεις των κωδίκων είναι $d_1 = 1$, $d_2 = 5$, $d_3 = 2$ και $d_4 = 3$. Στην περίπτωση του κώδικα C_1 παίρνουμε το πρότυπο σφάλματος «010» βάρους 1. Αυτό το πρότυπο σφάλματος δε διορθώνεται από τον κώδικα, αφού κατά τη μετάδοση της κωδικής λέξης «101» λαμβάνεται η λέξη «111» που είναι και αυτή κωδική. Στην περίπτωση του κώδικα C_2 παίρνουμε το πρότυπο σφάλματος «01110» βάρους 3. Αυτό το πρότυπο σφάλματος δε διορθώνεται από τον κώδικα, αφού κατά τη μετάδοση της κωδικής λέξης «11111» λαμβάνεται η λέξη «10001» που είναι εγγύτερη προς την κωδική λέξη «00000». Στην περίπτωση του κώδικα C_3 παίρνουμε το πρότυπο σφάλματος «10000» βάρους 1. Αυτό το πρότυπο σφάλματος δε διορθώνεται από τον κώδικα, αφού κατά τη μετάδοση της κωδικής λέξης «10001» λαμβάνεται η λέξη «00001» που απέχει εξίσου από τις κωδικές λέξεις «10001» και «00000». Τέλος, στην περίπτωση του κώδικα C_4 παίρνουμε το πρότυπο σφάλματος «010100» βάρους 2. Αυτό το πρότυπο σφάλματος δεν διορθώνεται από τον κώδικα, αφού κατά τη μετάδοση της κωδικής λέξης «101010» λαμβάνεται η λέξη «111110» που εμφανίζει τη μικρότερη απόσταση από την κωδική λέξη «111111».

4.8

Όλοι οι κώδικες είναι γραμμικοί εκτός του C_1 . Οι αποστάσεις των κωδίκων είναι: $d_2 = 2$, $d_3 = 3$ και $d_4 = 3$.

Αν τα καταφέρατε, ωραία! Αν όχι, προσπαθήστε και πάλι. Προηγουμένως όμως μελετήστε τον ορισμό των γραμμικών κωδίκων. Επίσης, λάβετε υπόψη ότι η απόσταση ενός γραμμικού κώδικα είναι ίση με το ελάχιστο από τα βάρη των μη μηδενικών κωδικών λέξεων. Έτσι, μπορείτε να δείτε ότι ο κώδικας $C_1 = \{101, 111, 011\}$ δεν είναι γραμμικός, αφού η λέξη 010 = 101 + 111 δεν είναι κωδική. Ο κώδικας όμως $C_2 = \{0000, 1001, 0110, 1111\}$ είναι γραμμικός, αφού το άθροισμα κάθε δυνατού ζεύγους κωδικών λέξεων οδηγεί σε κωδική λέξη. Επίσης, πολύ εύκολα βλέπουμε ότι οι μη μηδενικές κωδικές λέξεις 1001 και 0110 έχουν το πιο μικρό βάρος, ίσο με 2, το οποίο είναι και η απόσταση του κώδικα. Κατά τον ίδιο τρόπο ελέγχουμε αν είναι γραμμικοί οι κώδικες C_3 και C_4 και διαπιστώνουμε την απόστασή τους.

4.9

Μία βάση του κώδικα C είναι {001000, 000100, 000010, 000001} και μια βάση του δυϊκού κώδικα $C^{\perp}$ είναι {000010, 000001}.

Αν τα καταφέρατε, συγχαρητήρια! Είστε σε θέση να εφαρμόζετε με επιτυχία τον Αλγόριθμο 4.1. Αν δεν τα καταφέρατε, μην απογοητεύεστε. Προσπαθήστε και πάλι αφού επαναλάβετε τη μελέτη του Αλγορίθμου 1. Την απάντησή σας μπορείτε να την ελέγξετε και με τα ακόλουθα ενδιάμεσα αποτελέσματα:

$$L = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \; M = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; H = \begin{bmatrix} M \\ I \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Από τον 1ο πίνακα P, τον οποίο σχηματίζουμε με τις λέξεις του S, οδηγούμαστε στο 2ο πίνακα θέτοντας ως 1η του γραμμή το άθροισμα της 1ης και της 4ης γραμμής του 1ου πίνακα, ως 2η γραμμή την 4η γραμμή του 1ου πίνακα, ως 3η γραμμή το άθροισμα της 1ης και της 3ης γραμμής του 1ου πίνακα, ως 4η γραμμή την 5η γραμμή του 1ου πίνακα και ως 5η γραμμή την 3η γραμμή του 1ου πίνακα. Από το 2ο πίνακα οδηγούμαστε στον 3ο, θέτοντας ως 2η γραμμή του 3ου το άθροισμα της 2ης και της 4ης γραμμής του 2ου πίνακα και ως 5η γραμμή του 3ου πίνακα το άθροισμα της 1ης, της 2ης, της 3ης και της 5ης γραμμής του 2ου πίνακα. Παρατηρούμε ότι ο 3ος πίνακας είναι σε μορφή ΠΚΔΓ (και επομένως και σε μορφή ΚΔΓ).

Επομένως μία βάση του κώδικα C είναι {001000, 000100, 000010, 000001}.

Για την εύρεση μιας βάσης του δυϊκού κώδικα $C^{\perp}$, εφαρμόζουμε και τα βήματα 3 – 6 του Αλγόριθμου 1.

$$G=\begin{bmatrix}0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix},\ M=\begin{bmatrix}0&0\\0&0\\0&0\\0&0\end{bmatrix},\ H=\begin{bmatrix}M\\I\end{bmatrix}=\begin{bmatrix}0&0\\0&0\\0&0\\0&0\\1&0\\0&1\end{bmatrix}$$

Επομένως, μια βάση του δυϊκού κώδικα $C^{\perp}$ είναι {000010, 000001}.

4.10

Οι κωδικές λέξεις που αντιστοιχούν στα μηνύματα *Z* και *H* είναι 10110 και 11010, αντίστοιχα.

Αν τα καταφέρατε, μπράβο! Σίγουρα είστε σε θέση να εφαρμόζετε τις απαραίτητες για την κωδικοποίηση πράξεις από τη γραμμική άλγεβρα και τη θεωρία πινάκων.

Αν δεν τα καταφέρατε, μην απογοητεύεστε. Αφού μελετήσετε και πάλι το Παράδειγμα 16, ελέγξτε τις πράξεις σας με τις ακόλουθες:

$$Z\rightarrow c_6=\begin{bmatrix}1&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}=1.(10001)+0.(01011)+1.(00111)=10110.$$

$$H\rightarrow c_7=\begin{bmatrix}1&1&0\end{bmatrix}\begin{bmatrix}1&0&0&0&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}=1.(10001)+1.(01011)+0.(00111)=11010.$$

4.11

Η ακολουθία των κωδικών λέξεων με την οποία κωδικοποιείται το μήνυμα *ΚΑΙΡΟΣ* είναι 0110011 0000000 0101000 1101110 1011101 1110101.

Αν τα καταφέρατε, μπράβο! Αν δεν τα καταφέρατε, μην απογοητεύεστε.

Προσπαθήστε και πάλι και ελέγξτε τις πράξεις σας με τις ακόλουθες:

$$K \to \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} G = 0.(1000110) + 1.(0100101) + 1.(0010110) + 0.(0001101)$$
$$= 0100101 + 0010110 = 0110011$$

$$A \to \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} =$$
$$= 0.(1000110) + 0.(0100101) + 0.(0010110) + 0.(0001101) = 0000000$$

$$I \to \begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} =$$
$$= 0.(1000110) + 1.(0100101) + 0.(0010110) + 1.(0001101)$$
$$= 0100101 + 0001101 = 0101000$$

$$P \to \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix} G = 1.(1000110) + 1.(0100101) + 0.(0010110) + 1.(0001101)$$
$$= 1000110 + 0100101 + 0001101 = 1101110$$

$$O \to \begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix} G = 1.(1000110) + 0.(0100101) + 1.(0010110) + 1.(0001101)$$
$$= 1000110 + 0010110 + 0001101 = 1011101$$

$$\Sigma \to \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix} G = 1.(1000110) + 1.(0100101) + 1.(0010110) + 0.(0001101)$$
$$= 1000110 + 0100101 + 0010110 = 1110101$$

4.12

Οι οκτώ συνομάδες του C είναι οι εξής:

1. C = {000000, 001111, 010011, 011100, 100110, 101001, 110101, 111010},
2. {000001, 001110, 010011, 011101, 100111, 101000, 110100, 111011},
3. {000010, 001101, 010001, 011100, 100100, 101011, 110111, 111000},
4. {000011, 001100, 010000, 011111, 100101, 101010, 110110, 111001},
5. {000100, 001011, 010111, 011000, 100010, 101101, 110001, 111110},
6. {000101, 001010, 010110, 011001, 100011, 101100, 110000, 111111},
7. {000110, 001001, 010101, 011010, 100000, 101111, 110011, 111100},
8. {000111, 001000, 010100, 011011, 100001, 101110, 110010, 111101}.

Ο δέκτης , από τη λήψη της λέξης 111011, συμπεραίνει την κωδική λέξη 111010. Ενώ από τη λήψη της λέξης 111111, ο δέκτης ζητά αναμετάδοση, αν εφαρμόζεται η

ΑΑΜΠ ή οδηγείται σε μια από τις κωδικές λέξεις 001111, 111010, και 110101 αν εφαρμόζεται η ΠΑΜΠ, ανάλογα με την αυθαίρετη επιλογή του από τα τρία πρότυπα σφάλματος με το μικρότερο βάρος.

Αν τα καταφέρατε, μπράβο! Σίγουρα είστε σε θέση να σχηματίζετε τις συνομάδες συστηματικών γραμμικών κωδίκων και να εφαρμόζετε τη διαδικασία αποκωδικοποίησης (Αλγόριθμο 2).

Αν δεν τα καταφέρατε, μην απογοητεύεστε! Ίσως σας διέφυγαν κάποια λάθη κατά το σχηματισμό των συνομάδων. Αν είχατε δυσκολίες στο σχηματισμό των συνομάδων ή κατά την εφαρμογή του Αλγορίθμου 2, αφού μελετήσετε εκ νέου τον Αλγόριθμο 2 και το Παράδειγμα 19, προσπαθήστε και πάλι.

Για το σχηματισμό των συνομάδων, μπορείτε να δημιουργήσετε μια λίστα με όλες τις δυνατές λέξεις και, αφού θεωρήσετε τον κώδικα C ως την πρώτη συνομάδα, να αρχίσετε να σχηματίζετε τις υπόλοιπες 7 συνομάδες, γνωρίζοντας ότι σε καθεμία από αυτές θα περιέχονται 8 λέξεις. Κάθε λέξη που περιέχεται σε μία από τις συνομάδες διαγράφεται από τη λίστα σας. Την πρώτη λέξη της λίστας y που δεν έχει διαγραφεί, μπορείτε να τη χρησιμοποιήσετε ως την καθοριστική κάθε φορά για το σχηματισμό της επόμενης συνομάδες, δηλαδή $C + y$. Διαγράφοντας κάθε λέξη που εμφανίζεται σε μία συνομάδα, ελέγχουμε ενδεχόμενα λάθη, όπως της εμφάνισης μιας λέξης σε δύο συνομάδες.

Σχετικά με τη διαδικασία αποκωδικοποίησης (Αλγόριθμο 2), στη νέα σας προσπάθεια μπορείτε να ελέγξετε τα ενδιάμεσα αποτελέσματά σας και με τα ακόλουθα.

Αν ο δέκτης λάβει τη λέξη 111011, παρατηρεί ότι αυτή περιέχεται στη 2η συνομάδα, στην οποίο η λέξη με το μικρότερο βάρος είναι η 000001. Επομένως, σύμφωνα με τη διαδικασία αποκωδικοποίησης, ο δέκτης συμπεραίνει ότι μεταδόθηκε η κωδική λέξη 111011 + 000001 = 111010.

Στην περίπτωση λήψης της λέξης 111111, ο δέκτης παρατηρεί ότι αυτή περιέχεται στην 6η συνομάδα του C, όπου διαπιστώνει ότι υπάρχουν τρεις λέξεις (ή τρία πρότυπα σφάλματος) με το ελάχιστο βάρος, οι 000101, 001010 και 110000. Όπως και στο Παράδειγμα 19, η επιλογή του δέκτη εξαρτάται από το αν βασίζεται στην ΠΑΜΠ ή την ΑΑΜΠ. Αν έχουμε εφαρμογή της ΑΑΜΠ, ο δέκτης ζητά από το μεταδότη αναμετάδοση του μηνύματος. Αν εφαρμόζεται η ΠΑΜΠ, ο δέκτης επιλέγει αυθαίρετα ένα από τα πρότυπα σφάλματος με το ελάχιστο βάρος, έστω το 110000 και συμπεραίνει επομένως ότι μεταδόθηκε η κωδική λέξη 111111 + 110000 = 001111.

Ο δέκτης, αν είχε επιλέξει το πρότυπο σφάλματος 000101, θα είχε συμπεράνει τη

μετάδοση της κωδικής λέξης 111010 και αν είχε επιλέξει το πρότυπο σφάλματος 001010, θα είχε οδηγηθεί στην κωδική λέξη 110101.

4.13

Από τη λήψη της λέξης 011111, ο δέκτης συμπεραίνει ότι μεταδόθηκε η κωδική λέξη 011111 + 010000 = 001111, αλλά και από τη λήψη της 101111 συμπεραίνει την ίδια κωδική λέξη 101111 + 100000 = 001111.

Αν τα καταφέρατε, μπράβο! Σίγουρα είστε σε θέση να εφαρμόζετε τη διαδικασία αποκωδικοποίησης που βασίζεται στην ΤΔΑ (Αλγόριθμο 3), αλλά και να σχηματίζετε τον πίνακα ισοτιμίας H ενός συστηματικού γραμμικού κώδικα.

Αν δεν τα καταφέρατε όμως μην απογοητεύεστε. Ίσως να είχατε κάποιες δυσκολίες στο σχηματισμό του πίνακα ισοτιμίας. Ίσως πάλι να σας διέφυγαν κάποια λάθη κατά την εφαρμογή της διαδικασίας αποκωδικοποίησης (του Αλγόριθμου 3). Σε αυτή την περίπτωση, θα πρότεινα να προσπαθήσετε και πάλι, αφού προηγουμένως επαναλάβετε τη μελέτη του Αλγόριθμου 1, της διαδικασίας σχηματισμού τυπικών διατάξεων αποκωδικοποίησης (ΤΔΑ) και του Αλγόριθμου 3 (της διαδικασίας αποκωδικοποίησης που βασίζεται στην ΤΔΑ), καθώς και των Παραδειγμάτων 20 και 21. Στη νέα σας προσπάθεια μπορείτε να συγκρίνετε τα ενδιάμεσα αποτελέσματά σας με τα ακόλουθα:

$$P=\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&1&1\\1&1&0&1&0&1\\1&0&1&0&0&1\\1&1&1&0&1&0\\0&1&1&1&0&0\\0&0&0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&0&0&1&1&0\\0&1&0&0&1&1\\0&0&1&1&1&1\\0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&0&0&0&0\\0&0&0&0&\mathbf{0}&0\\0&0&0&0&0&0\end{bmatrix}\Rightarrow$$

$$M=\begin{bmatrix}1&1&0\\0&1&1\\1&1&1\end{bmatrix},\ H=\begin{bmatrix}M\\I\end{bmatrix}=\begin{bmatrix}1&1&0\\0&1&1\\1&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

Ο 2ος πίνακας του P προέρχεται από τον 1ο ως εξής: Οι τρεις πρώτες γραμμές του 1ου πίνακα παραμένουν και στο 2ο πίνακα στις ίδιες θέσεις. Η 4η γραμμή του 2ου πίνακα προκύπτει από το άθροισμα της 4ης, της 1ης και της 2ης γραμμής του 1ου πίνακα. Ανάλογα, η 5η γραμμή του 2ου πίνακα είναι το άθροισμα της 5ης, της 1ης και της 3ης γραμμής του 1ου πίνακα, η 6η γραμμή του 2ου πίνακα είναι το άθροισμα της 6ης, της 1ης, της 2ης και της 3ης γραμμής του 1ου πίνακα και η 7η γραμμή του 2ου πίνακα είναι το άθροισμα της 7ης, της 2ης και της 3ης γραμμής του 1ου πίνακα.

ΤΔΑ για ΠΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
000000	$y.H = 000$
000001	$(000001).H = 001$
000100	$(000100).H = 100$
000010	$(000010).H = 010$
010000	$(010000).H = 011$
000101	$(000101).H = 101$
100000	$(100000).H = 110$
001000	$(001000).H = 111$

ΤΔΑ για ΑΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
000000	000
000001	001
000100	100
000010	010
010000	011
———	101
100000	110
001000	111

Το σύνδρομο της ληφθείσας λέξης 011111 είναι ίσο με $(011111).H = 011$ και της ληφθείσας λέξης 101111 είναι ίσο με $(101111).H = 110$. Επομένως, οι αντίστοιχοι οδηγοί (ή τα αντίστοιχα πρότυπα σφάλματος) είναι 010000 και 100000. Παρατηρούμε ότι ο δέκτης οδηγείται στο ίδιο συμπέρασμα και από τις δύο ληφθείσες λέξεις, αφού $011111 + 010000 = 001111$ και $101111 + 100000 = 001111$. Επίσης, παρατηρούμε ότι το συμπέρασμα του δέκτη δε διαφοροποιείται από την εφαρμογή της ΠΑΜΠ ή της ΑΑΜΠ. Διαφοροποίηση θα υπήρχε μόνο στην περίπτωση της ΑΑΜΠ, αν το σύνδρομο της ληφθείσας λέξης ήταν 101, αφού τότε ο δέκτης θα ζητούσε αναμετάδοση.

4.14

Πράγματι, ο κώδικας είναι τέλειος αφού $|C| = \frac{2^5}{\left(\binom{5}{0}+\binom{5}{1}+\binom{5}{2}\right)} = \frac{32}{1+5+10} = 2$.

Μπορεί να αποδειχθεί ότι κάθε γραμμικός κώδικας διάστασης $k = 2$ και μήκους $n = 5$ ίσου με την απόστασή του $d = 2t + 1$ είναι τέλειος κώδικας. Η μια κωδική λέξη έχει και τα n ψηφία ίσα με «0» και η άλλη ίσα με «1», όπως και στην περίπτωση του κώδικα της άσκησης αυτοαξιολόγησης 14. Οι κώδικες αυτοί χαρακτηρίζονται τετριμμένοι (**trivial**), αφού η χρησιμότητά τους είναι περιορισμένη.

4.15

Η απόσταση είναι $d = 3$ (ελάχιστο βάρος), το πλήθος των κωδικών λέξεων είναι $|C| = 16 = 2^4$ (αφού η διάσταση του κώδικα είναι 4) και ο ρυθμός πληροφορίας είναι 4/7, αφού από τα 7 bits μόνο τα 4 χρησιμοποιούνται για την παράσταση της πληροφορίας.

4.16

Αφού ο βαθμός του πολυωνύμου – γεννήτορα είναι 3, η διάσταση του κώδικα C είναι $k = n - 3 = 4$. Επομένως, ένας πίνακας – γεννήτορας του C έχει ως γραμμές το $\gamma(x) = 1 + x^2 + x^3$ και τις τρεις πρώτες κυκλικές μετατοπίσεις του, δηλαδή τα πολυώνυμα $x\gamma(x) = x + x^3 + x^4$, $x^2\gamma(x) = x^2 + x^4 + x^5$ και $x^3\gamma(x) = x^3 + x^5 + x^6$. Συνεπώς, ένας πίνακας – γεννήτορας του C είναι $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. Τα μηνύματα 1110 και 0110 παριστάνονται από τα πολυώνυμα $1 + x + x^2$ και $x + x^2$ και επομένως το γινόμενό τους με το πολυώνυμο – γεννήτορα είναι $(1 + x + x^2)\gamma(x) = (1 + x + x^2)(1 + x^2 + x^3) = 1 + x^2 + x^3 + x + x^3 + x^4 + x^2 + x^4 + x^5 = 1 + x + x^5$ και $(x + x^2)\gamma(x) = (x + x^2)(1 + x^2 + x^3) = x + x^3 + x^2 + x^5 = x + x^2 + x^3 + x^5$, που αντιστοιχούν στις κωδικές λέξεις 1100010 και 0111010. (Υπόμνηση: $x^l + x^l = 0$, αφού $1 + 1 = 0$ στο $K = \{0, 1\}$).

4.17

Η διάσταση του κώδικα είναι $k = 4 = n - 3$ και η απόσταση είναι $d = n - k = 3$ και επομένως, $t = 1$. Η ληφθείσα λέξη $l = 1111000$ αντιστοιχεί στο πολυώνυμο $l(x) = 1 + x + x^2 + x^3$ και επομένως $\sigma(x) = l(x) \bmod \gamma(x) = 1 + x + x^2 + x^3 \bmod (1 + x + x^3) = x^2$,

$\sigma_1(x) = x\sigma(x) \bmod \gamma(x) = x(x^2) \bmod (1 + x + x^3) = x^3 \bmod (1 + x + x^3) = 1 + x$, του οποίου ο βαθμός είναι 1, ίσος με t. Επομένως, το πρότυπο σφάλματος είναι $\varepsilon = 1100000$ και η κωδική λέξη που μεταδόθηκε $c = l + \varepsilon = 1111000 + 1100000 = 0011000$.

Η ληφθείσα λέξη $l = 1100101$ αντιστοιχεί στο πολυώνυμο $l(x) = 1 + x + x^4 + x^6$ και επομένως $\sigma(x) = l(x) \bmod \gamma(x) = 1 + x + x^4 + x^6 \bmod (1 + x + x^3) = 0$, δηλαδή η ληφθείσα λέξη είναι κωδική λέξη. Επομένως, το πρότυπο σφάλματος είναι $\varepsilon = 0000000$ και η κωδική λέξη που μεταδόθηκε $c = l = 1100101$.

Σχετικά με τον υπολογισμό του $\sigma(x) = l(x) \bmod \gamma(x) = 1 + x + x^4 + x^6 \bmod (1 + x + x^3) = 0$, προσέχουμε ότι $x^3 \bmod (1 + x + x^3) = (1 + x)$ και επομένως, $x^6 \bmod (1 + x + x^3) = (1 + x)^2 = (1 + x^2)$, $x^4 \bmod (1 + x + x^3) = x(1 + x) = (x + x^2)$ και $(1 + x + x^4 + x^6) \bmod (1 + x + x^3) = (1 + x + 1 + x^2 + x + x^2) = 0$.

4.18

Η λέξη που μεταδόθηκε είναι $c = 110001111010000$.

Αν τα καταφέρατε, συγχαρητήρια! Σίγουρα είστε σε θέση να εφαρμόζετε με επιτυχία τον αλγόριθμο αποκωδικοποίησης *BCH* κωδίκων (Αλγόριθμο 6).

Αν δεν τα καταφέρατε, θα πρότεινα να προσπαθήσετε και πάλι. Στη νέα σας προσπάθεια μπορείτε να λάβετε υπόψη και τα ακόλουθα.

Πρώτα υπολογίζουμε το σύνδρομο $lH = [\sigma_1, \sigma_3] = [l(\lambda), l(\lambda^3)] = [0111, 0011]$. Είναι λοιπόν $\sigma_1 = 0111 = \lambda^{11}$ και $\sigma_3 = 0011 = \lambda^6$. Επειδή ${\sigma_1}^3 = (\lambda^{11})^3 = \lambda^{33} = \lambda^3 \neq \sigma_3$, εξετάζουμε τις ρίζες της εξίσωσης

$$x^2 + \sigma_1 x + \frac{\sigma_3}{\sigma_1} + \sigma_1^2 = x^2 + \lambda^{11} x + \frac{\lambda^6}{\lambda^{11}} + \left(\lambda^{11}\right)^2 = x^2 + \lambda^{11} x + \lambda^{10} + \lambda = 0 .$$

(Λαμβάνουμε υπόψη ότι $\lambda^{15} = 1$ και $\lambda^{-11} = \lambda^{-11}\lambda^{15} = \lambda^4$). Δοκιμάζοντας με τη σειρά τα στοιχεία του πεδίου, δηλαδή τα $\lambda, \lambda^2, \lambda^3, \ldots$ βρίσκουμε τις ρίζες λ^3 και λ^5. Επομένως, σύμφωνα με το σημείο 6 της διαδικασίας αποκωδικοποίησης, διορθώνονται 2 σφάλματα στις θέσεις 3 και 5, δηλαδή το πρότυπο σφάλματος είναι $\varepsilon = 000101000000000$. Συνεπώς, η λέξη που μεταδόθηκε προκύπτει από $c = l + \varepsilon = 110100111010000 + 000101000000000 = 110001111010000$.

5.1

Εφόσον ο εισβολέας δεν υπέκλεψε και την τυχαία ακολουθία, το σύστημα μπορεί να χαρακτηριστεί ως απόλυτα ασφαλές.

Αν τα καταφέρατε, μπράβο! Αν δεν τα καταφέρατε με την πρώτη, προσπαθήστε και πάλι, αφού λάβετε υπόψη ότι η ασφάλεια του παρόμοιου με το one – time pad συστήματος εξαρτάται από την τυχαία ακολουθία, η οποία είναι του ιδίου μήκους με το μήνυμα, παρόλο που το κλειδί K είναι πολύ μικρότερου μήκους. Το κλειδί K χρησιμοποιείται μόνο για την ανταλλαγή των αναγκαίων για την κρυπτογράφηση και αποκρυπτογράφηση τυχαίων ακολουθιών.

Ορίζουμε το ακόλουθο γεγονός ασφάλειας: ένας εισβολέας, έχοντας καταφέρει να υποκλέψει το κρυπτογραφημένο μήνυμα, προσπαθεί να ανακτήσει το καθαρό μήνυμα, χωρίς να έχει υποκλέψει την τυχαία ακολουθία. Χωρίς την τυχαία ακολουθία R_i δεν είναι δυνατή η ανάκτηση του καθαρού M_i από το κρυπτογραφημένο μήνυμα C_i και τότε, δηλαδή αν λαμβάνει χώρα το ανωτέρω γεγονός ασφάλειας, το σύστημά μας μπορεί να θεωρηθεί ως απόλυτα ασφαλές, αφού η ασφάλειά του είναι αυτή του αλγόριθμου one – time pad που αναλύσαμε στο Παράδειγμα 3.

Ωστόσο, αν η τυχαία ακολουθία περιέλθει στην κατοχή του εισβολέα, τότε το σύστημα αποδεικνύεται ανασφαλές. Για παράδειγμα, ο εισβολέας θα μπορούσε να δοκιμάσει στην τύχη q αριθμούς για να πάρει από τον εξυπηρετητή την τυχαία ακολουθία. Σ' αυτή την περίπτωση, η πιθανότητα να σχηματίσει ο εισβολέας το σωστό κλειδί, δηλαδή να μη λάβει χώρα το γεγονός ασφάλειας που ορίσαμε ανωτέρω και να πάρει την τυχαία ακολουθία είναι ίση με $p = q/2^n$. Αν $q = 2^{100}$ και αν το μήκος του κλειδιού, n, είναι 500 bits, τότε $p = 1/2^{400}$. Η πιθανότητα, επομένως, να μη λάβει χώρα το ανωτέρω γεγονός είναι αμελητέα.

Αφού το μήκος του μηνύματος και της τυχαίας ακολουθίας είναι πολύ μεγαλύτερο από αυτό του κλειδιού, η αμοιβαία πληροφορία μεταξύ αυτών είναι μεγαλύτερη του 0. Το ότι χαρακτηρίσαμε το σύστημα απόλυτα ασφαλές έρχεται, επομένως, σε αντίφαση με το συμπέρασμα που περιέχεται στην παράγραφο που προηγείται του Παραδείγματος 2, της Υποενότητας 5.2.1. Πράγματι, η εισαγωγή της έννοιας του γεγονότος ασφάλειας επιτρέπει την απόκλιση από τα προηγούμενα αποτελέσματα που είδαμε, εφόσον όμως το γεγονός αυτό λαμβάνει χώρα.

5.2

Απαιτείται κρυπτόγραμμα μήκους τουλάχιστον 132 γραμμάτων για τον προσδιορισμό του κλειδιού.

Αν τα καταφέρατε, μπράβο! Αν όχι, μετά την επανάληψη της μελέτης του θεωρήματος 5.2 και της Υποενότητας 5.2.2 προσπαθήστε και πάλι. Τα βασικά σημεία της απάντησης παρατίθενται στη συνέχεια.

Η εντροπία της πηγής ανά σύμβολο του ελληνικού αλφάβητου είναι 4 bits και η μέγιστη εντροπία 4,6 bits. Αφού πρόκειται για μονοαλφαβητική αντικατάσταση, τα δυνατά κλειδιά είναι 24! = 6,2 x 10^{23}. Επομένως, η εντροπία του κλειδιού είναι ίση με 79,03765 bits και η μοναδιαία απόσταση ίση με 79/0,6 = 131,7.

5.3

Στον ακόλουθο πίνακα περιέχονται οι χρόνοι χειρότερης περίπτωσης. Η αναζήτηση του σωστού κλειδιού μπορεί να ευοδωθεί πολύ πριν την ολοκλήρωση όλων των δοκιμών.

	Απαιτούμενος χρόνος με υπολογιστική ισχύ		
Απαιτούμενες δοκιμές	2^{40} πράξεις/sec	2^{56} πράξεις/sec	2^{64} πράξεις/sec
2^{40}	1 sec	0,01 msec	0,06 μsec
2^{56}	18,2 ώρες	1 sec	4 msec
2^{128}	9,8 10^{18} έτη	1,5 10^{14} έτη	1,4 10^{13} έτη

Αν τα καταφέρατε, πολύ ωραία! Αν όχι, καλό θα ήταν να προσπαθήσετε και πάλι. Ο ζητούμενος χρόνος προκύπτει από τη διαίρεση των απαιτούμενων δοκιμών προς την υπολογιστική ισχύ.

5.4

Το δημόσιο κλειδί του Α είναι $P_A = 28$, το «κρυπτογραφικό κλειδί» του Β, για $r = 3$, είναι $K = 13$. Η κρυπτογραφημένη μορφή του $M = 47$ είναι ($C_1 = 59$, $C_2 = 43$). Η αποκρυπτογράφηση επιτυγχάνεται ως εξής: $K = 59^{13} \bmod 71 = 13$ και $M = 43/13 \bmod 71 = 47$.

Αν τα καταφέρατε, μπράβο! Αν όμως είχατε δυσκολίες και ιδιαίτερα με τις πράξεις ισοτιμίας, στην επόμενη προσπάθειά σας μπορείτε να λάβετε υπόψη ότι για την επίλυση της πράξης ισοτιμίας $(\alpha/\beta) \bmod p$, αρκεί να επιλύσουμε την πράξη $(\alpha\,\beta^{-1}) \bmod p$, όπου β^{-1} είναι ο αντίστροφος του $\beta \pmod p$, δηλαδή το γινόμενό του είναι ισοδύναμο με $1 \bmod p$. Ο αντίστροφος μπορεί να υπολογιστεί με το γενικευμένο αλγόριθμο του Ευκλείδη. Στη συνέχεια, θα επαναλάβουμε τα βήματα που ακολουθούμε για τον υπολογισμό του δημόσιου κλειδιού, καθώς και για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος.

Από τη γεννήτρια του πεδίου Z_{71}, α = 7 και το ιδιωτικό κλειδί $S_A = 13$ υπολογίζεται

το αντίστοιχο δημόσιο κλειδί του $P_A = a^{SA} \bmod p = P_A = 7^{13} \bmod 71 = 28$, το οποίο δημοσιοποιείται..

Για την κρυπτογράφηση του μηνύματος $M = 47$, ο χρήστης Β, έχοντας επιλέξει τον τυχαίο αριθμό $r = 3$, υπολογίζει το «κρυπτογραφικό κλειδί» K, $K = P_A{}^k \bmod p = 28^3 \bmod 71 = 13$. Κατόπιν κρυπτογραφεί το μήνυμα, $C_1 = a^r \bmod p = 7^3 \bmod 71 = 59$ και $C_2 = KxM \bmod p = 13x47 \bmod 71 = 43$. Το ζεύγος των ακεραίων (59, 43) αποτελεί την κρυπτογραφημένη μορφή του μηνύματος $M = 47$.

Για την αποκρυπτογράφηση, ο χρήστης Α, ανακτά το «κρυπτογραφικό κλειδί» K, $K = (C_1)^{SA} \bmod p = 59^{13} \bmod 71 = 13$ και το μήνυμα M, $M = (C_2 / K) \bmod p = (43/13) \bmod 71 = 47$.

Απαντήσεις Δραστηριοτήτων

3.1

Στις ιδιότητες της χωρητικότητας συγκαταλέγονται και οι ακόλουθες τρεις:

$$C >= 0, \text{ αφού } I(X;Y) >= 0.$$

$C \leq \log|X|$, όπου $|X|$ είναι το πλήθος των κωδικών συμβόλων εισόδου, αφού

$$C = \max I(X;Y) \leq \max H(X) = \log|X|.$$

$C \leq \log|Y|$, όπου $|Y|$ είναι το πλήθος των κωδικών συμβόλων εξόδου, αφού

$$C = \max I(X;Y) \leq \max H(Y) = \log|Y|.$$

Γενικά, ο υπολογισμός της χωρητικότητας καναλιού είναι σύνθετος. Μόνο στις περιπτώσεις απλών καναλιών, όπως αυτών των Παραδειγμάτων 2 – 4, είναι ο υπολογισμός της χωρητικότητας εύκολος. Κατά κανόνα, χρησιμοποιούνται μη γραμμικές τεχνικές αριστοποίησης.

Αν τα καταφέρατε, συγχαρητήρια! Αν όχι, τότε θα πρότεινα να επαναλάβετε τη μελέτη της Υποενότητας 3.1.1, ιδιαίτερα τους ορισμούς της χωρητικότητας. Βέβαια, στις ιδιότητες ίσως να έχετε συμπεριλάβει άλλες, όπως το ότι η χωρητικότητα είναι μια συνεχής συνάρτηση της $p(x)$ ή ακόμα ότι η χωρητικότητα είναι μια κοίλη συνάρτηση του $p(x)$. Και αυτές οι απαντήσεις είναι σωστές. Οι ανωτέρω τρεις ιδιότητες είναι οι πιο προφανείς.

Γλωσσάριο Όρων

Αβεβαιότητα καναλιού (Channel equivocation)

Η υπό συνθήκη ποσότητα πληροφορίας της εισόδου του επικοινωνιακού κλειδιού, δεδομένης της εξόδου του.

Αβεβαιότητα κλειδιού (Key equivocation)

Η υπό συνθήκη ποσότητα πληροφορίας του κλειδιού δεδομένου του κρυπτογραφημένου μηνύματος.

Αβεβαιότητα μηνύματος (Message equivocation)

Η υπό συνθήκη ποσότητα πληροφορίας του μηνύματος με δεδομένο το κρυπτογραφημένο μήνυμα.

Αθροιστικός γκαουσιανός λευκός θόρυβος (Additive Gaussian white noise)

Αθροιστικός και ανεξάρτητος του σήματος εισόδου θόρυβος, ο οποίος χαρακτηρίζεται από κανονική συνάρτηση πυκνότητας πιθανότητας**.**

Αθροιστικός (Προσθετικός) θόρυβος (Additive noise)

Θόρυβος, ο οποίος επενεργεί προσθετικά στο σήμα εισόδου.

Αθροιστικό κανάλι επικοινωνίας (Additive channel)

Κάθε κανάλι επικοινωνίας στο οποίο ο στατιστικά ανεξάρτητος θόρυβος επενεργεί προσθετικά στο μεταδιδόμενο σήμα.

Αλφάβητο πηγής (Source alphabet)

Το σύνολο των διαφορετικών συμβόλων που εκπέμπει η πηγή.

Άμεσος κώδικας (Instantaneous code)

Μοναδικά αποκωδικοποιήσιμος κώδικας πηγής, ο οποίος επιτρέπει την άμεση αποκωδικοποίηση μιας ληφθείσας λέξης.

Αμοιβαία πληροφορία ή αμοιβαία ποσότητα πληροφορίας (Mutual information)

Μέτρο ποσότητας πληροφορίας, το οποίο εκφράζει τη σχετική εξάρτηση μεταξύ

δύο τυχαίων μεταβλητών.

Αξιοπιστία καναλιού (Channel reliability)

Η πιθανότητα ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού.

Αποκρυπτογράφηση (Decryption, Deciphering)

Η αντίστροφος διαδικασία της κρυπτογράφησης, η οποία οδηγεί στο καθαρό μήνυμα από το κλειδί και το κρυπτογραφημένο μήνυμα.

Αποκωδικοποίηση μέγιστης πιθανότητας (Maximum likelihood decoding)

Διαδικασία αποκωδικοποίησης, σύμφωνα με την οποία μια ληφθείσα λέξη αποκωδικοποιείται ως η εγγύτερη προς αυτήν κωδική λέξη.

Απόλυτα ασφαλής κρυπτογραφικός αλγόριθμος (Unconditionally secure cryptographic algorithm)

Κάθε κρυπτογραφικός αλγόριθμος, ο οποίος δεν παραβιάζεται ανεξαρτήτως των υπολογιστικών πόρων και του χρόνου που διαθέτει ο κρυπταναλυτής. Ή με όρους της Θεωρίας Πληροφορίας: απόλυτα ασφαλές είναι κάθε κρυπτογραφικό σύστημα, το οποίο χαρακτηρίζεται από μηδενική αμοιβαία πληροφορία μεταξύ καθαρών και κρυπτογραφημένων μηνυμάτων.

Απόσταση Hamming (Hamming distance)

Το πλήθος των θέσεων, στις οποίες δύο λέξεις εμφανίζουν ασυμφωνία δυαδικού ψηφίου.

Απόσταση κώδικα (Code distance)

Η ελάχιστη απόσταση μεταξύ των κωδικών λέξεων όλων των δυνατών ζευγών ενός κώδικα.

Ασύμμετροι κρυπτογραφικοί αλγόριθμοι (Asymmetric cryptographic algorithms)

Κατηγορία κρυπτογραφικών αλγορίθμων, οι οποίοι βασίζονται σε ζεύγος κρυπτογραφικών κλειδιών, το δημόσιο κλειδί για την κρυπτογράφηση και το ιδιωτικό (ή μυστικό) κλειδί για την αποκρυπτογράφηση.

Ασφάλεια κρυπτογραφικών συστημάτων (Cryptosystem security)

Ιδιότητα και ταυτόχρονα κριτήριο αξιολόγησης κρυπτογραφικών συστημάτων (ή αλγορίθμων), η οποία αναφέρεται στην ανθεκτικότητά τους σε απόπειρες παραβίασης και η οποία χαρακτηρίζεται από την απαιτούμενη για την παραβίασή τους υπολογιστική ισχύ ή αποθηκευτική ικανότητα που εκφράζεται ως χρονική ή αποθηκευτική πολυπλοκότητα.

Βάρος Hamming (Hamming weight)

Το πλήθος των ψηφίων μιας λέξης, τα οποία είναι ίσα με 1.

Βάση κώδικα (Basis for a code)

Κάθε γραμμικώς ανεξάρτητο, μέγιστης διάστασης, υποσύνολο ενός συνόλου S, του οποίου το γραμμικό ανάπτυγμα αποτελεί τον κώδικα.

Γεννήτορας πίνακας κώδικα (Generator matrix)

Κάθε πίνακας, του οποίου οι γραμμές αποτελούν μια βάση του κώδικα.

Γραμμικός κώδικας (Linear code)

Κάθε κώδικας με τη χαρακτηριστική ιδιότητα, το άθροισμα οποιωνδήποτε κωδικών του λέξεων να είναι επίσης κωδική λέξη.

Διάσταση κώδικα (Code dimension)

Το πλήθος των στοιχείων (λέξεων) μιας βάσης του κώδικα.

Δυαδικό συμμετρικό κανάλι επικοινωνίας (Binary symmetric channel)

Κάθε δυαδικό κανάλι επικοινωνίας, το οποίο χαρακτηρίζεται από ίσες πιθανότητες ορθής μεταφοράς των δύο κωδικών συμβόλων, του «0» και του «1»

Δυϊκός κώδικας (Dual code)

Το ορθογώνιο συμπλήρωμα του κώδικα.

Ενθόρυβο επικοινωνιακό κανάλι (Noisy channel)

Κάθε επικοινωνιακό κανάλι, στο οποίο επενεργεί θόρυβος.

Εντροπία

(Δείτε μέση πληροφορία).

Επίθεση (Attack)

Κάθε επιχειρούμενη κρυπταναλυτική προσπάθεια ή απόπειρα παραβίασης πρωτοκόλλων ή μηχανισμών ασφαλείας.

Επίθεση γνωστού καθαρού κειμένου (Known – plaintext attack)

Κρυπταναλυτική επίθεση, η οποία προϋποθέτει τόσο κρυπτογραφημένα κείμενα όσο και τα αντίστοιχα καθαρά κείμενα.

Επίθεση επιλεγμένου καθαρού κειμένου (Chosen – plaintext attack)

Κρυπταναλυτική επίθεση,η οποία προϋποθέτει τα κρυπτογραφημένα κείμενα επιλεγμένων, από τον κρυπταναλυτή, καθαρών κειμένων.

Επίθεση επιλεγμένου κρυπτογραφημένου κειμένου (Chosen – ciphertext attack)

Κρυπταναλυτική επίθεση, η οποία προϋποθέτει τόσο επιλεγμένα, από τον κρυπταναλυτή, κρυπτογραφημένα κείμενα όσο και τα αντίστοιχα καθαρά κείμενα.

Επίθεση κρυπτογραφημένου κειμένου (Ciphertext – only attack)

Κρυπταναλυτική επίθεση, η οποία προϋποθέτει μόνο κρυπτογραφημένο κείμενο.

Ισομήκης κώδικας (Block code)

Δείτε Κώδικας Μπλοκ.

Καθαρό ή Απλό μήνυμα (Plaintext)

Το μήνυμα στην αναγνώσιμη, εύληπτή του μορφή. Το μη κρυπτογραφημένο μήνυμα.

Καταιγισμός σφαλμάτων (Burst error)

Μια ακολουθία συσχετισμένων σφαλμάτων.

Κρυπτανάλυση (Cryptanalysis)

Ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη, σχεδίαση και ανάπτυξη μεθό-

δων και τεχνικών παραβίασης κρυπτογραφικών συστημάτων και πρωτοκόλλων.

Κρυπτογραφημένο μήνυμα ή Κρυπτόγραμμα (Ciphertext)

Το μήνυμα σε κρυπτογραφημένη μορφή.

Κρυπτογράφηση (Encryption, Enciphering)

Η διαδικασία μετασχηματισμού δεδομένων (ή μηνυμάτων), η οποία οδηγεί σε δεδομένα (ή μηνύματα) σε κρυπτογραφημένη μορφή.

Κρυπτογραφία (Cryptography)

Ο επιστημονικός κλάδος, ο οποίος πραγματεύεται τη μελέτη, σχεδίαση και ανάπτυξη κρυπτογραφικών μεθόδων, τεχνικών, συστημάτων και πρωτοκόλλων.

Κρυπτογραφικά κλειδιά (Cryptographic key)

Ακολουθίες δυαδικών ψηφίων (ή συμβόλων), οι οποίες επηρεάζουν καθοριστικά τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης. Χρησιμοποιούνται σε κρυπτογραφικά συστήματα, σχήματα ψηφιακών υπογραφών, στεγανογραφικά συστήματα και συναρτήσεις κατακερματισμού.

Κρυπτογραφικό πρωτόκολλο (Cryptographic protocol)

Κάθε πρωτόκολλο, το οποίο βασίζεται σε κρυπτογραφικούς αλγόριθμους. Οι όροι «κρυπτογραφικό πρωτόκολλο» και «κρυπτογραφικός μηχανισμός» χρησιμοποιούνται πολύ συχνά με την ίδια σημασία.

Κρυπτογραφικό σύστημα (Cryptosystem)

Η υλοποίηση του κρυπτογραφικού αλγόριθμου. Πολλές φορές οι όροι «κρυπτογραφικός αλγόριθμος» και «κρυπτογραφικό σύστημα» χρησιμοποιούνται, στη βιβλιογραφία και στο βιβλίο αυτό, με την ίδια σημασία.

Κρυπτολογία (Cryptology)

Η επιστήμη, η οποία απαρτίζεται από τους κλάδους της Κρυπτογραφίας και της Κρυπτανάλυσης. Επίσης, στην Κρυπτολογία μπορούμε να εντάξουμε και τον κλάδο της Απόκρυψης Πληροφορίας (Information Hiding), ο οποίος αναπτύχθηκε ιδιαίτερα τα τελευταία χρόνια.

Κυκλικός κώδικας

Κάθε γραμμικός κώδικας, του οποίου οι κυκλικές μετατοπίσεις των κωδικών του λέξεων είναι επίσης κωδικές λέξεις.

Κώδικας Hamming

Κάθε γραμμικός κώδικας μήκους $n = 2^r - 1$ ($r \geq 2$), του οποίου ο πίνακας ελέγχου ισοτιμίας περιέχει όλες τις δυνατές μη μηδενικές λέξεις μήκους r.

Κώδικας μπλοκ ή Ισομήκης κώδικας (Block code)

Κάθε κώδικας, του οποίου όλες οι κωδικές λέξεις έχουν το ίδιο μήκος.

Κώδικας πηγής (Κωδικοποίηση πηγής)

Σύνολο κωδικών λέξεων και η αντιστοίχησή τους με τα σύμβολα (ή μηνύματα) της πηγής.

Μέθοδος του Καίσαρα (Caesar substitution)

Κωδικοποιητής αντικατάστασης, σύμφωνα με τον οποίο κάθε χαρακτήρας του καθαρού μηνύματος αντικαθίσταται από το γράμμα που βρίσκεται τρεις θέσεις δεξιά του στο αλφάβητο. Η μέθοδος αυτή επινοήθηκε από τον Καίσαρα.

Μέση πληροφορία ή μέση ποσότητα πληροφορίας ή μέσο πληροφορικό περιεχόμενο ή εντροπία (Shannon's information measure)

Το μέτρο ποσότητας πληροφορίας του Shannon.

Μέτρα πληροφορίας (Information measures)

Η μέση πληροφορία ή εντροπία ή μέσο πληροφορικό περιεχόμενο ή μέση ποσότητα πληροφορίας, η συνδυασμένη ποσότητα πληροφορίας, η υπό συνθήκη ποσότητα πληροφορίας και η αμοιβαία πληροφορία.

Μη ιδιάζων κώδικας (Non – singular code)

Κώδικας πηγής, του οποίου όλες οι κωδικές λέξεις είναι διάφορες μεταξύ τους.

Μοναδιαία απόσταση (Unicity distance)

Το ελάχιστο μήκος του κρυπτογραφημένου μηνύματος, το οποίο απαιτείται για τον προσδιορισμό του κλειδιού.

Μοναδικά αποκωδικοποιήσιμος κώδικας(Uniquely decodable code)

Μη ιδιάζων κώδικας πηγής, του οποίου όλες οι δυνατές ακολουθίες κωδικών λέξεων είναι διάφορες μεταξύ τους.

Μονοαλφαβητική κωδικοποίηση (Monoalphabetical substitution)

Κατηγορία κρυπτογραφικών μεθόδων, οι οποίες βασίζονται στην τεχνική της αντικατάστασης και των οποίων το κλειδί έχει μήκος ίσο με 1.

Μπλοκ μιας χρήσης (One – time pad)

Δείτε Δυαδικό Κωδικοποιητή και Κωδικοποιητή Vernam.

NP – πλήρη (NP – Complete) προβλήματα

NP προβλήματα, για οποιοδήποτε από τα οποία και αν δειχθεί ότι έχει ως λύση πολυωνυμικό αλγόριθμο ή ότι δεν υπάρχει ντερμινιστικός πολυωνυμικός αλγόριθμος που το επιλύει, τότε αυτό ισχύει και για τα υπόλοιπα NP – πλήρη προβλήματα.

NP προβλήματα

Προβλήματα των οποίων η λύση μπορεί να εκτελεστεί σε χρόνο φραγμένο από πολυωνυμική συνάρτηση μεγέθους αυτού του προβλήματος, δεδομένης της ικανότητας να εικάζουμε με απόλυτη ακρίβεια (nondeterministic Turing machine).

Οδηγός συνομάδας (Coset leader)

Λέξη της συνομάδας ελάχιστου βάρους.

Πηγή Markoff (Markoff information source)

Κάθε πηγή πληροφορίας, η οποία μπορεί να αναπαρασταθεί ως Μαρκοβιανή αλυσίδα.

Πηγή πληροφορίας με μνήμη (Information source with memory)

Κάθε πηγή πληροφορίας, της οποίας η εκπομπή ενός συμβόλου εξαρτάται στατιστικά από την εκπομπή προηγούμενων συμβόλων.

Πηγή πληροφορίας χωρίς μνήμη (Memoryless information source)

Κάθε πηγή πληροφορίας, της οποίας η εκπομπή ενός συμβόλου δεν εξαρτάται

στατιστικά από την εκπομπή προηγούμενων συμβόλων.

Πίνακας ελέγχου ισοτιμίας κώδικα C (Parity – check matrix)

Κάθε πίνακας, του οποίου οι στήλες αποτελούν μια βάση για το δυϊκό κώδικα $C^{\perp}$.

Πολυώνυμο – γεννήτορας κώδικα (Genrator polynomial)

Πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε μη μηδενική λέξη του κώδικα.

Ποσότητα πληροφορίας του Hartley (Hartley's amount of information)

Ο δεκαδικός λογάριθμος του πλήθους των διαφορετικών λέξεων που μπορούν να σχηματιστούν, αποτελούμενες από ένα δεδομένο πλήθος συμβόλων.

Πρότυπο σφάλματος (Error pattern)

Το άθροισμα της κωδικής λέξης που μεταδόθηκε με τη ληφθείσα λέξη.

RSA

Ασύμμετρος κρυπτογραφικός αλγόριθμος, ο οποίος βασίζεται στο δύσκολο πρόβλημα της ανάλυσης πολύ μεγάλων ακεραίων αριθμών σε γινόμενο πρώτων παραγόντων και επινοήθηκε από τους Rivest, Shamir και Adleman.

Ρυθμός μετάδοσης καναλιού (Transmission rate)

Η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του επικοινωνιακού καναλιού.

Ρυθμός πληροφορίας (information rate)

Το ποσοστό της κωδικής λέξης ενός κώδικα που μεταφέρει το μήνυμα.

Συνάρτηση Euler (Euler's Totient Function)

Συνάρτηση η οποία απεικονίζει κάθε φυσικό αριθμό n στο πλήθος των φυσικών που είναι μικρότεροι ή ίσοι του n και σχετικά πρώτοι με αυτόν. (Το πλήθος των στοιχείων του ανηγμένου συστήματος υπολοίπων *modulo n*.)

Σύνδρομο (Syndrome)

Το γινόμενο μιας ληφθείσας λέξης με τον πίνακα ελέγχου ισοτιμίας του κώδικα.

Συνομάδα κώδικα C προσδιορισμένη από τη λέξη x (Coset)

Το σύνολο όλων των λέξεων της μορφής $c + x$, όπου $c \in C$.

Συστηματικός κώδικας (Systematic code)

Κάθε κώδικας που έχει γεννήτορα πίνακα σε μορφή περιορισμένης κλιμακωτής διάταξης γραμμών (ΠΚΔΓ).

Τεχνική αντικατάστασης (Substitution Technique)

Βασική τεχνική κλασικών κρυπτογραφικών συστημάτων, σύμφωνα με την οποία χαρακτήρες του μηνύματος αντικαθίστανται από άλλους στη βάση κάποιου κανόνα.

Τεχνική μετάθεσης (Transposition technique)

Βασική τεχνική κλασικών κρυπτογραφικών συστημάτων, σύμφωνα με την οποία η διάταξη των χαρακτήρων του μηνύματος μεταβάλλεται στη βάση κάποιου κανόνα.

Τυπική διάταξη αποκωδικοποίησης κώδικα (Standard decoding array)

Πίνακας αποτελούμενος από τα σύνδρομα και τους οδηγούς των συνομάδων του κώδικα.

Υπολογιστικά ασφαλής κρυπτογραφικός αλγόριθμος (Computationally secure ή strong)

Κρυπτογραφικός αλγόριθμος μη παραβιάσιμος με τους διαθέσιμους υπολογιστικούς πόρους.

Χωρητικότητα διακριτού καναλιού χωρίς θόρυβο (Capacity of discrete noisyless channel)

Η μέγιστη εντροπία της εισόδου του διακριτού καναλιού.

Χωρητικότητα διακριτού ενθόρυβου καναλιού (Capacity of discrete noisy channel)

Η μέγιστη ποσότητα πληροφορίας που μπορεί να μεταδοθεί μέσω του ενθόρυβου διακριτού καναλιού ή η μέγιστη αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του ενθόρυβου καναλιού ή ο μέγιστος ρυθμός μετάδοσης του καναλιού.