ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΠΜΣ)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

` Εφαρμογές της Θεωρίας Πληροφορίας στην ασφάλεια δικτύων `

ΦΟΙΤΗΤΡΙΑ: Καμπανά Νεκταρία ΜΕ/08051

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ

ΝΟΕΜΒΡΙΟΣ 2010

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Ξενάκη Χρήστο, για τη βοήθεια και καθοδήγηση που μου προσέφερε και κυρίως για την κατανόηση και την υπομονή του. Επίσης ευχαριστώ τον κ. Λαμπρινουδάκη Κωνσταντίνο, επίκουρο καθηγητή και τον κ. Σωκράτη Κάτσικα, καθηγητή για την τιμή που μου έκαναν να είναι μέλη της τριμελούς επιτροπής.

Τέλος θέλω να ευχαριστήσω την οικογένεια μου, τους γονείς μου Ανδρέα και Μαρία και την αδερφή μου Τάνια, για την ενθάρρυνσή τους και τη διαρκή τους υποστήριξη στο κάθε τι.

Πρόλογος

Η θεωρία της πληροφορίας είναι το επιστημονικό πεδίο που ασχολείται με τα μέτρα και τις εφαρμογές της έννοιας της ‘’πληροφορίας’’. Απαντάει κατά βάση σε δύο θεμελιώδη ερωτήματα της επιστήμης των τηλεπικοινωνιών: Ποιά είναι η μέγιστη συμπίεση δεδομένων και ποιός είναι ο μέγιστος ρυθμός μετάδοσης, και ως εκ τούτου βρίσκει εφαρμογή και στην ασφάλεια των δικτύων. Οριο της συμπίεσης δεδομένων αποτελεί η μέση ποσότητα πληροφορίας ή εντροπία, ενώ όριο του ρυθμού μετάδοσης δεδομένων αποτελεί η χωρητικότητα του καναλιού. Η θεωρία κωδικοποίησης είναι η μελέτη μεθόδων για την αποτελεσματική και ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό.

Το πεδίο της Θεωρίας της Πληροφορίας και Κωδικοποίησης είναι πολύ ευρύ. Στην παρούσα πτυχιακή εργασία γίνεται μελέτη των μεθόδων ασφάλειας δικτύων που βασίζονται στη θεωρία της πληροφορίας.

Αρχικά, γίνεται μια ιστορική αναδρομή στο επιστημονικό πεδίο της θεωρίας της πληροφορίας. Επίσης, γίνεται αναφορά στο βασικό τηλεπικοινωνιακό μοντέλο που αποτελεί το πλαίσιο μέσα στο οποίο παρουσιάζονται οι βασικές αρχές και έννοιες της Θεωρίας Πληροφορίας.

Στη συνέχεια, γίνεται πολύ συνοπτικά αναφορά σε βασικά στοιχεία από την Θεωρία Πιθανοτήτων. Επίσης εισάγεται η έννοια και το μέτρο ποσότητας πληροφορίας καθώς και η επέκταση του για την περίπτωση πληροφορίας που εκφράζεται ως συνδυασμός δύο τυχαίων μεταβλητών.

Τέλος ακολουθούν οι πηγές πληροφορίας. Πιο συγκεκριμένα, περιγράφονται οι διακριτές πηγές πληροφορίας χωρίς μνήμη και τεχνικές κωδικοποίησης για αυτές τις πηγές καθώς και οι διακριτές πηγές πληροφορίας με μνήμη και σχετικές τεχνικές κωδικοποίησης.

Κεφάλαιο 1. Εισαγωγή

Στις μέρες μας υπάρχει ραγδαία ανάπτυξη των μέσων καταγραφής, αποθήκευσης, επεξεργασίας και μετάδοσης των δεδομένων, καθώς επίσης και των συναφών τεχνολογιών επικοινωνίας, όπως το τηλέφωνο, η τηλεόραση και τα δίκτυα υπολογιστών. Κοινός τόπος όλων αυτών των τεχνολογικών επιτευγμάτων είναι η ακριβής, ταχεία, ασφαλής και οικονομική αποθήκευση και μετάδοση της πληροφορίας.

Όλη αυτή η ανάπτυξη έδωσε περισσότερους καρπούς μετά τη μαθηματική θεμελίωση της έννοιας της πληροφορίας. Πριν τα μέσα του εικοστού αιώνα, η έννοια της πληροφορίας ήταν κατά βάση αφηρημένη και ποιοτική. Επομένως, οποιαδήποτε προσπάθεια εξαγωγής νόμων που διέπουν την πληροφορία και την επικοινωνία ήταν αρχικά αδύνατη. Αυτή η αδυναμία ποσοτικοποίησης της έννοιας της πληροφορίας αντιμετωπίστηκε αρχικά από τον **Hartley** και στη συνέχεια από το **Shannon**.

Πρώτος ο Hartley το 1928 όρισε την «**ποσότητα πληροφορίας**». Είπε πως η «πληροφορία» προκύπτει από τη διαδοχική επιλογή συμβόλων ή λέξεων από ένα δοσμένο «αλφάβητο» ή λεξιλόγιο, προκειμένου να οικοδομηθεί ένα μήνυμα (κείμενο) με κάποιο νόημα (τάξη, λογική). Ένα χρόνο αργότερα, το 1929, ο **Szilard** συνέδεσε την πληροφορία και τη θερμοδυναμική εντροπία.

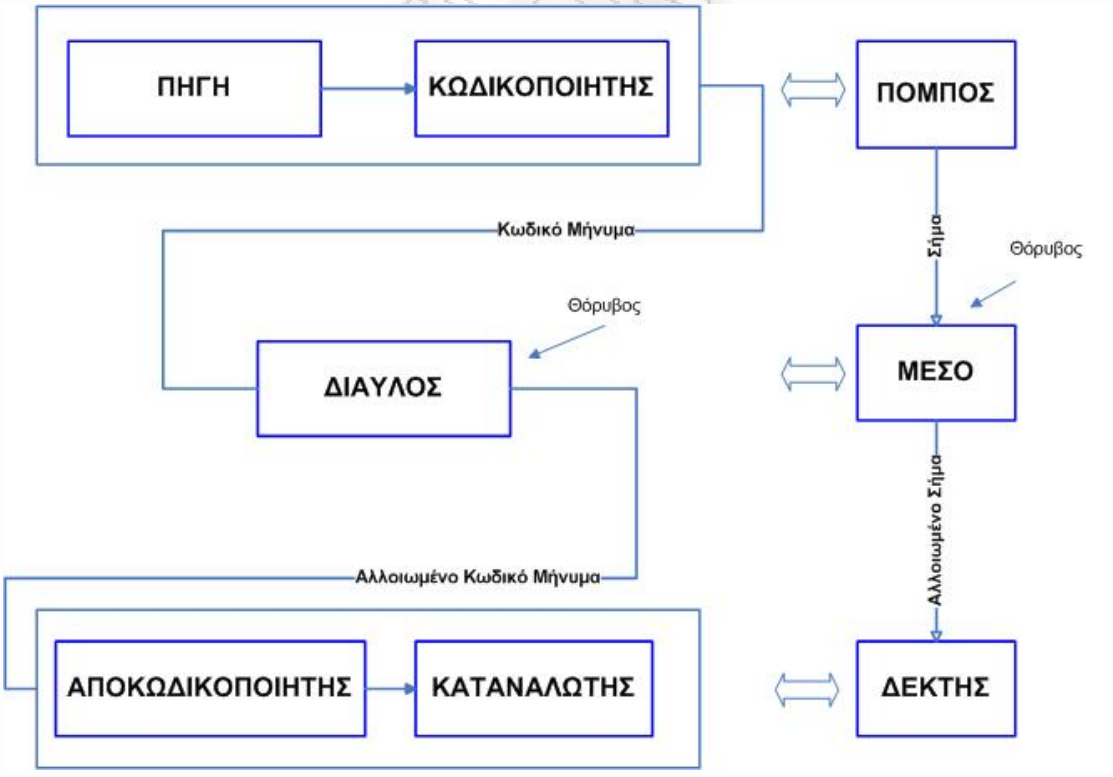
Το 1948, με την δημοσίευση της εργασίας του C. E. Shannon με τίτλο «A Mathematical Theory of Communication», γεννήθηκε μια νέα επιστημονική περιοχή, η **Θεωρία της Πληροφορίας** ή **Θεωρία Πληροφοριών**. Στόχος της είναι η θεμελίωση εννοιών και θεωρημάτων που επιτρέπουν τη μαθηματική περιγραφή της διαδικασίας της επικοινωνίας. Με αυτό το τρόπο, η μετάδοση πληροφοριών μπορεί να αναλυθεί με μαθηματική αυστηρότητα και ακρίβεια, ενώ σε ένα επόμενο βήμα είναι δυνατόν να σχεδιαστούν καλύτερα συστήματα επικοινωνιών. Η νέα θεωρία βασισμένη στη στατιστική, τη θεωρία πιθανοτήτων και την άλγεβρα μπορεί να απαντήσει με μαθηματική ακρίβεια σε ερωτήματα που σχετίζονται με τη βέλτιστη συμπίεση των δεδομένων, την περιγραφή των διαύλων επικοινωνίας, την κωδικοποίηση των μηνυμάτων πληροφορίας, το ρυθμό μετάδοσης των πληροφοριών σε περιβάλλον θορύβου, την κρυπτογράφηση κ.α..

Αν και αρχικά η θεωρία της πληροφορίας αποτέλεσε τμήμα της επιστήμης των επικοινωνιών, σε σχετικά σύντομο χρονικό διάστημα αναπτύχθηκε σε ανεξάρτητη επιστήμη με συμβολή σε επιστήμες και θέματα πέρα από τις παραδοσιακές περιοχές των τηλεπικοινωνιών και των μαθηματικών. Ενδεικτικά, αναφέρουμε τη Στατιστική Φυσική (Θερμοδυναμική), την Επιστήμη υπολογιστών (αλγοριθμική πολυπλοκότητα), τη Στατιστική, τη Βιολογία (Γενετική τεχνολογία), τη γλωσσολογία, τη σχεδίαση υπολογιστικών

συστημάτων κ.α.. Έτσι, μπορούμε να πούμε ότι στις μέρες μας, η θεωρία της πληροφορίας, λόγω της μαθηματικής της ακρίβειας και των γενικευμένων συμπερασμάτων της, αποτελεί χωριστό κλάδο των μαθηματικών.

Μέχρι το 1948 κάθε τηλεπικοινωνιακός μηχανικός θα υποστήριζε σθεναρά την άποψη ότι για να βελτιστοποιηθεί η αξιοπιστία της επικοινωνίας είναι απαραίτητο να ελαττωθεί ο ρυθμός μετάδοσης της πληροφορίας ή αντίστροφα, ότι το πλήθος των σφαλμάτων αυξάνει το ρυθμό μετάδοσης του μηνύματος. Ο Shannon απέδειξε ότι είναι δυνατόν να μείνει σταθερός (μικρότερος της χωρητικότητας του διαύλου) ο ρυθμός μετάδοσης της πληροφορίας και παρόλα αυτά η πιθανότητα σφάλματος να παραμείνει εξαιρετικά μικρή. Η χωρητικότητα του διαύλου μπορεί να υπολογιστεί με βάση τα χαρακτηριστικά θορύβου του διαύλου. Οι ιδέες του Shannon αξιοποιήθηκαν από πλήθος ερευνητών, τόσο τηλεπικοινωνιακών μηχανικών όσο και μαθηματικών, με αποτέλεσμα να αναπτύξουν σε σχετικά λίγα χρόνια τη νέα επιστήμη της θεωρίας της πληροφορίας.

Ένα σύστημα επικοινωνίας στα πλαίσια της θεωρίας της πληροφορίας αντιστοιχεί στο κλασικό τηλεπικοινωνιακό σύστημα πομπού, διαύλου και δέκτη, όπως απεικονίζεται στο παρακάτω σχήμα (Εικόνα 1).



Εικόνα 1. Γενικό διάγραμμα συστήματος τηλεπικοινωνίας

Ο πομπός αποτελείται από την πηγή πληροφορίας και τον κωδικοποιητή. Η πληροφορία παράγεται στην πηγή (πληροφορίας) και οργανώνεται σε μηνύματα πληροφορίας, τα οποία στη συνέχεια μετατρέπονται σε κωδικά μηνύματα. Ο δίαυλος πληροφορίας, ο οποίος είναι στην ουσία το μέσο που παρεμβάλλεται μεταξύ του πομπού και του δέκτη, διοχετεύει την κωδικοποιημένη πληροφορία στο σημείο προορισμού. Όταν η πληροφορία διαπερνά το δίαυλο, είναι δυνατόν να αλλοιωθεί λόγω της παρουσίας θορύβου. Η πληροφορία λαμβάνεται από το δέκτη, όπου αρχικά αποκωδικοποιείται και στη συνέχεια παρουσιάζεται στον προορισμό της.

Παρακάτω περιγράφονται αναλυτικά οι έννοιες του συστήματος επικοινωνίας από την άποψη των τηλεπικοινωνιών.

Επικοινωνία είναι κάθε διαδικασία μεταφοράς πληροφορίας μεταξύ δύο σημείων του χώρου – χρόνου (π.χ. τηλεφωνική συνδιάλεξη).

Πηγή πληροφορίας είναι το τμήμα του συστήματος επικοινωνίας που παράγει πληροφορία με τη μορφή συμβόλων (π.χ. δελτίο καιρού). Η πληροφορία προσαρτάται στα σύμβολα με κριτήριο τη πιθανότητα εμφάνισης τους στην έξοδο της πηγής πληροφορίας.

Αλφάβητο είναι το σύνολο των συμβόλων που χρησιμοποιεί η πηγή πληροφορίας (π.χ. αριθμοί, γράμματα, διαγράμματα, χάρτες).

Λέξη Πληροφορίας είναι η βραχεία διάταξη συμβόλων πληροφορίας (π.χ. λέξη αποτελούμενη απο γράμματα, όπως σταθμός).

Μήνυμα Πληροφορίας είναι η διάταξη των λέξεων πληροφορίας (π.χ. μια πρόταση αποτελούμενη από λέξεις, όπως ο σιδηροδρομικός σταθμός είναι συνέχεια ανοικτός).

Κωδικοποίηση είναι η αντικατάσταση των συμβόλων πληροφορίας από άλλα (κωδικά) σύμβολα με αντικειμενικό σκοπό τη βελτιστοποίηση της επικοινωνίας (π.χ. αντικατάσταση γραμμάτων από τελείες και παύλες κατά τον κώδικα Morse). Η κωδικοποιημένη πληροφορία οργανώνεται επίσης σε επιμέρους κωδικές λέξεις και κωδικά μηνύματα.

Κώδικας είναι κάθε τεχνική κωδικοποίηση. Το σύνολο των κωδικών συμβόλων είναι το αλφάβητο του κώδικα. Η αμφιμονοσήμαντη απεικόνιση συμβόλων, λέξεων και μηνυμάτων πληροφορίας σε κωδικά σύμβολα, κωδικές λέξεις και κωδικά μηνύματα είναι το κλειδί του κώδικα. Έστω για παράδειγμα ότι έχουμε το κωδικό αλφάβητο $\Gamma = \{0,1\}$. Η δυαδική κωδικοποίηση είναι η συνηθέστερη επιλογή στα ψηφιακά συστήματα επικοινωνίας. Με βάση αυτό το κωδικό αλφάβητο, ας υποθέσουμε ότι για την πηγή πληροφορίας με αλφάβητο $A = \{\alpha_1, \alpha_2, \alpha_3\}$ υπάρχουν οι τρείς παρακάτω δυαδικοί κώδικες:

$\alpha_1 \rightarrow 0$	$\alpha_1 \rightarrow 00$	$\alpha_1 \rightarrow 0$
$\alpha_2 \rightarrow 1$	$\alpha_2 \rightarrow 01$	$\alpha_2 \rightarrow 11$
$\alpha_3 \rightarrow 1$	$\alpha_3 \rightarrow 10$	$\alpha_3 \rightarrow 10$
I	II	III

Ο κώδικας I είναι απεικόνιση του Α στο Γ, ο κώδικας II είναι απεικόνιση του Α στο Γ^2 ενώ ο κώδικας III είναι απεικόνιση του Α στο $\Gamma \cup \Gamma^2$. Οι δύο πρώτοι κώδικες έχουν σταθερό αριθμό δυαδικών συμβόλων (ισομήκεις) ενώ ο τρίτος μεταβλητό (δεν είναι ισομήκης)

Απαραίτητο στοιχείο του πομπού είναι **ο μεταλλάκτης** που μετατρέπει το κωδικοποιημένο μήνυμα σε σήμα, δηλαδή μορφή κατάλληλη για μετάδοση (π.χ. σειρά ηλεκτρικών παλμών). Το σήμα αποτελεί τον υλικό φορέα της πληροφορίας.

Δίαυλος Πληροφορίας ή κανάλι είναι αλυσίδα μέσων και συσκευών (π.χ. καλώδια, κυματοδηγοί, οπτικές ίνες) που μεταδίδουν το σήμα με την αποτυπωμένη σε αυτό πληροφορία.

Χωρητικότητα διαύλου πληροφορίας είναι ο μέγιστος ρυθμός μετάδοσης πληροφορίας (π.χ. το τηλέτυπο μεταδίδει 10 λέξεις / sec). Καθορίζει το χρόνο και το κόστος που απαιτούνται για τη μετάδοση μηνύματος ή το πλήθος των μηνυμάτων που είναι δυνατό να διοχετεύει ταυτόχρονα ο δίαυλος πληροφορίας.

Θόρυβος είναι κάθε ανεξέλεγκτη παρεμβολή του περιβάλλοντος του διαύλου που προκαλεί αλλοίωση του σήματος και συνεπώς σφάλματα μετάδοσης (απώλεια πληροφορίας). Συνήθως στα κανάλια επικοινωνίας υπάρχουν διαφόρων ειδών θόρυβοι όπως ο θερμικός θόρυβος, ο κρουστικός θόρυβος, ο θόρυβος περιβάλλοντος ή η παρεμβολή ομιλίας από άλλες γραμμές (κανάλια). Μέχρι το 1948 ο τηλεπικοινωνιακός μηχανικός επιδίωκε την προστασία του σήματος απο τον θόρυβο, δηλαδή την πιστή αναπαραγωγή του σήματος στο δέκτη. Με την ωρίμανση της θεωρίας της πληροφορίας, το ενδιαφέρον μετατοπίσθηκε στην πιστή αναπαραγωγή του μηνύματος πληροφορίας που είναι αποτυπωμένο το σήμα. Σύγχρονα τηλεπικοινωνιακά συστήματα εξασφαλίζουν αξιόπιστη ροή πληροφορίας με σήμα βαθιά θαμμένο σε θόρυβο.

Αποκωδικοποιητής αντιπροσωπεύει την επεξεργασία που γίνεται στο σήμα που προκύπτει στην έξοδο του καναλιού προκειμένου να αναπαραχθεί ένα

όσο το δυνατόν πιστότερο αντίγραφο του σήματος στην έξοδο της πηγής πληροφορίας

Καταναλωτής της πληροφορίας είναι το τελευταίο τμήμα του συστήματος επικοινωνίας, όπου αναδομείται το αρχικό μήνυμα πληροφορίας. Έπεται του μεταλλάκτη, που μετατρέπει το σήμα σε κωδικό μήνυμα και του αποκωδικοποιητή, που μετατρέπει το κωδικό μήνυμα στο αρχικό μήνυμα πληροφορίας, αφού αποκαλύψει και διορθώσει σφάλματα μετάδοσης. Η πληροφορία αποτυπώνεται σε κείμενο, ήχο, εικόνα ή άλλη μορφή με αποτέλεσμα ο χρήστης να αυξάνει τη γνώση του ή να αποθηκεύει την ανωτέρω πληροφορία για μελλοντική χρήση.

Κεφάλαιο 2. Πληροφορία και Εντροπία

Σκοπός του κεφαλαίου αυτού είναι να εξοικειωθούμε με τις βασικές αρχές και έννοιες της θεωρίας της πληροφορίας μέσα στο πλαίσιο ενός μοντέλου επικοινωνίας με τη βοήθεια της Θεωρίας των Πιθανοτήτων. Αρχικά θα εξετάσουμε, θα περιγράψουμε και θα επεξηγήσουμε το μέτρο ποσότητας πληροφορίας και τις ιδιότητες του. Στη συνέχεια θα ερευνήσουμε πώς ορίζεται η εντροπία για μια ή περισσότερες τυχαίες μεταβλητές. Τέλος, θα δούμε τις διάφορες μορφές εντροπίας που υπάρχουν (π.χ. υπό συνθήκη, σχετική) και τις ιδιότητες που διέπουν την εντροπία ως μέτρο πληροφορίας.

2.1 Βασικές έννοιες - αξιώματα Πιθανοτήτων

Σκοπός της ενότητας αυτής είναι να επαναφέρουμε στη μνήμη μας βασικές έννοιες - αξιώματα πιθανοτήτων που απαιτούνται στους ορισμούς των μέτρων ποσότητας πληροφορίας και στη μελέτη ζητημάτων της Θεωρίας Πληροφορίας.

Το αποτέλεσμα ενός τυχαίου πειράματος, παραδείγματος χάριν, της ρίψης ενός ζαριού ή κέρματος, δεν είναι εκ των προτέρων βέβαιο.

Εκβάσεις ή ενδεχόμενα ή δειγματικά σημεία (elementary event) λέγονται τα ατομικά αδιαίρετα αποτελέσματα $\{\omega_1, \omega_2, ...\omega_n\}$ ενός πειράματος, όπως στην περίπτωση του ζαριού τα 1,2,3,4,5,6. Με τον ίδιο τρόπο η επιλογή απο την πηγή πληροφορίας των συμβόλων ενός μηνύματος είναι ένα τυχαίο πείραμα και τα σύμβολα τα δειγματικά σημεία.

Δειγματικός χώρος (sample space) λέγεται το σύνολο των πιθανών αποτελεσμάτων $(\Omega = \{\omega_1, \omega_2, ...\omega_n\})$ (δείγματα) ενός τυχαίου πειράματος, δηλαδή ενός πειράματος το οποίο εάν επαναληφθεί κάτω από τις ίδιες συνθήκες το αποτέλεσμα του θα διαφέρει κατά τρόπο απρόβλεπτο. Στην περίπτωση της ρίψης του ζαριού ο δειγματικός χώρος είναι το σύνολο $\Omega = \{1, 2, 3, 4, 5, 6\}$ και στην περίπτωση επιλογής ενός συμβόλου κατα το σχηματισμό μηνύματος απο πηγή πληροφορίας είναι το αλφάβητο που χρησιμοποιείται.

Γεγονός (event) λέγεται κάθε υποσύνολο Α του δειγματικού χώρου, δηλαδή μια συλλογή εκβάσεων ή απλών ενδεχομένων ή δειγματικών σημείων. Στην περίπτωση του ζαριού το $\Omega_1 = \{1,4\}$ και στην περίπτωση της πηγής μία λέξη.

Επίσης ορίζεται ως **βέβαιο γεγονός (certain event)** το σύνολο του δειγματοχώρου αφού θα συμβαίνει πάντα και ως **μηδενικό γεγονός (null event)** το σύνολο που δεν περιέχει κανένα αποτέλεσμα και συνεπώς δεν θα συμβεί ποτέ.

Αν θεωρηθεί ότι ένα γεγονός Α αποτελείται απο ν δειγματικά σημεία και οτι όλα τα σημεία του δειγματικού χώρου είναι N και ισοπίθανα , τότε ορίζεται ως **πιθανότητα** του Α ο λόγος ν / N . Η πιθανότητα $P(A)$ ικανοποιεί τα ακόλουθα αξιώματα της θεωρίας πιθανοτήτων:

1. $0 \le P(A) \le 1$ για κάθε γεγονός $A \in \Omega$
2. $P(\Omega) = 1$ για το δειγματοχώρο Ω
3. Για κάθε δύο αποκλειστικά αμοιβαία (mutually exclusive) γεγονότα A_1 και A_2 (δηλαδή $A_1 \cap A_2$) ισχύει: $P(A_1 \cup A_2) = P(A_1) + P(A_2)$

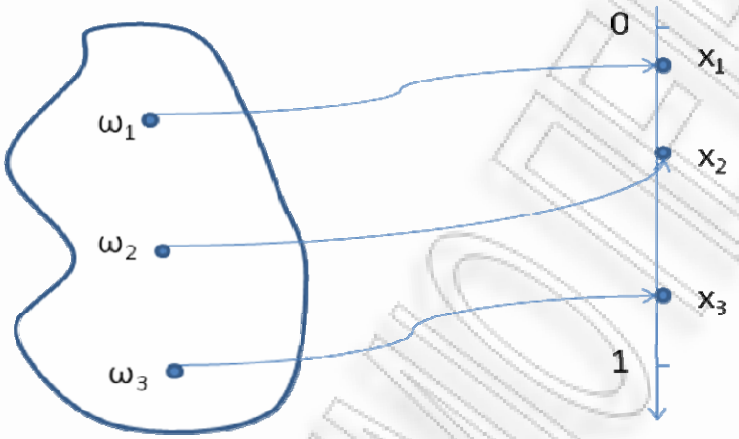
Επακόλουθα των παραπάνω αξιωμάτων είναι και τα ακόλουθα:

1. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
2. Αν $A \subset B$, τότε θα είναι $P(A) \le P(B)$
3. Αν $A_1, A_2, ...A_N$ είναι γεγονότα ανά δύο αμοιβαία αποκλειστικά τότε ισχύει: $P(\bigcup_{k=1}^{N} A_k) = \sum_{k=1}^{N} P(A_k)$ για $N \ge 2$
4. $P(\varnothing) = 0$, όπου $\varnothing$ το κενό σύνολο
5. $P(A^C) = 1 - P(A)$, όπου A^C είναι το συμπλήρωμα του συνόλου A

Παράδειγμα 2.1:

Πείραμα ρίψης τίμιου ζαριού: $\Omega = \{1,2,3,4,5,6\}$ και $P\{1\} = P\{2\} = ... = P\{6\} = 1/6$. Επίσης $P\{2,5\} = 1/3, P\{3,6\} = 1/3, P\{1,4\} = 1/3$, και $P\{1,3,5\} = 1/2$, $P\{2,4,6\} = 1/2$

Τυχαία μεταβλητή είναι μια μονοσήμαντη συνάρτηση με πεδίο ορισμού ένα δειγματικό χώρο Ω και πεδίο τιμών ένα υποσύνολο των πραγματικών αριθμών. Ο ορισμός της τυχαίας μεταβλητής ως αντιστοίχηση στοιχειωδών γεγονότων ενός δειγματοχώρου με σημεία στον άξονα των πραγματικών αριθμών απεικονίζεται στο παρακάτω σχήμα (Εικόνα 2):



Εικόνα 2. Αντιστοίχηση στοιχειωδών γεγονότων με σημεία στον άξονα των πραγματικών αριθμών

Μία τυχαία μεταβλητή λέγεται **διακριτή** αν το σύνολο των τιμών της είναι πεπερασμένο ή απείρως αριθμήσιμο. Οι **συνεχείς τυχαίες μεταβλητές** αντιστοιχούν σε συνεχείς δειγματικούς χώρους.

Παράδειγμα 2.2:

Σε τρεις διαδοχικές ρίψεις κέρματος ορίζουμε την τυχαία μεταβλητή X. Να βρεθεί πόσες φορές ήρθε κεφαλή στις τρεις διαδοχικές ρίψεις.

Λύση:

Δειγματοχώρος: $\Omega = \{HHH, HHT, HTH, THH, HTT, THT, TTH, TTT\}$

$$X(\Omega) = \{3,2,2,2,1,1,1,0\}$$

Εύρος τιμών ΤΜ: $S_x = \{0,1,2,3\}$

Έστω ένα τυχαίο πείραμα Ω με δειγματοχώρο $\Omega = \{\omega_1, \omega_2, ...\omega_n\}$ και η διακριτή τυχαία μεταβλητή X με πεδίο τιμών $X = \{x_1, x_2, ...x_n\}$. Κάθε γεγονός ω_i μπορεί να συμβεί με πιθανότητα $P(\Omega = \omega_i) = P(X = x_i) = p_i$. **Συνάρτηση μάζας πιθανότητας (Probability Mass Function)** λέγεται η $P(X = x_i) = p_i$ και το σύνολο των πιθανοτήτων αυτών είναι $P = \{p_1, p_2, ...p_n\}$. Η συνάρτηση μάζας πιθανότητας έχει τις παρακάτω ιδιότητες:

1. $p(x_i) \geq 0$, για κάθε i
2. $\sum_{i}^{n} p(x_i) = 1$

Η συνάρτηση κατανομής αθροιστικής πιθανότητας (cumulative distribution function) μιας διακριτής τυχαίας μεταβλητής X δίνεται από τη παρακάτω 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 παρακάτω 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 οι παρακάτω ιδιότητες:

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

Ορισμένες χαρακτηριστικές ιδιότητες της συνάρτησης κατανομής συνεχούς τυχαίας μεταβλητής είναι οι ακόλουθες:

1. $0 \leq F(X \leq x) \leq 1$, για κάθε x
2. Η συνάρτηση κατανομής είναι μη φθίνουσα, δηλαδή αν $x_i \leq x_k$ τότε:

$$F(X \leq x_i) \leq F(X \leq x_k)$$

3. $\lim_{x \to \infty} F(X \leq x) = 1$ και $\lim_{x \to \infty} F(X \leq x) = 0$

Μερικές φορές συνδυάζουμε δύο πειράματα ή τυχαίες μεταβλητές. Σε αυτή τη περίπτωση έχουμε δύο δειγματικούς χώρους, έστω Χ και Υ, όπου ο δειγματικός χώρος Υ αναφέρεται στο αντίστοιχο πείραμα ή στην αντίστοιχη διακριτή τυχαία μεταβλητή $Y = \{y_1, y_2, ...y_m\}$. Η κατανομή πιθανότητας της Υ είναι $P(Y) = \{p(y_1), p(y_2), ..., p(y_m)\}$, δηλαδή $p(y_i) = P(Y = y_j)$.

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 $X = x_i$ και $Y = y_j$. Απο 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 2.3:

Υποθέτουμε οτι οι Χ και Υ είναι διακριτές τυχαίες μεταβλητές και οτι η συνάρτηση συνδυασμένης πιθανότητας μάζας δίνεται από τη σχέση:

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

Λύση:

Οι συναρτήσεις ακραίας πιθανότητας μάζας υπολογίζονται ως ακολούθως:

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

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”. Η πιθανότητα εμφάνισης 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 παρακάτω 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

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

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

Παράδειγμα 2.4:

Έστω ότι μια ανίατη αρρώστια μολύνει το 1/1000 του πληθυσμού των αγελάδων. Έστω επίσης ότι υπάρχει ένα τεστ για την αρρώστια που παράγει θετικό αποτέλεσμα στο 95% των δοκιμών σε μολυσμένη αγελάδα, ενώ αν η αγελάδα δεν είναι μολυσμένη το τεστ εξακολουθεί να βγάζει θετικό αποτέλεσμα στο 5% των περιπτώσεων. Θέλουμε να ερμηνεύσουμε τα αποτελέσματα. Δηλαδή αν το αποτέλεσμα του τεστ είναι θετικό ποια είναι η πιθανότητα να είναι όντως μολυσμένη η αγελάδα.

Λύση:

Έστω τα γεγονότα:

D=δεδομένα: το τεστ είναι θετικό

H_1=υπόθεση: είναι μολυσμένη

H_2=υπόθεση: δεν είναι μολυσμένη

Γνωρίζουμε την εκ των προτέρων (a-priori) πιθανότητα να έχει την αρρώστια $p(H_1) = 0.001$

Θέλουμε να υπολογίσουμε την a-priori πιθανότητα:

$$p(D) = p(D \mid H_1)p(H_1) + p(D \mid H_2)p(H_2) = (0.95)(0.001) + (0.05)(0.999) = 0.051$$

Χρησιμοποιώντας Bayes:

$$p(H_1 \mid D) = \frac{p(D \mid H_1)p(H_1)}{p(D)} = \frac{(0.95)(0.001)}{(0.051)} = 0.019 < 2\%$$

Η παραπάνω ποσότητα λέγεται εκ των υστέρων (posterior) πιθανότητα γιατί υπολογίζεται μετά την παρατήρηση των δεδομένων.

2.2 Μέτρο της Πληροφορίας

Κεντρικό ρόλο στη θεωρία της πληροφορίας παίζει η ίδια η έννοια της πληροφορίας. Σύμφωνα με τη θεωρία, η πληροφορία έχει ποσοτικό χαρακτήρα και συνεπώς διαφέρει σημαντικά απο το εννοιολογικό περιεχόμενο που της αποδίδουμε στην καθημερινή μας ζωή. Το πρόβλημα της

ποσοτικοποίησης της έννοιας της πληροφορίας και ο ορισμός ενός κατάλληλου μέτρου για τον υπολογισμό της απασχόλησε τον Hartley το 1928. Ο Hartley κατά τη μελέτη των τηλεγραφικών επικοινωνιών διαπίστωσε ότι όσο πιο μεγάλη είναι η πιθανότητα εμφάνισης ενός γεγονότος, τόσο πιο μικρή είναι η αβεβαιότητα για το αν θα συμβεί το γεγονός. Στην περίπτωση που το γεγονός συμβεί, η πληροφορία που θα λάβουμε θα είναι μικρή. Από τα παραπάνω είναι φανερό ότι συνηθισμένα γεγονότα, όπως για παράδειγμα «Σήμερα ο ήλιος ανέτειλε» συνοδεύονται από μικρή ποσότητα πληροφορίας, ενώ σπάνια γεγονότα, όπως παραδείγματος χάρη «Σήμερα έγινε ολική έκλειψη ηλίου» συνοδεύονται από μεγάλη ποσότητα πληροφορίας. Αυτό συμβαίνει επειδή το δεύτερο γεγονός έχει μικρή πιθανότητα να συμβεί σε σχέση με το πρώτο, που είναι βέβαιο.

Επομένως αν A είναι ένα τυχαίο γεγονός με πιθανότητα $p(A)$ και $I(A)$ είναι η συνάρτηση του μέτρου της πληροφορίας του A, τότε η $I(A)$ θα πρέπει να ικανοποιεί τις παρακάτω ιδιότητες:

1. Οταν η πιθανότητα να συμβεί ένα γεγονός είναι μονάδα, τότε η ποσότητα της μεταφερόμενης πληροφορίας είναι μηδενική. Αυτό σημαίνει ότι δεν χρειάζεται η διαβίβαση του μηνύματος, αφού το γεγονός είναι σίγουρο ότι θα συμβεί, δηλαδή:

$$\mathrm{I_A} = 0 \quad \text{όταν} \quad \mathrm{P_A} = 1 \qquad (2.1)$$

2. Είναι γεγονός οτι η πληροφορία ενος γεγονότος είναι ένα μη αρνητικό μέγεθος, αφού ισχύει $0 \le \mathrm{P_A} \le 1$, δηλαδή:

$$\mathrm{I_A} \ge 0 \quad \text{όταν} \quad 0 \le \mathrm{P_A} \le 1 \qquad (2.2)$$

3. Όσο πιο απίθανο είναι να συμβεί ένα γεγονός, τόσο περισσότερη πληροφορία λαμβάνουμε από την πραγματοποίηση του, δηλαδή:

$$\mathrm{I_A} \ge \mathrm{I}_B \quad \text{όταν} \quad \mathrm{P_A} \le \mathrm{P}_B \qquad (2.3)$$

4. Τέλος, αν τα γεγονότα Α και Β είναι ανεξάρτητα με αντίστοιχες πιθανότητες P_A, P_B , τότε το μέτρο της πληροφορίας του γεγονότος

εμφάνισης και των δύο επιμέρους γεγονότων είναι ίσο με το άθροισμα των δύο επιμέρους μέτρων πληροφορίας, δηλαδή:

$$I_{AB} = I_A + I_B \quad \text{, όταν } P_{AB} = P_A \cdot P_B \qquad (2.4)$$

Η παραπάνω σχέση αποδεικνύεται εύκολα παρακάτω:

$$I_{AB} = -\log_b \left(P_A\, P_B\right) \Rightarrow$$

$$I_{AB} = -\log_b \left(P_A\right) - \log_b \left(P_B\right) \Rightarrow$$

$$I_{AB} = I_A + I_B$$

Ετσι, υιοθετούμε το παρακάτω ορισμό

Ορισμός Πληροφορίας. Η πληροφορία I_A την οποία αποκτούμε από την πραγματοποίηση ενός γεγονότος A, το οποίο έχει πιθανότητα P_A , δίνεται από τον τύπο

$$I_A = -\log_b P_A \equiv \log_b \left(\frac{1}{P_A}\right) \quad \text{, όπου b > 1} \qquad (2.5)$$

Απόδειξη:

Εστω, η συνεχής συνάρτηση

$$f(x):[0,1] \to R_+ \qquad (2.6)$$

Η συνεχής συνάρτηση (2.6) έχει εξ' ορισμού τς τρείς πρώτες ιδιότητες (2.1), (2.2) και (2.3) . Θεωρούμε οτι η $I(x)$ είναι παραγωγίσιμη, οπότε για κάθε $x \in (0,1)$ έχουμε:

$$f'(x) = \lim_{\delta \to 0} \frac{f(x+\delta) - f(x)}{\delta} = \lim_{\delta \to 0} \frac{f\left[\frac{x}{m} \cdot \left(m + \frac{m\delta}{x}\right)\right] - f\left(\frac{x}{m} \cdot m\right)}{\delta} =$$

$$= \lim_{\delta \to 0} \frac{f\left(\frac{x}{m}\right) + f\left(m + \frac{m\delta}{x}\right) - f\left(\frac{x}{m}\right) - f(m)}{\delta} = \frac{m}{x} \lim_{m\delta/x \to 0} \frac{f\left(m + \frac{m\delta}{x}\right) - f(m)}{\frac{m\delta}{x}} =$$

$$= \frac{m}{x} f'(m) = \frac{c}{x} \quad (2.7)$$

Όπου m είναι ένα αυθαίρετα επιλεγμένο σημείο στο διάστημα $(0,1)$ και c σταθερά. Στην παραπάνω ανάλυση έγινε χρήση της ιδιότητας $f(\alpha b) = f(\alpha) + f(b)$. Για να είναι η $f(x)$ γνησίως φθίνουσα θα πρέπει σύμφωνα με το αποτέλεσμα της σχέσης (2.7) να ισχύει $c < 0$. Επίσης από την σχέση (2.7) προκύπτει οτι

$$f(x) = c\ln(x),\ c < 0 \quad (2.8)$$

Αν ορίσουμε τη σταθερά $b = e^{-1/c}$, τότε η σχέση (2.8) μπορεί να γραφεί με τη μορφή

$$f(x) = -\frac{\ln(x)}{\ln(b)} = -\log_b(x) \quad (2.9)$$

Επειδή $c < 0$, θα έχουμε $b > 1$. Ετσι καταλήξαμε στον προσδιορισμό της συνάρτησης του μέτρου πληροφορίας

$$I(A) = f(x) = -\log_b(p(A)),\ \text{όπου}\ b > 1$$

Οπως φαίνεται από την σχέση (2.5), η πληροφορία είναι ένα αδιάστατο μέγεθος, ενώ η βάση b του λογαρίθμου μπορεί να επιλεγεί ελεύθερα, αρκεί b>1.

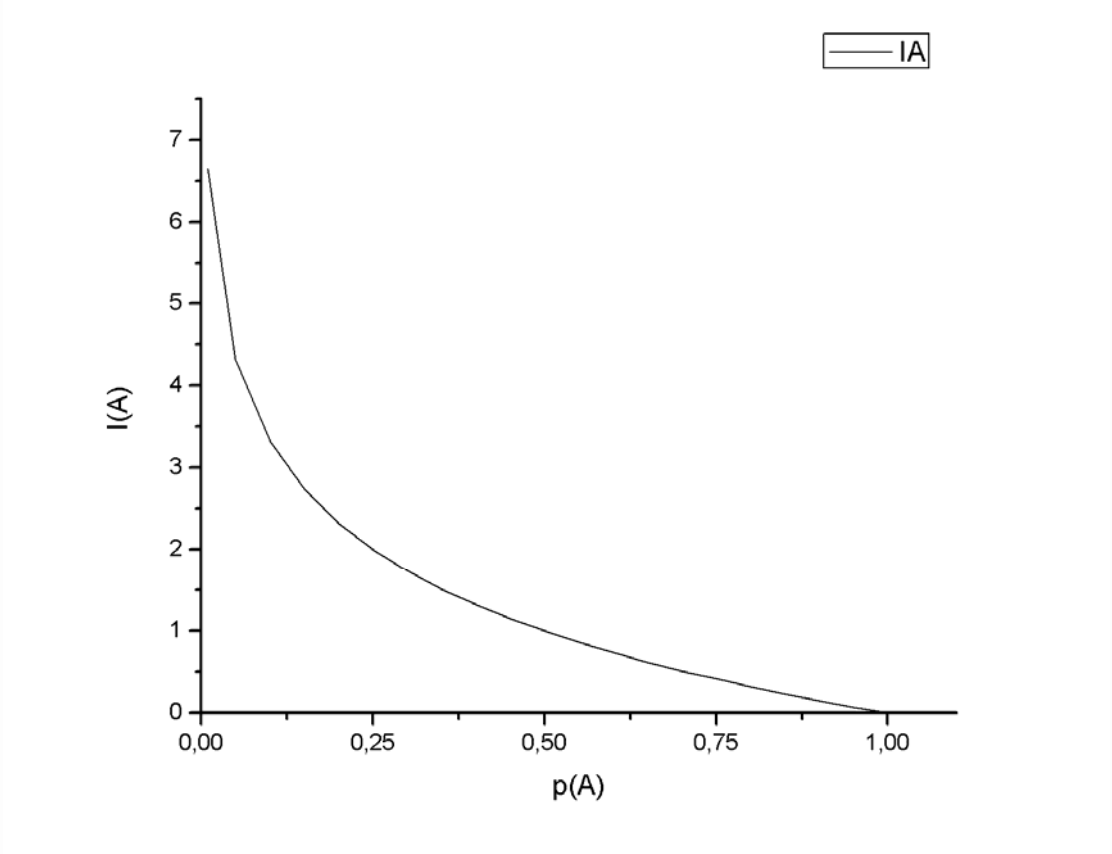
Η μονάδα μέτρησης της πληροφορίας καθορίζεται ανάλογα με τη βάση υπολογισμού του λογαρίθμου. Έτσι, όταν χρησιμοποιείται ο φυσικός λογάριθμος (natural), τότε η μονάδα είναι το **nat**, ενώ οταν χρησιμοποιείται ο δεκαδικός λογάριθμος, τότε η μονάδα είναι το **Hartley** ή **decit**. Η επικρατέστερη μονάδα μέτρησης της πληροφορίας είναι το **bit**. Ο λόγος που επικράτησε έναντι των έταιρων μονάδων είναι η χρησιμοποίηση του δυαδικού συστήματος αρίθμησης στους υπολογιστές.

Είναι εύκολο να μετασχηματίσουμε από τη μία λογαριθμική βάση στην άλλη μέσω της σχέσης

$$\log_b x = \log_a x \ / \ \log_a b \quad (2.10)$$

Για την περίπτωση του λογαρίθμου με βάση το 2 μπορεί να χρησιμοποιηθεί επίσης και η σχέση $\log_2 X = \ln X / \ln 2$, όπου ln ο λογάριθμος με βάση e. Εφόσον το $\ln 2 = 0.693$, μπορούμε να γράψουμε $\log_2 x = \ln x / 0.693$

Στο παρακάτω σχήμα (Εικόνα 3) παρουσιάζεται η γραφική παράσταση του μέτρου πληροφορίας, για b = 2, συναρτήσει της πιθανότητας.



Εικόνα 3. Γραφική παράσταση της συνάρτησης του μέτρου της πληροφορίας για b=2

Παράδειγμα 2.5:

Θεωρούμε οτι 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.

Λύση:

Με τη βοήθεια του παρακάτω τύπου γνωρίζουμε οτι:

$$I = \log_{10}\left(N^k\right) = k\log_{10}N$$

όπου:

k: το μήκος μηνύματος συμβόλων από ένα αλφάβητο

N: τα σύμβολα

Εφαρμόζουμε τον τύπο, αρχικά για τον υπολογισμό της ποσότητας πληροφορίας σε decit

$$I = k\log_{10}N = 2\log_{10}2 = 2\cdot 0.301 = 0,602 \text{ decit}$$

Στη συνέχεια, εφαρμόζουμε τον τύπο για τον υπολογισμό της ποσότητας πληροφορίας σε bit

$$I = k\log_2 N = 2\log_2 2 = 2\frac{\ln 2}{\ln 2} = 2bit$$

2.3 Η μονάδα ποσότητας πληροφορίας: το bit

Το Bit είναι η συντομογραφία των λέξεων binary digit και είναι η μικρότερη μονάδα αποθήκευσης πληροφορίας στα υπολογιστικά συστήματα. Ένα bit είναι ένα και μόνο ψηφίο σε έναν δυαδικό αριθμό, και είναι είτε 1 είτε 0, αποκαλούμενο συχνά και ως "on" ή "off". Η αντιστοιχία μεταξύ των μονάδων αναφορικά με το ευρύτατα διαδεδομένο σύστημα μέτρησης που χρησιμοποιείται και που θα χρησιμοποιήσουμε και εδώ είναι το bit εκτός και αν αναφερθούμε κάπου πιο ειδικευμένα, σε κάποια άλλη μονάδα:

$$1 \text{ hartley} = 3.32 \text{ bits} \ , \ 1 \text{ nat} = 1.44 \text{ bits}$$

Σε πολλές περιπτώσεις το **byte** λαμβάνεται ως αναφορά, όπου ένα byte ισούται με οκτώ bits.

Στο σημείο αυτό θα πρέπει να τονίσουμε οτι πρώτα από όλα μας ενδιαφέρουν οι πληροφορίες που παράγονται απο τον άνθρωπο. Αυτές οι πληροφορίες είναι αποθηκευμένες, παραποιημένες, μεταφερόμενες και αφομοιωμένες απο το ανθρώπινο μυαλό. Η Θεωρία της Πληροφορίας μας βοηθά να το κάνουμε αυτό αποτελεσματικά.

2.4 Μέση Πληροφορία ή Εντροπία

Στην προηγούμενη ενότητα αναφερθήκαμε σε τυχαία γεγονότα για τα οποία ορίσαμε το μέτρο πληροφορίας. Δεδομένου οτι η εμφάνιση ενός συμβόλου της πηγής αποτελεί ένα τυχαίο γεγονός, ορίζουμε την πληροφορία συμβόλου και κατ' επέκταση την πληροφορία λέξεων ή μηνυμάτων.

Θεωρούμε μια πηγή πληροφορίας με αλφάβητο $\mathrm{A} = (\alpha_1, \alpha_2, ..., \alpha_\mathrm{N})$. Κάθε ένα σύμβολο α_n, όπου $\mathrm{n} = 1, 2, ..., \mathrm{N}$, έχει πιθανότητα εμφάνισης $\mathrm{p_n}$. Επομένως από τον ορισμό της πληροφορίας προκύπτει: $\mathrm{I}(\alpha_\mathrm{n}) = -\log(\mathrm{p_n})$. Ως γνωστόν από τη θεωρία των πιθανοτήτων ισχύει:

$$p_n \in [0,1] \text{ και } \sum_{n=1}^{N} p_n = 1 \qquad (2.11)$$

Η κατανομή των πιθανοτήτων των συμβόλων του αλφαβήτου Α περιγράφεται απο το σύνολο $P_A = \{p_1, p_2, ...p_N\}$. Ετσι, η πηγή πληροφορίας περιγράφεται και αναπαρίσταται από το ζεύγος *(A, P_A)*.

Θα ήταν ενδιαφέρον να γνωρίζουμε, εκτός απο την πληροφορία του κάθε συμβόλου χωριστά, τη μέση πληροφορία ανά σύμβολο που μας παρέχει η

έξοδος της πηγής. Με άλλα λόγια, ζητάμε ένα μέγεθος πληροφορίας που να σχετίζεται με την πηγή συνολικά, συνεπώς και με το αλφάβητο της. Για το λόγο αυτό εισάγεται η έννοια της **εντροπίας πηγής**. Η εντροπία είναι θεμελιώδης έννοια για τη θεωρία της πληροφορίας που προτάθηκε από τον Shannon το 1948.

Ορισμός Εντροπίας ή μέσης πληροφορίας ανά σύμβολο πληροφορίας. Για μια πηγή πληροφορίας με αλφάβητο $\mathrm{A}=\{\alpha_1,\ \alpha_2,....,\ \alpha_\mathrm{N}\}$ η εντροπία ή μέση πληροφορία του Α, όπως αλλιώς ονομάζεται, είναι ο μέσος όρος της αυτοπληροφορίας των συμβόλων στην έξοδο και ορίζεται ως:

$$\mathrm{H(A)}\ =\ \mathrm{H}(\alpha_1,\ \alpha_2,....,\ \alpha_\mathrm{N})\ =\ -\ \sum_{n=1}^{N} p(a_n)\log p(a_n) \quad (2.12)$$

Αν θέλουμε να χρησιμοποιήσουμε την ορολογία των πιθανοτήτων, για μια τυχαία μεταβλητή x με δειγματοχώρο $\mathrm{X}=\{\ \mathrm{x}_1,\ \mathrm{x}_2,\ ....,\ \mathrm{x}_\mathrm{N}\ \}$ και με συνάρτηση μάζας πιθανότητας $p(x_n)$, η μέση πληροφορία που κερδίζουμε ανά σύμβολο ή η συνάρτηση αβεβαιότητας ή η εντροπία του Χ, όπως αλλιώς ονομάζεται, είναι

$$\mathrm{H(x)}\ =\ -\ \sum_{n=1}^{N} p(x_n)\log p(x_n) \quad (2.13)$$

Οι μονάδες μέτρησης της εντροπίας εξαρτώνται από τη βάση του λογαρίθμου που χρησιμοποιείται στον ορισμό. Αν η βάση του λογαρίθμου είναι το 2, τότε οι μονάδες λέγονται bits. Αν η βάση του λογαρίθμου είναι το 10, τότε λέγονται digits. Αν η βάση του λογαρίθμου είναι το e, τότε λέγονται nats και συνήθως τις χρησιμοποιούμε για συνεχείς τυχαίες μεταβλητές. Συνήθως προτιμάται το 2 για βάση του λογαρίθμου.

Η συνάρτηση που περιγράφει την εντροπία έχει τις παρακάτω βασικές ιδιότητες:

1. Η εντροπία είναι το μέτρο της μέσης αβεβαιότητας μιας τυχαίας μεταβλητής.
2. Ορίζει τον μέσο αριθμό bits που απαιτούνται για να περιγράψουν την τυχαία μεταβλητή.

3. Η εντροπία μιας τυχαίας μεταβλητής εξαρτάται μόνο απο τις πιθανότητες που χαρακτηρίζουν την τυχαία μεταβλητή και όχι απο τις πιθανές τιμές της τυχαίας μεταβλητής.
4. Θεωρούμε ότι $0\log(0) = 0$, αφού $\lim_{x\to 0}(x\log x) \to 0$. Επομένως, δεν αλλάζουν την εντροπία οι όροι με μηδενική πιθανότητα.
5. Η εντροπία σύμφωνα με τον παραπάνω ορισμό μπορεί να θεωρηθεί συνάρτηση της τυχαίας μεταβλητής. Αυτή η διαπίστωση μας οδηγεί σε έναν δεύτερο ορισμό της εντροπίας, ο οποίος είναι ο παρακάτω:

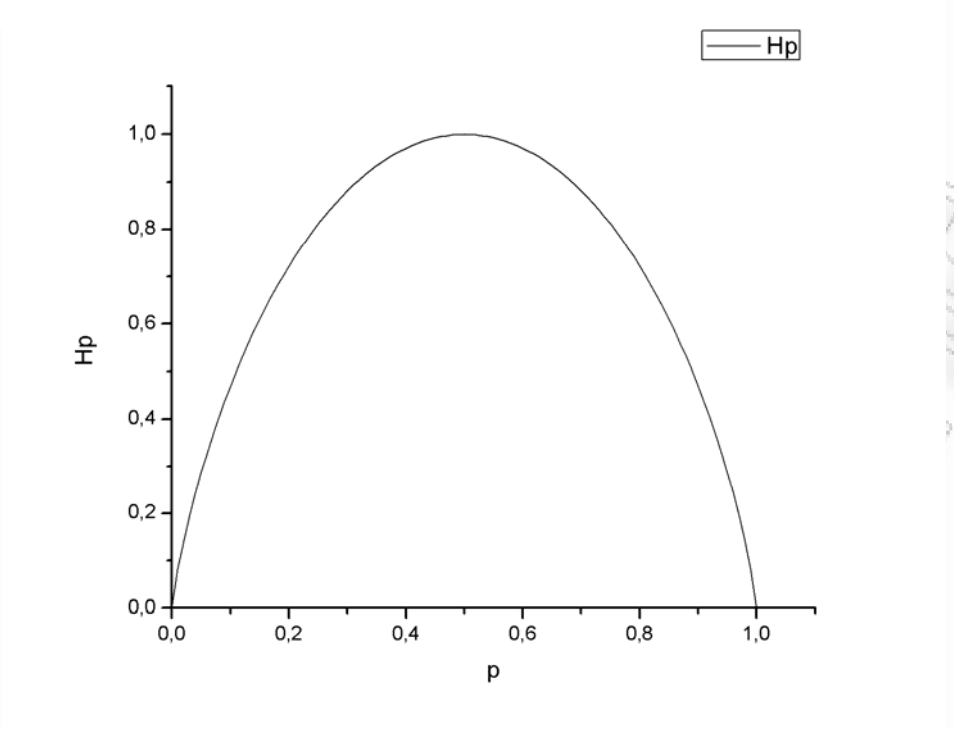
   Ο ορισμός της αναμενόμενης τιμής της συνάρτησης τυχαίας μεταβλητής $F(x) = \log\frac{1}{p(x)}$ είναι $E[F(x)] = \sum_i F(a_i)\,p(x = a_i)$. Επομένως ο δεύτερος ορισμός της εντροπίας που προκύπτει δίνεται απο τον παρακάτω τύπο:

$$H(x) = E\{\log\frac{1}{p(x)}\}$$

Συχνά, στη θεωρία της πληροφορίας εμφανίζεται η εντροπία δυαδικής πηγής. Η δυαδική πηγή πληροφορίας έχει αλφάβητο που αποτελείται από δύο μόνο σύμβολα π.χ. το 0 και το 1. Προφανώς, αν p είναι η πιθανότητα εμφάνισης του συμβόλου 0, τότε η πιθανότητα εμφάνισης του συμβόλου 1 θα είναι ίση με (1 – p). Συνεπώς η εντροπία της δυαδικής πηγής, η οποία συμβολίζεται με $H_b(p)$, θα είναι ίση με:

$$H_b(p) = -p\log(p) - (1-p)\log(1-p) \qquad (2.14)$$

Η **εντροπία δυαδικής πηγής** $H_b(p)$ είναι συνάρτηση μόνο της πιθανότητας p του ενός συμβόλου και λέγεται **συνάρτηση Shannon**. Όπως φαίνεται και από το παρακάτω σχήμα (Εικόνα 4), η συνάρτηση Shannon είναι συμμετρική και παίρνει τη μέγιστη τιμή της (1 bit / symbol) όταν τα δύο σύμβολα είναι ισοπίθανα (p = 0.5).



Εικόνα 4. Γραφική παράσταση της συνάρτησης Shannon.

Από την παραπάνω σχέση και με τη βοήθεια της γραφικής παράστασης παρατηρούμε τα εξής:

1. Όταν $p = 0$, είναι $H(X) = 0$. Αυτό προκύπτει από τη σχέση

   $$\lim_{x \to 0} x \log_2 x = 0$$

   Για την τιμή αυτή της πιθανότητας, η μεταβλητή παύει να είναι τυχαία και η αβεβαιότητα μηδενίζεται.
2. Οταν $p = 1$, είναι $H(X) = 0$.

   Για την τιμή αυτή της πιθανότητας, η μεταβλητή παύει να είναι τυχαία και η αβεβαιότητα μηδενίζεται.
3. Η εντροπία $H(X)$ λαμβάνει τη μέγιστη τιμή της $H_{max} = 1\text{bit}$, όταν $p_o = p_1 = \frac{1}{2}$, δηλαδή όταν τα σύμβολα 1 και 0 είναι ισοπίθανα.
4. Υπάρχει συμμετρία γύρω από το $p = 0.5$
5. Είναι μία κοίλη συνάρτηση της πιθανότητας

Παράδειγμα 2.6:

Έστω μία πηγή X με τέσσερα σύμβολα $X = \{ A, B, \Gamma, \Delta \}$ και κατανομή πιθανοτήτων P(X) = { $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{8}$}. Να βρεθεί η μέση πληροφορία ή εντροπία της πηγής αυτής.

Λύση:

Η εντροπία της πηγής δίνεται απο τον τύπο

$$H(x) = -\sum_{n=1}^{N} p(x_n) \log p(x_n)$$

Αντικαθιστώντας στον παραπάνω τύπο η εντροπία της πηγής ισούται με

$$H(X) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = \frac{7}{4}\text{ bits}$$

2.4.1 Ιδιότητες της μέσης ποσότητας πληροφορίας ή εντροπίας

Οι ιδιότητες της μέσης πληροφορίας ή εντροπίας, που έχουν τεθεί και σαν απαιτήσεις κατά τον ορισμό της, είναι οι παρακάτω:

1. Η μέση πληροφορία H(x) είναι συνεχής συνάρτηση των πιθανοτήτων $p(x_n)$, όπου $n = 1, 2, \ldots, N$, όπως φαίνεται στη γραφική παράσταση της προηγούμενης ενότητας (Εικόνα 4).

2. Η μέση πληροφορία H(x) είναι συμμετρική συνάρτηση των πιθανοτήτων $p(x_n)$, όπου $n = 1, 2, \ldots,$. 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 Η(x) παίρνει τη μέγιστη τιμή, η οποία είναι $\mathrm{H(x)} = \mathrm{logn}$, όταν όλα τα ενδεχόμενα είναι ισοπίθανα, δηλαδή όταν $\mathrm{p(x_1)} = \mathrm{p(x_2)} = \ldots\ldots = \mathrm{p(x_N)} = \frac{1}{N}$. Τότε, η αβεβαιότητα είναι η μέγιστη δυνατή και κατά συνέπεια, η επιλογή ενός μηνύματος προσφέρει τη μέγιστη δυνατή μέση πληροφορία.

4. Αν θεωρήσουμε ότι b και α είναι δύο διαφορετικές βάσεις στο λογάριθμο του ορισμού της εντροπίας, τότε θα ισχύει $H_b(x) = (\log_b a)H_a(x)$. Δηλαδή πολλαπλασιάζοντας με τον κατάλληλο παράγοντα, μπορεί να αλλάξει η βάση της εντροπίας.

5. Η εντροπία $H(x)$ είναι μια μη αρνητική ποσότητα, δηλαδή $H(x) \geq 0$. Αυτό μπορούμε να το αποδείξουμε αν λάβουμε υπόψιν ότι η πιθανότητα $p(x_n)$ παίρνει τιμές στο διάστημα [0,1]. Επομένως, δεν μπορεί να είναι αρνητική. Επίσης ο λογάριθμος της είναι μικρότερος ή ίσος του μηδενός. Άρα, το γινόμενο $p(x_n)\log_e p(x_n)$ είναι μικρότερο ή ίσο του μηδενός. Επομένως η εντροπία είναι μεγαλύτερη ή ίση του μηδενός.

6. Για μια τυχαία μεταβλητή x, ισχύει $H(x) \leq \log N$. Η ισότητα ισχύει όπως είδαμε στην ιδιότητα 3, αν και μόνο αν $p(x_i) = \frac{1}{N}$ για όλα τα $i \neq 1$. Ας αποδείξουμε αυτή την ιδιότητα.

   Απόδειξη:

   Για κάθε θετικό αριθμό γνωρίζουμε οτι ισχύει $\ln x \leq x - 1$. Χρησιμοποιώντας την παραπάνω ανισότητα έχουμε:

$$H(x) - \ln N = -\sum_{n=1}^{N} p(x_n)(\ln p(x_n)) - \sum_{n=1}^{N} p(x_n)(\ln N) \Rightarrow$$

$$= -\sum_{n=1}^{N} p(x_n) \ln \frac{1}{Np(x_n)} \Rightarrow$$

$$\leq -\sum_{n=1}^{N} p(x_n)(\ln \frac{1}{Np(x_n)} - 1) \Rightarrow$$

$$= \sum_{n=1}^{N}\left(\frac{1}{N}\right) - \sum_{n=1}^{N} p(x_n) = 0$$

Η ισότητα ισχύει όταν $Np(x_n) = 1$, για όλα τα n

7. Ισχύει η αρχή της προσθετικότητας

$$\mathrm{H}\left(\mathrm{X},\ \mathrm{Y}\right) = \mathrm{H}\left(\mathrm{X}\right) + \mathrm{H}\left(\mathrm{Y}\right) \quad (2.15)$$

Με τον όρο προσθετικότητα εννοούμε οτι αν έχουμε δύο αναξάρτητα γεγονότα που το πρώτο συμβαίνει με πιθανότητα p_x και το δεύτερο με πιθανότητα p_y, τότε η συνολική πληροφορία που μας δίνουν τα δύο γεγονότα είναι το άθροισμα των επιμέρους πληροφοριών.

Η σχέση $\mathrm{H}\left(\mathrm{X},\ \mathrm{Y}\right) = \mathrm{H}(\mathrm{X}) + \mathrm{H}(\mathrm{Y})$ αποδεικνύεται με τη βοήθεια του ορισμού της μέσης πληροφορίας.

Απόδειξη:

Απο τον ορισμό της εντροπίας έχουμε:

$$\mathrm{H}\left(\mathrm{X},\mathrm{Y}\right) = -\sum_{x\in X, y\in Y} p_x p_y \log p_x p_y$$

$$= -\sum_{x\in X, y\in Y} p_x p_y [\log p_x + \log p_y]$$

$$= -\sum_{y\in Y} p_y [\sum_{x\in X} p_x \log p_x] - \sum_{x\in X} p_x [\sum_{y\in Y} p_y \log p_y]$$

$$= \mathrm{H}\left(\mathrm{X}\right) + \mathrm{H}\left(\mathrm{Y}\right)$$

2.5 Από Κοινού Εντροπία, Υπο Συνθήκη Εντροπία και Αμοιβαία Πληροφορία

Η εντροπία μπορεί να χρησιμοποιηθεί και για τον ορισμό άλλων μετρήσεων πληροφορίας, οι οποίες αναδεικνύουν τις σχέσεις μεταξύ δύο τυχαίων μεταβλητών Χ και Υ. Έχουμε λοιπόν:

1. Την από κοινού ή συνδετική εντροπία (joint entropy), η οποία μετράει τη συνολική πληροφορία των Χ και Υ.
2. Την υπό συνθήκη εντροπία (conditional entropy), η οποία μετράει την πληροφορία του Χ, όταν η Υ είναι γνωστή και αντίστροφα.
3. Την αμοιβαία εντροπία (mutual entropy), η οποία μετράει τη σχέση των Χ και Υ, υπό την έννοια ότι μας δείχνει πόσο μειώνεται η πληροφορία του Χ όταν μαθαίνουμε το Υ και αντιστρόφως.

2.5.1 Απο Κοινού Εντροπία

Θεωρούμε δύο πηγές πληροφορίας, την $(\mathrm{X},\ \mathrm{P_X})$ με αλφάβητο $\mathrm{X} = \{\mathrm{x}_1,\ \mathrm{x}_2,\ \ldots,\ \mathrm{x}_\mathrm{N}\}$ και κατανομή πιθανοτήτων $P_X = \{p_{x1}, p_{x2}, ..., p_{xN}\}$ και την (Y, P_Y) με αλφάβητο $Y = \{\mathrm{y}_1,\ \mathrm{y}_2,\ \ldots,\ \mathrm{y}_\mathrm{M}\}$ και κατανομή πιθανοτήτων $P_Y = \{p_{y1}, p_{y2}, ..., p_{yM}\}$, αντίστοιχα. Οι δύο πηγές συνθέτουν μια σύνθετη πηγή (XY, P_{XY}), της οποίας το αλφάβητο προκύπτει από το καρτεσιανό γινόμενο $XY = X \times Y = \{(x_i, y_i) : x_i \in X, y_i \in Y\}$. Επομένως, η **συνδετική εντροπία ή από κοινού εντροπία** των δύο πηγών είναι η εντροπία της σύνθετης πηγής (XY, P_{XY}). Ετσι, η συνδετική εντροπία ή από κοινού εντροπία της σύνθετης πηγής (XY, P_{XY}) δίνεται από τη σχέση:

$$\mathrm{H(X, Y)} = -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j)\log(p(x_i, y_j)) \qquad (2.16)$$

Η σχέση (2.16) επεξηγείται ως εξής: η αβεβαιότητα που έχουμε για την τιμή των μεταβλητών x και y είναι ίση με το άθροισμα της αβεβαιότητας για το x συν την αβεβαιότητα για το y, αν και μόνο αν οι μεταβλητές x και y είναι στατιστικά ανεξάρτητες. Αν οι μεταβλητές x και y είναι ανεξάρτητες, τότε από την από κοινού πιθανότητα έχουμε $p(x_i, y_j) = p(x_i) \cdot p(y_j)$

Επομένως χρησιμοποιώντας τη σχέση (2.12), έχουμε

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

$$= -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i) p(y_j)[\log p(x_i) + \log p(y_j)]$$

$$= -\sum_{i=1}^{N} p(x_i) \log p(x_i) \sum_{j=1}^{M} p(y_j) - \sum_{j=1}^{M} p(y_j) \log p(y_j) \sum_{i=1}^{N} p(x_i)$$

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

Μια βασική ιδιότητα της συνδετικής εντροπίας δύο πηγών είναι οτι δεν μπορεί να υπερβεί το άθροισμα των εντροπιών των δύο επιμέρους πηγών. Επομένως, η μέση πληροφορία της σύνθετης πηγής είναι μικρότερη ή το πολύ ίση με το άθροισμα των μέσων πληροφοριών των απλών πηγών πληροφορίας, δηλαδή :

$$H(X,Y) \le H(X) + H(Y) \quad (2.17)$$

Οι έννοιες της σύνθετης πηγής και συνδετικής εντροπίας μπορούν να επεκταθούν και για περισσότερες απο δύο πηγές. Έτσι, αν έχουμε K απλές πηγές πληροφορίας $(\mathrm{X}_1, \mathrm{P}_{\mathrm{X1}}), (\mathrm{X}_2, \mathrm{P}_{\mathrm{X2}}), ..., (\mathrm{X}_K, \mathrm{P}_{\mathrm{XK}})$, τότε η συνδετική εντροπία δίνεται από τη σχέση:

$$H(X_1 X_2 .... X_K) = -\sum_{i_1=1}^{N_1}\sum_{i_2=2}^{N_2} ..... \sum_{i_K=1}^{N_1} p(x_{i1}, x_{i2}, ... x_{iK}) \log(p(x_{i1}, x_{i2}, ..., x_{iK})) \quad (2.18)$$

Στην παραπάνω σχέση (2.18) με $N_k \ \ (k = 1,2,...K)$ δηλώνεται το πλήθος των συμβόλων του αλφάβητου X_k

$$H(X,Y) = -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j)\log p(x_i, y_j)$$
$$= -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i)p(y_j)[\log p(x_i) + \log p(y_j)]$$

Η σχέση (2.17) μπορεί να γενικευθεί για την περίπτωση K απλών πηγών, δηλαδή:

$$H(X_1X_2....X_K) < H(\mathrm{X}_1) + H(\mathrm{X}_2) + ... + H(\mathrm{X}_K) \quad (2.19)$$

2.5.2 Υπό Συνθήκη Εντροπία

Θεωρούμε δύο πηγές πληροφορίας, την $(\mathrm{X},\ \mathrm{P_X})$ με αλφάβητο $\mathrm{X} = \{\mathrm{x}_1,\ \mathrm{x}_2,\ \ldots,\ \mathrm{x}_N\}$ και κατανομή πιθανοτήτων $P_X = \{p_{x1}, p_{x2}, ..., p_{xN}\}$ και την (Y, P_Y) με αλφάβητο $Y = \{\mathrm{y}_1,\ \mathrm{y}_2,\ \ldots,\ \mathrm{y}_M\}$ και κατανομή πιθανοτήτων $P_Y = \{p_{y1}, p_{y2}, ..., p_{yM}\}$, αντίστοιχα. Υποθέτουμε ότι γνωρίζουμε εκ των προτέρων πως η πηγή (Y, P_Y) παράγει το σύμβολο y_j. Με αυτή την προϋπόθεση η πιθανότητα εμφάνισης του συμβόλου x_i στην έξοδο της πηγής $(\mathrm{X},\ \mathrm{P_X})$ δίνεται από τη παρακάτω σχέση :

$$p(x_i / y_j) = \frac{p(x_i, y_j)}{p(y_j)} \quad (2.20)$$

Η $p(x_i / y_j)$ εκφράζει την πιθανότητα εμφάνισης του ζεύγους (x_i, y_j) στην έξοδο της σύνθετης πηγής (XY, P_{XY}) δεδομένου ότι η απλή πηγή (Y, P_Y) παράγει το σύμβολο y_j.

Η μέση τιμή της υπο συνθήκη ποσότητας πληροφορίας της τυχαίας μεταβλητής X, δεδομένου του αποτελέσματος y_j δίνεται από τη παρακάτω σχέση:

$$H(X \mid y_j) = -\sum_{i=1}^{N} p(x_i / y_j) \log(p(x_i / y_j)) \quad (2.21)$$

Η μέση τιμή του $H(X \mid y_j)$ ως προς όλα τα σύμβολα y_j λέγεται υπό συνθήκη εντροπία της σύνθετης πηγής (XY, P_{XY}), όταν είναι γνωστή η έξοδος της απλής πηγής (Y, P_Y) και δίνεται από τη παρακάτω σχέση

$$H(X \mid y_j) = -\sum_{j=1}^{M} H(X \mid y_j) p(y_j) = -\sum_{i=1}^{N} \sum_{j=1}^{M} p(x_i, y_j) \log(p(x_i / y_j)) \quad (2.22)$$

Η υπό συνθήκη εντροπία της σύνθετης πηγής όταν είναι γνωστή η έξοδος της απλής πηγής $(\mathrm{X},\ \mathrm{P_X})$ δίνεται από την παρακάτω σχέση:

$$H(Y \mid X) = -\sum_{i=1}^{N} H(Y \mid x_i) p(x_i) = -\sum_{i=1}^{N} \sum_{j=1}^{M} p(x_i, y_j) \log(p(y_j / x_i)) \quad (2.23)$$

Παρακάτω θα δούμε οτι η από κοινού και η υπό συνθήκη εντροπία συνδέονται μεταξύ τους. Το θεώρημα που μας δίνει αυτή τη σύνδεση λέγεται **κανόνας της αλυσίδας** και δίνεται από τη σχέση:

$$H(X,Y) = H(XY) - H(Y) \quad (2.24)$$

Η σχέση (2.24) αποδεικνύεται παρακάτω

Απόδειξη:

Σύμφωνα με τον ορισμό της $\mathrm{H}(\mathrm{X},\mathrm{Y})$, ισχύει:

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

$$= -\sum_{i=1}^{N} \sum_{j=1}^{M} p(x_i, y_j) \log\left[\frac{p(x_i, y_j)}{p(y_j)}\right]$$

$$= -\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j)\log(p(x_i, y_j)) + \sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j)\log(p(y_j))$$

$$= H(XY) + \sum_{j=1}^{M} p(y_j)\log(p(y_j))$$

$$= H(XY) - H(Y)$$

Επίσης, ισχύει η σχέση:

$$H(Y \mid X) = H(XY) - H(X) \quad (2.25)$$

Παράδειγμα 2.7:

Θεωρούμε δύο δυαδικές πηγές πληροφορίας $\mathrm{X} = \{\mathrm{A}, \mathrm{B}\}$ και $\mathrm{y} = \{\Gamma, \Delta\}$ αντίστοιχα. Δίνονται οι τιμές των πιθανοτήτων $\mathrm{p(A)} = 0.2, \mathrm{p}(\mathrm{A}, \Delta) = 0.15$ *και* $\mathrm{p}(\Gamma) = 0.3$. Να βρεθούν οι τιμές:

1. της εντροπίας της κάθε πηγής χωριστά.
2. της σύνθετης πηγής XY .
3. των υπό συνθήκη εντροπιών $\mathrm{H(X/Y)}$ και $\mathrm{H(Y/X)}$.

Λύση:

1. Αρχικά υπολογίζουμε τις τιμές όλων των περιθωριακών πιθανοτήτων των συμβόλων των δύο πηγών. Αυτές προκύπτουν βάσει της ιδιότητας ότι το άθροισμα των πιθανοτήτων όλων των συμβόλων μιας πηγής είναι ίσο με τη μονάδα. Άρα, έχουμε:

p(A) + p(B) = 1 $\Rightarrow$ p(B) = 1 - 0.2 $\Rightarrow$ p(B) = 0.8

p(Γ) + p(Δ) = 1 $\Rightarrow$ p(Δ) = 1 – 0.3 $\Rightarrow$ p(Δ) = 0.7

Στη συνέχεια, υπολογίζουμε τις από κοινού πιθανότητες χρησιμοποιώντας περιθωριακές. Έχουμε:

p(A,Δ) + p(A,Γ) = p(A) $\Rightarrow$ p(A,Γ) = 0.2 – 0.15 $\Rightarrow$ p(A,Γ) = 0.05

p(A,Γ) + p(B,Γ) = p(Γ) $\Rightarrow$ p(B,Γ) = 0.3 – 0.05 $\Rightarrow$ p(B,Γ) = 0.25

p(A,Δ) + p(B,Δ) = p(Δ) $\Rightarrow$ p(B,Δ) = 0.7 – 0.15 $\Rightarrow$ p(B,Δ) = 0.55

Οι παραπάνω τιμές των κοινών πιθανοτήτων συνθέτουν τον πίνακα

$$P_{XY} = \begin{bmatrix} p(\text{A},\Gamma) & \text{p(A},\Delta) \\ \text{p(B},\Gamma) & \text{p(B},\Delta) \end{bmatrix} = \begin{bmatrix} 0.05 & 0.15 \\ 0.25 & 0.55 \end{bmatrix}$$

Στον παραπάνω πίνακα παρατηρούμε οτι το άθροισμα ανά στήλη ή γραμμή δίνουν τις περιθωριακές πιθανότητες των συμβόλων. Στη συνέχεια, μπορούμε να υπολογίσουμε τις υπό συνθήκη πιθανότητες βάσει της γνωστής σχέσης p(a/b) = p(a,b) / p(b). Συνεπώς, οι υπό συνθήκη πιθανότητες είναι:

p(A,Γ) = p(A,Γ) / p(Γ) = 0.05 / 0.3 = 0.1667
p(A,Δ) = p(A,Δ) / p(Δ) = 0.15 / 0.7= 0.2143
p(B,Γ) = p(B,Γ) / p(Γ) = 0.25 / 0.3 = 0.8333
p(B,Δ) = p(B,Δ) / p(Δ) = 0.55 / 0.7= 0.7857
p(Γ,A) = p(A,Γ) / p(A) = 0.05 / 0.2 = 0.25
p(Γ,B) = p(B,Γ) / p(B) = 0.25 / 0.8 = 0.3125
p(Δ,A) = p(A,Δ) / p(A) = 0.15 / 0.2 = 0.75
p(Δ,B) = p(B,Δ) / p(B) = 0.55 / 0.8 = 0.6875

Οι υπό συνθήκη πιθανότητες συνθέτουν τους πίνακες:

$$P_{X/Y} = \begin{bmatrix} p(\text{A},\Gamma) & \text{p(B},\Gamma) \\ \text{p(A},\Delta) & \text{p(B},\Delta) \end{bmatrix} = \begin{bmatrix} 0.1667 & 0.8333 \\ 0.2143 & 0.7857 \end{bmatrix}$$

$$P_{\text{Y/X}} = \begin{bmatrix} p(\Gamma,\text{A}) & \text{p}(\Delta,\text{A}) \\ \text{p}(\Gamma,\text{B}) & \text{p}(\Delta,\text{B}) \end{bmatrix} = \begin{bmatrix} 0.25 & 0.75 \\ 0.3125 & 0.6875 \end{bmatrix}$$

Παρατηρούμε ότι στους δύο παραπάνω πίνακες τα αθροίσματα των στοιχείων τους ανά γραμμή είναι πάντα ίσα με τη μονάδα.

Η εντροπία καθεμιάς απλής πηγής υπολογίζεται σύμφωνα με τη παρακάτω σχέση ως εξής:

$$\mathrm{H(X)} = -\sum_{x\in\{A,B\}} p(x)\log(p(x)) = -0.2\log(0.2) - 0.8\log(0.8) = 0.722 bits/symbol$$

$$\mathrm{H}(Y) = -\sum_{y\in\{\Gamma,\Delta\}} p(y)\log(p(y)) = -0.3\log(0.3) - 0.7\log(0.7) = 0.881 bits/symbol$$

2. Η εντροπία της σύνθετης πηγής XY υπολογίζεται απο τη σχέση της συνδετικής εντροπίας, δηλαδή:

$$\mathrm{H(X}Y) = -\sum_{x\in\{A,B\}}\sum_{y\in\{\Gamma,\Delta\}} p(x,y)\log(p(x,y)) =$$

$$= -0.05\log(0.05) - 0.15\log(0.15) - 0.25\log(0.25) - 0.55\log(0.55) = 1.601 bits/symbol$$

Παρατηρούμε ότι πράγματι ισχύει η ταυτοανισότητα:

$$H(XY) \le H(X) + H(Y) \Rightarrow 1.601 \le 0.722 + 0.881$$

3. Τέλος υπολογίζουμε τις υπό συνθήκη εντροπίες:

$$\mathrm{H(X}/Y) = -\sum_{x\in\{A,B\}}\sum_{y\in\{\Gamma,\Delta\}} p(x,y)\log(p(x/y)) =$$

$$= -0.05\log(0.1667) - 0.15\log(0.2143) - 0.25\log(0.8333) -$$
$$-0.55\log(0.7857) = 0.720 bits/symbol$$

$$\mathrm{H(Y}/\mathrm{X}) = -\sum_{x\in\{A,B\}}\sum_{y\in\{\Gamma,\Delta\}} p(x,y)\log(p(y/x)) =$$

$$= -0.05\log(0.25) - 0.15\log(0.75) - 0.25\log(0.3125) -$$

$$-0.55\log(0.6875) = 0.879 bits / symbol$$

Φυσικά θα καταλήγαμε στο ίδιο αποτέλεσμα συντομότερα, χωρίς να απαιτηθεί ο υπολογισμός των υπό συνθήκη πιθανοτήτων, αν χρησιμοποιούσαμε απευθείας τις σχέσεις.

2.5.3 Αμοιβαία πληροφορία

Ένα σημαντικό μέγεθος που ορίζεται στα πλαίσια της θεωρίας της πληροφορίας είναι η **αμοιβαία πληροφορία**. Αν $X = \{x_1, x_2, ...x_N\}$ και $Y = \{y_1, y_2, ...y_M\}$ είναι δύο πηγές, με κατανομές πιθανοτήτων P_X και P_Y αντίστοιχα, τότε η αμοιβαία πληροφορία των δύο πηγών δίνεται από την παρακάτω σχέση:

$$I(X;Y) = H(X) - H(X|Y) \quad (2.26)$$

Απόδειξη:

Σύμφωνα με τον ορισμό της I (X;Y), ισχύει

$$\begin{aligned} I(X;Y) &= \sum_{i=1}^{N}\sum_{j=1}^{M} I(x_i, y_j) p(x_i, y_j) \\ &= \sum_{i=1}^{N}\sum_{j=1}^{M} [\log(p(x_i / y_j)) - \log p(x_i)] p(x_i, y_j) \\ &= \sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j) \log(p(x_i / y_j)) - \sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i, y_j) \log(p(x_i)) \\ &= -H(X|Y) + \sum_{i=1}^{N} p(x_i) \log(p(x_i)) \\ &= -H(X|Y) + H(X) \end{aligned}$$

Η συνάρτηση της αμοιβαίας πληροφορίας έχει τις παρακάτω ιδιότητες:

- Είναι συμμετρική ως προς Χ και Υ, δηλαδή

$$I(X;Y) = I(Y;X) \qquad (2.27)$$

Για να αποδείξουμε την παραπάνω ιδιότητα αρκεί να αντικαταστήσουμε στον ορισμό της αμοιβαίας πληροφορίας την υπό συνθήκη εντροπία.

Απόδειξη:

$$\begin{aligned} I(X;Y) &= H(X) - H(X \mid Y) \\ &= H(X) - H(XY) - H(Y)) \\ &= H(X) + H(Y) - H(XY) \end{aligned} \qquad (2.28)$$

Από την παραπάνω σχέση είναι φανερό οτι η αμοιβαία πληροφορία είναι συμμετρική $I(X;Y) = I(Y;X)$

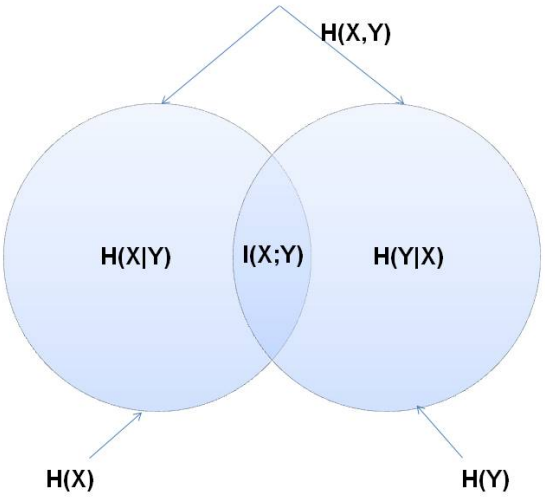
- Είναι μη αρνητική, δηλαδή:

$$I(X;Y) \geq 0 \qquad (2.29)$$

- Η αμοιβαία πληροφορία μιας τυχαίας μεταβλητής με τον εαυτό της είναι η εντροπία της τυχαίας μεταβλητής. Γι' αυτό το λόγο, η εντροπία μιας τυχαίας μεταβλητής συχνά λέγεται και ***αυτοπληροφορία***.

$$I(X;X) = H(X) - H(X \mid X) = H(X) \quad (2.30)$$

Εναλλακτικά, η σχέση της αμοιβαίας πληροφορίας με τις από κοινού και υπό συνθήκες εντροπίες θα μπορούσε να αναπαρασταθεί με το διάγραμμα Venn του σχήματος (Εικόνα 5):



Εικόνα 5. Διάγραμμα Venn για τη σχέση μεταξύ εντροπίας και αμοιβαίας πληροφορίας.

Παράδειγμα 2.8:

Να υπολογιστεί η αμοιβαία πληροφορία μεταξύ των πηγών X και Y του προηγούμενου παραδείγματος.

Λύση:

Από τον ορισμό της αμοιβαίας πληροφορίας γνωρίζουμε ότι:

$$I(X;Y) = H(X) - H(X|Y) = 0.722 - 0.720 = 0.002 \text{ bits/symbol}$$

ή ισοδύναμα:

$$I(X;Y) = H(Y) - H(Y|X) = 0.881 - 0.879 = 0.002 \text{ bits/symbol}$$

Ασκήσεις:

1. Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο $S = \{a, \beta, \gamma, \delta, \varepsilon, \zeta, \eta\}$. Οι πιθανότητες των συμβόλων αυτών είναι 1/32, 1/16, 1/8, 1/8, 1/8, 1/2 και 1/32 αντίστοιχα.

1.Να προσδιορίσετε το σύμβολο της πηγής με το πιο χαμηλό πληροφοριακό περιεχόμενο.

2.Τα σύμβολα της πηγής με το πιο υψηλό πληροφοριακό περιεχόμενο.

2. Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο $S = \{\tau, \upsilon, \varphi, \chi, \psi, \omega\}$. Οι πιθανότητες των συμβόλων αυτών είναι 1/4, 1/4, 1/8, 1/8, 1/8 και 1/8 αντίστοιχα. Να προσδιορίσετε το πληροφορικό περιεχόμενο του συμβόλου ‘τ’ και το πληροφορικό περιεχόμενο του συμβόλου ‘ω’.

3. Θεωρούμε μια δυαδική πηγή με δύο σύμβολα το 0 και το 1. Η πιθανότητα εκπομπής του 0 είναι ίση με 0.7. Να βρεθεί η πληροφορία του κάθε συμβόλου εκπομπής καθώς και η εντροπία της πηγής.

4. Πόση πληροφορία περιέχεται στον αριθμό κυκλοφορίας αυτοκινήτου της μορφής ΓΓΓαααα, όπου Γ είναι κεφαλαίο γράμμα και α ο αριθμός; (Θεωρούμε ελληνικές πινακίδες κυκλοφορίας)

5. Σ’ ένα κανάλι στέλνουμε σήματα 0 ή 1 με ίσες πιθανότητες αποστολής του 0 ή 1. Ποια είναι η μέση πληροφορία ή εντροπία του ενός των ψηφίων λ.χ του 1.

6.Έστω ότι έχουμε το αλφάβητο με τις αντίστοιχες πιθανότητες $\mathrm{P(A)} = 0.5$, $\mathrm{P(B)} = 0.4$, $\mathrm{P}(\Gamma) = 0.1$

Ποια είναι η μέτρηση της πληροφορίας στο δέκτη οταν παίρνουμε την πληροφορία (ΑΑΒ). Ποια είναι η μέση πληροφορία της πηγής;

Δίνεται η πληροφορία υπάρξεως αυτής της πληροφορίας είναι $\mathrm{P(AAB)} = \mathrm{P(A)}\,\mathrm{P(A)}\,\mathrm{P}(\Gamma) = 0.1$

7. Θεωρούμε πηγή που εκπέμπει έξι σύμβολα με τις παρακάτω πιθανότητες

P(A) = ½ , P(B) = ¼ , P(Γ) = 1/8 , P(Δ) = 1/16 , P(E) = 1/32 , P(Ξ) = 1/32

Να βρεθεί η μέση πληροφορία ή εντροπία της πηγής

8. Έστω ένα σήμα με δυαδικά ψηφία "0" και "1", με πιθανότητες $p(0) = 1/8$ και $p(1) = 7/8$. Να βρεθεί η ποσότητα πληροφορίας του κάθε ψηφίου.

9. Έστω ότι υπάρχουν M ισοπίθανα και ανεξάρτητα μηνύματα και N είναι ακέραιος τέτοιος ώστε $M = 2^N$. Να βρεθεί η πληροφορία κάθε μηνύματος

10.Έστω τα μηνύματα *Α*, *Β*, *Γ*, *Δ* με αντίστοιχες πιθανότητες 1/2, 1/4, 1/8, 1/8. Να βρεθεί η πληροφορία του μηνύματος *Χ = ΒΔΑ*, θεωρώντας ότι τα μηνύματα είναι ανεξάρτητα.

11.Έστω τα μηνύματα *Α*, *Β*, *Γ*, *Δ* με αντίστοιχες πιθανότητες 1/2, 1/4, 1/8, 1/8. Να υπολογιστεί η εντροπία *Η* για τον τετραδικό κώδικα καθώς και η εντροπία στην περίπτωση, που τα τέσσερα μηνύματα είναι ισοπίθανα.

12.Μια πηγή παράγει 8 διαφορετικά σύμβολα, τα $\mathrm{A},\mathrm{B},\Gamma,\Delta,\mathrm{E},\mathrm{Z},\mathrm{H},\Theta$ με πιθανότητες $\frac{1}{8},\frac{1}{4},\frac{1}{16},\frac{1}{32},\frac{1}{4},\frac{1}{32},\frac{1}{8},\frac{1}{8}$ αντίστοιχα. Ζητούνται τα ακόλουθα:

1. Ποιο γράμμα (σύμβολο) μεταφέρει τη μεγαλύτερη ποσότητα πληροφορίας και ποια τη μικρότερη;
2. Αν σκεφτώ μια λέξη που πρέπει να μαντέψετε και σας πω το πρώτο γράμμα της, ποιο θα είναι μεγαλύτερης χρησιμότητας το Β ή το Z;

13. Έστω δύο δυαδικές πηγές Α και Β. Υποθέτουμε ότι $0 < p_A(0) < p_B(0) < 0.5$. Ποια δυαδική πηγή έχει τη μεγαλύτερη εντροπία;

(η άσκηση μπορεί να λυθεί είτε υπολογιστικά είτε απλούστερα μέσω γραφικής παράστασης γνωστής συνάρτησης)

14. 1) Έστω μια τριαδική πηγή $A = \{0,1,2\}$. Υπολογίστε τις πιθανότητες p(0), p(1) και p(2), έτσι ώστε να μεγιστοποιείται η εντροπία της πηγής Α.

2) Έστω μια πηγή Χ με εντροπία $H(X) = 1.52$. Υπολογίστε την εντροπία της τρίτης επέκτασης της.

15. Ενα ισοπίθανο κέρμα ρίπτεται μέχρι το πρώτο ‘’κεφάλι’’ εμφανιστεί. Εστω X συμβολίζει τον αριθμό των ρίψεων που χρειάστηκαν. Οι ακόλουθες εκφράσεις ίσως να φανούν χρήσιμες:

$$\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$$

$$\sum_{n=1}^{\infty} nr^n = \frac{r}{(1-r)^2}$$

α) Βρείτε την εντροπία του $H(X)$ σε bits

β) Η τυχαία μεταβλητή X έστω οτι ακολουθεί την προηγούμενη κατανομή. Βρείτε μια σειρά απο ερωτήσεις με **ναι** και **όχι** της μορφής : ‘ Το X ανήκει στο σύμβολο S; ‘ . Να συγκριθεί η εντροπία $H(X)$ με τον αριθμό των ερωτήσεων που απαιτούνται προκειμένου να οριστεί το X.

16. Εστω ένα παιχνίδι που μεταξύ δύο ομάδων νικήτρια είναι εκείνη η ομάδα που συμπληρώνει 4 νίκες. Αρα μπορεί να γίνουν το πολύ 7 παιχνίδια μέχρι να βγεί νικητής. Εστω X είναι η μεταβλητή που αναπαριστά τη πιθανή διαδοχή των παιχνιδιών. Δηλ. Αν A και B είναι οι ομάδες τότε πιθανές τιμές των ομάδων είναι **AAAABABABAB** κ.ο.κ. Επίσης έστω Y **ο αριθμός** των παιχνιδιών με εύρος παιχνιδιών 4 και 7. Αν οι ομάδες A και B έχουν την ίδια πιθανότητα νίκης και τα παιχνίδια είναι ανεξάρτητα βρείτε:

α) $H(\mathrm{X})$, $H(Y)$

β) $H(\mathrm{X},Y)$, $H(Y,X)$

Κεφάλαιο 3. Πηγές Πληροφορίας

Σκοπός του κεφαλαίου αυτού είναι να περιγραφούν οι διακριτές πηγές πληροφορίας με και χωρίς μνήμη, καθώς επίσης και οι τεχνικές κωδικοποίησης των πηγών αυτών για την όσο το δυνατόν πιο συμπυκνωμένη αναπαράσταση της πληροφορίας.

3.1 Διακριτές πηγές πληροφορίας χωρίς μνήμη

Με τον όρο **διακριτή πηγή πληροφορίας** εννοούμε το τμήμα του συστήματος επικοινωνίας που παράγει πληροφορία με τη μορφή συμβόλων ή γραμμάτων. Το σύνολο των συμβόλων που χρησιμοποιεί η πηγή (π.χ. γράμματα, αριθμοί, διαγράμματα, χάρτες) ονομάζεται **αλφάβητο πηγής**. Τα σύμβολα δημιουργούνται από την πηγή σε διακριτές χρονικές στιγμές. Για τον παραπάνω λόγο και λόγω του πεπερασμένου πλήθους των συμβόλων η πηγή ονομάζεται διακριτή. Μια διατεταγμένη ακολουθία συμβόλων ονομάζεται **λέξη**, ενώ μία διατεταγμένη ακολουθία λέξεων ονομάζεται **μήνυμα**.

Η επιλογή ενός συμβόλου κατά τη δημιουργία μηνυμάτων από τη πηγή λαμβάνει χώρα με κάποια πιθανότητα. Θεωρούμε πως οι πιθανότητες επιλογής των συμβόλων παραμένουν αμετάβλητες με το πέρασμα του χρόνου, καθώς επίσης και πως η επιλογή ενός συμβόλου δεν εξαρτάται από τα προηγούμενα σύμβολα του μηνύματος. Σύμφωνα με τα παραπάνω, θα λέμε πως μία **διακριτή πηγή πληροφορίας δεν έχει μνήμη**, όταν τα σύμβολα που εκπέμπει είναι ανεξάρτητα, δηλαδή όταν η πιθανότητα εκπομπής ενός συμβόλου δεν εξαρτάται από ποιά σύμβολα εξέπεμψε προηγουμένως.

Μια τέτοια πηγή περιγράφεται τέλεια από το πλήθος n των διακριτών συμβόλων που μπορεί να εκπέμψει (αλφάβητο), από την πιθανότητα p_i που έχει το καθένα από τα σύμβολα αυτά να εκπεμφθεί και από τη διάρκεια t_i του καθενός (αφού δεν είναι απαραίτητο ούτε να είναι ισοπίθανα ούτε να έχουν την ίδια διάρκεια).

3.1.1 Εντροπία διακριτής πηγής χωρίς μνήμη

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 επικοινωνίας 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 των συμβόλων που παράγει η πηγή.

Ορισμός εντροπίας ή μέσης ποσότητας πληροφορίας διακριτής πηγής χωρίς μνήμη. Η μέση ποσότητα πληροφορίας η οποία παράγεται από μια διακριτή πηγή χωρίς μνήμη με αλφάβητο $S = \{s_1, s_2, ..., s_n\}$, όπου n το πλήθος των συμβόλων του αλφαβήτου και p_i η πιθανότητα επιλογής του συμβόλου s_i, δίνεται απο την παρακάτω σχέση

$$H(S) = -\sum_{i=1}^{n} p_i \log p_i \quad bits/symbol \qquad (3.1)$$

Από τον ορισμό διαπιστώνουμε ότι η τιμή της εντροπίας εξαρτάται αποκλειστικά από τις πιθανότητες p_i των συμβόλων της πηγής.

Στην περίπτωση που μια διακριτή πηγή πληροφορίας χωρίς μνήμη είναι δυνατό να έχει όλα τα σύμβολα της ισοπίθανα, τότε η πηγή παρουσιάζει μέγιστη τιμή της εντροπίας $\max H(S)$, η οποία δίνεται από τη σχέση:

$$\max H(S) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = \log n \quad bits/symbol \quad (3.2)$$

Ο πλεονασμός μιας πηγής πληροφορίας χωρίς μνήμη μας εκφράζει το ποσό της «άχρηστης» πληροφορίας που μεταφέρει η έξοδος μιας πηγής και ουσιαστικά μας δίνει τη διαφορά της τρέχουσας κατάστασης από την ιδανική περίπτωση, στην οποία τα σύμβολα της πηγής χρησιμοποιούνται ισοπίθανα (μέγιστη εντροπία). Ο πλεονασμός ορίζεται ως:

$$\Pi\lambda εονασμός = \frac{\max H(S) - H(S)}{\max H(S)} 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{H(S)}{\log n} \quad (3.3)$$

και δίνεται συνήθως σε ποσοστό %. Ο πλεονασμός της πηγής λαμβάνει τιμές στο διάστημα [0,1], εφόσον η εντροπία είναι μικρότερη ή ίση της μέγιστης εντροπίας μιας πηγής.

Ο πλεονασμός μιας πηγής πληροφορίας οφείλεται στους παρακάτω λόγους:

- Στο γεγονός ότι τα σύμβολα της πηγής είναι μη ισοπίθανα.
- Στην πιθανότητα να παρουσιάζει μνήμη η πηγή πληροφορίας.

Δηλαδή η ελάττωση της εντροπίας μιας πηγής σε σχέση με τη μέγιστη τιμή οφείλεται στο ότι τα σύμβολά της είναι μη ισοπίθανα και στο ότι κατά την εκπομπή των συμβόλων παρουσιάζεται προτίμηση στην εκπομπή ορισμένων συμβόλων της πηγής.

3.1.2 Ρυθμός παροχής εντροπίας

Ένα άλλο ενδιαφέρον χαρακτηριστικό της πηγής είναι ο ρυθμός με τον οποίο παρέχει πληροφορία η πηγή. Είναι φανερό οτι αν έχουμε δύο πηγές που έχουν την ίδια εντροπία H, αλλά διαφορετικούς ρυθμούς παροχής, η ταχύτερη πηγή θα εκπέμψει περισσότερα σύμβολα μέσα σε δοσμένο χρόνο και άρα περισσότερη πληροφορία. Επομένως, στις επιδόσεις της πηγής, εκτός από την εντροπία, πρέπει να προστεθεί και το μέγεθος R του ρυθμού παροχής πληροφορίας

Ορισμός ρυθμού πληροφορίας. Αν μια πηγή πληροφορίας εκπέμπει σύμβολα με ρυθμό συμβόλων r_s (σε σύμβολα / sec) και η πηγή παρουσιάζει εντροπία H (σε bits / σύμβολο), τότε ο ρυθμός παροχής πληροφορίας από την πηγή R (σε bits / sec) βρίσκεται άμεσα από τη σχέση:

$$R = r_s \cdot H \quad bits / \sec \qquad (3.4)$$

Παράδειγμα 3.1:

Μια διακριτή πηγή χωρίς μνήμη εκπέμπει ένα απο τα πέντε μηνύματα κάθε 1 msec. Αν οι πιθανότητες των μηνυμάτων είναι $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$ και $\frac{1}{16}$, βρείτε:

a) την εντροπία της πηγής

b) τη μέγιστη μέση ποσότητα πληροφορίας

c) το πλεονασμό της πηγής και

d) το μέσο ρυθμό πληροφορίας.

Λύση:

a) Η εντροπία, για μια διακριτή πηγή χωρίς μνήμη, δίνεται απο τον τύπο:

$$H(S) = -\sum_{i=1}^{n} p_i \log p_i$$

Αντικαθιστώντας στον παραπάνω τύπο έχουμε:

$$H(S) = -\sum_{i=1}^{5} p_i \log p_i$$

$$= -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{16}\log\frac{1}{16} = 1.875 bit/symbol$$

b) Η μέγιστη ποσότητα πληροφορίας, δίνεται απο τον τύπο:

$$\max H(S) = -\sum_{i=1}^{n} \frac{1}{n}\log\frac{1}{n} = \log n$$

Αντικαθιστώντας στον παραπάνω τύπο έχουμε:

$$\max H(S) = \log 5 = 2,321 bit/symbol$$

c) Ο πλεονασμός της πηγής, δίνεται απο τον τύπο

$$\Pi\lambda\varepsilon ονασμός = 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{H(S)}{\log n}$$

Αντικαθιστώντας στον παραπάνω τύπο έχουμε:

$$\Pi\lambda\varepsilon ονασμός = 1 - \frac{1.875}{2.321} = 0.192$$

d) Τέλος, ο μέσος ρυθμός πληροφορίας δίνεται απο τον τύπο:

$$R = r_s H$$

Αντικαθιστώντας στον παραπάνω τύπο έχουμε:

$$R = 10^{-3} 1.875 = 1875 bits/\sec$$

3.1.3 Επέκταση διακριτής πηγής πληροφορίας χωρίς μνήμη n τάξης

Στη θεωρία πληροφορίας, βολεύει συχνά να θεωρούμε ομάδες συμβόλων παρά μεμονωμένα σύμβολα. Ως ομάδα συμβόλων θεωρούμε *n* σύμβολα, τα οποία εκπέμπονται απο μια διακριτή πηγή σε διαδοχικές χρονικές στιγμές. Οι ομάδες συμβόλων μπορούμε να θεωρήσουμε πως αποτελούν σύμβολα μιας νέας διακριτής πηγής η οποία έχει το αλφάβητο S^n που αποτελείται από K^n σύμβολα, όπου K το πλήθος των συμβόλων του αλφαβήτου S της αρχικής πηγής.

Στην περίπτωση που η αρχική πηγή είναι μια διακριτή πηγή χωρίς μνήμη, τα σύμβολα στην έξοδό της είναι μεταξύ τους στατιστικά ανεξάρτητα. Έτσι, η πιθανότητα εμφάνισης ενός συμβόλου από το αλφάβητο S^n είναι ίση με το γινόμενο των πιθανοτήτων των *n* επιμέρους συμβόλων που το αποτελούν από το αλφάβητο S της αρχικής πηγής. Με βάση την παρατήρηση αυτή, μπορεί να αποδειχθεί πως η εντροπία μιας διακριτής πηγής χωρίς μνήμη και η εντροπία της αντίστοιχης *n* τάξης επέκτασής της σχετίζονται με τον τύπο:

$$H(S^n) = nH(S) \quad (3.5)$$

Παράδειγμα 3.2:

Θεωρήστε μια διακριτή πηγή χωρίς μνήμη με αλφάβητο $S = \{s_1, s_2, s_3\}$ και πιθανότητες εμφάνισης συμβόλων

$$p(s_1) = p_1 = \frac{1}{4},\ p(s_2) = p_2 = \frac{1}{4},\ p(s_3) = p_3 = \frac{1}{2}$$

Να υπολογιστεί:

a) η εντροπία της πηγής και

b) η εντροπία της δεύτερης τάξης επέκτασής της.

Λύση:

a) Η εντροπία της αρχικής πηγής είναι:

$$H(S) = -\sum_{i=1}^{3} p_i \log p_i$$

$$= -\frac{1}{4}\log\frac{1}{4} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{2}\log\frac{1}{2} = \frac{3}{2} bits$$

b) Η δεύτερης τάξης επέκταση της πηγής που εξετάζουμε θα είναι μια νέα διακριτή πηγή χωρίς μνήμη με αλφάβητο

$$S^2 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\}$$

$$= \{s_1 s_1, s_1 s_2, s_1 s_3, s_2 s_1, s_2 s_2, s_2 s_3, s_3 s_1, s_3 s_2, s_3 s_3\}$$

θα αποτελείται δηλαδή απο 3^2 = 9 σύμβολα. Θα υπολογίσουμε τώρα τις αντίστοιχες πιθανότητες των συμβόλων $\sigma_0, \sigma_1, ..., \sigma_8$ ως $q_0, q_1, ..., q_8$. Οι πιθανότητες αυτές υπολογίζονται ως γινόμενα των πιθανοτήτων των επιμέρους συμβόλων του S που αποτελούν τα σύμβολα του S^2.

q_0	q_1	q_2	q_3	q_4	Q_5	q_6	q_7	q_8
$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$

και έτσι η εντροπία της πηγής θα είναι:

$$H(S^2) = -\sum_{i=1}^{8} q_i \log q_i$$

$$= -4\frac{1}{16}\log\frac{1}{16} - 4\frac{1}{8}\log\frac{1}{8} - \frac{1}{4}\log\frac{1}{4} = 3bits$$

Ακόμη ευκολότερα μπορεί να υπολογιστεί αντικαθιστώντας στον τύπο $H(S^n) = nH(S)$

$$H(S^2) = 2\frac{3}{2} = 3bits$$

3.2 Κωδικοποίηση Πηγής

Ένα σημαντικό πρόβλημα το οποίο συναντάται στις τηλεπικοινωνίες είναι η αποδοτική αναπαράσταση της πληροφορίας, η οποία παράγεται απο μια διακριτή πηγή δεδομένων. Για το λόγο αυτό, επιδιώκεται η όσο το δυνατόν πιο συμπυκνωμένη αναπαράσταση των μηνυμάτων, η οποία επιτυγχάνεται με την αφαίρεση του πλεονασμού που εμπεριέχεται σε αυτά.

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 ονομάζεται **κωδικοποίηση πηγής.** Ένας άλλος όρος που χρησιμοποιείται συχνά στη βιβλιογραφία είναι ο όρος **συμπίεση** αντί του όρου κωδικοποίηση πηγής. Η διάταξη η οποία επιτελεί την εργασία αυτή ονομάζεται **κωδικοποιητής πηγής**. 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. Για να μπορέσει ένας κωδικοποιητής πηγής να αναπαραστήσει αποδοτικά τα δεδομένα μιας διακριτής πηγής είναι απαραίτητο να γνωρίζει ορισμένες στατιστικές ιδιότητες για την πηγή αυτή. Παραδείγματος χάρη, αν ένα σύμβολο της πηγής εμφανίζεται με μεγάλη πιθανότητα, τότε θα επιθυμούσαμε να αναπαραστήσουμε το σύμβολο αυτό με κάποιο απλό και σύντομο τρόπο. Αντίθετα, τα σύμβολα τα οποία εμφανίζονται σπάνια και επομένως έχουν μικρές πιθανότητες δεν μας ενοχλεί ιδιαίτερα να τα κωδικοποιήσουμε με κάποια πιο πολύπλοκη και μακροσκελή αναπαράσταση.

Οι αναπαραστάσεις των συμβόλων που προκύπτουν στην έξοδο ενός κωδικοποιητή πηγής ονομάζονται **κωδικές λέξεις** και το σύνολο των κωδικών λέξεων που χρησιμοποιεί ένας κωδικοποιητής πηγής με σκοπό να αναπαραστήσει όλα τα σύμβολα μιας διακριτής πηγής ονομάζεται **κώδικας πηγής**.

Βασικό χαρακτηριστικό κάθε κώδικα είναι ο αριθμός των bits που χρησιμοποιεί για να παραστήσει το κάθε σύμβολο. Αν ένας κώδικας χρησιμοποιεί μ αριθμό bits, ο αριθμός των δυνατών συνδυασμών, δηλαδή των συμβόλων που μπορεί να περιγράψει με αυτά, θα είναι ίσος με 2^{μ}. Αν ένας κώδικας έχει ως στόχο την κωδικοποίηση N διαφορετικών συμβόλων, τότε ο αριθμός μ των bits που θα πρέπει να χρησιμοποιήσει δίνεται από τη σχέση:

$$2^{\mu-1} \leq N \leq 2^{\mu} \quad (3.6)$$

Όσο λιγότερα bits χρησιμοποιεί ένας κώδικας, τόσο πιο αποδοτικός είναι ως προς την ταχύτητα μετάδοσης συμβόλων.

Ανάλογα με το μήκος των κωδικών λέξεων οι κώδικες διακρίνονται σε **σταθερού μήκους** και **μεταβλητού μήκους**.

Στους **κώδικες σταθερού μήκους** το μήκος των κωδικών λέξεων είναι σταθερό για κάθε σύμβολο πηγής. Ένας κώδικας σταθερού μήκους είναι ο

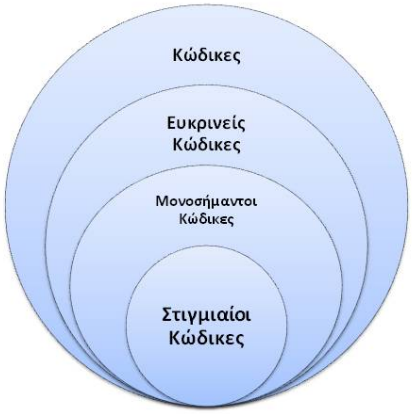
ASCII (American Standard Code for Information Interchange), όπου κάθε χαρακτήρας κωδικοποιείται με μια ακολουθία 7 δυαδικών ψηφίων κι έχει δυνατότητα κωδικοποίησης 128 χαρακτήρων.

Στην περίπτωση της συμπίεσης, το ενδιαφέρον εστιάζεται σε **κώδικες μεταβλητού μήκους**. Τα σύμβολα της πηγής που έχουν μεγαλύτερη πιθανότητα εμφάνισης αντιστοιχίζονται σε μικρότερες κωδικές λέξεις και αντιστρόφως. Με αυτόν τον τρόπο το συνολικό μήκος του κωδικού μηνύματος μπορεί να προκύψει μικρότερο από το αρχικό μήνυμα. Ας δούμε για παράδειγμα τον κώδικα Morse, ο οποίος είναι ο πιο γνωστός κώδικας με μη ισομήκεις λέξεις. Έχει κωδικό αλφάβητο τεσσάρων συμβόλων (τελεία, παύλα, κενό γράμματος, κενό λέξης). Γράμματα με μεγάλη πιθανότητα εμφάνισης εμφανίζονται με βραχείες κωδικές λέξεις (π.χ. το λατινικό γράμμα e αναπαρίσταται με μια τελεία '.'), ενώ τα λιγότερα συχνά με κωδικές λέξεις μεγαλύτερου μήκους (π.χ. το γράμμα Q αναπαρίσταται με παύλα, παύλα, τελεία, παύλα '--.-').

Ένα βασικό χαρακτηριστικό ενός κώδικα συμπίεσης για να χαρακτηριστεί επιτυχής είναι το κατά πόσο είναι δυνατή κι εύκολη η αποκωδικοποίηση ενός κωδικού μηνύματος από το δέκτη. Θεωρούμε βέβαια ότι κατά την αναπαραγωγή του αρχικού μηνύματος από το δέκτη ο κώδικας είναι γνωστός. Σύμφωνα με τα παραπάνω, οι κώδικες ταξινομούνται στις εξής κατηγορίες:

- **Ευκρινείς κώδικες (non-singular):** Ευκρινής κώδικας είναι εκείνος που χρησιμοποιεί διαφορετική κωδική λέξη για κάθε σύμβολο ή λέξη πληροφορίας. Η ευκρίνεια του κώδικα είναι η πρώτη προϋπόθεση για να υπάρχει δυνατότητα αποκωδικοποίησης.
- **Μονοσήμαντοι κώδικες (uniquely decodable):** Ένας κώδικας θεωρείται μονοσήμαντος αν κάθε κωδική λέξη αναγνωρίζεται μέσα σε μακρά διαδοχή κωδικών συμβόλων. Δύο οποιαδήποτε μηνύματα πληροφορίας αντιστοιχίζονται με μονοσήμαντο κώδικα σε δύο διαφορετικά κωδικά μηνύματα. Για να είναι ο κώδικας μονοσήμαντος πρέπει να διαθέτει την προθεματική ιδιότητα, δηλαδή καμια κωδική λέξη να μην είναι πρόθεμα άλλης κωδικής λέξης.
- **Στιγμιαία αποκωδικοποιήσιμοι κώδικες (instantaneous code):** Στιγμιαία αποκωδικοποιήσιμος κώδικας είναι κάθε μονοσήμαντος κώδικας (uniquely decodable), ο οποίος επιτρέπει αποκωδικοποίηση των μηνυμάτων λέξη προς λέξη χωρίς να απαιτείται εξέταση επόμενων κωδικών συμβόλων.

Στο παρακάτω σχήμα βλέπουμε την ταξινόμηση των κωδίκων με κριτήριο την αποκωδικοποίηση.



Εικόνα 6. Ταξινόμηση των κωδίκων με κριτήριο την αποκωδικοποίηση.

Από το παραπάνω σχήμα (Εικονα 6) προκύπτουν τα εξής συμπεράσματα:

1. Κάθε στιγμιαία αποκωδικοποιήσιμος κώδικας είναι και μονοσήμαντος, δεν ισχύει όμως το αντίστροφο.
2. Κάθε μονοσήμαντος κώδικας είναι και ευκρινής, αλλά δεν ισχύει το αντίστροφο.
3. Κάθε ευκρινής κώδικας σταθερού μήκους είναι και στιγμιαία αποκωδικοποιήσιμος.

Παράδειγμα 3.3:
Στον παρακάτω πίνακα δίνονται οι πιθανότητες των συμβόλων μιας πηγής, καθώς και τέσσερεις διαφορετικοί κώδικες που χρησιμοποιούνται για την κωδικοποίηση των συμβόλων. Να ταξινομηθούν οι κώδικες σε κατηγορίες (ευκρινής, μονοσήμαντος, στιγμιαία αποκωδικοποιήσιμος)

x_i	p_i	κώδικας 1	κώδικας 2	κώδικας 3	κώδικας 4
A	0.5	0	110	000	01
B	0.3	01	01	010	011
Γ	0.15	11	00	101	0111
Δ	0.05	10	10	111	0

Ο **κώδικας 1** είναι ευκρινής, γιατί καμία κωδική λέξη δεν αντιστοιχεί σε δύο ή περισσότερα σύμβολα. Δεν είναι όμως μονοσήμαντος, γιατί η ακολουθία συμβόλων 0110 μπορεί να αποκωδικοποιηθεί ως ΑΓΑ ή ως ΒΔ. Αφού δεν είναι μονοσήμαντος, κατ' επέκταση δεν μπορεί να είναι και στιγμιαία αποκωδικοποιήσιμος.
Ο **κώδικας 2** είναι στιγμιαία αποκωδικοποιήσιμος, γιατί οι κωδικές λέξεις του διαθέτουν την προθεματική ιδιότητα. Κατ' επέκταση είναι μονοσήμαντος και ευκρινής.
Ο **κώδικας 3** είναι στιγμιαία αποκωδικοποιήσιμος, μονοσήμαντος και ευκρινής, γιατί έχει την προθεματική ιδιότητα.
Τέλος, ο **κώδικας 4** δεν είναι στιγμιαία αποκωδικοποιήσιμος, επειδή για παράδειγμα η κωδική λέξη 01 είναι πρόθεμα της κωδικής λέξης 001. Όμως, είναι ευκρινής και μονοσήμαντος, γιατί κάθε κωδική λέξη μπορεί να αναγνωριστεί μέσα σε οποιοδήποτε κωδικό μήνυμα, δεδομένου ότι αρχίζει πάντα με το σύμβολο 0, ενώ τα υπόλοιπα σύμβολα της κωδικής λέξης μπορούν να είναι μόνο 1.

Στο παρακάτω σχήμα (Εικόνα 7) βλέπουμε την κωδικοποίηση της πηγής, όπου η έξοδος a_i (σύμβολο) μιας διακριτής πηγής χωρίς μνήμη οδηγείται σε έναν κωδικοποιητή πηγής, ο οποίος δίνει στην έξοδο του μια ακολουθία από 0 και 1 c_i (κωδική λέξη).

Εικόνα 7. Κωδικοποίηση πηγής.

Ορισμός μέσου μήκους κώδικα $\overline{L}$: Έστω ότι η πηγή έχει $A=(a_1,a_2,.....,a_M)$ διακριτά σύμβολα με πιθανότητες εμφάνισης $p_i=p(X=i)$ αντίστοιχα. Επίσης, υποθέτουμε ότι η κωδική λέξη $C=(c_1,c_2,.....,c_M)$ που αντιστοιχεί στο σύμβολο a_i έχει μήκος l_i. Επομένως, ορίζουμε το μέσο μήκος κώδικα $\overline{L}$ ως:

$$\overline{L}=\sum_{i=1}^{N}p_i l_i \quad (3.7)$$

Το μέσο μήκος κώδικα $\overline{L}$ εκφράζει το μέσο πλήθος δυαδικών ψηφίων ανά σύμβολο πηγής, τα οποία χρησιμοποιούνται στη διαδικασία της κωδικοποίησης.

Αν θεωρήσουμε ως $\mathrm{L}_{\min}$ την ελάχιστη δυνατή τιμή του $\overline{L}$, τότε μπορούμε να ορίσουμε την **αποδοτικότητα** του κώδικα ως:

$$n = \frac{L_{\min}}{\overline{L}} \quad (3.8)$$

Παρατηρούμε πως αφού $\mathrm{L}_{\min} \leq \overline{L}$, η αποδοτικότητα n λαμβάνει τιμές μικρότερες της μονάδας. Ένας κώδικας ονομάζεται αποδοτικός, αν η αποδοτικότητα του πλησιάζει την τιμή 1.

Η τιμή $\mathrm{L}_{\min}$ στην οποία αναφερθήκαμε προηγουμένως είναι χαρακτηριστικό της πηγής δεδομένων και όχι του κωδικοποιητή. Η τιμή της L_{min} υπολογίζεται με βάση το θεώρημα κωδικοποίησης πηγής ή πρώτο θεώρημα του Shannon.

Ορισμός θεωρήματος κωδικοποίησης πηγής ή πρώτου θεωρήματος του Shannon. Για μια δοσμένη κωδικοποίηση πηγής χωρίς μνήμη με εντροπία $H(X)$, το μέσο μήκος κώδικα $\overline{L}$ οποιουδήποτε κωδικοποιητή πηγής φράσσεται από την ανισότητα:

$$\overline{L} \geq H(X) \quad (3.9)$$

Το παραπάνω θεώρημα μας πληροφορεί πως δεν υπάρχει κωδικοποιητής πηγής, ο οποίος να πετυχαίνει μικρότερο μέσο μήκος κώδικα $\overline{L}$ από την εντροπία της πηγής. Έτσι, η τιμή $\mathrm{L}_{\min}$ που χρησιμοποιήσαμε προηγουμένως ισούται με την εντροπία της διακριτής πηγής την οποία κωδικοποιούμε, και μπορούμε να ορίσουμε έτσι την αποδοτικότητα ενός κωδικοποιητή πηγής ως:

$$n = \frac{H(X)}{\overline{L}} \quad (3.10)$$

Από την ταξινόμηση με βάση την ευκολία με την οποία επιτυγχάνεται η αποκωδικοποίηση προέκυψε ότι ένας στιγμιαία αποκωδικοποιήσιμος κώδικας παρουσιάζει σημαντικό ενδιαφέρον, αφού η αποκωδικοποίηση είναι στιγμιαία, χωρίς να δημιουργούνται κωδικά μηνύματα με ασάφειες ή διαφορετικά ισοδύναμα αποτελέσματα αποκωδικοποίησης. Για τους παραπάνω λόγους, στη συνέχεια θα μας απασχολήσουν μόνο στιγμιαία αποκωδικοποιήσιμοι κώδικες.

3.2.1 Προθεματικοί κώδικες

Θεωρούμε μια διακριτή πηγή χωρίς μνήμη με αλφάβητο $\{s_0, s_1, \ldots, s_{K-1}\}$ και πιθανότητες συμβόλων $p_0, p_1, \ldots, p_{K-1}$. Ένας κωδικοποιητής πηγής που αντιστοιχίζει κάθε σύμβολο της πηγής αυτής σε μια κωδική λέξη είναι χρήσιμος μόνο στην περίπτωση που μπορούμε να ανακατασκευάσουμε την αρχική ακολουθία συμβόλων της πηγής από την ακολουθία των κωδικών λέξεων. Ο περιορισμός αυτός σημαίνει ότι η ακολουθία κωδικών λέξεων που αντιστοιχεί σε μια πεπερασμένη ακολουθία συμβόλων της πηγής είναι διαφορετική από όλες τις ακολουθίες κωδικών λέξεων, οι οποίες προκύπτουν για διαφορετικές ακολουθίες συμβόλων της πηγής. Με άλλα λόγια, η κωδικοποίηση είναι μία ένα προς ένα συνάρτηση από το σύνολο Φ (αλφάβητο πηγής στο σύνολο $B = \{b_0, b_1, \ldots, b_{K-1}\}$, το οποίο περιέχει τις κωδικές λέξεις.

Υποθέτουμε πως η κωδική λέξη b_k , η οποία αντιστοιχεί στο σύμβολο s_k , είναι

$$b_k = \left(m_{k_1}, m_{k_2}, \ldots, m_{k_n} \right) \quad (3.11)$$

όπου

m_{k_i} : το i-οστό δυαδικό ψηφίο (0 ή 1) της κωδικής λέξης

n : το μήκος της κωδικής λέξης b_k

Ορίζουμε ως πρόθεμα της κωδικής λέξης b_k οποιαδήποτε ακολουθία δυαδικών ψηφίων της μορφής

$$\left(m_{k_1}, m_{k_2}, \ldots, m_{k_i} \right) \text{ όπου } i \le n \quad (3.12)$$

Ορισμός προθεματικού κώδικα. Ορίζουμε ως προθεματικό κώδικα έναν κώδικα για τον οποίο καμία κωδική λέξη του δεν αποτελεί πρόθεμα κάποιας άλλης κωδικής λέξης. Η συνθήκη αυτή καθιστά τους προθεματικούς κώδικες πάντα αποκωδικοποιήσιμους.

Παράδειγμα 3.4:

Ας θεωρήσουμε, τους 3 κώδικες που φαίνονται στον παρακάτω πίνακα.

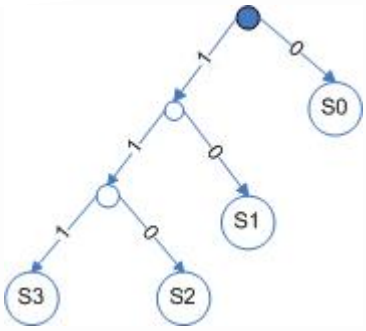
Σύμβολο πηγής	Πιθανότητα εμφάνισης	κώδικας 1	κώδικας 2	κώδικας 3
s_0	0.5	0	0	0
s_1	0.25	1	10	01
s_2	0.125	00	110	011
s_3	0.125	11	111	0111

Να βρεθεί ποιοί από τους κώδικες του πίνακα είναι προθεματικοί και ποιοί οχι. Να αιτιολογηθεί η απάντηση.

Λύση:

Εύκολα παρατηρούμε πως ο κώδικας 1 δεν είναι προθεματικός, αφού η κωδική λέξη ‘0’ που αντιστοιχεί στο σύμβολο s_0 αποτελεί πρόθεμα της κωδικής λέξης ‘00’ που αντιστοιχεί στο σύμβολο s_2. Με όμοιο τρόπο μπορούμε να δούμε πως ο κώδικας 2 είναι προθεματικός, αφού η κωδική λέξη ‘0’ που αντιστοιχεί στο σύμβολο s_0 δεν αποτελεί πρόθεμα καμίας προθεματικής λέξης των συμβόλων s_1, s_2 και s_3, ενώ ο κώδικας 3 δεν είναι.

Η διαδικασία της μετατροπής των κωδικών λέξεων στα αντίστοιχα σύμβολα πηγής ονομάζεται αποκωδικοποίηση και οι διατάξεις που εκτελούν την εργασία αυτή αποκωδικοποιητές πηγής. Η αποκωδικοποίηση ενός προθεματικού κώδικα γίνεται με χρήση δέντρων απόφασης. Ένα δέντρο απόφασης είναι μια γραφοθεωρητική αναπαράσταση όλων των κωδικών λέξεων ενός προθεματικού κώδικα. Στο παρακάτω σχήμα παρουσιάζεται το δέντρο απόφασης του κώδικα 2 που είδαμε στο παραπάνω παράδειγμα.



Εικόνα 8. Δέντρο απόφασης για τον κώδικα 2.

Παρατηρούμε πως κάθε ακμή του γραφήματος έχει μια ετικέτα 0 ή 1. Κάθε μονοπάτι από τη ρίζα του δέντρου απόφασης ως τα φύλλα του αντιστοιχεί σε μια κωδική λέξη, την κωδική λέξη που προκύπτει από τις ετικέτες των ακμών που αποτελούν το μονοπάτι.

Ο αποκωδικοποιητής ενός προθεματικού κώδικα ξεκινά από τη ρίζα του δέντρου απόφασης. Για καθένα δυαδικό ψηφίο που εμφανίζεται στην είσοδο του, ακολουθεί την ακμή με την αντίστοιχη ετικέτα και έτσι μεταβαίνει σε ένα νέο κόμβο. Αν σε κάποιο βήμα καταλήξει σε φύλλο του δέντρου, τότε βγάζει στην έξοδο του το αντίστοιχο σύμβολο πηγής κι επιστρέφει στη ρίζα του δέντρου για να ξεκινήσει την αποκωδικοποίηση του νέου συμβόλου. Έτσι, στο παραπάνω παράδειγμα για τον κώδικα 2 βλέποντας το δέντρο απόφασης και ακολουθώντας τη διαδικασία που περιγράψαμε, με είσοδο τα δυαδικά ψηφία '1011111000', καταλήγουμε στην ακολουθία συμβόλων s_1, s_3, s_2, s_0,s_0.

Για μια δοσμένη διακριτή πηγή χωρίς μνήμη, το μέσο μήκος κώδικα $\overline{L}$, για τους προθεματικούς κώδικες αποδεικνύεται πως φράσσεται από την ανισότητα:

$$\mathrm{H}(\Phi) \leq \overline{L} < \mathrm{H}(\Phi) + 1 \quad (3.13)$$

Για μια δοσμένη διακριτή πηγή χωρίς μνήμη, μπορούμε να σχεδιάσουμε πάντα εναν προθεματικό κώδικα ο οποίος να πετυχαίνει μέσο μήκος κώδικα $\overline{L}$ κοντά στην εντροπία της πηγής. Παρακάτω αποδεικνύουμε πώς γίνεται αυτό.

Θεωρούμε τη n-τάξης επέκταση της διακριτής πηγής, η οποία είναι μια νέα διακριτή πηγή χωρίς μνήμη με αλφάβητο Φ^n. Έστω ένας προθεματικός κώδικας για τη νέα πηγή. Αυτός ο κώδικας θα ονομάζεται n-τάξης επεκταμένος κώδικας. Για το ζεύγος νέας πηγής και νέου κώδικα θα ισχύει:

$$H(\Phi) \leq \overline{L_n} < H(\Phi^n) + 1 \qquad (3.14)$$

Όπου $\overline{L_n}$ το μέσο μήκος κώδικα του n-τάξης επεκταμένου κώδικα.

Χρησιμοποιώντας την ιδιότητα

$$H(\Phi^n) = n \cdot H(\Phi) \qquad (3.15)$$

Έχουμε:

$$n \cdot H(\Phi) \leq \overline{L_n} < n \cdot H(\Phi) + 1 \Leftrightarrow$$

$$H(\Phi) \leq \frac{\overline{L_n}}{n} < H(\Phi) + \frac{1}{n} \qquad (3.16)$$

Από την τελευταία σχέση βλέπουμε ότι όταν η τάξη n του κώδικα τείνει στο άπειρο, το μέσο μήκος του $\overline{L_n}$ συγκλίνει στην εντροπία της πηγής. Άρα, το μέσο μήκος ενός προθεματικού επεκταμένου κώδικα μπορεί να προσεγγίσει την εντροπία μιας διακριτής πηγής χωρίς μνήμη, αρκεί η τάξη n του κώδικα να είναι αρκετά μεγάλη. Αξίζει να αναφέρουμε στο σημείο αυτό ότι το μειονέκτημα της χρήσης ενός επεκταμένου κώδικα είναι η μεγάλη πολυπλοκότητα του αλγόριθμου αποκωδικοποίησής του.

3.2.2 Αλγόριθμοι Κωδικοποίησης

Υπάρχουν πολλοί αλγόριθμοι για την εύρεση αποδοτικών κωδίκων. Σ' αυτούς συγκαταλέγονται οι αλγόριθμοι κωδικοποίησης του Shannon, του Fano 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 παραπάνω αλγορίθμους κωδικοποίησης.

3.2.2.1 Αλγόριθμος Κωδικοποίησης Shannon

Ο αλγόριθμος κωδικοποίησης του Shannon μπορεί να χρησιμοποιηθεί για την κωδικοποίηση των συμβόλων ή των μηνυμάτων της πηγής. Διαμορφώνεται σε τέσσερα βήματα:

1. Τα σύμβολα της πηγής πληροφορίας συντάσσονται στη σειρά με κριτήριο την πιθανότητα τους (από την μέγιστη στην ελάχιστη πιθανότητα).

$$\begin{array}{ccccc} x_1 & & x_2 & \ldots & x_M \\ \updownarrow & & \updownarrow & & \updownarrow \\ p(x_1) & \geq & p(x_2) & \geq \ldots \geq & p(x_M) \end{array}$$

2. Σε κάθε σύμβολο πληροφορίας αντιστοιχίζεται ένας αριθμός με τη λογική που περιγράφεται παρακάτω:

$$x_1 \leftrightarrow \varepsilon_1 = 0$$
$$x_2 \leftrightarrow \varepsilon_2 = p(x_1) + \varepsilon_1 = p(x_1)$$
$$x_3 \leftrightarrow \varepsilon_3 = p(x_2) + \varepsilon_2 = p(x_1) + p(x_2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_M \leftrightarrow \varepsilon_M = p(x_{M-1}) + \varepsilon_{M-1} = p(x_1) + p(x_2) + \ldots + p(x_{M-1})$$

3. Το μήκος της κωδικής λέξης που αντιστοιχεί στο σύμβολο πληροφορίας x_i είναι ο ελάχιστος ακέραιος που ικανοποιεί την ταυτοανισότητα

$$l_i \geq \log\left(\frac{1}{p(x_i)}\right) \Rightarrow 2^{l_i}\, p(x_i) \geq 1 \qquad (3.17)$$

4. Οι δεκαδικοί αριθμοί ε_i, όπου $i = 1, 2, \ldots\ldots M$ μετατρέπονται σε δυαδικούς αριθμούς και από τους τελευταίους διατηρούνται μόνο l_i σημαντικά ψηφία που θα αποτελέσουν τις αντίστοιχες κωδικές λέξεις για τα σύμβολα πληροφορίας $x_1, x_2, \ldots\ldots, x_M$

Παράδειγμα 3.5:

Έστω πηγή πληροφορίας $X = \{x_1, x_2, \ldots\ldots, x_M\}$ με κατανομή πιθανότητας $p(X) = \{0.5, 0.3, 0.1, 0.1\}$. Να βρεθούν:

1. Οι κωδικές λέξεις κατά Shannon
2. Το μέσο μήκος των κωδικών λέξεων
3. Η εντροπία της πηγής

Λύση:

1. Το βήμα 1 της κωδικοποίησης Shannon είναι έτοιμο (σωστά διατεταγμένα σύμβολα).

Για το βήμα 2:

$\varepsilon_1 = 0 = 0.0 = 0.\underline{0}0000...$

$\varepsilon_2 = 0.5 + \varepsilon_1 = 0.5 = 0.\underline{10}000...$

$\varepsilon_3 = 0.3 + \varepsilon_2 = 0.8 = 0.\underline{1100}1...$

$\varepsilon_4 = 0.1 + \varepsilon_3 = 0.9 = 0.\underline{1110}0...$

Εφαρμόζοντας την εξίσωση του βήματος 3 προκύπτει:

$2^{l_1}(0.5) \geq 1 \Rightarrow l_1 = 1$

$2^{l_2}(0.3) \geq 1 \Rightarrow l_2 = 2$

$2^{l_3}(0.1) \geq 1 \Rightarrow l_3 = 4$

$2^{l_4}(0.1) \geq 1 \Rightarrow l_4 = 4$

Συνεπώς οι λέξεις κώδικα για τα $X = \{x_1, x_2, x_3, x_4\}$ θα είναι $(0,10,1100,1110)$ αντίστοιχα.

2. Το μέσο μήκος των κωδικών λέξεων είναι $L = 1 \cdot (0.1) + 2 \cdot (0.3) + 4 \cdot (0.1) + 4 \cdot (0.1) = 1.9$ ψηφία ανά λέξη. Επειδή κάθε δυαδικό ψηφίο αντιστοιχεί σε 1 bit, θα είναι $L = 1.9$ bits ανά λέξη.

3. Η εντροπία της πηγής πληροφορίας είναι :

$H(X) = -0.5\log(0.5) - 0.3\log(0.3) - 0.1\log(0.1) - 0.1\log(0.1) = 1.685 bits / σύμβολο$

Άρα, $L = 1.9 > H(X)/\log 2 = 1.685$ που αποτελεί το κατώτερο φράγμα.

3.2.2.2 Αλγόριθμος Κωδικοποίησης Shannon – Fano

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

1. Τα σύμβολα της πηγής πληροφορίας συντάσσονται στη σειρά με κριτήριο την πιθανότητα τους (από την μέγιστη στην ελάχιστη πιθανότητα). Για παράδειγμα:

$$\begin{array}{cccc} x_1 & x_2 & \ldots & x_M \\ \updownarrow & \updownarrow & & \updownarrow \\ p(x_1) \geq & p(x_2) \geq & \ldots \geq & p(x_M) \end{array}$$

2. Επιλέγεται συγκεκριμένη διάταξη για τα κωδικά σύμβολα $\gamma_1, \gamma_2, \ldots \gamma_D$, η οποία δεν αλλάζει σε καμία φάση της κωδικοποίησης, αλλά και κατά την αποκωδικοποίηση.

3. Σχηματίζονται D ομάδες συμβόλων πηγής πληροφορίας με συγχώνευση γειτονικών συμβόλων. Οι πιθανότητες των συμβόλων που συμμετέχουν σε κάθε ομάδα αθροίζονται και το αποτέλεσμα επιδιώκεται να είναι όσο το δυνατόν πλησιέστερα στον αριθμό 1/D δηλαδή όλες οι ομάδες συμβόλων είναι κατά το δυνατόν ισοπίθανες.

4. Στα σύμβολα της πρώτης ομάδας αντιστοιχούμε ως πρώτο κωδικό σύμβολο το γ_1, της δεύτερης το γ_2 κ.ο.κ.

5. Διαιρούμε κάθε ομάδα συμβόλων σε D υποομάδες πάλι με το ίδιο κριτήριο (κατά το δυνατόν ισοπίθανες). Στα σύμβολα της κάθε υποομάδας αντιστοιχίζεται ως δεύτερο κωδικό σύμβολο ένα κωδικό σύμβολο με την προκαθορισμένη διάταξη. Η συγκεκριμένη αναδρομική διαδικασία συνεχίζεται μέχρι να προκύψουν υποομάδες με ένα μόνο σύμβολο.

Παράδειγμα 3.6*:*

Έστω πηγή πληροφορίας $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ με κατανομή πιθανότητας $p(X) = \{0.25, 0.25, 0.125, 0.125, 0.0625, 0.0625, 0.0625, 0.0625\}$. Να βρεθούν:

1. Οι κωδικές λέξεις κατά Shannon - Fano
2. Το μέσο μήκος των κωδικών λέξεων
3. Η εντροπία της πηγής

Λύση:

1. Με βάση την κατανομή πιθανότητας βλέπουμε ότι τα σύμβολα πληροφορίας είναι διατεταγμένα σωστά (το βήμα (1) έχει πραγματοποιηθεί).

Στο βήμα (2) επιλέγεται για τα σύμβολα του δυαδικού κώδικα Shannon-Fano η διάταξη (0,1). Ο παρακάτω πίνακας περιγράφει τη σταδιακή κατασκευή του κώδικα.

Σύμβολο	Πιθανότητα	1ο βήμα	2ο Βήμα	3ο Βήμα	4ο Βήμα
x_1	0.25	0	00	00	00
x_2	0.25	0	01	01	01
x_3	0.125	1	10	100	100
x_4	0.125	1	10	101	101
x_5	0.0625	1	11	110	1100
x_6	0.0625	1	11	110	1101
x_7	0.0625	1	11	111	1110
x_8	0.0625	1	11	111	1111

2. Το μέσο μήκος των κωδικών λέξεων είναι:

$$L = 2(0.25) + 2(0.25) + 3(0.125) + 3(0.125) + 4(4(0.0625)) = 2.75 bits / \lambda\acute{\epsilon}\xi\eta$$

3. Η εντροπία της πηγής πληροφορίας είναι:

$$\mathrm{H(X)} = 2(-0.25)\log(0.25)) + 2(-0.125\log(0.125)) + 4(-0.0625\log(0.0625)) = 2.75 bits / symbol$$

Επομένως ο κώδικας αυτός, σύμφωνα με το θεώρημα του Shannon, είναι βέλτιστος.

3.2.2.3 Αλγόριθμος Κωδικοποίησης Huffman

Ο κώδικας Huffman είναι ένας κώδικας πηγής, το μέσο μήκος του οποίου πλησιάζει την εντροπία της διακριτής πηγής την οποία κωδικοποιεί. Ο κώδικας αυτός είναι βέλτιστος με την έννοια ότι για μια δοσμένη διακριτή πηγή χωρίς μνήμη δεν υπάρχει άλλος αποκωδικοποιήσιμος κώδικας, ο οποίος να πετυχαίνει μικρότερο μέσο μήκος.

Η ιδέα του αλγορίθμου με βάση τον οποίο κατασκευάζουμε τον κώδικα Huffman είναι η σταδιακή μείωση του αλφαβήτου της πηγής. Σε κάθε βήμα, επιλέγουμε 2 σύμβολα από το αλφάβητο της πηγής και τα συγχωνεύουμε σε ένα σύμβολο που λαμβάνει μέρος στην επόμενη φάση του αλγορίθμου. Ακολουθώντας τη διαδικασία αυτή, καταλήγουμε σε ένα αλφάβητο το οποίο αποτελείται από 2 μόνο σύμβολα. Τα σύμβολα αυτά γνωρίζουμε πως κωδικοποιούνται βέλτιστα από τις κωδικές λέξεις ‘0’ και ‘1’. Στη συνέχεια, ξεκινώντας από την τελευταία φάση εργαζόμαστε προς τα πίσω και καταλήγουμε σε έναν βέλτιστο κώδικα. Πιο συγκεκριμένα, ο αλγόριθμος κατασκευής του κώδικα Huffman έχει ως εξής:

1. Τα σύμβολα της πηγής ταξινομούνται από το πλέον πιθανό ως το λιγότερο πιθανό. Στα δύο λιγότερο πιθανά σύμβολα ανατίθενται τα δυαδικά ψηφία 0 και 1 αντίστοιχα.

2. Τα δύο σύμβολα αυτά συγχωνεύονται σε ένα σύμβολο με πιθανότητα ίση με το άθροισμα των πιθανοτήτων των συμβόλων αυτών. Με τον τρόπο αυτό το αλφάβητο μειώνεται κατά ένα σύμβολο. Το νέο σύμβολο τοποθετείται στη σωστή θέση με βάση την πιθανότητα που υπολογίστηκε.

3. Η διαδικασία επαναλαμβάνεται μέχρι να απομείνουν μόνο 2 σύμβολα. Στα σύμβολα αυτά αναθέτουμε τα δυαδικά ψηφία 0 και 1.

4. Οι κωδικές λέξεις για κάθε σύμβολο βρίσκονται ξεκινώντας από την τελευταία φάση, συλλέγοντας τα δυαδικά ψηφία που έχουμε αναθέσει μέχρι να καταλήξουμε στο αρχικό σύμβολο (στη φάση 1) στο οποίο αντιστοιχεί η κωδική λέξη.

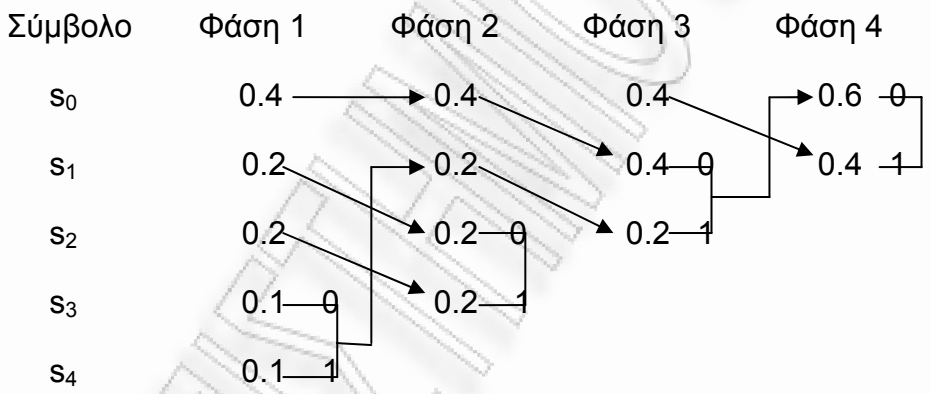
Παράδειγμα 3.7:

Να βρεθεί η κωδικοποίηση Huffman για μια διακριτή πηγή χωρίς μνήμη με αλφάβητο $\Phi = \{ s_0, s_1, s_2, s_3, s_4 \}$ και πιθανότητες συμβόλων $p_0 = 0.4, p_1 = 0.2, p_2 = 0.2, p_3 = 0.1, p_4 = 0.1$. Στη συνέχεια να

υπολογιστεί το μέσο μήκος κώδικα και η εντροπία της πηγής και να σχολιαστούν τα αποτελέσματα.

Λύση:

Καταρχάς, θα αναπαραστήσουμε τη διαδικασία εύρεσης της κωδικοποίησης Huffman για την πηγή που εξετάζουμε. Σύμφωνα λοιπόν με τον αλγόριθμο, διατάσουμε τα πέντε σύμβολα σε τάξη φθίνουσας πιθανότητας εκπομπής. Η πρώτη στήλη περιέχει τα σύμβολα και η δεύτερη στήλη (Φάση 1) τις πιθανότητες τους. Στο επόμενο βήμα, τα σύμβολα s_3 και s_4, με τις μικρότερες πιθανότητες, ενώνονται σε ένα με πιθανότητα ίση με το άθροισμα αυτών των πιθανοτήτων, δηλαδή ίση με 0.2. Τώρα διατάσσονται εκ νέου τα σύμβολα λαμβάνοντας υπόψη την ένωση των s_3 και s_4 στο s_3 , όπως φαίνεται στο παρακάτω σχήμα.



Στη συνέχεια τοποθετούμε σε έναν πίνακα τις κωδικές λέξεις που προκύπτουν από το σχήμα.

Σύμβολο	Πιθανότητα	Κωδική λέξη
s_0	0.4	0
s_1	0.2	10
s_2	0.2	11
s_3	0.1	10
s_4	0.1	11

Το μέσο μήκος του κώδικα θα είναι:

$\bar{L}$ = 0.4 · 2 + 0.2 · 2 + 0.2 · 2 + 0.1 · 3 + 0.1 · 3 = 2.2

Η εντροπία της πηγής θα είναι:

$H(\Phi) = 0.4 \log_2\left(\frac{1}{0.4}\right) + 0.2 \log_2\left(\frac{1}{0.2}\right) + 0.2 \log_2\left(\frac{1}{0.2}\right) + 0.1 \log_2\left(\frac{1}{0.1}\right) + 0.1 \log_2\left(\frac{1}{0.1}\right) \approx 2.12193$

Από τα παραπάνω αποτελέσματα, παρατηρούμε ότι το μέσο μήκος κώδικα $\bar{L}$ υπερβαίνει την εντροπία της πηγής μόνο κατά ένα ποσοστό 3.67%. Επίσης, παρατηρούμε ότι το μέσο μήκος κώδικα ικανοποιεί την ανισότητα $H(\Phi) \leq \bar{L} < H(\Phi) + 1$

3.3 Διακριτές πηγές πληροφορίας με μνήμη

Στην ενότητα 3.1 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%.

Λέμε λοιπόν, ότι μια διακριτή πηγή πληροφορίας **έχει μνήμη** όταν τα σύμβολα $A = \{a_1, a_2, ...a_k\}$ που εκπέμπονται από την πηγή δεν είναι ανεξάρτητα μεταξύ τους, δηλαδή η πιθανότητα εμφάνισης (εκπομπής) $P_A = \{p(a_i), i = 1, ...K\}$ ενός συμβόλου εξαρτάται από την εκπομπή ή όχι προηγούμενων συμβόλων.

Μια πηγή με μνήμη λέγεται m-τάξης αν η πιθανότητα εκπομπής ενός συμβόλου εξαρτάται από τα m προηγούμενα σύμβολα που έχουν ήδη εκπεμφθεί. Συγκεκριμένα, θα μιλάμε για πηγή πληροφορίας με μνήμη m-τάξης αν ισχύει:

$$p(a_i^{(k)}) \neq p(a_i^{(k)} \mid a_i^{(k-1)}, a_i^{(k-2)}, ..., a_i^{(k-m)}) \quad (3.18)$$

Αυτό συμβαίνει με πολλές φυσικές πηγές των οποίων το ‘σήμα’ προέρχεται, όπως λέμε, από αιτιοκρατικό (μη τελείως τυχαίο) στατιστικό φαινόμενο. Από

τα παραπάνω παρατηρούμε ότι η πηγή πληροφορίας χωρίς μνήμη είναι ουσιαστικά πηγή πληροφορίας με μνήμη μηδενικής τάξης.

Συνήθως, όμως, υποθέτουμε ότι η εξάρτηση υφίσταται για έναν περιορισμένο αριθμό συμβόλων. Έτσι, μπορούν να χρησιμοποιηθούν Μαρκοβιανές αλυσίδες ή αλυσίδες Markov ως στατιστικά υποδείγματα (μοντέλα) για τις πηγές πληροφορίας.

3.3.1 Πηγές Markov

Οι διαδικασίες Markov διακριτού χρόνου είναι ένα σύνολο τυχαίων μεταβλητών, X_n, όπου $n = 0,1,2.....$. Οι διαδικασίες Markov συνεχούς χρόνου είναι ένα σύνολο τυχαίων μεταβλητών $X(t_n)$, όπου $n = 0,1,2.....$.

Η τιμή της τυχαίας μεταβλητής, X_n $(X(t_n))$, της διαδικασίας Markov δείχνει την κατάσταση του συστήματος τη συγκεκριμένη χρονική στιγμή $n(t_n)$.

Η βασική ιδιότητα μιας διαδικασίας Markov είναι ότι η κατάσταση τη χρονική στιγμή $n+1(t_{n+1})$ εξαρτάται μόνο από την κατάσταση τη χρονική στιγμή $n(t_n)$ και όχι από τις καταστάσεις τις προηγούμενες χρονικές στιγμές.

Ορισμός Μαρκοβιανών Αλυσίδων Διακριτού Χρόνου. Μια Μαρκοβιανή Αλυσίδα Διακριτού Χρόνου είναι ένα σύνολο τυχαίων μεταβλητών, X_n, όπου $n = 0,1,2.....$. Η τιμή της τυχαίας μεταβλητής, X_n, της διαδικασίας Markov δείχνει την κατάσταση του συστήματος στη συγκεκριμένη χρονική στιγμή n.

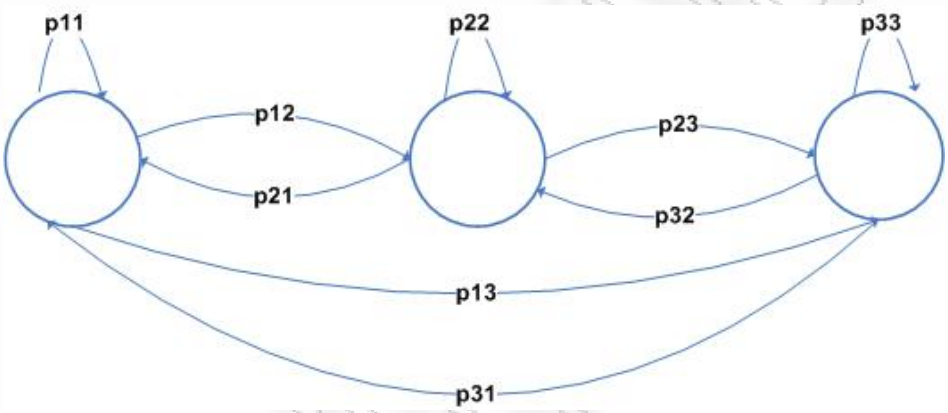
Η βασική ιδιότητα των διαδικασιών Markov, στην περίπτωση αλυσίδων διακριτού χρόνου, μπορεί να εκφρασθεί ως εξής:

$$P[X_{n+1} = j \mid X_n = i_n, ..., X_1 = i_1] = P(X_{n+1} = j \mid X_n = i_n] = P_{ij} \quad (3.19)$$

Η βασική ιδιότητα μιας διαδικασίας Markov είναι οτι η κατάσταση τη χρονική στιγμή $n+1$ εξαρτάται μόνο απο την κατάσταση τη χρονική στιγμή n, και όχι από τις καταστάσεις τις προηγούμενες χρονικές στιγμές.

Συνήθως η εκπομπή ενος συμβόλου από μια τέτοια πηγή πληροφορίας θεωρείται ως η μετάβαση της πηγής από μια κατάσταση σε μια άλλη. Έτσι, οι

εκπομπές των συμβόλων από μια πηγή με μνήμη, αναπαρίστανται με το λεγόμενο **διάγραμμα καταστάσεων** της πηγής. Οι κόμβοι του διαγράμματος καταστάσεων παριστάνουν τις καταστάσεις. Οι ακμές δίνουν τις δυνατές μεταβάσεις των καταστάσεων. Κάθε ακμή $(i, j) \in E$ σημαίνει οτι είναι δυνατή η μετάβαση, σε ένα βήμα απο την i στην j. **Μετάβαση** σε ένα βήμα σημαίνει ότι αν μια μαρκοβιανή αλυσίδα διακριτού χρόνου βρεθεί κάποια στιγμή στην κατάσταση i, τότε είναι πιθανόν την επόμενη χρονική στιγμή να βρεθεί στην κατάσταση j. Παρακάτω βλέπουμε το διάγραμμα καταστάσεων (με 3 καταστάσεις) για μια αλυσίδα Markov.



Εικόνα 9. Μαρκοβιανή αλυσίδα τριών καταστάσεων.

Το πόσο πιθανές είναι οι μεταβάσεις καθορίζεται από τον **πίνακα πιθανοτήτων μετάβασης** $\hat{P}$. Οι διαστάσεις του πίνακα είναι $|V| \times |V|$, όπου $|V|$ είναι το πλήθος των καταστάσεων. Έτσι, μια πηγή με v δυνατά σύμβολα (καταστάσεις), μπορεί να περιγραφεί με την επόμενη μήτρα πιθανοτήτων της μετάπτωσης P, δηλαδή:

$$\hat{P} = \begin{pmatrix} p_{11} & \cdots & p_{1v} \\ \vdots & \ddots & \vdots \\ p_{v1} & \cdots & p_{vv} \end{pmatrix} \quad (3.20)$$

Κάθε στοιχείο του πίνακα, p_{ij} λέγεται **πιθανότητα μετάβασης** και καθορίζει το πόσο πιθανή είναι η μετάβαση σε ένα βήμα από την κατάσταση i στη j. Γενικά, ισχύει

$$\sum_{j \in V} p_{ij} = 1, \forall i \in V . \quad (3.21)$$

Το ζητούμενο όταν αναλύουμε μια Μαρκοβιανή αλυσίδα διακριτού χρόνου είναι ένα διάνυσμα πιθανοτήτων $\hat{\pi} = [\pi_1, \pi_2, ..., \pi_{|v|}]$, το οποίο ονομάζεται **στατική κατανομή πιθανότητας** ή κατανομή μόνιμης κατάστασης (steady state distribution) ή κατανομή κατάστασης ισορροπίας (equilibrium state distribution). Η κάθε πιθανότητα $\pi_\iota \ (\forall \iota \in V)$ εκφράζει το πόσο πιθανή είναι η κάθε κατάσταση i ή, με άλλα λόγια, το ποσοστό του χρόνου που η μαρκοβιανή αλυσίδα διακριτού χρόνου θα βρίσκεται στην κατάσταση i. Ισχύει η σχέση $M_i = (1/\pi_i)$, όπου M_i είναι ο μέσος χρόνος επανάληψης (mean recurrence time) της κατάστασης i.

Το διάνυσμα πιθανοτήτων $\hat{\pi}$ δίνεται από το σύστημα εξισώσεων:

- $\hat{\pi} = \hat{\pi}\hat{P}$ (3.22α)
- $\sum_{i \in V} \pi_i = 1$ (3.23)

Το σύστημα $\hat{\pi} = \hat{\pi}\hat{P}$ αναλυτικότερα γράφεται:

$$[\pi_1, \pi_2, ..., \pi_{|v|}] = [\pi_1, \pi_2, ..., \pi_{|v|}] \begin{pmatrix} p_{11} & \cdots & p_{1v} \\ \vdots & \ddots & \vdots \\ p_{v1} & \cdots & p_{vv} \end{pmatrix} \quad (3.22\beta)$$

Το παραπάνω σύστημα μπορεί επίσης να γραφεί

$\pi_i = \sum_{j \in V} \pi_j \cdot p_{ji}$ για $\forall \iota \in V$ (3.22γ)

Από το παραπάνω σύστημα παίρνουμε $|V|$ εξισώσεις, οπότε σε συνδυασμό με τη σχέση (3.23) έχουμε ένα σύστημα $|V|+1$ εξισώσεων με $|V|$ αγνώστους.

Αγνοούμε μια εξίσωση από αυτές που προκύπτουν από το σύστημα (3.22β) ή (3.22γ), οπότε σε συνδυασμό με τη σχέση (3.23) έχουμε ένα σύστημα $|V|$ εξισώσεων με $|V|$ αγνώστους, το οποίο μπορεί να λυθεί με αντικατάσταση.

Αν τα στοιχεία της P δεν εξαρτώνται από το χρόνο, η Μαρκοβιανή πηγή είναι **στατική**. Στην πράξη αντιμετωπίζουμε μόνο τέτοιες πηγές. Δεν σημαίνει όμως

ότι κάθε στατική πηγή είναι και εργοδική, δηλαδή ότι η πραγματική πιθανότητα μετάπτωσης από κατάσταση σε κατάσταση είναι για μεγάλο χρονικό διάστημα αυτό που προβλέπει η P. Γενικότερα θα λέμε πως, μια Μαρκοβιανή πηγή είναι **εργοδική**, αν μετά από ένα ορισμένο αριθμό μεταπτώσεων, είναι και πάλι δυνατό να μεταπέσει από οποιαδήποτε κατάσταση σε οποιαδήποτε άλλη με **μη** μηδενική πιθανότητα. Οι πιθανότητες αυτές μάλιστα, τείνουν να αποκατασταθούν σε σταθερές τιμές και ίσες προς εκείνες του P.

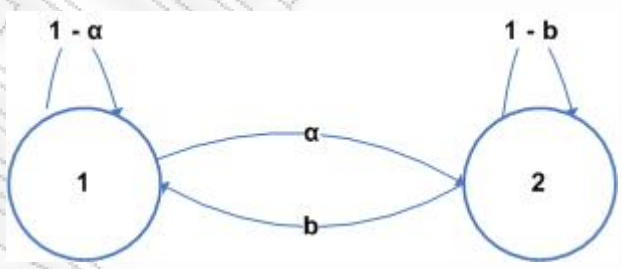
Παράδειγμα 3.8:

Ας θεωρήσουμε μια Μαρκοβιανή αλυσίδα με δύο καταστάσεις και με πίνακα

Μετάβασης, όπως φαίνεται παρακάτω.

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

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



Εικόνα 10. Μαρκοβιανή αλυσίδα δύο καταστάσεων.

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

$$\left[\ \pi_1 \quad \pi_2\ \right]\begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix} = \left[\ \pi_1(1\text{-}\alpha)+\pi_2 b \quad \pi_1\alpha+\pi_2(1\text{-}b\right] = \left[\ \pi_1 \quad \pi_2\ \right]$$

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

$$\pi_1(1\text{-}\alpha)+\pi_2 b=\pi_1 \Rightarrow -\pi_1\alpha+b\text{-}\pi_1 b=0 \Rightarrow \pi_1=\frac{b}{\alpha+b}$$

$$\pi_1\alpha+\pi_2(1\text{-}b)=\pi_2 \Rightarrow -\pi_2\alpha+\alpha\text{-}\pi_2 b=0 \Rightarrow \pi_2=\frac{\alpha}{\alpha+b}$$

3.3.2 Εντροπία των πηγών Markoff

Εντροπία της πηγής Markoff ορίζεται 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 παρακάτω σχέση:

$$H(K_i)=-\sum_{j=1}^{m} P_{ij}\log P_{ij}\ \ bits/symbol \quad (3.24)$$

Επομένως η εντροπία της πηγής, η οποία είναι ο μέσος όρος της εντροπίας των καταστάσεων, δίνεται από τον παρακάτω τύπο:

$$H(S)=\sum_{i=1}^{m} p_i H(K_i)=-\sum_{i=1}^{m} p_i \sum_{j=1}^{m} P_{ij}\log P_{ij}\ \ bits/symbol \quad (3.25)$$

Ο **μέσος ρυθμός πληροφορίας της πηγής** R δίνεται από τον παρακάτω τύπο:

$$R=r_s H(S)\ \ bits/\sec \quad (3.26)$$

Όπου r_s είναι ο ρυθμός εκπομπής συμβόλων της πηγής

Η μέση ποσότητα πληροφορίας μηνυμάτων της πηγής δίνεται από τη σχέση:

$$H(M) = -\sum_i p(m_i) \log p(m_i) \quad (3.27)$$

Όπου το άθροισμα αναφέρεται σε όλα τα μηνύματα μήκους N συμβόλων και $p(m_i)$ συμβολίζει την πιθανότητα εκπομπής του μηνύματος m_i.

Η μέση ποσότητα πληροφορίας των συμβόλων της πηγής ορίζεται αν διαιρέσουμε τη μέση ποσότητα πληροφορίας μηνυμάτων της πηγής με το μήκος τους και δίνεται από τη σχέση:

$$H_N = \frac{1}{N} H(M) \quad (3.28)$$

3.3.3 Ζητήματα κωδικοποίησης των Μαρκοβιανών πηγών

Στην ενότητα 3.1.1 ορίσαμε την έννοια του πλεονασμού, που αποτελεί μέτρο της ποιότητας της πηγής χωρίς μνήμη. Με τον ίδιο τρόπο, μπορούμε να ορίσουμε το **μέτρο του πλεονασμού εξάρτησης για πηγές με μνήμη**, που δίνεται από τον τύπο:

$$red_{\varepsilon\xi} = 1 - \frac{H_{\mu\varepsilon\mu\nu\acute{\eta}\mu\eta}(S)}{H_{\chi\omega\rho\acute{\iota}\varsigma\mu\nu\acute{\eta}\mu\eta}(S)} \quad (3.29)$$

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.

$$red_{o\lambda} = 1 - \frac{H_{\mu\varepsilon\mu\nu\acute{\eta}\mu\eta}(S)}{\max H_{\chi\omega\rho\acute{\iota}\varsigma\mu\nu\acute{\eta}\mu\eta}(S)} = 1 - \frac{H_{\mu\varepsilon\mu\nu\acute{\eta}\mu\eta}(S)}{\log q} \quad (3.30)$$

Παράδειγμα 3.9:

Μια διακριτή πηγή με μνήμη εκπέμπει τα σύμβολα χ, ψ και ω. Η πηγή χαρακτηρίζεται από τον ακόλουθο πίνακα μετάβασης.

$$P = \begin{bmatrix} 0.5 & 0 & 0.5 \\ 0 & 0.5 & 0.5 \\ 0.5 & 0.25 & 0.25 \end{bmatrix}$$

Ζητείται να υπολογιστούν:

a) Η εντροπία της πηγής,

b) Το μέσο πληροφοριακό περιεχόμενο μηνυμάτων αποτελούμενο από δύο σύμβολα,

c) Ο πλεονασμός, ο πλεονασμός εξάρτησης και ο ολικός πλεονασμός της διακριτής πηγής.

Λύση:

a) Για τον υπολογισμό των πιθανοτήτων παραγωγής των χ, ψ, ω επιλύουμε σύστημα τεσσάρων εξισώσεων με τρεις αγνώστους . Θεωρούμε $\pi_1 = p(x)$, $\pi_2 = p(\psi)$, $\pi_3 = p(\omega)$

$$\pi_1 = \pi_1 P(x/x) + \pi_2 P(x/\psi) + \pi_3 P(x/\omega) = \pi_1(0.5) + \pi_2 0 + \pi_3(0.5) \quad (1)$$

$$\pi_2 = \pi_1 P(\psi/\chi) + \pi_2 P(\psi/\psi) + \pi_3 P(\psi/\omega) = \pi_1(0) + \pi_2(0.5) + \pi_3(0.25) \quad (2)$$

$$\pi_3 = \pi_1 P(\omega/\chi) + \pi_2 P(\omega/\psi) + \pi_3 P(\omega/\omega) = \pi_1(0.5) + \pi_2(0.5) + \pi_3(0.25) \quad (3)$$

$$\pi_1 + \pi_2 + \pi_3 = 1 \quad (4)$$

Από την σχέση (1) έχουμε:

$$0.5\pi_1 = 0.5\pi_3 \Rightarrow \pi_1 = \pi_3$$

Από την σχέση (2) έχουμε:

$$0.5\pi_2 = 0.25\pi_3 \Rightarrow 2\pi_2 = \pi_3$$

Αντικαθιστώντας τα αποτελέσματα αυτά στη σχέση (4) λαμβάνουμε:

$$\pi_3 + 0.5\pi_3 + \pi_3 = 1 \Rightarrow \pi_3 = 0.4$$

Αντικαθιστώντας στη σχέση (1) και στη σχέση (2) έχουμε:

$\pi_1 = 0.4$ και $\pi_2 = 0.2$

Για τον υπολογισμό της εντροπίας της πηγής Markoff, υπολογίζουμε την εντροπία των συμβόλων που εκπέμπεται από κάθε κατάσταση.

$$\mathrm{H}(\mathrm{K}_1) = -0.5\log 0.5 - 0 - 0.5\log 0.5 = 1$$

$$\mathrm{H}(\mathrm{K}_2) = -0 - 0.5\log 0.5 - 0.5\log 0.5 = 1$$

$$\mathrm{H}(\mathrm{K}_3) = -0.5\log 0.5 - 0.25\log 0.25 - 0.25\log 0.25 = 1.5$$

Για να υπολογίζουμε την εντροπία της πηγής αρκεί να υπολογίσουμε τη μέση τιμή των παραπάνω, λαμβάνοντας υπόψη και τη βαρύτητα καθεμίας κατάστασης (δηλαδή την πιθανότητα της).

$$H(S) = 0.4\times 1 + 0.2\times 1 + 0.4\times 1.5 = 1.2 \;\; bits/symbol$$

b) Για να υπολογίσουμε το μέσο πληροφοριακό περιεχόμενο μηνυμάτων αποτελούμενων από δύο σύμβολα, πρέπει πρώτα να υπολογίσουμε τις πιθανότητες όλων των δυνατών μηνυμάτων μήκους δύο συμβόλων .

Για τον υπολογισμό της πιθανότητας του μηνύματος (χ,χ), η οποία είναι συνδυασμένη πιθανότητα, αρκεί να πολλαπλασιάσουμε την πιθανότητα p(x) με την πιθανότητα P(ψ/χ), δηλαδή

$$p(m_1) = p(x,x) = \pi_1 P_{11} = \pi_1 P(x/x) = 0.4\times 0.5 = 0.02$$

Με τον ίδιο τρόπο υπολογίζουμε και τις πιθανότητες των άλλων 8 μηνυμάτων. Έτσι λαμβάνουμε:

$$p(m_1) = p(x,x) = \pi_1 P_{11} = \pi_1 P(x/x) = 0.2$$

$$p(m_2) = p(x,\psi) = \pi_1 P_{12} = \pi_1 P(\psi/x) = 0$$

$$p(m_3) = p(x,\omega) = \pi_1 P_{13} = \pi_1 P(\omega/x) = 0.2$$

$$p(m_4) = p(\psi,\chi) = \pi_2 P_{21} = \pi_2 P(\chi/\psi) = 0$$

$$p(m_5) = p(\psi,\psi) = \pi_2 P_{22} = \pi_2 P(\psi/\psi) = 0.1$$

$$p(m_6) = p(\psi,\omega) = \pi_2 P_{23} = \pi_2 P(\omega/\psi) = 0.1$$

$$p(m_7) = p(\omega,\chi) = \pi_3 P_{31} = \pi_3 P(\chi/\omega) = 0.2$$

$$p(m_8) = p(\omega,\psi) = \pi_3 P_{32} = \pi_3 P(\psi/\omega) = 0.1$$

$$p(m_9) = p(\omega,\omega) = \pi_3 P_{33} = \pi_3 P(\omega/\omega) = 0.1$$

Στη συνέχεια εφαρμόζουμε τον τύπο για τον υπολογισμό της ζητούμενης μέσης ποσότητας πληροφορίας.

$$\mathrm{H(M)} = -p(m_1)\log p(m_1) - p(m_2)\log p(m_2) - .... - p(m_9)\log p(m_9) = 2.72 bits / message$$

Ισχύει ακόμα:

$$H(M) = H(X,Y) = H(X) + H(S) = H_{\chi\omega\rho\acute{\iota}\varsigma\mu\nu\acute{\eta}\mu\eta}(S) + H(S) = 1.52 + 1.2 = 2.72 bits / message$$

c) Για τον υπολογισμό του πλεονασμού, του πλεονασμού εξάρτησης και του ολικού πλεονασμού υπολογίζουμε πρώτα την εντροπία πηγής χωρίς μνήμη.

$$H_{\chi\omega\rho\acute{\iota}\varsigma\mu\nu\acute{\eta}\mu\eta}(S) = -0.4\log 0.4 - 0.2\log 0.2 - 0.4\log 0.4 = 1.52 bits / symbol$$

Αφού έχουμε 3 σύμβολα, η μέγιστη εντροπία της πηγής χωρίς μνήμη είναι log3=1.585 bits

Άρα:

$$red = 1 - (1.52 / 1.585) = 0.0041$$

$$red_{\varepsilon\xi} = 1 - (1.2 / 1.52) = 0.210$$

$$red_{o\lambda} = 1 - (1.2 / 1.585) = 0.243$$

Ασκήσεις:

1. Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο $S = \{a, \beta, \gamma, \delta, \varepsilon, \zeta, \eta\}$. Οι πιθανότητες των συμβόλων αυτών είναι 1/32, 1/16, 1/8, 1/8, 1/8, 1/2 και 1/32 αντίστοιχα.

1. το μέσο πληροφοριακό περιεχόμενο των συμβόλων της πηγής
2. το μέσο πληροφοριακό περιεχόμενο των μηνυμάτων της πηγής αποτελούμενων από δύο σύμβολα
3. Τον πλεονασμό της πηγής
4. Το μέσο ρυθμό πληροφορίας της πηγής για ρυθμό 12500 σύμβολα/sec

2. Η έξοδος μιας στατικής πηγής πληροφορίας χωρίς μνήμη, εκπέμπει 128 σύμβολα. Τα 16 σύμβολα από αυτά έχουν πιθανότητα εμφάνισης $\frac{1}{32}$ και έχουν χρονική διάρκεια t. Τα υπόλοιπα σύμβολα είναι ισοπίθανα και έχουν διάρκεια εκπομπής 2t. Η πηγή εκπέμπει χωρίς κενά.

1. Υπολογίστε την εντροπία της πηγής (H_π)

2. Ποιος ο ρυθμός παροχής της πηγής (R_π)

3. Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο $S = \{\varphi, \chi, \psi, \omega\}$. Οι πιθανότητες των συμβόλων αυτών είναι $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}$ αντίστοιχα. Θεωρώντας την πηγή χωρίς μνήμη, ζητείτε να υπολογίσετε:

1. Το μέσο πληροφοριακό περιεχόμενο των συμβόλων της πηγής
2. Το μέσο πληροφοριακό περιεχόμενο των μηνυμάτων της πηγής αποτελούμενων από δύο σύμβολα
3. Τον πλεονασμό της πηγής
4. Το μέσο ρυθμό πληροφορίας της πηγής για ρυθμό 15 συμβόλων/sec

4. Θεωρούμε μια πηγή τριών διακριτών συμβόλων χωρίς μνήμη (Discrete Memoryless Source, DMS) με αλφάβητο

$$\Phi = \{S_0, S_1, S_2\}$$

όπου οι πιθανότητες εμφάνισης των συμβόλων είναι:

$$p(S_0) = p_o = 0.4,\ p(S_1) = p_1 = 0.3,\ p(S_2) = p_2 = 0.3$$

Ακόμα γνωρίζουμε ότι η πηγή αυτή παράγει σύμβολα με ρυθμό $r_s = 1000 symbol/\sec$. Να υπολογίσετε την εντροπία της πηγής και το μέσο ρυθμό πληροφορίας στην έξοδο της πηγής.

5. Θεωρούμε τώρα τη δεύτερης τάξης επέκταση της πηγής της άσκησης 4. Η νέα πηγή θα αποτελείται από $3^2 = 9$ σύμβολα και πιο συγκεκριμένα το νέο αλφάβητο θα είναι το $\Phi^2 = \{S_0S_0, S_0S_1, S_0S_2, S_1S_0, ..., S_2S_2\} = \{\sigma_0, \sigma_1, ..., \sigma_8\}$

Για την πηγή αυτή, να υπολογιστεί η εντροπία και ο μέσος ρυθμός πληροφορίας

6. Η εικόνα μιας ασπρόμαυρης τηλεόρασης αποτελείται από 500·600 pixels. Κάθε ένα από αυτά μπορεί να λαμβάνει 8 διαφορετικούς τόνους φωτεινότητας. Αν η μείωση της εντροπίας της πηγής εξαιτίας της μη ισοπίθανης χρησιμοποίησης των τόνων φωτεινότητας και αφετέρου εξαιτίας του πλεονασμού είναι 80%, τότε για μια ικανοποιητική παρακολούθηση εικόνας (30 εικόνες/sec) υπολογίστε ποιος είναι ο ρυθμός πληροφορίας R ο οποίος φτάνει στον εγκέφαλο ενός προσεκτικού παρατηρητή.

7. Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο $S = \{\tau, \upsilon, \varphi, \chi, \psi, \omega\}$. Οι πιθανότητες των συμβόλων αυτών είναι 1/4, 1/4, 1/8, 1/8, 1/8 και 1/8 αντίστοιχα. Θεωρώντας τη πηγή χωρίς μνήμη ζητείται να υπολογίσετε:

1. Το μέσο πληροφοριακό περιεχόμενο των συμβόλων της πηγής
2. το μέσο πληροφοριακό περιεχόμενο των μηνυμάτων της πηγής αποτελούμενων από δύο σύμβολα
3. Τον πλεονασμό της πηγής $(\log 6 = 2.585)$
4. Το μέσο ρυθμό πληροφορίας της πηγής για ρυθμό 500 σύμβολα/sec

8. Η έξοδος μιας έγχρωμης ψηφιακής κάμερας η οποία έχει ανάλυση 500×400 εικονοστοιχεία (pixels) κωδικοποιείται με χρήση παλέτας 256 χρωμάτων. Αν υποθέσουμε ότι οι τιμές των γειτονικών pixels είναι μεταξύ τους στατιστικά ανεξάρτητες και ότι σε κάθε pixel τα 256 επίπεδα εμφανίζονται με τις εξής πιθανότητες:

Περιοχή επιπέδων	0- 99	100-149	150- 209	210-255
Πιθανότητα εμφάνισης	0.1	0.5	0.3	0.1

Υποθέτουμε ακόμα πως στα πλαίσια κάθε περιοχής τα χρώματα εμφανίζονται ισοπίθανα. Να υπολογιστούν:

1. Το μέσο πληροφοριακό περιεχόμενο κάθε pixel
2. Το ολικό πληροφοριακό περιεχόμενο μιας εικόνας
3. Ο μέσος ρυθμός πληροφορίας στην έξοδο της κάμερας αν γνωρίζουμε πως αυτή δίνει $r = 25 frame / \sec$

9. Ο διεθνής κώδικας Morse χρησιμοποιεί μια ακολουθεία από τελείες και παύλες για τη μετάδοση του αγγλικού αλφαβήτου. Η παύλα παριστάνεται με ένα παλμό ρεύματος διάρκειας 3 msec και η τελεία με έναν παλμό ρεύματος διάρκειας 1 msec. Η πιθανότητα εμφάνισης της παύλας είναι το 1/3 της πιθανότητας εμφάνισης της τελείας.

(α) Υπολογίστε το πληροφοριακό περιεχόμενο της τελείας και της παύλας.

(β) Υπολογίστε τη μέση πληροφορία του κώδικα.

(γ) Αν μεταξύ κάθε δύο συμβόλων παρεμβάλλεται ένα διάστημα παύσης 1 msec, υπολογίστε το μέσο ρυθμό μετάδοσης πληροφορίας.

$$R = r \cdot H = 324.4 bits / \sec$$

10.Θεωρούμε τους ακόλουθους κώδικες I, II, III, και IV:

	I	II	III	IV
φ	0	00	1	1
χ	10	01	10	01
ψ	01	10	100	001
ω	1	11	1000	0001

Ζητείται να εξετάσετε αν οι κώδικες I, II, III και IV είναι:

1. μη – ιδιάζοντες
2. μοναδικά αποκωδικοποιήσιμοι
3. άμεσοι

11.Έστω ένας Μ – αδικός ευκρινής κώδικας σταθερού μήκους (k κωδικών λέξεων μήκους l η κάθε μία). Στον κώδικα αυτόν, προσθέτω μια ακόμα κωδική λέξη ίδιου μήκους l.

α) Τι πρέπει να προσέξουμε στην κατασκευή της νέας κωδικής λέξης έτσι ώστε ο νέος κώδικας να είναι στιγμιαία αποκωδικοποιήσιμος;

β) Σε ποια περίπτωση δεν μπορεί να κατασκευαστεί στιγμιαία αποκωδικοποιήσιμος κώδικας με τον παραπάνω τρόπο;

12. Ζητείται να εξεταστεί αν οι ακόλουθοι κώδικες είναι ευκρινείς, μονοσήμαντοι και στιγμιαία αποκωδικοποιήσιμοι:

1. $\{0,10,11,01\}$
2. $\{00,10,01,11\}$
3. $\{0,1,10,01\}$
4. $\{11,10,110,1110\}$
5. $\{0,10,110,1110\}$
6. $\{11,00,100,110\}$
7. $\{110,11,10\}$
8. $\{1,10,01\}$

13. Δίδεται πηγή που εκπέμπει τα σύμβολα $A=\{\alpha,\beta,\gamma,\delta\}$ με πιθανότητες εμφάνισης $\{0.6,0.3,0.08,0.02\}$, αντίστοιχα.

1. Να δείξετε ότι **δεν** υπάρχει άμεσος και μοναδικά αποκωδικοποιήσιμος δυαδικός κώδικας με μήκη κωδικών λέξεων $\{1,2,2,3\}$.
2. Να βρεθεί ένας βέλτιστος μοναδικά αποκωδικοποιήσιμος δυαδικός κώδικας. Ποια είναι η βέλτιστη και ποια η ελάχιστη τιμή του μέσου μήκους κωδικής λέξης; Σε ποια περίπτωση ο βέλτιστος κώδικας παράγει μήκη κωδικών λέξεων που είναι επίσης ελάχιστα; Δώστε ένα τέτοιο παράδειγμα

14. Μια πηγή παράγει 10 διαφορετικά σύμβολα , τα $\mathrm{A},\mathrm{B},\Gamma,\Delta,\mathrm{E},\mathrm{Z},\mathrm{H},\Theta,\mathrm{I},\mathrm{K}$ με πιθανότητες $0.25,0.125,0.125,0.125,0.0625,0.0625,0.0625,0.0625,0.0625,0.0625$ αντίστοιχα. Ζητούνται τα ακόλουθα:

1. Η εντροπία της πηγής
2. Να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Fano, με δυαδικό κωδικό αλφάβητο.
3. Να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Shannon, με δυαδικό κωδικό αλφάβητο.
4. Οι επιδόσεις των κωδίκων που προκύπτουν από τα ερωτήματα 2 και 3

15. Μια πηγή παράγει 8 διαφορετικά σύμβολα, τα $\mathrm{A},\mathrm{B},\Gamma,\Delta,\mathrm{E},\mathrm{Z},\mathrm{H},\Theta$ με πιθανότητες $\frac{1}{8},\frac{1}{4},\frac{1}{16},\frac{1}{32},\frac{1}{4},\frac{1}{32},\frac{1}{8},\frac{1}{8}$ αντίστοιχα. Ζητούνται τα ακόλουθα:

1. Να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Huffman, με δυαδικό κωδικό αλφάβητο.
2. Να υπολογιστεί και να σχολιαστεί η επίδοση του κώδικα Huffman

16. Για την πηγή της Άσκησης 15, ζητούνται τα ακόλουθα:

1. Να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Fano, με δυαδικό κωδικό αλφάβητο
2. Να σχηματιστεί κώδικας σύμφωνα με τον αλγόριθμο του Shannon, με δυαδικό κωδικό αλφάβητο.

17. Θεωρούμε μια τυχαία μεταβλητή (πηγή) που παίρνει (παράγει) 4 διαφορετικές τιμές (σύμβολα) με πιθανότητες $\{\frac{1}{3},\frac{1}{3},\frac{1}{4},\frac{1}{12}\}$ Ζητούνται τα ακόλουθα:

1. Να σχηματιστεί δυαδικός κώδικας σύμφωνα με τον αλγόριθμο του Huffman για την πηγή αυτή
2. Να δείξετε ότι υπάρχουν δύο βέλτιστα σύνολα μηκών των 4 κωδικών λέξεων, τα $(1,2,3,3)$ και $(2,2,2,2)$

Επίσης ζητείται :

3. Να εξεταστεί ποιοι από τους ακόλουθους κώδικες και για πιο λόγο δεν μπορεί να προκύψουν σύμφωνα με τον αλγόριθμο κωδικοποίησης του Huffman για καμιά συνάρτηση πιθανότητας μάζας πηγής (PMF) που παράγει 2, 3 και 4 σύμβολα , αντίστοιχα: $\{01,10\},\{0,10,11\},\{00,01,10,11\}$

18. Για την πηγή της άσκησης 4, να βρεθεί η κωδικοποίηση Huffman, το μέσο μήκος του κώδικα και η απόδοση της κωδικοποίησης Huffman.

19. Για την πηγή της άσκησης 5, να βρεθεί η κωδικοποίηση Huffman και να υπολογιστεί η κωδικοποίηση της πηγής αυτής.

20. Έστω μια πηγή Α που εκπέμπει 6 σύμβολα είτε με τις πιθανότητες που δίνονται στη στήλη A_1 είτε με αυτές που δίνονται στη στήλη A_2.

Σύμβολο	Πιθανότητα Α1	Πιθανότητα Α2
Α	0,4	0,3
Β	0,25	0,15
Γ	0,1	0,15
Δ	0,1	0,15
Ε	0,1	0,15
Ζ	0,05	0,1

1. Να κατασκευάσετε το δενδροδιάγραμμα μετά την εφαρμογή του αλγορίθμου Huffman, να γράψετε τις κωδικές λέξεις για κάθε σύμβολο του Α (σύμφωνα με τις πιθανότητες A_1) και να υπολογίσετε το μέσο μήκος του κώδικα.
2. Να κατασκευάσετε το δενδροδιάγραμμα μετά την εφαρμογή του αλγορίθμου Huffman, να γράψετε τις κωδικές λέξεις για κάθε σύμβολο του Α (σύμφωνα με τις πιθανότητες A_2) και να υπολογίσετε το μέσο μήκος του κώδικα.
3. Αν δεν γνωρίζουμε εξαρχής αν οι πιθανότητες της πηγής είναι οι A_1 οι A_2 αλλά γνωρίζουμε οτι μπορεί να είναι οι A_1 με πιθανότητα 0.3 και οι A_2 με πιθανότητα 0.7, ποιον κώδικα θα επιλέγατε για την κωδικοποίηση της πηγής , αυτόν που βρήκατε στο ερώτημα α ή αυτόν που βρήκατε στο ερώτημα 2;

21. Μια πηγή Markoff εκπέμπει τα σύμβολα α, β και γ. Η πηγή χαρακτηρίζεται από τον ακόλουθο πίνακα μετάβασης (Μαρκοβιανή αλυσίδα πρώτης τάξης):

$$P = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

Ζητείται να υπολογιστούν:

1. Οι πιθανότητες εκπομπής των συμβόλων α, β και γ δηλαδή οι p(α), p(β) και p(γ).
2. Η εντροπία της πηγής
3. Το μέσο πληροφοριακό περιεχόμενο μηνυμάτων αποτελούμενο από δύο σύμβολα

4. Ο πλεονασμός, ο πλεονασμός εξάρτησης και ο ολικός πλεονασμός της διακριτής πηγής.

22. Εστω 5 σύμβολα A, B, C, D και E και ο πίνακας μετάπτωσης

$$P = \begin{bmatrix} 0.25 & 0.5 & 0.75 & 0.5 & 0.00 \\ 0.375 & 0.00 & 0.00 & 0.5 & 0.00 \\ 0.25 & 0.25 & 0.00 & 0.00 & 0.50 \\ 0.125 & 0.00 & 0.25 & 0.00 & 0.00 \\ 0.00 & 0.25 & 0.00 & 0.00 & 0.50 \end{bmatrix}$$

α) Να φτιάξετε το διάγραμμα μετάπτωσης

β) Ποια η εντροπία της πηγής με μνήμη;

Επίλογος

Στην παρούσα διπλωματική εργασία παρουσιάσαμε βασικές αρχές της Θεωρίας της πληροφορίας στις τηλεπικοινωνίες. Η θεωρία της πληροφορίας μπορεί να χαρακτηριστεί ώς η μελέτη της μετάδοσης και συμπίεσης δεδομένων, και ώς εκ τούτου βρίσκει εφαρμογή και στη ασφάλεια δικτύων. Οριο της συμπίεσης δεδομένων αποτελεί η ποσότητα πληροφορίας ή εντροπία και του ρυθμού μετάδοσης σε ένα κανάλι η χωρητικότητα του.

Ο πρώτος που διατύπωσε ορισμό ενός μέτρου ποσότητας πληροφορίας είναι ο Hartley. Ακολούθησαν οι εργασίες του Shannon και Wiener. Ιδιαίτερα ο Shannon, συσχετίζοντας το μέτρο της πληροφορίας με την έννοια της πιθανότητας, θεωρείται ως ο πατέρας της σύγχρονης Θεωρίας της Πληροφορίας.

Σε κάθε επικοινωνία λαμβάνει χώρα μεταφορά πληροφορίας από μια πηγή σε 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 να γίνει κατάλληλη επεξεργασία ή κωδικοποίηση στη πλευρά του μεταδότη και επομένως αποκωδικοποίηση στον αποδέκτη. Επίσης, για την καλύτερη αξιοποίηση ενός επικοινωνιακού καναλιού με περιορισμένη χωρητικότητα, η πληροφορία υποβάλλεται στην πλευρά του αποστολέα σε συμπίεση και στην πλευρά του 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.

Οι πηγές πληροφορίας χωρίζονται σε διακριτές πηγές πληροφορίας χωρίς μνήμη και διακριτές πηγές πληροφορίας με μνήμη. 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.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αγγλική Βιβλιογραφία:

- ✓ Wiley.Interscience.Elements.of.Information.Theory.Jul.2006
- ✓ Information Theory, Inference, and Learning Algorithms, David J.C. MacKay, University Press 2003
- ✓ Information Science, David G. Luenberger, Princeton University Press, Princeton and Oxford
- ✓ Contemporary Communication Systems using MATLAB, John J. Proakis – Masoud Salehi, BookWare Companion Series
- ✓ A Mathematical Theory of Communication, By C. E. SHANNON

Ελληνική Βιβλιογραφία:

- ✓ Αθανάσιος Χρ. Τζέμος :Τομέας Θεωρητικής Φυσικής, Εντροπία Shannon
- ✓ Θεωρία Πληροφοριών – Κώδικες, Βούκαλης Δημήτρης, ION 1994
- ✓ Τηλεπικοινωνιακά Συστήματα, Taub/Schilling, Εκδόσεις Α. Τζιόλα Ε.
- ✓ Θεωρία Πληροφοριών και Κωδίκων, Χρυσουλίδης
- ✓ Θεωρία Πληροφορίας και Κωδικοποίησης, ΒΑΣΙΛΕΙΟΣ ΖΟΡΚΑΔΗΣ, ΠΑΤΡΑ 2002