Θεωρία Πληροφοριών και Κωδίκων

Π Ι Ν Α Κ Α Σ Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Ω Ν

Κεφάλαιο Ένα

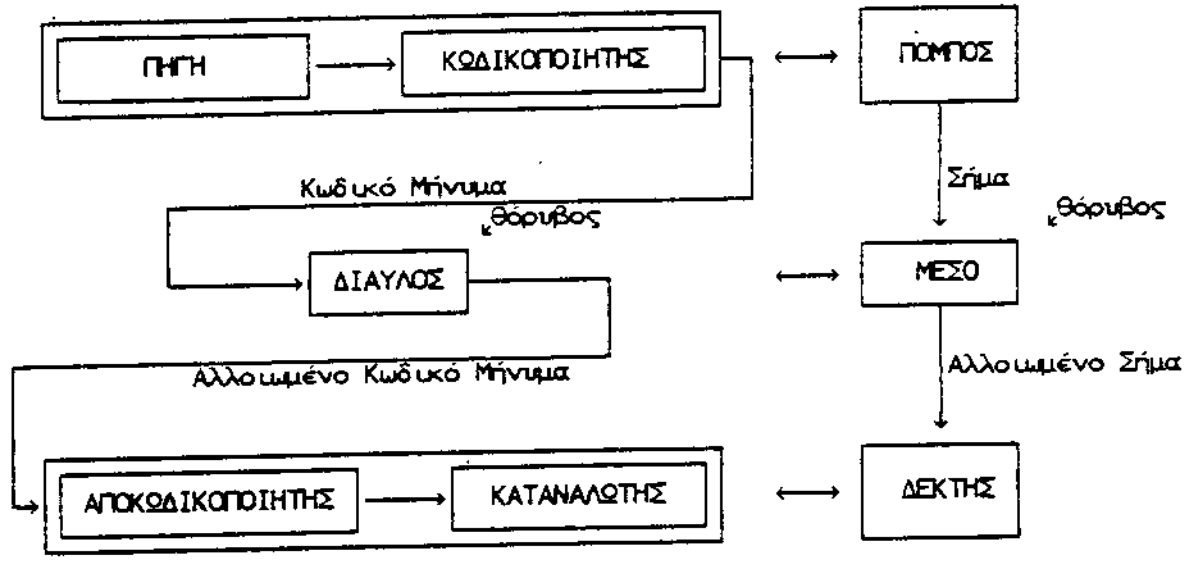
ΠΛΗΡΟΦΟΡΙΑ - ΕΝΤΡΟΠΙΑ

1.1 ΕΙΣΑΓΩΓΗ

Η *Θεωρία Πληροφοριών* αναγνωρίσθηκε σαν ιδιαίτερη επιστημονική περιοχή μετά τη δημοσίευση των κλασσικών εργασιών του C.E. Shannon με τίτλο *A Mathematical Theory of Communication* το 1948. Η γέννηση της είναι χαρακτηριστικό παράδειγμα της αλληλεπίδρασης μεταξύ θεωρίας και πράξης. Το πλέγμα των εννοιών και θεωρημάτων που συνθέτουν τη θεωρία πληροφοριών διαμορφώθηκε από την ανάγκη για περισσότερη και καλύτερη επικοινωνία. Από την άποψη της εφαρμογής η θεωρία πληροφοριών είναι αναπόσπαστο τμήμα της επιστήμης των τηλεπικοινωνιών. Το υπόβαθρο της περιλαμβάνει μεταξύ άλλων τη στατιστική, τη θεωρία πιθανοτήτων, την άλγεβρα συνδυασμών και την άλγεβρα των πεπερασμένων πεδίων. Από την άποψη της δομής και του περιεχομένου της είναι επομένως τμήμα των μαθηματικών. Σε σχετικά σύντομο χρονικό διάστημα η θεωρία πληροφοριών αναπτύχθηκε σε ανεξάρτητη επιστήμη με συμβολή σε επιστήμες και θέματα πέρα από τις παραδοσιακές περιοχές των τηλεπικοινωνιών και των μαθηματικών. Αρχές, μεθοδολογίες και συμπεράσματα της θεωρίας πληροφοριών βρίσκουν εφαρμογές στην βιολογική κυβερνητική, στη γενετική τεχνολογία, στη γλωσσολογία, στη σχεδίαση ηλεκτρονικών υπολογιστών, στην αυτοματοποίηση μηχανικών εργασιών, στην ανάπτυξη συστημάτων τεχνητής νοημοσύνης στη διοικητική συστημάτων παραγωγής και στη λήψη τακτικών αποφάσεων.

Η συμβολή του Shannon στην κατανόηση του προβλήματος της επικοινωνίας ήταν καταλυτική. Στις εργασίες του περιγράφεται η σύγχρονη, μακροσκοπική, στατιστική

λειτουργία του συστήματος επικοινωνίας (σχ. 1.1), που περιλαμβάνει *πηγή πληροφορίας, κωδικοποιητή, δίαυλο πληροφορίας, αποκωδικοποιητή* και τελικά τον *καταναλωτή* της πληροφορίας. Είναι φανερό ότι η πηγή πληροφορίας και ο κωδικοποιητής βρίσκονται στην περιοχή του *πομπού* ενώ η αποκωδικοποίηση και αξιοποίηση της πληροφορίας γίνεται στο *δέκτη*. Η *πληροφορία*, που έχει τη μορφή *συμβόλων, λέξεων* και *μηνυμάτων*, αντιστοιχεί στο *σήμα* ενώ ο *δίαυλος πληροφορίας* αντιστοιχεί στο *μέσο* που διοχετεύει το σήμα από τον πομπό στο δέκτη.



Σχ. 1.1 Το σύστημα επικοινωνίας από την άποψη της θεωρίας πληροφοριών και από την άποψη των τηλεπικοινωνιών.

Μέχρι το 1948 κάθε τηλεπικοινωνιακός μηχανικός θα υποστήριζε σθεναρά την άποψη ότι για να βελτιωθεί η αξιοπιστία της επικοινωνίας είναι απαραίτητο να ελαττωθεί ο ρυθμός μετάδοσης της πληροφορίας ή, αντίστροφα, ότι το πλήθος των σφαλμάτων αυξάνει με το ρυθμό μετάδοσης του μηνύματος. Ο Shannon απέδειξε ότι είναι δυνατό να βελτιστοποιηθούν ταυτόχρονα η αξιοπιστία και ο ρυθμός μετάδοσης της πληροφορίας, δηλαδή να επιταχυνθεί η επικοινωνία μέχρι το άνω φράγμα του ρυθμού μετάδοσης, που χαρακτηρίζεται *χωρητικότητα* του διαύλου πληροφορίας, και ταυτόχρονα να μηδενισθεί η πιθανότητα σφάλματος. Οι ιδέες του Shannon αξιοποιήθηκαν από πλήθος ερευνητών, τόσο τηλεπικοινωνιακών μηχανικών όσο και μαθηματικών, που διαμόρφωσαν σε σχετικά λίγα χρόνια τη νέα επιστήμη της θεωρίας πληροφοριών.

Κάθε νέα επιστήμη εισάγει και χρησιμοποιεί νέες έννοιες (π.χ. ραδιόφωνο, ακτίνες Χ, ολίσθηση Doppler), που περιγράφονται είτε με νέες λέξεις που αποδίδουν το περιεχόμενο της έννοιας είτε με γνωστές λέξεις που αποκτούν νέο περιεχόμενο.

Είναι φανερό ότι η λέξη *πληροφορία* έχει διαφορετικό περιεχόμενο από εκείνο της καθημερινής χρήσης στο πλαίσιο της θεωρίας πληροφοριών και είναι λογικό να μη γνωρίζει κανείς το νέο περιεχόμενο πριν μιηθεί στη νέα επιστήμη.

ΠΑΡΑΔΕΙΓΜΑ : Εστω ότι τηλεγράφημα του Reuter ανακοινώνει *σεισμό στο χρηματιστήριο του Λονδίνου*. Είναι σαφές ότι δεν κλονίσθηκε από σεισμό το κτίριο του χρηματιστηρίου στο Λονδίνο αλλά ότι ο γενικός δείκτης τιμών FTSE100 διακυμάνθηκε σημαντικά. Αν ο γενικός δείκτης τιμών του χρηματιστηρίου του Λονδίνου διακυμαίνεται από ημέρα σε ημέρα κατά ± 5 μονάδες, τότε η είδηση εξυπονοεί διακύμανση τουλάχιστο ± 50 μονάδων.

Η πληροφορία είναι ένα αφηρημένο μέγεθος που συνοδεύει κάθε γεγονός. Δεν είναι τόσο χαρακτηριστικό του γεγονότος όσο της πειραματικής διαδικασίας που παράγει το γεγονός. Η πληροφορία μετρά την αβεβαιότητα για την εμφάνιση του γεγονότος με κάθε επανάληψη του πειράματος και είναι προφανές ότι δεν υπάρχει πληροφορία αν το πείραμα παράγει μόνο ένα γεγονός. Στο πλαίσιο της θεωρίας πληροφοριών η λέξη πληροφορία περιέχει το μέτρο της αβεβαιότητας για κάποιο γεγονός ενώ στην καθημερινή χρήση η λέξη πληροφορία περιέχει την είδηση για το γεγονός που συνέβη. Επομένως η λέξη πληροφορία έχει *ποσοτικό* περιεχόμενο στη θεωρία πληροφοριών και *ποιοτικό* περιεχόμενο στην καθημερινή χρήση.

Η αβεβαιότητα για κάποιο γεγονός συνδέεται με την πιθανότητα να συμβεί σαν αποτέλεσμα της σχετικής πειραματικής διαδικασίας που μπορεί να το παράγει. Δύο διαφορετικά γεγονότα που συμβαίνουν με την ίδια πιθανότητα συνοδεύονται στο πλαίσιο της θεωρίας πληροφοριών από την ίδια ποσότητα πληροφορίας.

ΠΑΡΑΔΕΙΓΜΑ : Εστω ότι η πιθανότητα για σεισμό ισχυρότερο από 5 Richter στην Ελλάδα είναι 0.1 % . Αυτό σημαίνει ότι σε κάθε χιλιάδα σεισμών στη χώρα μας αναμένεται να υπάρχει ένας με μέγεθος μεγαλύτερο από 5 Richter. Εστω ακόμη ότι η πιθανότητα να αρρωστήσει κάποιος Ελληνας από απλό κρυολόγημα είναι επίσης 0.1 % . Τα δύο γεγονότα συνοδεύονται από την ίδια ποσότητα πληροφορίας στο πλαίσιο της θεωρίας πληροφοριών επειδή έχουν την ίδια πιθανότητα. Ενώ όμως στις καθημερινές ειδήσεις των 2100 στην τηλεόραση είναι λογικό να ανακοινωθεί ότι έγινε σεισμός ισχύος μεγαλύτερης από 5 Richter κάπου στην Ελλάδα δεν ανακοινώνονται ποτέ τα ονόματα εκείνων που πάσχουν από απλό κρυολόγημα. Είναι επομένως φανερό ότι στην καθημερινή χρήση η πληροφορία που συνοδεύει κάθε γεγονός δεν εκτιμάται μόνο με βάση την πιθανότητα του αλλά με περισσότερα και συνθετώτερα κριτήρια που διαμορφώνουν τη σημασία του γεγονότος.

Το σύστημα επικοινωνίας από την άποψη της θεωρίας πληροφοριών διοχετεύει απλά πληροφορία από ένα σημείο σε κάποιο άλλο. Μεταφορά πληροφορίας μπορεί να πραγματοποιηθεί και στην ίδια θέση αλλά από προηγούμενη σε επόμενη χρονική στιγμή. Τέτοια διαχρονική επικοινωνία με το παρελθόν προσφέρει η ανασκαφή αρχαιοτήτων. Είναι εντυπωσιακό ότι ο αποστολέας και ο αποδέκτης της πληροφορίας βρίσκονται στην ίδια θέση με σχετική καθυστέρηση αιώνων. Η μεταφορά πληροφορίας στο χρόνο, σε αντίθεση με τη μεταφορά πληροφορίας στο χώρο, δεν μπορεί να είναι αμφίδρομη αφού είναι αδύνατη η μεταφορά πληροφορίας στο παρελθόν.

Το σύστημα επικοινωνίας από την άποψη της θεωρίας πληροφοριών αντιστοιχεί στο κλασσικό τηλεπικοινωνιακό σύστημα πομπού - μέσου - δέκτη (σχ. 1.1). Η πληροφορία παράγεται στην πηγή πληροφορίας, οργανώνεται σε μηνύματα πληροφορίας που στη συνέχεια μετατρέπονται σε κωδικά μηνύματα. Ο δίαυλος πληροφορίας διοχετεύει την κωδικοποιημένη πληροφορία στο σημείο προορισμού, όπου γίνεται αποκάλυψη και διόρθωση των σφαλμάτων, αποκωδικοποίηση και τελικά αξιοποίηση της πληροφορίας. Πριν περιγραφούν και αναλυθούν τα διάφορα τμήματα του συστήματος επικοινωνίας από την άποψη της θεωρίας πληροφοριών είναι απαραίτητο να δοθούν οι ορισμοί των νέων εννοιών και να καθορισθεί η σχέση τους με έννοιες του συστήματος επικοινωνίας από την άποψη των τηλεπικοινωνιών.

ΟΡΙΣΜΟΣ : *Επικοινωνία* είναι κάθε διαδικασία μεταφοράς πληροφορίας μεταξύ δύο σημείων του χωρο-χρόνου (π.χ. τηλεφωνική συνδιάλεξη).

ΟΡΙΣΜΟΣ : *Πηγή Πληροφορίας* είναι το τμήμα του συστήματος επικοινωνίας που παρέχει πληροφορία με τη μορφή *συμβόλων* (π.χ. το δελτίο καιρού). Πληροφορία προσαρτάται στα σύμβολα με κριτήριο την πιθανότητα εμφάνισης τους στην έξοδο της πηγής πληροφορίας.

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

ΟΡΙΣΜΟΣ : *Λέξη Πληροφορίας* είναι βραχεία διάταξη συμβόλων πληροφορίας (π.χ. *σταθμός*).

ΟΡΙΣΜΟΣ : *Μήνυμα Πληροφορίας* είναι διάταξη λέξεων πληροφορίας (π.χ. *Ο σιδηροδρομικός σταθμός είναι συνέχεια ανοικτός*).

ΟΡΙΣΜΟΣ : *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 *κωδικές λέξεις* και *κωδικά μηνύματα*.

ΟΡΙΣΜΟΣ : *Κώδικας* είναι κάθε τεχνική κωδικοποίησης. 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.

Η πηγή πληροφορίας και ο κωδικοποιητής αντιστοιχούν στον πομπό του συστήματος επικοινωνίας. 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.

ΟΡΙΣΜΟΣ : *Δίαυλος Πληροφορίας* είναι αλυσίδα μέσων και συσκευών (π.χ. καλώδια, κυματοδηγοί, οπτικές ίνες) που μεταδίδουν το σήμα με την αποτυπωμένη σ' αυτό πληροφορία.

ΟΡΙΣΜΟΣ : *Χωρητικότητα* διαύλου πληροφορίας είναι ο ρυθμός μετάδοσης πληροφορίας (π.χ. το τηλέτυπο μεταδίδει 600 λέξεις/min ή 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.

ΟΡΙΣΜΟΣ : *θόρυβος* είναι κάθε ανεξέλεγκτη παρεμβολή του περιβάλλοντος του διαύλου πληροφορίας που προκαλεί στοχαστική αλλοίωση του σήματος. Ο θόρυβος προκαλεί γενικά σφάλματα μετάδοσης, δηλαδή απώλεια πληροφορίας, ή και ματαίωση της επικοινωνίας. Μέχρι το 1948 ο τηλεπικοινωνιακός μηχανικός επεδίωκε την προστασία του σήματος από το θόρυβο, δηλαδή την πιστή αναπαραγωγή του σήματος στο δέκτη. Με την ωρίμανση της θεωρίας πληροφοριών μετατοπίσθηκε το ενδιαφέρον στην πιστή αναπαραγωγή του μηνύματος πληροφορίας που είναι αποτυπωμένο στο σήμα. Σύγχρονα τηλεπικοινωνιακά συστήματα εξασφαλίζουν αξιόπιστη ροή πληροφορίας με σήμα βαθειά θαμμένο σε θόρυβο.

ΟΡΙΣΜΟΣ : *Παραμόρφωση* είναι κάθε καθοριστική αλλοίωση του σήματος (π.χ. απόσβεση κατά 30 dB).

ΟΡΙΣΜΟΣ : *Καταναλωτής* της πληροφορίας είναι το τελευταίο τμήμα του συστήματος επικοινωνίας όπου αναδομείται το αρχικό μήνυμα πληροφορίας. Επεται 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 επιδεικνύεται σε κείμενο, ήχο, εικόνα ή άλλη μορφή και καταναλώνεται αυξάνοντας τη γνώση του χρήστη ή αποθηκεύεται για μελλοντική χρήση.

1.2 ΜΕΤΡΟ ΠΛΗΡΟΦΟΡΙΑΣ - ΕΝΤΡΟΠΙΑ

Για τη μέτρηση της πληροφορίας που συνοδεύει κάποιο γεγονός χρησιμοποιείται στη θεωρία πληροφοριών μόνον η αντίστοιχη πιθανότητα. Είναι φανερό ότι συνηθισμένα γεγονότα (π.χ. η ανατολή του ήλιου) συνοδεύονται από μικρή ποσότητα πληροφορίας ενώ σπάνια γεγονότα (π.χ. ισχυρός σεισμός) συνοδεύονται από μεγάλη ποσότητα πληροφορίας. Επομένως η συνάρτηση που προσδιορίζει την πληροφορία έχει μόνο μία ανεξάρτητη μεταβλητή, την πιθανότητα του αντίστοιχου γεγονότος, και μάλιστα είναι φθίνουσα συνάρτηση.

Η διαίσθηση υποδεικνύει ότι κάθε συνδυασμός δύο ή περισσότερων ανεξάρτητων γεγονότων συνοδεύεται από πληροφορία ίση με το άθροισμα εκείνων που συνοδεύουν καθένα από αυτά. Η συνάρτηση που προσδιορίζει την πληροφορία σύνθετου γεγονότος είναι επομένως απαραίτητο να διαθέτει την αθροιστική ιδιότητα.

ΟΡΙΣΜΟΣ : *Αυτοπληροφορία* ή *πληροφοριακό περιεχόμενο* γεγονότος είναι ο αρνητικός λογάριθμος της αντίστοιχης πιθανότητας :

$$I(\alpha) = -\log_{\epsilon}(\pi) \qquad (1.1)$$

Τα σύμβολα α,π στην εξ.(1.1) εκπροσωπούν το γεγονός και την πιθανότητα του, αντίστοιχα, I είναι η πληροφορία που συνοδεύει το γεγονός (αυτοπληροφορία) και ε είναι η βάση υπολογισμού του λογαρίθμου. Η συνάρτηση $I(\alpha)$ αναφέρεται στο γεγονός αλλά εξαρτάται ουσιαστικά μόνο από την πιθανότητα του. Επιπλέον είναι φανερό ότι $I(\alpha)$ είναι φθίνουσα συνάρτηση της ανεξάρτητης μεταβλητής π.

Η μονάδα μέτρησης της πληροφορίας εξαρτάται από τη βάση υπολογισμού των λογαρίθμων και ονομάζεται bit για $\epsilon = 2$, nat για $\epsilon = e$ ($\log_e(\cdot) = \ln(\cdot)$) και hartley για $\epsilon = 10$. Είναι φανερό από την εξ.(1.1) ότι η αυτοπληροφορία γεγονότος είναι μη αρνητικό μέγεθος αφού $0 \leq \pi \leq 1$. Η λογαριθμική συνάρτηση διαθέτει και την αθροιστική ιδιότητα. Αν $\alpha_1\alpha_2$ είναι συνδυασμός δύο ανεξάρτητων γεγονότων

α_1, α_2 με αντίστοιχες πιθανότητες π_1, π_2, η αυτοπληροφορία του σύνθετου γεγονότος $\alpha_1\alpha_2$ είναι ίση με το άθροισμα της αυτοπληροφορίας καθενός από τα απλά γεγονότα α_1,α_2:

$$I(\alpha_1\alpha_2) = -\log_e(\pi_1\pi_2) = -\log_e(\pi_1) - \log_e(\pi_2) = I(\alpha_1) + I(\alpha_2) \qquad (1.2)$$

Ο ορισμός της εξ.(1.1) προκύπτει με την αξιωματική θεμελίωση Feinberg. Στο πλαίσιο όμως αυτού του συγγράμματος αρκεί ότι η λογαριθμική έκφραση της εξ.(1.1) συμμορφώνεται στις απαιτήσεις της διαίσθησης.

ΠΑΡΑΔΕΙΓΜΑ : Πηγή πληροφορίας εκπέμπει δύο ισοπίθανα σύμβολα, έστω 0 και 1. Η πληροφορία που συνοδεύει την εμφάνιση καθενός δυαδικού συμβόλου είναι $I(1) = I(0) = -\log_2(0.5) = 1$ bit.

ΠΑΡΑΔΕΙΓΜΑ : Έστω πηγή πληροφορίας που εκπέμπει ισοπίθανες δεκάδες δυαδικών ψηφίων. Είναι φανερό ότι υπάρχουν 2^{10} δυαδικές δεκάδες. Η πιθανότητα εμφάνισης οποιασδήποτε δυαδικής δεκάδας είναι $1/2^{10}$ και επομένως το πληροφοριακό περιεχόμενο της είναι $-\log_2(1/2^{10}) = 10$ bits. Αν η πηγή πληροφορίας παράγει ισοπίθανες τριάδες δεκαδικών ψηφίων, προκύπτει με τον ίδιο συλλογισμό ότι το πληροφοριακό περιεχόμενο κάθε δεκαδικής τριάδας είναι $-\log_2(1/10^3)$. Αλλά $10^3 \simeq 2^{10}$ και επομένως $-\log_2(1/10^3) \simeq -\log_2(1/2^{10}) = 10$ bits, δηλαδή *τρία δεκαδικά ψηφία ισοδυναμούν με δέκα δυαδικά ψηφία* από την άποψη του πληροφοριακού περιεχομένου.

Έστω πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$ και κατανομή πιθανοτήτων $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$, όπου π_i είναι η πιθανότητα εμφάνισης του συμβόλου πληροφορίας α_i, $i = 1, 2, \ldots, \rho$. Για κάθε κατανομή πιθανοτήτων ισχύει $0 \leq \pi_i \leq 1$ και $\pi_1 + \pi_2 + \ldots + \pi_\rho = 1$.

ΟΡΙΣΜΟΣ : *Εντροπία ή μέση πληροφορία ανά σύμβολο πληροφορίας* είναι ο μέσος όρος της αυτοπληροφορίας που συνοδεύει την εμφάνιση καθενός συμβόλου στην έξοδο της πηγής πληροφορίας. Για την πηγή πληροφορίας A, Π_A η εντροπία δίνεται από την έκφραση :

$$H(A) = H(\alpha_1, \alpha_2, \ldots, \alpha_\rho) = -\sum_{i=1}^{\rho} \pi_i \log_2(\pi_i) \quad \text{bits/σύμβολο} \qquad (1.3)$$

και έχει τις παρακάτω ιδιότητες :

(α) Είναι συνεχής συνάρτηση των πιθανοτήτων π_i, $i = 1, 2, \ldots, \rho$.

(β) Είναι συμμετρική συνάρτηση των $\pi_1, \pi_2, \ldots, \pi_\rho$.

(γ) Είναι μη αρνητική, δηλαδή $H(A) \geq 0$.

(δ) Μεγιστοποιείται για ισοπίθανα σύμβολα εκπομπής, δηλαδή όταν $\pi_1 = \pi_2 = \ldots = \pi_\rho = 1/\rho$ και η μέγιστη τιμή της είναι $H(A) = \log_e \rho$.

(ε) Ικανοποιεί την ταυτοανισότητα :

$$H(A) = -\sum_{i=1}^{\rho} \pi_i \log_e(\pi_i) \leq -\sum_{i=1}^{\rho} \pi_i \log_e(\tau_i) \qquad (1.4)$$

όπου $\Gamma_A = \{ \tau_1, \tau_2, \ldots, \tau_\rho \}$ είναι εναλλακτική κατανομή πιθανότητας για τα σύμβολα πληροφορίας $\alpha_1, \alpha_2, \ldots, \alpha_\rho$, δηλαδή $0 \leq \tau_i \leq 1$, $i = 1, 2, \ldots, \rho$, και $\tau_1 + \tau_2 + \ldots + \tau_\rho = 1$.

Οι ιδιότητες (α)-(γ) είναι προφανείς. Η ιδιότητα (δ) περιγράφει πρόβλημα μεγιστοποίησης υπό συνθήκη που αντιμετωπίζεται με τη μέθοδο των πολλαπλασιαστών Lagrange. Η συνάρτηση που πρέπει να μεγιστοποιηθεί είναι $F(A,\Pi_A) = H(A) = -\pi_1 \log_e(\pi_1) - \pi_2 \log_e(\pi_2) - \ldots - \pi_\rho \log_e(\pi_\rho)$ και η συνθήκη είναι $F_1(A,\Pi_A) = \pi_1 + \pi_2 + \ldots + \pi_\rho = 1$. Η κατανομή πιθανότητας Π_A που μεγιστοποιεί την $F(A,\Pi_A)$ προκύπτει επιλύοντας τις διαφορικές εξισώσεις :

$$\frac{\partial F(A,\Pi_A)}{\partial \pi_j} + \kappa \frac{\partial F_1(A,\Pi_A)}{\partial \pi_j} = 0 \quad ; \quad j = 1, 2, \ldots, \rho \qquad (1.5)$$

με κ το σταθερό πολλαπλασιαστή. Η εξ.(1.5) υποδεικνύει ότι το μέγιστο της $F(A,\Pi_A) = H(A)$ αντιστοιχεί στην κατανομή πιθανοτήτων με $\log_e \pi_1 = \log_e \pi_2 = \ldots = \log_e \pi_\rho = \kappa - \log_e(e)$, δηλαδή σε ισοπίθανα σύμβολα πληροφορίας με $\pi_1 = \pi_2 = \ldots = \pi_\rho = 1/\rho$ και $\kappa = \log_e(e/\rho)$. Επομένως η μέγιστη τιμή της εντροπίας είναι :

$$H(A) = -\sum_{i=1}^{\rho} (1/\rho) \log_e(1/\rho) = \log_e \rho \qquad (1.6)$$

και η ιδιότητα (δ) έχει αποδειχθεί. Προκειμένου να αποδειχθεί η ιδιότητα (ε) η

εξ.(1.4) γράφεται με τη μορφή που ακολουθεί :

$$H(A,\Pi_A/T_A) = \sum_{i=1}^{\rho} \pi_i \log_e\left(\frac{\pi_i}{\tau_i}\right) \geq 0 \qquad (1.7)$$

όπου $H(A,\Pi_A/T_A)$ είναι η *σχετική εντροπία* (ή *αριθμός Kullback-Leibler*) των καταναμών πιθανότητας Π_A, T_A για το αλφάβητο A . Με εφαρμογή της γνωστής ταυτοανισότητας $\ln x \leq x - 1$ προκύπτει ότι η σχετική εντροπία $H(A,\Pi_A/T_A)$ είναι μη αρνητική :

$$\sum_{i=1}^{\rho} \pi_i \log_e\left(\frac{\pi_i}{\tau_i}\right) = -\frac{1}{\ln\epsilon}\sum_{i=1}^{\rho} \pi_i \ln\left(\frac{\tau_i}{\pi_i}\right) \geq -\frac{1}{\ln\epsilon}\sum_{i=1}^{\rho} \pi_i\left(1-\frac{\tau_i}{\pi_i}\right) =$$

$$= \frac{1}{\ln\epsilon}\sum_{i=1}^{\rho}\left(\tau_i - \pi_i\right) = \frac{1}{\ln\epsilon}\left(\sum_{i=1}^{\rho}\tau_i - \sum_{i=1}^{\rho}\pi_i\right) = \frac{1}{\ln\epsilon}\left(1-1\right) = 0$$

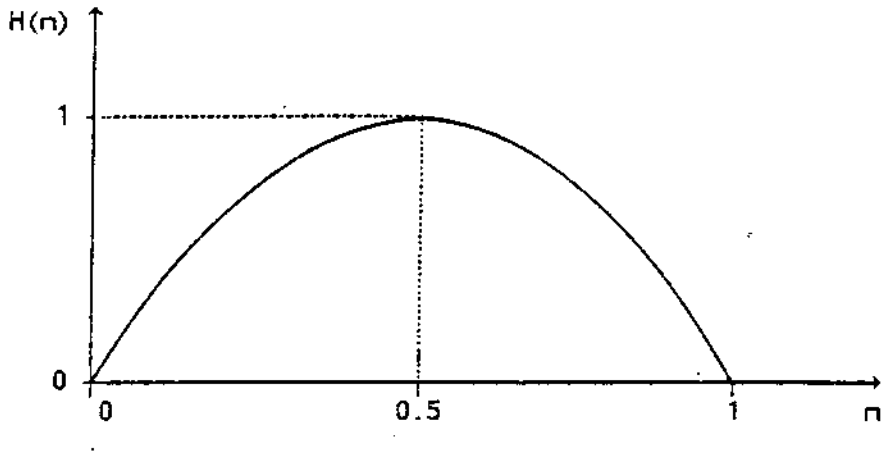
όπως απαιτεί η εξ.(1.7). Επομένως η ιδιότητα (ε) έχει αποδειχθεί. Οι ταυτοανισότητες των εξ.(1.4), (1.7) βρίσκουν πολλές εφαρμογές στη θεμελίωση της θεωρίας πληροφοριών.

ΠΑΡΑΔΕΙΓΜΑ : Η εντροπία δυαδικής πηγής πληροφορίας με ισοπίθανα σύμβολα είναι $H(0,1) = -\pi_0\log_2(\pi_0) - \pi_1\log_2(\pi_1) = -0.5\log_2(0.5) - 0.5\log_2(0.5) = -\log_2(0.5)$ = 1 bit/σύμβολο.

Η δυαδική πηγή πληροφορίας εμφανίζει γενικά τα σύμβολα, έστω 0 και 1, με πιθανότητες π και 1−π, αντίστοιχα. Η εντροπία της είναι :

$$H(\pi) = -\pi\log_2(\pi) - (1-\pi)\log_2(1-\pi) \quad \text{bits/σύμβολο} \qquad (1.8)$$

και η έκφραση στο δεξιό μέλος της εξ.(1.8), που εμπλέκει μόνο τη μεταβλητή π, ονομάζεται *συνάρτηση Shannon* (σχ. 1.2). Το μέγιστο της συνάρτησης Shannon αντιστοιχεί σε ισοπίθανα σύμβολα, δηλαδή $\pi = 1 - \pi = 0.5$. Στα άκρα του διαστήματος ορισμού της μηδενίζεται, αφού $0\log_2 0 = 1\log_2 1 = 0$. Αν δεν δημιουργείται αβεβαιότητα για το σύμβολο που εμφανίζεται στην έξοδο δυαδικής πηγής πληροφορίας, τότε αυτή δεν παρέχει πληροφορία. Το ίδιο μπορεί να αποδειχθεί και για πηγές πληροφορίας με μεγαλύτερο πλήθος συμβόλων.



Σχ. 1.2 Συνάρτηση Shannon.

ΠΑΡΑΔΕΙΓΜΑ : Η εντροπία ν–αδικής πηγής πληροφορίας με ισοπίθανα σύμβολα είναι $H(\alpha_1, \alpha_2, \ldots, \alpha_v) = -v(1/v)\log_2(1/v) = \log_2 v$ bits/σύμβολο.

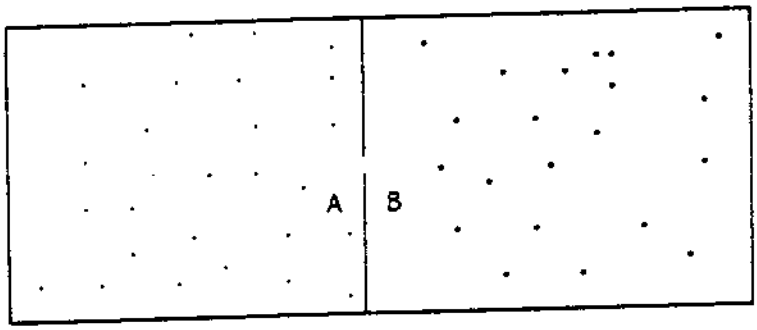
ΠΑΡΑΔΕΙΓΜΑ : Η εντροπία ομιλούμενης γλώσσας καθορίζεται αφού πρώτα υπολογισθούν οι πιθανότητες εμφάνισης των γραμμάτων της. Στο αλφάβητο της γλώσσας συμπεριλαμβάνεται και το διάκενο σαν ιδιαίτερο σύμβολο. Στον πίνακα 1.1 δίνονται οι πιθανότητες εμφάνισης των γραμμάτων της Αγγλικής και της Γερμανικής γλώσσας. Με εφαρμογή της εξ.(1.3) προκύπτει ότι η εντροπία της Αγγλικής γλώσσας είναι 4.08 bits/σύμβολο και αντίστοιχα για τη Γερμανική γλώσσα είναι 4.11 bits/σύμβολο.

Είναι απαραίτητο να διερευνηθεί αν η εντροπία της θεωρίας πληροφοριών έχει σχέση με την εντροπία της θερμοδυναμικής και της στατιστικής μηχανικής. Το αποτέλεσμα αυτής της προσπάθειας θα καθορίσει τη θέση της θεωρίας πληροφοριών σε σχέση με κλασσικές φυσικές επιστήμες και θα βοηθήσει στη σύνδεση της πληροφορίας, δηλαδή του μεγέθους που χαρακτηρίζει τον 20ο αιώνα, με την ισχύ, δηλαδή το μέγεθος που χαρακτήρισε το 19ο αιώνα.

Η εντροπία στο πλαίσιο της θερμοδυναμικής περιγράφει την οργάνωση του θερμικού συστήματος σε σχέση με κάποια (αυθαίρετη) αναφορά. Έστω θερμικό σύστημα που αποτελείται από δοχείο με κρύο νερό και δοχείο με ζεστό νερό. Με ανάμειξη του περιεχομένου των δύο δοχείων προκύπτει χλιαρό νερό σε δοχείο διπλάσιας χωρητικότητας και το τελικό θερμικό σύστημα έχει κατώτερη οργάνωση από το αρχικό παρόλο που ούτε παράγεται ούτε χάνεται θερμότητα κατά την ανάμειξη. Εκείνο που χάθηκε κατά την ανάμειξη είναι ο αρχικός διαμερισμός ζεστού και κρύου νερού, δηλαδή η οργάνωση του θερμικού συστήματος. Είναι φανερό ότι η παραπάνω μεταβολή δεν είναι αντιστρέψιμη, δηλαδή δεν είναι δυνατό από δοχείο χλιαρού νερού να

παραχθούν δύο δοχεία με κρύο και ζεστό νερό, αντίστοιχα.

Η μετάδοση πληροφορίας σε σύστημα επικοινωνίας αυξάνει τη γνώση του αποδέκτη της πληροφορίας και διαφοροποιεί την εγκεφαλική οργάνωση του. Η πρόσθετη γνώση χρησιμοποιείται γενικά στη λήψη αποφάσεων ή στην εκτέλεση ενεργειών που οδηγούν σε παραγωγή έργου. Είναι φανερό λοιπόν ότι η εντροπία της θεωρίας πληροφοριών αντιστοιχεί στην εντροπία της θερμοδυναμικής και στη διαπίστωση αυτή συμβάλλει το παρακάτω νοητικό πείραμα που εμπλέκει το *δαίμονα του Maxwell*.



Σχ. 1.3 Ο δαίμονας ξεχωρίζει αργά (·) από γρήγορα (˙) μόρια προκαλώντας διαφορά θερμοκρασίας μεταξύ των διαμερισμάτων A, B.

Εστω κλειστός χώρος όπου ζει ο δαίμονας του Maxwell, δηλαδή υπερφυσικό ον προικισμένο με τη δυνατότητα να διακρίνει μόρια του παγιδευμένου αερίου (σχ. 1.3). Ο χώρος υποδιαιρείται σε δύο διαμερίσματα και η μοναδική θυρίδα επικοινωνίας ελέγχεται από το δαίμονα. Τα μόρια του αερίου εκτελούν άτακτη κίνηση και μετακινούμενα τυχαία ανακλώνται στα τοιχώματα του χώρου. Είναι φανερό ότι κάθε μόριο του αερίου προσεγγίζει κάποτε τη θυρίδα μεταξύ των δύο διαμερισμάτων. Εκεί παραμονεύει ο δαίμονας που επιτρέπει σε γρήγορα μόρια τη διέλευση από το διαμέρισμα Α στο διαμέρισμα Β και σε αργά μόρια τη διέλευση από το διαμέρισμα Β στο διαμέρισμα Α . Αν το άνοιγμα και κλείσιμο της θυρίδας δεν απαιτούν έργο, μετά από αρκετό χρόνο το διαμέρισμα Β θα περιέχει μόνο γρήγορα μόρια ενώ το διαμέρισμα Α θα περιέχει μόνο αργά μόρια. Επειδή η κινητική κατάσταση των μορίων κάθε χώρου περιγράφεται μακροσκοπικά από τη θερμοκρασία του, είναι φανερό ότι η έξυπνη δραστηριότητα του δαίμονα καταλήγει σε διαφορά θερμοκρασίας μεταξύ των δύο διαμερισμάτων. Είναι γνωστό από τη θερμοδυναμική ότι κάθε διαφορά θερμοκρασίας προσφέρει τη δυνατότητα παραγωγής έργου. Το νοητικό πείραμα δεν υποδεικνύει ότι είναι δυνατό να παραχθεί έργο από το μηδέν αλλά ότι η πληροφορία που αποκτά και επεξεργάζεται ο δαίμονας ισοδυναμεί με ενέργεια, δηλαδή με δυνατότητα παραγωγής έργου.

Πίνακας 1.1

Πιθανότητες συμβόλων Αγγλικής και Γερμανικής γλώσσας

i	ΑΓΓΛΙΚΑ		ΓΕΡΜΑΝΙΚΑ	
	Γράμμα	π_i	Γράμμα	π_i
1		0.1859		0.15149
2	E	0.1031	E	0.14700
3	T	0.0796	N	0.08835
4	A	0.0642	R	0.06858
5	O	0.0632	I	0.06378
6	I	0.0575	S	0.05388
7	N	0.0574	T	0.04731
8	S	0.0514	D	0.04385
9	R	0.0484	H	0.04355
10	H	0.0467	A	0.04331
11	L	0.0321	U	0.03188
12	D	0.0317	L	0.02931
13	U	0.0228	C	0.02673
14	C	0.0218	G	0.02667
15	F	0.0208	M	0.02134
16	M	0.0198	O	0.01772
17	W	0.0175	B	0.01597
18	Y	0.0164	Z	0.01423
19	G	0.0152	W	0.01420
20	P	0.0152	F	0.01360
21	B	0.0127	K	0.00956
22	V	0.0083	V	0.00735
23	K	0.0049	Ue	0.00580
24	X	0.0013	P	0.00499
25	J	0.0008	Ae	0.00491
26	Q	0.0008	Oe	0.00255
27	Z	0.0005	J	0.00165
28			Y	0.00017
29			Q	0.00014
30			X	0.00013
Εντροπία	4.08 bits/σύμβολο		4.1134 bits/σύμβολο	

Η εντροπία στο πλαίσιο της στατιστικής μηχανικής περιγράφει τη διευθέτηση στοιχείων του συστήματος σε σχέση με αριθμό ενεργειακών καταστάσεων. Εστω κλειστό δοχείο που περιέχει ν μόρια αερίου. Αν $\nu_1, \nu_2, \ldots, \nu_\rho$ μόρια βρίσκονται στις ενεργειακές καταστάσεις $E_1, E_2, \ldots, E_\rho$, αντίστοιχα, με $\nu_1 + \nu_2 + \ldots + \nu_\rho = \nu$, τότε η πιθανότητα κάποιου μορίου να βρίσκεται στην ενεργειακή κατάσταση E_i είναι $\pi_i = \nu_i/\nu$, $i = 1, 2, \ldots, \rho$ και η πιθανότητα συγκεκριμένης διανομής των ν μορίων στις ρ ενεργειακές καταστάσεις είναι ανάλογη του πλήθους των δυνατών διανομών ν πραγμάτων σε ρ ομάδες με $\nu_1, \nu_2, \ldots, \nu_\rho$ μέλη σε κάθε ομάδα :

$$n_{v,\rho} = \frac{v!}{v_1!\, v_2! \ldots v_\rho!} \qquad (1.9)$$

Στη στατιστική μηχανική χρησιμοποιείται ο παρακάτω ορισμός για την εντροπία του συστήματος :

$$H = k \ln(n_{v,\rho}) \qquad (1.10)$$

όπου k είναι η σταθερά Boltzmann. Αποδεικνύεται με την κινητική θεωρία ότι ο ορισμός της εξ.(1.10) είναι ισοδύναμος του γνωστού μακροσκοπικού ορισμού $d\varphi = dQ/T$ που χρησιμοποιείται για την εντροπία στο πλαίσιο της θερμοδυναμικής. Είναι μάλιστα σημαντικό ότι στη στατιστική μηχανική χρησιμοποιείται για την εντροπία το σύμβολο H αντί των συμβόλων φ ή S που χρησιμοποιούνται στη θερμοδυναμική. Αν συνδυασθούν οι εξ.(1.9), (1.10) και χρησιμοποιηθεί η προσέγγιση Stirling $v! \approx \sqrt{2\pi v}\, e^{-v}\, v^{v+1/2}$, προκύπτει :

$$H = k \left(v \ln v - \sum_{i=1}^{\rho} v_i \ln v_i \right) + \frac{k}{2} \left(\ln(2\pi v) - \sum_{i=1}^{\rho} v_i \ln(2\pi v_i) \right) \qquad (1.11)$$

Οι δύο τελευταίοι όροι στο δεξιό μέλος της εξ.(1.11) είναι δυνατό να παραλειφθούν για $v >> 1$. Η έκφραση της εντροπίας απλοποιείται στην παρακάτω :

$$H = - k v \ln e \sum_{i=1}^{\rho} n_i \log_e(n_i) \qquad (1.12)$$

που ουσιαστικά ταυτίζεται με την έκφραση της εξ.(1.3) για την εντροπία στο πλαίσιο της θεωρίας πληροφοριών.

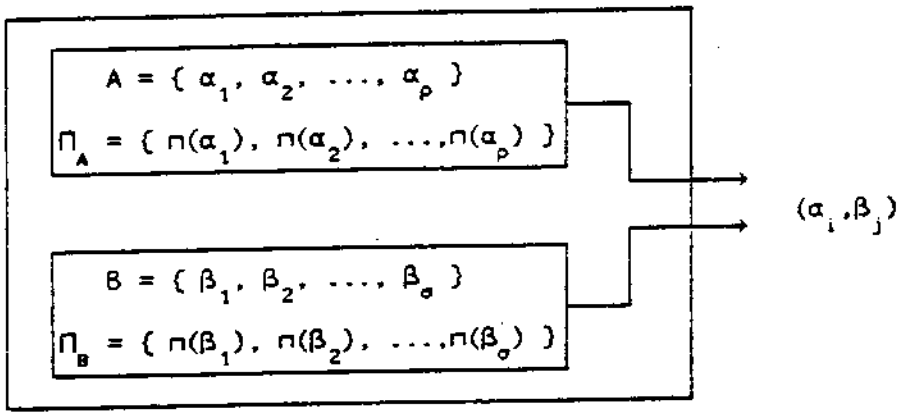
1.3 ΣΥΝΔΕΤΙΚΗ ΕΝΤΡΟΠΙΑ

Δύο απλές πηγές πληροφορίας A, Π_A και B, Π_B συνθέτουν πηγή πληροφορίας με αλφάβητο AB και κατανομή πιθανότητας Π_{AB} (σχ. 1.4). Σύμβολα της σύνθετης πηγής

πληροφορίας είναι τα ζεύγη (α,β) με $\alpha \in A$, $\beta \in B$ και πιθανότητα εμφάνισης $\pi(\alpha,\beta)$ που καθορίζεται από τη συνδετική κατανομή πιθανότητας Π_{AB} (βλ. §1.I.4). Η τελευταία έχει σαν περιθωριακές κατανομές πιθανότητας τις Π_A και Π_B. Κατ' επέκταση της εξ.(1.3) ορίζεται η *συνδετική εντροπία* των δύο πηγών πληροφορίας σαν εντροπία της σύνθετης πηγής πληροφορίας AB, Π_{AB} :

$$H(AB) = -\sum_{AB} \pi(\alpha,\beta) \log_c \left[\pi(\alpha,\beta)\right] \qquad (1.13)$$

που περιγράφει τη μέση πληροφορία ανά ζεύγος συμβόλων (α,β) με $\alpha \in A$ και $\beta \in B$.



Σχ. 1.4 Σύνθετη πηγή πληροφορίας

Βασική ιδιότητα της συνδετικής εντροπίας είναι :

$$H(AB) \leq H(A) + H(B) \qquad (1.14)$$

που υποδεικνύει ότι η μέση πληροφορία ανά σύμβολο της σύνθετης πηγής πληροφορίας δεν υπερβαίνει το άθροισμα της μέσης πληροφορίας ανά σύμβολο για κάθε απλή πηγή πληροφορίας. Η ισότητα στην εξ.(1.14) ισχύει μόνο στην περίπτωση που οι έξοδοι των απλών πηγών πληροφορίας είναι στατιστικά ανεξάρτητες, οπότε $\pi(\alpha,\beta) = \pi(\alpha)\pi(\beta)$. Για την απόδειξη της εξ.(1.14) χρησιμοποιείται η εξ.(1.4), που επεκτείνεται κατάλληλα για τη σύνθετη πηγή πληροφορίας $AB = \{ (\alpha,\beta) \,/\, \alpha \in A, \beta \in B \}$, $\Pi_{AB} = \{ \Pi\iota\theta[\, (\alpha,\beta) \,/\, \alpha \in A, \beta \in B \,] = \pi(\alpha,\beta) \}$. Είναι φανερό ότι η κατανομή πιθανότητας $T_{AB} = \{ \Pi\iota\theta[\, (\alpha,\beta) \,/\, \alpha \in A, \beta \in B \,] = \pi(\alpha)\pi(\beta) \}$ είναι εναλλακτική κατανομή πιθανότητας για τη σύνθετη πηγή πληροφορίας. Επομένως :

$$H(AB) = -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_e\left[n(\alpha_i,\beta_j)\right] \leq -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_e\left[n(\alpha_i)n(\beta_j)\right] =$$

$$= -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_e\left[n(\alpha_i)\right] - \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_e\left[n(\beta_j)\right] =$$

$$= -\sum_{i=1}^{\rho}\left[\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\right]\log_e\left[n(\alpha_i)\right] - \sum_{j=1}^{\sigma}\left[\sum_{i=1}^{\rho} n(\alpha_i,\beta_j)\right]\log_e\left[n(\beta_j)\right] =$$

$$= -\sum_{i=1}^{\rho} n(\alpha_i)\log_e\left[n(\alpha_i)\right] - \sum_{j=1}^{\sigma} n(\beta_j)\log_e\left[n(\beta_j)\right] = H(A) + H(B)$$

Αν ν απλές πηγές πληροφορίας A_1,Π_1, A_2,Π_2, ..., A_ν,Π_ν χρησιμοποιηθούν γιά τη σύνθεση πηγής πληροφορίας με σύμβολα ν-άδες $(\alpha_1,\alpha_2,\ldots,\alpha_\nu)$, όπου $\alpha_1 \in A_1$, $\alpha_2 \in A_2$, ..., $\alpha_\nu \in A_\nu$, ο ορισμός της συνδετικής εντροπίας επεκτείνεται στον παρακάτω :

$$H(A_1A_2\ldots A_\nu) = -\sum_{A_1}\sum_{A_2}\cdots\sum_{A_\nu} n(\alpha_1,\alpha_2,\ldots,\alpha_\nu)\log_e\left[n(\alpha_1,\alpha_2,\ldots,\alpha_\nu)\right] \qquad (1.15)$$

και είναι εύκολο να αποδειχθεί ότι ισχύει η ταυτοανισότητα :

$$H(A_1A_2\ldots A_\nu) \leq H(A_1) + H(A_2) + \ldots + H(A_\nu) \qquad (1.16)$$

που αποτελεί γενίκευση της εξ.(1.14).

1.4 ΥΠΟ ΣΥΝΘΗΚΗ ΕΝΤΡΟΠΙΑ

Έστω ότι σε σύνθετη πηγή πληροφορίας που αποτελείται από δύο απλές πηγές πληροφορίας (σχ. 1.4) μία από τις δύο εμφανίζει μόνιμα κάποιο σύμβολο, π.χ. η πηγή πληροφορίας B,Π_B εμφανίζει στην έξοδο της συνέχεια το σύμβολο β_j. Το αλφάβητο της σύνθετης πηγής πληροφορίας περιορίζεται τότε στο σύνολο των ζευγών (α_i,β_j) με α_i οποιοδήποτε σύμβολο από το σύνολο A. Η πιθανότητα εμφάνισης του

σύνθετου συμβόλου (α_i,β_j) ισούται με την πιθανότητα εμφάνισης του απλού συμβόλου α_i στην έξοδο της πηγής πληροφορίας A,Π_A με δεδομένο ότι η πηγή πληροφορίας B,Π_B εμφανίζει στην έξοδο της μόνο το σύμβολο β_j. Επομένως πρόκειται για την υπό συνθήκη πιθανότητα :

$$\pi(\alpha_i/\beta_j) = \frac{\pi(\alpha_i,\beta_j)}{\pi(\beta_j)} \tag{1.17}$$

και η μέση πληροφορία ανά σύμβολο της σύνθετης πηγής πληροφορίας με δεδομένη έξοδο σε μία από τις δύο απλές πηγές πληροφορίας είναι :

$$H(A/\beta_j) = -\sum_{i=1}^{\rho} \pi(\alpha_i/\beta_j)\log_e\left[\pi(\alpha_i/\beta_j)\right] \tag{1.18}$$

Η εξ.(1.18) είναι προέκταση της εξ.(1.3). Η μέση τιμή του μεγέθους $H(A/\beta_j)$ ως προς τα σύμβολα β_j είναι η *υπό συνθήκη εντροπία* :

$$H(A/B) = \sum_{j=1}^{\sigma} H(A/\beta_j)\pi(\beta_j) = -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} \pi(\alpha_i/\beta_j)\pi(\beta_j)\log_e\left[\pi(\alpha_i/\beta_j)\right] =$$

$$= -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} \pi(\alpha_i,\beta_j)\log_e\left[\pi(\alpha_i/\beta_j)\right] \tag{1.19}$$

που περιγράφει τη μέση αβεβαιότητα για την έξοδο της πηγής πληροφορίας A,Π_A με γνωστή την έξοδο της πηγής πληροφορίας B,Π_B. Ανάλογα ορίζεται και η υπό συνθήκη εντροπία $H(B/A)$.

Αν χρησιμοποιηθεί η εξ.(1.17) στην εξ.(1.19) προκύπτει :

$$H(A/B) = -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} \pi(\alpha_i,\beta_j)\log_e\left[\frac{\pi(\alpha_i,\beta_j)}{\pi(\beta_j)}\right] =$$

$$= -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} \pi(\alpha_i,\beta_j)\log_e\left[\pi(\alpha_i,\beta_j)\right] + \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} \pi(\alpha_i,\beta_j)\log_e\left[\pi(\beta_j)\right] =$$

$$= H(AB) + \sum_{j=1}^{\sigma} \pi(\beta_j) \log_e \left[\pi(\beta_j) \right] = H(AB) - H(B) \qquad (1.20)$$

και με ανάλογη διαδικασία αποδεικνύεται ότι :

$$H(B/A) = H(AB) - H(A) \qquad (1.21)$$

Αν χρησιμοποιηθεί η εξ.(1.14), διαπιστώνεται επιπλέον ότι :

$$H(A/B) \leq H(A)$$

$$H(B/A) \leq H(B) \qquad (1.22)$$

Η ισότητα ισχύει στην περίπτωση που οι έξοδοι των δύο απλών πηγών πληροφορίας είναι στατιστικά ανεξάρτητες. Είναι φανερό από τις εξ.(1.22) ότι η αβεβαιότητα για την έξοδο απλής πηγής πληροφορίας ελαττώνεται όταν δίνεται κάποια πληροφορία σχετικά με την έξοδο γειτονικής πηγής πληροφορίας, εφόσον βέβαια μεταξύ των δύο πηγών πληροφορίας υπάρχει στατιστική εξάρτηση.

ΠΑΡΑΔΕΙΓΜΑ : Έστω απλή πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$ και κατανομή πιθανότητας $\Pi_A = \{ 1/2, 1/4, 1/4 \}$. Δίνεται και δεύτερη απλή πηγή πληροφορίας, με αλφάβητο $B = \{ \beta_1, \beta_2, \beta_3 \}$, που σχετίζεται με την πρώτη απλή πηγή πληροφορίας μέσω των υπό συνθήκη πιθανοτήτων:

$$\pi(\beta_1/\alpha_1) = 1/3 \qquad \pi(\beta_2/\alpha_1) = 1/3 \qquad \pi(\beta_3/\alpha_1) = 1/3$$

$$\pi(\beta_1/\alpha_2) = 1/2 \qquad \pi(\beta_2/\alpha_2) = 1/4 \qquad \pi(\beta_3/\alpha_2) = 1/4$$

$$\pi(\beta_1/\alpha_3) = 1/4 \qquad \pi(\beta_2/\alpha_3) = 1/4 \qquad \pi(\beta_3/\alpha_3) = 1/2$$

Οι πιθανότητες των συμβόλων β_1, β_2, β_3 προσδιορίζονται από την παρακάτω σχέση :

$$\pi(\beta_j) = \sum_{i=1}^{3} \pi(\alpha_i, \beta_j) = \sum_{i=1}^{3} \pi(\beta_j/\alpha_i) \pi(\alpha_i)$$

που στο δεξιό μέλος της εμπλέκει γνωστά μεγέθη. Μετά τις πράξεις προκύπτει $\pi(\beta_1) = 17/48$, $\pi(\beta_2) = 14/48$, $\pi(\beta_3) = 17/48$ και είναι προφανές ότι $\pi(\beta_1) + \pi(\beta_2) + \pi(\beta_3) = 1$ όπως απαιτείται για κάθε κατανομή πιθανότητας. Η εντροπία της

δεύτερης πηγής πληροφορίας υπολογίζεται με εφαρμογή της εξ.(1.3) :

$$H(B) = -\sum_{j=1}^{3} \pi(\beta_j)\log_2\left[\pi(\beta_j)\right] =$$

$$= -(17/48)\log_2(17/48) - (14/48)\log_2(14/48) - (17/48)\log_2(17/48) =$$

$$= 1.5787 \text{ bits/σύμβολο}$$

Η υπό συνθήκη εντροπία H(A/B) υπολογίζεται από την εξ.(1.19) :

$$H(A/B) = -\sum_{i=1}^{3}\sum_{j=1}^{3} \pi(\beta_j/\alpha_i)\pi(\alpha_i)\log_2\left[\frac{\pi(\beta_j/\alpha_i)\pi(\alpha_i)}{\pi(\beta_j)}\right]$$

όπως αυτή διαμορφώνεται με τη βοήθεια της εξ.(1.17). Όλα τα μεγέθη είναι γνωστά και το αποτέλεσμα είναι H(A/B) = 1.4632 bits/σύμβολο. Σημειώνεται ότι H(A/B) < H(A) = 1.5 bits/σύμβολο, όπως απαιτεί η εξ.(1.22α).

1.5 ΕΠΕΚΤΑΣΕΙΣ ΠΗΓΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Εστω ότι η σύνθετη πηγή πληροφορίας του σχήματος 1.4 αποτελείται από δύο όμοιες απλές πηγές πληροφορίας, δηλαδή B = A και $\Pi_B = \Pi_A$. Στην περίπτωση αυτή τα σύμβολα πληροφορίας είναι τα ζεύγη (α_i,α_j) με $\alpha_i,\alpha_j \in A$ και επομένως το αλφάβητο της σύνθετης πηγής πληροφορίας είναι το σύνολο $A^2 = A\cdot A$. Η κατανομή πιθανότητας των συμβόλων είναι το σύνολο :

$$\Pi_A^2 = \left\{ \pi(\alpha_i,\alpha_j) = \pi(\alpha_i)\pi(\alpha_j) \;/\; \pi(\alpha_i),\ \pi(\alpha_j) \in \Pi_A \right\} \qquad (1.23)$$

Η εξ.(1.23) υποδηλώνει ότι δύο επαναλήψεις της απλής πηγής πληροφορίας A,Π_A είναι στατιστικά ανεξάρτητες.

ΟΡΙΣΜΟΣ : *Δεύτερη επέκταση* πηγής πληροφορίας A,Π_A είναι η σύνθετη πηγή πληροφορίας A^2, Π_A^2.

Η εντροπία της δεύτερης επέκτασης πηγής πληροφορίας A,Π_A προσδιορίζεται με εφαρμογή της εξ.(1.13) :

$$H(A^2) = -\sum_{i=1}^{\rho}\sum_{j=1}^{\rho} n(\alpha_i,\alpha_j)\log_e\left[n(\alpha_i,\alpha_j)\right] = -\sum_{i=1}^{\rho}\sum_{j=1}^{\rho} n(\alpha_i)n(\alpha_j)\log_e\left[n(\alpha_i)n(\alpha_j)\right]$$

$$= -2\sum_{i=1}^{\rho} n(\alpha_i)\log\left[n(\alpha_i)\right] = 2H(A) \qquad (1.24)$$

και επομένως η επέκταση απλής πηγής πληροφορίας αυξάνει την αβεβαιότητα. Το αποτέλεσμα της εξ.(1.24) μπορεί να προσδιοριστεί και με τη βοήθεια της γνωστής ταυτοανισότητας $H(AB) \leq H(A) + H(B)$ που μετατρέπεται σε ισότητα αν A, B είναι στατιστικά ανεξάρτητες τυχαίες μεταβλητές. Εφόσον η δεύτερη επέκταση της απλής πηγής πληροφορίας A, Π_A διαμορφώνεται από δύο στατιστικά ανεξάρτητες επαναλήψεις της, η εξ.(1.14) καθορίζει ότι :

$$H(A^2) = H(A) + H(A) = 2H(A)$$

Γενικώτερα, η ν-οστή επέκταση της απλής πηγής πληροφορίας A, Π_A προκύπτει από ν ανεξάρτητες επαναλήψεις της. Το αλφάβητο της επεκταμένης πηγής πληροφορίας είναι το σύνολο $A^\nu = A\,A\,\ldots\,A$ με στοιχεία ν-άδες $(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_\nu})$, $\alpha_{i_j} \in A$. Η κατανομή πιθανοτήτων της είναι το σύνολο $\Pi_A^\nu = \{\, n(\alpha_{i_1})n(\alpha_{i_2})\ldots n(\alpha_{i_\nu}) \,/\, n(\alpha_{i_j}) \in \Pi_A \,\}$. Εύκολα αποδεικνύεται η σχέση :

$$H(A^\nu) = \nu H(A) \qquad (1.25)$$

που αποτελεί γενίκευση της εξ.(1.24).

ΠΑΡΑΔΕΙΓΜΑ : Έστω δυαδική πηγή πληροφορίας με αλφάβητο $A = \{ 0, 1 \}$, κατανομή πιθανοτήτων $\Pi_A = \{ n, 1-n \}$ και εντροπία $H(A) = H(n)$, όπου $H(n)$ είναι η συνάρτηση Shannon (βλ. §1.2). Η τρίτη επέκταση της χρησιμοποιεί τα σύμβολα :

000, 010, 100, 001, 101, 110, 011, 111

που ανήκουν στο σύνολο $A^3 = A\cdot A\cdot A$. Η κατανομή πιθανοτήτων των δυαδικών τριάδων είναι :

$$\Pi_A^3 = \left\{ \pi^3,\ \pi^2(1-\pi),\ \pi^2(1-\pi),\ \pi^2(1-\pi),\ \pi(1-\pi)^2,\ \pi(1-\pi)^2,\ \pi(1-\pi)^2,\ (1-\pi)^3 \right\}$$

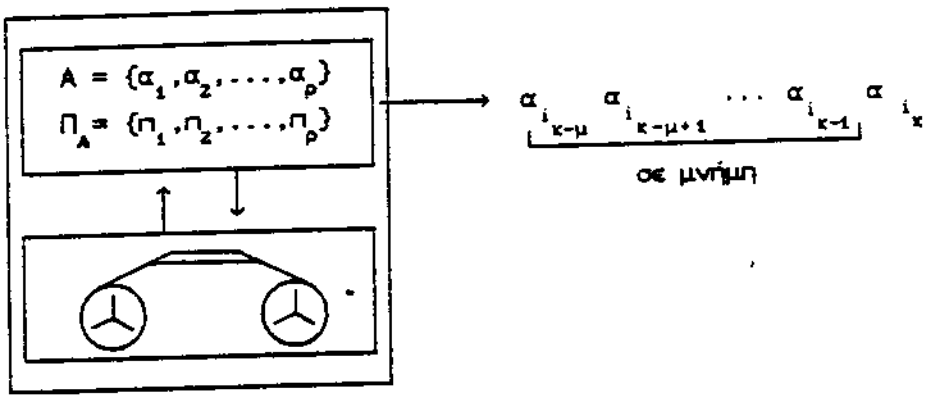
και σύμφωνα με την εξ.(1.25) η εντροπία της είναι $H(A^3) = 3H(\pi)$.

Με την επέκταση οποιασδήποτε πηγής πληροφορίας επιτυγχάνεται μεγαλύτερο πλήθος συμβόλων πληροφορίας στα οποία είναι δυνατό να αντιστοιχισθούν πολλαπλά ενδεχόμενα.

1.6 ΠΗΓΗ ΠΛΗΡΟΦΟΡΙΑΣ ΜΕ ΜΝΗΜΗ

Πηγή πληροφορίας $A.\Pi_A$ εκπέμπει διαδοχικά τα σύμβολα $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{\kappa-1}}, \alpha_{i_\kappa}, \ldots$ με $\alpha_{i_j} \in A$. Αν η εμφάνιση κάθε συμβόλου εξαρτάται από κάποιο πλήθος προηγουμένων συμβόλων, τότε η πηγή πληροφορίας διαθέτει μνήμη. Συγκεκριμένα η πηγή πληροφορίας $A.\Pi_A$ διαθέτει μνήμη μ–τάξης αν ισχύει :

$$\pi(\alpha_{i_\kappa}) \neq \pi(\alpha_{i_\kappa} / \alpha_{i_{\kappa-1}}, \alpha_{i_{\kappa-2}}, \ldots, \alpha_{i_{\kappa-\mu}}) \qquad (1.26)$$



Σχ. 1.5 Πηγή πληροφορίας με μνήμη μ–τάξης

που υποδηλώνει ότι υπάρχει στατιστική εξάρτηση μεταξύ του συμβόλου α_{i_κ} και των μ προηγουμένων συμβόλων $\alpha_{i_{\kappa-1}}, \alpha_{i_{\kappa-2}}, \ldots, \alpha_{i_{\kappa-\mu}}$. Η πηγή πληροφορίας χωρίς μνήμη

είναι ουσιαστικά πηγή πληροφορίας με μνήμη μηδενικής τάξης. Εφόσον μ προηγούμενα σύμβολα πρέπει να διατηρούνται στη μνήμη προκειμένου να διαμορφωθεί η πιθανότητα εμφάνισης του επόμενου συμβόλου, δεν χρησιμοποιούνται μεμονωμένα σύμβολα του αλφαβήτου Α αλλά διατάξεις μ+1 στοιχείων του (σχ. 1.5). Επομένως το αλφάβητο της πηγής πληροφορίας με μνήμη μ-τάξης είναι το σύνολο $A^{\mu+1}$, που χρησιμοποιείται από τη (μ+1)-επέκταση της πηγής πληροφορίας χωρίς μνήμη. Αν το σύνολο Α έχει ρ στοιχεία, η πηγή πληροφορίας με μνήμη μ-τάξης έχει στη διάθεση της $\rho^{\mu+1}$ σύμβολα.

ΠΑΡΑΔΕΙΓΜΑ : Κλασσικό παράδειγμα πηγής πληροφορίας με μνήμη είναι οι διάφορες γλώσσες. Στον πίνακα 1.1 παρουσιάζονται οι πιθανότητες εμφάνισης των γραμμάτων της Αγγλικής και Γερμανικής γλώσσας σε αντίστοιχα αντιπροσωπευτικά κείμενα. Αν προγραμματισθεί ηλεκτρονικός υπολογιστής να λειτουργεί σαν τυχαία γεννήτρια γραμμάτων από το λατινικό αλφάβητο σύμφωνα με τις πιθανότητες εμφάνισης αυτών των γραμμάτων είτε στην Αγγλική είτε στη Γερμανική γλώσσα, τότε μια τυχαία παράγραφος για κάθε γλώσσα θα είχε τη μορφή :

OCRO HLI RTWR NMIELWIS ER IL
NBNESEBYA TH EEI ALHENETTPAQ
OOBTTVA NAH BRL STAXX DEC ET

NNBNNDOET TSI ISLEENS LRI BN
RMET EIKE N HBF BRDAFNN IENH
EN RHN LHO SRD EESRNNLCBR TI

Είναι φανερό ότι δεν υπάρχει δυνατότητα αναγνώρισης της γλώσσας στην οποία αντιστοιχεί κάθε παράγραφος. Αυτό υποδηλώνει ότι τόσο η Αγγλική όσο και η Γερμανική γλώσσα, αλλά και κάθε άλλη γλώσσα, έχουν δομή που δεν αποκαλύπτεται με απλή παράθεση γραμμάτων από το αλφάβητο τους. Είναι γνωστό ότι ορισμένες διατάξεις γραμμάτων είναι περισσότερο πιθανές από άλλες. Σαν παράδειγμα μπορεί να αναφερθεί ότι στην Αγγλική γλώσσα συναντάται συχνά Η μετά από Τ αλλά σπάνια Ζ μετά από Τ. Αν επομένως προσδιορισθούν από αντιπροσωπευτικά κείμενα της Αγγλικής και Γερμανικής γλώσσας οι πιθανότητες εμφάνισης δυάδων γραμμάτων του λατινικού αλφαβήτου, τότε είναι δυνατό να κατασκευασθούν από ηλεκτρονικό υπολογιστή τυχαίες παράγραφοι όπως οι παρακάτω :

ON IE ANTOYTINYS ARE INCTORE
ST BE S DEAMY ACHIN IONASIVE
TYCOO SEACE EDDY CTSBE ANDYR

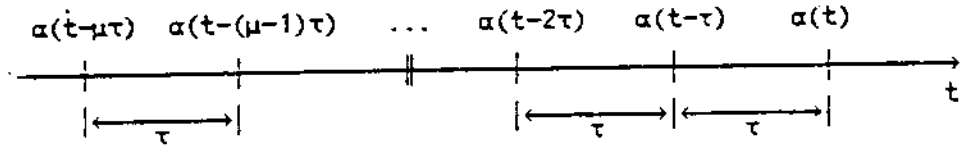
AFERIRTECHSTER DEHABAR DRENN
ZIBERKL DIMASO E DANAHL KENN
N DEI WELT WIERK EIILICHE TE

που αρχίζουν να αποκαλύπτουν, αν και όχι τόσο ξεκάθαρα, την προέλευση τους. Καταλήξεις ή μικρές λέξεις από την Αγγλική γλώσσα εμφανίζονται στην πρώτη παράγραφο και το ίδιο συμβαίνει για τη Γερμανική γλώσσα στη δεύτερη παράγραφο. Το επόμενο βήμα προς την κατεύθυνση αυτή πραγματοποιείται με τριάδες γραμμάτων του λατινικού αλφαβήτου. Οι πιθανότητες εμφάνισης τριάδων γραμμάτων εκτιμώνται από αντιπροσωπευτικά κείμενα των δύο γλωσσών και ο ηλεκτρονικός υπολογιστής μπορεί στη συνέχεια να κατασκευάσει τυχαίες παραγράφους όπως οι παρακάτω :

IN NO IST LAT WHEY CRATICTED
FROERE PRONDENOME PFT DEMONS
TRARES OF THE REPTAKIN IS TO

BET EREINER SOMMEIT SINACH T
ER ALM WIE BEST ALLIENDER CO
LAAFORCHT ABER KONNTE MAN NA

Είναι πλέον σαφές ότι η πρώτη παράγραφος έχει προκύψει από πίνακα με τις πιθανότητες εμφάνισης τριάδων γραμμάτων της Αγγλικής γλώσσας ενώ η δεύτερη παράγραφος αντιστοιχεί στη Γερμανική γλώσσα. Επομένως, οι δύο γλώσσες του παραδείγματος πρέπει να θεωρηθούν σαν πηγές πληροφορίας με μνήμη τουλάχιστο δεύτερης τάξης. Αν η χωρητικότητα του ηλεκτρονικού υπολογιστή επιτρέπει να αποθηκευθούν ολόκληρες λέξεις με την αντίστοιχη πιθανότητα εμφάνισης σε αντιπροσωπευτικό κείμενο της γλώσσας, κάθε τυχαία παράγραφος θα αποκαλύπτει την προέλευση της αλλά επιπλέον είναι δυνατό να κατασκευασθούν τυχαία και προτάσεις με νόημα.



Σχ. 1.6 Διαδοχικές έξοδοι πηγής πληροφορίας με μνήμη μ-τάξης

Το μαθηματικό μοντέλο για την περιγραφή πηγής πληροφορίας με μνήμη εμπλέκει και το χρόνο t αφού ενδιαφέρει η διαδοχή των συμβόλων στην έξοδο της πηγής. Επομένως η πηγή πληροφορίας με μνήμη πρέπει να εκπροσωπείται με διακριτή τυχαία συνάρτηση του χρόνου, έστω A(t) με τιμές $\alpha_1, \alpha_2, \ldots, \alpha_\rho$, και επιπλέον πρέπει να είναι καθορισμένες οι πιθανότητες μετάβασης από μία τιμή σε οποιαδήποτε άλλη. Τέτοιες ιδιότητες εξασφαλίζει κάθε στοχαστική διαδικασία Markov, δηλαδή ένα σύστημα καταστάσεων $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$ εφοδιασμένο με πιθανότητες μεταβάσεων $\pi(\alpha(t) / \alpha(t-\tau), \alpha(t-2\tau), \ldots, \alpha(t-\mu\tau))$, όπου $\alpha(t-\kappa\tau) \in A$, είναι η κατάσταση του συστήματος τη χρονική στιγμή $t-\kappa\tau$, $\kappa = 0, 1, \ldots, \mu$ (σχ. 1.6). Ο ακέραιος αριθμός μ είναι ο *βαθμός του συστήματος* και η *τάξη μνήμης* της αντίστοιχης πηγής πληροφορίας.

Στην απλή περίπτωση πηγής πληροφορίας με μνήμη πρώτης τάξης χρησιμοποιείται σύστημα Markov πρώτου βαθμού. Η πιθανότητα μετάβασης από την κατάσταση α_i στην κατάσταση α_j με ένα βήμα συμβολίζεται ως εξής :

$$\pi_{ij} = \pi_{ij}^{(1)} = \pi(\alpha(t) = \alpha_j / \alpha(t-\tau) = \alpha_i) \qquad (1.27)$$

Ο άνω δείκτης (1) δηλώνει το βαθμό του συστήματος και την τάξη μνήμης της πηγής πληροφορίας. Με τις πιθανότητες π_{ij}, $i,j = 1, 2, \ldots, \rho$, διαμορφώνεται το *μητρώο μεταβάσεων απλού βήματος* :

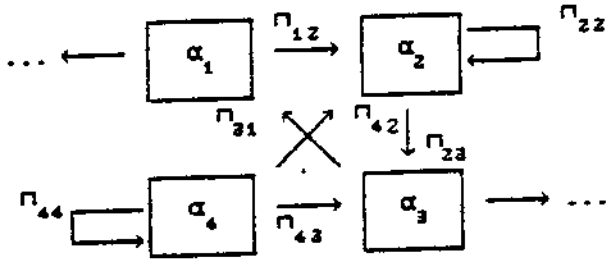
$$\Pi = \begin{bmatrix} \pi_{11} & \pi_{12} & \cdots & \pi_{1\rho} \\ \pi_{21} & \pi_{22} & \cdots & \pi_{2\rho} \\ \cdots & \cdots & \cdots & \cdots \\ \pi_{\rho 1} & \pi_{\rho 2} & \cdots & \pi_{\rho\rho} \end{bmatrix} \qquad (1.28)$$

και είναι φανερό ότι :

$$\sum_{j=1}^{\rho} \pi_{ij} = 1 \quad ; \quad i = 1, 2, \ldots, \rho \qquad (1.29)$$

αφού το σύστημα θα εξελιχθεί από την παρούσα κατάσταση σε κάποια από όλες τις δυνατές καταστάσεις. Γραφική παράσταση του συστήματος Markov προσφέρει το

διάγραμμα καταστάσεων (σχ. 1.7) που περιέχει όλες τις καταστάσεις $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ και τόξο από την α_i στην α_j εφόσον $\pi_{ij} \neq 0$.



Σχ. 1.7 Διάγραμμα καταστάσεων

Η πιθανότητα μετάβασης του συστήματος από την κατάσταση α_i στην α_j με πολλαπλό βήμα, μήκους έστω κτ, συμβολίζεται ως εξής :

$$\pi_{ij}(\kappa) = \pi_{ij}^{(1)}(\kappa) = \pi(\alpha(t) = \alpha_j \ / \ \alpha(t-\kappa\tau) = \alpha_i) \qquad (1.30)$$

και προσδιορίζεται από τις πιθανότητες μετάβασης απλού βήματος μέσω των εκφράσεων που ακολουθούν :

$$\pi_{ij}(\kappa) = \sum_{l=1}^{\rho} \pi_{il}(\kappa-1)\pi_{lj} = \sum_{l_1=1}^{\rho} \sum_{l_2=1}^{\rho} \cdots \sum_{l_{\kappa-1}=1}^{\rho} \pi_{il_1}\pi_{l_1l_2} \cdots \pi_{l_{\kappa-1}j} \qquad (1.31)$$

όπου $l_1, l_2, \ldots, l_{\kappa-1}$ είναι ενδιάμεσες καταστάσεις του συστήματος. Αντίστοιχα διαμορφώνεται το *μητρώο μεταβάσεων πολλαπλού βήματος* :

$$\Pi^{\kappa} = \begin{bmatrix} \pi_{11}(\kappa) & \pi_{12}(\kappa) & \cdots & \pi_{1\rho}(\kappa) \\ \pi_{21}(\kappa) & \pi_{22}(\kappa) & \cdots & \pi_{2\rho}(\kappa) \\ \cdots & \cdots & \cdots & \cdots \\ \pi_{\rho 1}(\kappa) & \pi_{\rho 2}(\kappa) & \cdots & \pi_{\rho\rho}(\kappa) \end{bmatrix} \qquad (1.32)$$

και μάλιστα αποδεικνύεται ότι :

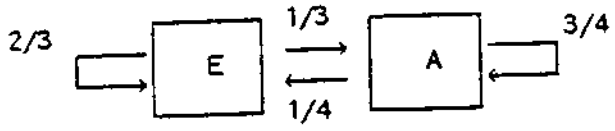
$$\Pi^{\kappa} = \underbrace{\Pi\Pi\ldots\Pi}_{\kappa} \qquad (1.33)$$

ΠΑΡΑΔΕΙΓΜΑ : Έστω παίκτης tennis που εκπαιδεύεται στο service και, όπως είναι φυσικό, επηρεάζεται ψυχολογικά από τον αντίπαλο του που προσπαθεί να επιστρέψει το μπαλάκι. Αν πετύχει σε κάποια προσπάθεια, τότε έχει πιθανότητα 2/3 να επιτύχει πάλι στην επόμενη προσπάθεια. Αν όμως αποτύχει σε κάποια προσπάθεια, δηλαδή αν ο αντίπαλος επιστρέψει το μπαλάκι, τότε στην επόμενη προσπάθεια έχει πιθανότητα 3/4 να αποτύχει πάλι.

Η αβεβαιότητα για την επιτυχία του service συνδιάζεται με ποσότητα πληροφορίας που παρέχεται στο θεατή με κάθε προσπάθεια του παίκτη. Η προπόνηση του παίκτη στο service θα μπορούσε να θεωρηθεί σαν πηγή πληροφορίας δύο συμβόλων, έστω Ε (επιτυχία) και Α (αποτυχία). Είναι φανερό ότι η πηγή πληροφορίας έχει μνήμη αφού κάθε προσπάθεια του παίκτη επηρεάζεται από τις προηγούμενες. Το αντίστοιχο σύστημα Markov έχει δύο καταστάσεις, Ε και Α, και προς το παρόν ακαθόριστο βαθμό. Το μητρώο μεταβάσεων απλού βήματος είναι :

$$\Pi = \begin{bmatrix} \pi_{EE} & \pi_{EA} \\ \pi_{AE} & \pi_{AA} \end{bmatrix} = \begin{bmatrix} 2/3 & 1/3 \\ 1/4 & 3/4 \end{bmatrix}$$

και το διάγραμμα καταστάσεων δίνεται στο σχ. 1.8.



Σχ. 1.8 Διάγραμμα καταστάσεων

Πίνακας 1.2

Πιθανότητες μεταβάσεων πολλαπλού βήματος

κ	1	2	3	4	5	6
$\pi_{EE}(\kappa)$	.667	.528	.470	.446	.436	.432
$\pi_{EA}(\kappa)$	.333	.472	.530	.554	.564	.568
$\pi_{AE}(\kappa)$	.250	.354	.398	.416	.423	.426
$\pi_{AA}(\kappa)$	.750	.646	.602	.584	.577	.573

Οι πιθανότητες μεταβάσεων πολλαπλού βήματος υπολογίζονται με εφαρμογή της εξ.(1.31) (βλ. πίνακα 1.2) και είναι φανερό ότι καθως το βήμα αυξάνει οι πιθανότητες μετάβασης από τη μία κατάσταση στην άλλη τείνουν ασυμπτωτικά προς οριακές τιμές. Αυτό υποδηλώνει ότι η επιτυχία ή αποτυχία της προσπάθειας του παίκτη δεν εξαρτάται από προηγούμενη επιτυχία ή αποτυχία αν έχουν μεσολαβήσει αρκετές προσπάθειες, δηλαδή, όπως είναι φυσικό, ο παίκτης δεν επηρεάζεται από παλιές αλλά μόνο από πρόσφατες προσπάθειες του.

Πριν περιγραφεί η έννοια της εντροπίας για την πηγή πληροφορίας με μνήμη είναι απαραίτητο να οριοθούν μερικές έννοιες σχετικές με το σύστημα Markov.

ΟΡΙΣΜΟΣ : *Αλυσίδα Markov* είναι κάθε ακολουθία διαδοχικών καταστάσεων του συστήματος Markov. Αν το σύστημα Markov περιλαμβανει τις καταστάσεις $\alpha_1, \alpha_2, \ldots, \alpha_\rho$, μια αλυσίδα μπορεί να έχει τη μορφή $\alpha_2\alpha_1\alpha_3\alpha_\rho\alpha_2\alpha_{\rho-2}\alpha_2\ldots$

ΟΡΙΣΜΟΣ : *Στάσιμη αλυσίδα Markov* είναι καθε αλυσιδα με στοιχεία που δεν μεταβάλλονται με το χρόνο. Η στασιμότητα εξυπονοεί ότι το σύστημα Markov χρησιμοποιεί πάντα τις ίδιες καταστάσεις.

ΟΡΙΣΜΟΣ : *Μεταβατική κατάσταση* συστήματος Markov είναι εκείνη που από μία τουλάχιστο διέξοδο προς γειτονική κατάσταση δεν εξασφαλίζει σε διερχόμενη αλυσίδα Markov τη δυνατότητα επανόδου στην εν λογω κατάσταση.

ΟΡΙΣΜΟΣ : *Επανερχόμενη κατάσταση* συστήματος Markov είναι εκείνη που από κάθε διέξοδο προς γειτονική κατάσταση εξασφαλίζει σε διερχόμενη αλυσίδα Markov τη δυνατότητα επανόδου στην εν λόγω κατάσταση.

ΟΡΙΣΜΟΣ : *Περιοδική κατάσταση* συστήματος Markov είναι εκείνη που επιτρέπει σε διερχόμενη αλυσίδα Markov να επιστρέψει στην εν λόγω κατάσταση μόνο με βήματα που είναι ακέραια πολλαπλάσια κάποιου ακεραίου $\lambda > 1$. Επομένως η κατάσταση α_i θεωρείται περιοδική αν $\pi_{ii}(\kappa) = 0$ για $\kappa \neq \lambda, 2\lambda, 3\lambda, \ldots$.

ΟΡΙΣΜΟΣ : *Απορροφητική κατάσταση* συστήματος Markov είναι εκείνη που δεν επιτρέπει σε διερχόμενη αλυσίδα να εξελιχθεί προς άλλη κατάσταση. Επομένως η κατάσταση α_i θεωρείται απορροφητική αν $\pi_{ij} = 0$ για $j \neq i$ οπότε $\pi_{ii} = 1$.

ΟΡΙΣΜΟΣ : *Εργοδικό σύστημα Markov* είναι εκείνο που επιτρέπει προσπέλαση κάθε κατάστασης από οποιαδήποτε άλλη.

ΟΡΙΣΜΟΣ : Αν υπάρχει ακέραιος λ ώστε το μητρώο Π^{κ} να μην περιέχει μηδενικά για $\kappa \geq \lambda$, το σύστημα Markov θεωρείται *κανονικό*. Επομένως σε κανονικό σύστημα Markov όλες οι καταστάσεις γίνονται προσπελάσιμες από οποιαδήποτε κατάσταση με κατάλληλου μεγέθους βήματα. Είναι φανερό ότι κάθε κανονικό σύστημα Markov είναι και εργοδικό. Το αντίστροφο όμως δεν ισχύει. Στο όριο $\kappa \to \infty$ το μητρώο Π^{κ} παίρνει τη μορφή :

$$\lim_{\kappa\to\infty} \begin{bmatrix} \pi_{11}(\kappa) & \pi_{12}(\kappa) & \cdots & \pi_{1\rho}(\kappa) \\ \pi_{21}(\kappa) & \pi_{22}(\kappa) & \cdots & \pi_{2\rho}(\kappa) \\ \cdots & \cdots & \cdots & \cdots \\ \pi_{\rho 1}(\kappa) & \pi_{\rho 2}(\kappa) & \cdots & \pi_{\rho\rho}(\kappa) \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & \cdots & v_\rho \\ v_1 & v_2 & \cdots & v_\rho \\ \cdots & \cdots & \cdots & \cdots \\ v_1 & v_2 & \cdots & v_\rho \end{bmatrix} \qquad (1.34)$$

όπου $Y = \{ v_1, v_2, \ldots, v_\rho \}$ είναι η *οριακή κατανομή πιθανοτήτων* για τις καταστάσεις $\alpha_1, \alpha_2, \ldots, \alpha_\rho$. Η εξ.(1.34) υποδηλώνει ότι η εξέλιξη αλυσίδας σε κανονικό σύστημα Markov γίνεται ανεξάρτητη της κατάστασης εκκίνησης καθώς το μέγεθος του βήματος αυξάνει. Οι οριακές πιθανότητες $v_1, v_2, \ldots, v_\rho$ υπολογίζονται από την μητρωική εξίσωση :

$$\lim_{\kappa\to\infty} \left(\Pi^{\kappa+1}\right) = \lim_{\kappa\to\infty} \left(\Pi^{\kappa}\Pi\right) = \lim_{\kappa\to\infty} \left(\Pi^{\kappa}\right)\Pi \Rightarrow Y = Y\Pi \qquad (1.35)$$

δηλαδή από το γραμμικό σύστημα :

$$\begin{aligned} v_1 &= v_1\pi_{11} + v_2\pi_{21} + \ldots + v_\rho\pi_{\rho 1} \\ v_2 &= v_1\pi_{12} + v_2\pi_{22} + \ldots + v_\rho\pi_{\rho 2} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ v_\rho &= v_1\pi_{1\rho} + v_2\pi_{2\rho} + \ldots + v_\rho\pi_{\rho\rho} \end{aligned} \qquad (1.36)$$

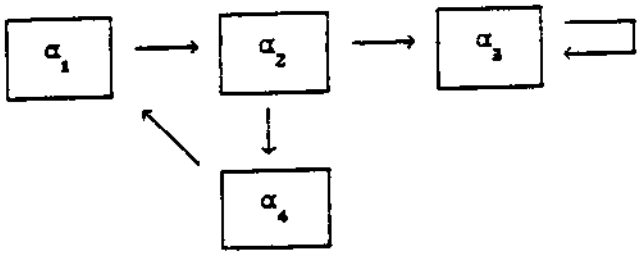
Είναι φανερό ότι υπάρχουν μόνο $\rho-1$ ανεξάρτητες εξισώσεις στο παραπάνω σύστημα. Ο προσδιορισμός των αγνώστων $v_1, v_2, \ldots, v_\rho$ γίνεται όμως δυνατός επειδή

διατίθεται και η συνθήκη :

$$v_1 + v_2 + \ldots + v_\rho = 1 \qquad (1.37)$$

που ισχύει για κάθε καταναμή πιθανοτήτων.

ΠΑΡΑΔΕΙΓΜΑ : Εστω σύστημα Markov με διάγραμμα καταστάσεων όπως στο σχ. 1.9. Το σύστημα Markov είναι στάσιμο αφού δεν υπάρχει κάποια ένδειξη ότι οι καταστάσεις του μεταβάλλονται με το χρόνο. Η κατάσταση α_2 είναι μεταβατική επειδή από τη διέξοδο $\alpha_2 \rightarrow \alpha_3$ οδηγεί διερχόμενη αλυσίδα σε διαδρομή χωρίς δυνατότητα επιστροφής στην α_2 (π.χ., $\ldots\alpha_1\alpha_2\alpha_3\alpha_3\alpha_3\ldots$). Η κατάσταση α_1 είναι επανερχόμενη επειδή από τη διέξοδο $\alpha_1 \rightarrow \alpha_2$, που είναι και η μοναδική για την α_1, επιτρέπει σε διερχόμενη αλυσίδα να επανέλθει στην α_1 (π.χ., $\ldots\alpha_4\alpha_1\alpha_2\alpha_4\alpha_1\ldots$). Η κατάσταση α_4 είναι περιοδική επειδή η διερχόμενη αλυσίδα μπορεί να επιστρέψει στην α_4 μόνο με βήματα μεγέθους 3, 6, 9, ...



Σχ. 1.9 Διάγραμμα καταστάσεων

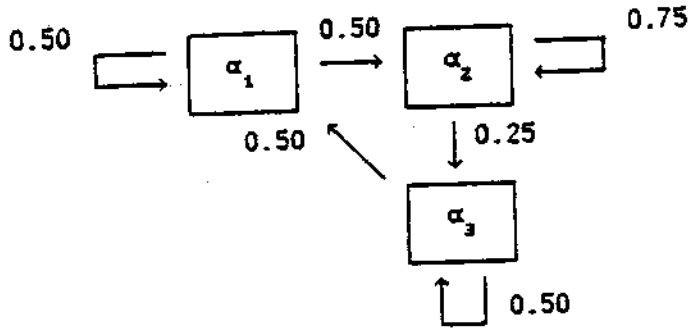
ΠΑΡΑΔΕΙΓΜΑ : Εστω σύστημα Markov με διάγραμμα καταστάσεων όπως στο σχ. 1.10. Είναι φανερό ότι κάθε κατάσταση είναι προσπελάσιμη από οποιαδήποτε κατάσταση και επομένως το σύστημα Markov είναι εργοδικό. Το μητρώο μεταβάσεων απλού βήματος προκύπτει από το διάγραμμα καταστάσεων :

$$\Pi = \begin{bmatrix} 0.50 & 0.50 & 0.00 \\ 0.00 & 0.75 & 0.25 \\ 0.50 & 0.00 & 0.50 \end{bmatrix}$$

Το μητρώο μεταβάσεων διπλού βήματος προκύπτει με εφαρμογή της εξ.(1.33) :

$$\Pi^2 = \begin{bmatrix} 0.50 & 0.50 & 0.00 \\ 0.00 & 0.75 & 0.25 \\ 0.50 & 0.00 & 0.50 \end{bmatrix} \begin{bmatrix} 0.50 & 0.50 & 0.00 \\ 0.00 & 0.75 & 0.25 \\ 0.50 & 0.00 & 0.50 \end{bmatrix} = \begin{bmatrix} 0.25 & 0.62 & 0.13 \\ 0.13 & 0.56 & 0.31 \\ 0.50 & 0.25 & 0.25 \end{bmatrix}$$

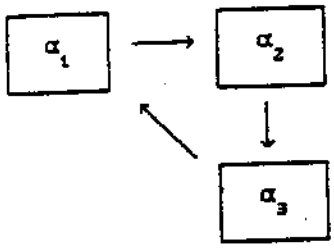
και επειδή δεν περιέχει μηδενικά διαπιστώνεται ότι το σύστημα Markov είναι κανονικό. Εξάλλου με εφαρμογή των εξ.(1.36).(1.37) προκύπτουν οι οριακές πιθανότητες $v_1 = 0.25$, $v_2 = 0.5$, $v_3 = 0.25$.



Σχ. 1.10 Διάγραμμα καταστάσεων

ΠΑΡΑΔΕΙΓΜΑ : Εστω σύστημα Markov με διάγραμμα καταστάσεων όπως στο σχ. 1.11. Είναι φανερό ότι κάθε κατάσταση είναι προσπελάσιμη από οποιαδήποτε κατάσταση και επομένως το σύστημα Markov είναι εργοδικό. Το μητρώο μεταβάσεων απλού βήματος προκύπτει από το διάγραμμα καταστάσεων :

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



Σχ. 1.11 Διάγραμμα καταστάσεων

Με εφαρμογή της εξ.(1.33) διαπιστώνεται ότι τα μητρώα Π^2, Π^3 έχουν μηδενικά στοιχεία. Επιπλέον αποδεικνύεται ότι $\Pi^4 = \Pi$ και επομένως το σύστημα Markov δεν μπορεί να είναι κανονικό.

Έστω κανονικό σύστημα Markov με καταστάσεις $\alpha_1, \alpha_2, \ldots, \alpha_\rho$, αντίστοιχες πιθανότητες $\pi_1, \pi_2, \ldots, \pi_\rho$ και αλυσίδα που διέρχεται από κάποια κατάσταση α_i. Στο επόμενο βήμα η αλυσίδα θα εξελιχθεί προς κάποια από τις διαθέσιμες καταστάσεις $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ και η αντίστοιχη πιθανότητα για καθένα από αυτά τα ενδεχόμενα είναι $\pi_{i1}, \pi_{i2}, \ldots, \pi_{i\rho}$. Η αβεβαιότητα για την εξέλιξη της αλυσίδας στο επόμενο βήμα αντιστοιχεί σε ποσότητα πληροφορίας που παρέχεται σε παρατηρητή του συστήματος και η μέση τιμή της είναι :

$$H(\alpha_i) = -\sum_{j=1}^{\rho} \pi_{ij} \log_e(\pi_{ij}) \qquad (1.38)$$

αφού οι αριθμοί $\pi_{i1}, \pi_{i2}, \ldots, \pi_{i\rho}$ συνιστούν κατανομή πιθανότητας. Η μέση τιμή της ποσότητας πληροφορίας $H(\alpha_i)$ ως προς τις δυνατές καταστάσεις εκκίνησης του επόμενου βήματος ορίζεται σαν *εντροπία επόμενου βήματος* της αντίστοιχης πηγής πληροφορίας με μνήμη και είναι :

$$H(A) = \sum_{i=1}^{\rho} \pi(\alpha_i) H(\alpha_i) = -\sum_{i=1}^{\rho} \sum_{j=1}^{\rho} \pi_i \pi_{ij} \log_e(\pi_{ij}) \qquad (1.39)$$

με $\pi_i = \pi(\alpha_i)$ την πιθανότητα να βρεθεί η αλυσίδα στην κατάσταση εκκίνησης α_i, $i = 1, 2, \ldots, \rho$. Αν αγνοηθεί η μνήμη του συστήματος (σχ. 1.5), τα σύνολα $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$ και $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$ ορίζουν την *προσαρτημένη πηγή πληροφορίας* που έχει εντροπία :

$$H(A^a) = -\sum_{i=1}^{\rho} \pi_i \log_e(\pi_i) \qquad (1.40)$$

Η εξέλιξη της αλυσίδας με πολλαπλό βήμα αντιστοιχεί στην *εντροπία πολλαπλού βήματος* :

$$H^{\kappa}(A) = \sum_{i=1}^{\rho} \pi_i H^{\kappa}(\alpha_i) = - \sum_{i=1}^{\rho} \sum_{j=1}^{\rho} \pi_i \pi_{ij}(\kappa) \log_e \left[\pi_{ij}(\kappa) \right] \qquad (1.41)$$

Αν $\Pi_A = Y$, οι εξ.(1.39), (1.41) δίνουν αντίστοιχα την *οριακή εντροπία απλού βήματος* :

$$H(A) = \sum_{i=1}^{\rho} u_i H(\alpha_i) = - \sum_{i=1}^{\rho} \sum_{j=1}^{\rho} u_i \pi_{ij} \log_e (\pi_{ij}) \qquad (1.42)$$

και την οριακή εντροπία πολλαπλού βήματος :

$$H^{\kappa}(A) = \sum_{i=1}^{\rho} u_i H^{\kappa}(\alpha_i) = - \sum_{i=1}^{\rho} \sum_{j=1}^{\rho} u_i \pi_{ij}(\kappa) \log_e \left[\pi_{ij}(\kappa) \right] \qquad (1.43)$$

Με την προϋπόθεση $\pi_i = u_i$, $i = 1, 2, \ldots, \rho$, αποδεικνύεται (βλ. §1.II) ότι $H^{\kappa}(A) = \kappa H(A)$, δηλαδή :

$$H^{\kappa+\lambda}(A) = H^{\kappa}(A) + H^{\lambda}(A) = (\kappa+\lambda) H(A) \qquad (1.44)$$

Η εξ.(1.44) περιγράφει την αθροιστική ιδιότητα της παροχής πληροφορίας από την εξέλιξη αλυσίδας σε κανονικό σύστημα Markov. Αντίστοιχα ορίζεται και η *οριακή εντροπία* :

$$H^{\infty}(A) = - \sum_{i=1}^{\rho} u_i \log_e (u_i) \qquad (1.45)$$

που είναι ουσιαστικά η εντροπία της προσαρτημένης πηγής πληροφορίας A, Y. Εύκολα αποδεικνύεται (βλ. §1.III) ότι :

$$H(A) \leq H^{\infty}(A) \leq \log_e (\rho) \qquad (1.46)$$

που δείχνει ότι η ύπαρξη μνήμης ελαττώνει την αβεβαιότητα για το επόμενο σύμβολο στην έξοδο της πηγής πληροφορίας.

ΠΑΡΑΔΕΙΓΜΑ : Έστω η πηγή πληροφορίας $A = (\alpha_1, \alpha_2, \alpha_3)$, $\Pi_A = (1/3, 1/2, 1/6)$ με μνήμη πρώτης τάξης. Δίνονται οι πιθανότητες μεταβάσεων απλού βήματος :

$$\Pi = \begin{bmatrix} 0.00 & 0.40 & 0.60 \\ 0.25 & 0.75 & 0.00 \\ 0.50 & 0.40 & 0.10 \end{bmatrix}$$

Το μητρώο μεταβάσεων δυπλού βήματος προκύπτει με εφαρμογή της εξ.(1.33) :

$$\Pi^2 = \begin{bmatrix} 0.00 & 0.40 & 0.60 \\ 0.25 & 0.75 & 0.00 \\ 0.50 & 0.40 & 0.10 \end{bmatrix} \begin{bmatrix} 0.00 & 0.40 & 0.60 \\ 0.25 & 0.75 & 0.00 \\ 0.50 & 0.40 & 0.10 \end{bmatrix} = \begin{bmatrix} 0.40 & 0.54 & 0.06 \\ 0.19 & 0.66 & 0.15 \\ 0.15 & 0.54 & 0.31 \end{bmatrix}$$

και δείχνει ότι το σύστημα Markov είναι κανονικό. Με εφαρμογή των εξ.(1.36), (1.37) προσδιορίζεται η οριακή καταναμή πιθανοτήτων :

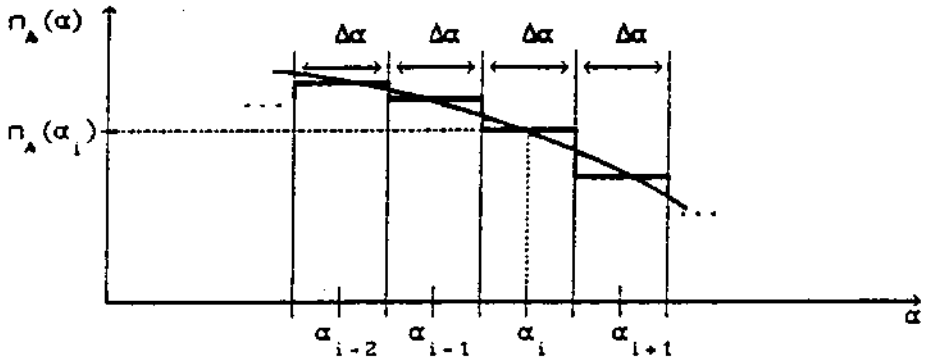
$$v_1 = 0.23, \; v_2 = 0.615, \; v_3 = 0.155$$

Από τις εξ.(1.39), (1.40) προκύπτουν αντίστοιχα η εντροπία απλού βήματος $H(A) = 0.956$ bits/σύμβολο, και η εντροπία της προσαρτημένης πηγής $H(A^2) = 1.459$ bits/σύμβολο. Εξάλλου από τις εξ.(1.42), (1.45) υπολογίζονται αντίστοιχα η οριακή εντροπία απλού βήματος $H(A) = 0.933$ bits/σύμβολο και η οριακή εντροπία $H^{\infty}(A) = 1.336$ bits/σύμβολο. Είναι φανερό ότι $H(A) \leq H^{\infty}(A) \leq \log_2 3 = 1.585$ bits/σύμβολο, όπως προβλέπει η εξ.(1.46).

1.7 ΑΝΑΛΟΓΙΚΗ ΠΗΓΗ ΠΛΗΡΟΦΟΡΙΑΣ

Οι πηγές πληροφορίας που εξετάσθηκαν μέχρι το σημείο αυτό περιγράφονται με διακριτή τυχαία μεταβλητή. Τα σύμβολα πληροφορίας αντιστοιχούν στις διακριτές τιμές της τυχαίας μεταβλητής και εμφανίζονται με συχνότητα που καθορίζεται από την αντίστοιχη καταναμή πιθανοτήτων. Σε πολλές εφαρμογές το μέγεθος που εγκλείει πληροφορία μεταβάλλεται συνεχώς σε κάποιο διάστημα τιμών. Επομένως υπάρχουν άπειρες τιμές για το μέγεθος και αντίστοιχα άπειρα σύμβολα πληροφορίας. Η πιθανότητα εμφάνισης καθενός από αυτά είναι απειροστή. Αντίθετα είναι πεπερασμένη η πιθανότητα να κυμαίνεται η έξοδος της αναλογικής πηγής σε

απειροστό διάστημα τιμών. Είναι επομένως φανερό ότι η αναλογική πηγή πληροφορίας πρέπει να εκπροσωπείται από συνεχή τυχαία μεταβλητή (βλ. §1.I.3), έστω A, δηλαδή συνεχές διάστημα τιμών $[\ \alpha_{min}, \alpha_{max}\ ]$ με την προσαρτημένη σ' αυτό καταναμή πυκνότητας πιθανότητας $\pi_A(\alpha)$.



Σχ. 1.12 Διακριτοποίηση συνεχούς τυχαίας μεταβλητής

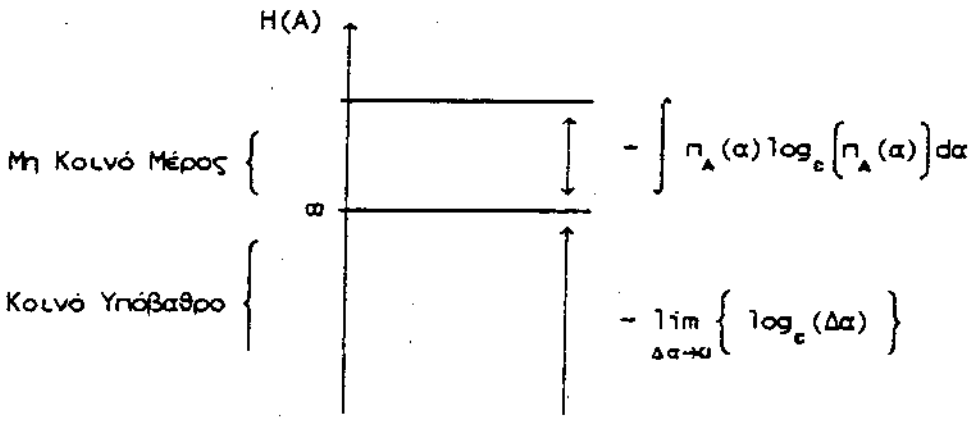
Η εντροπία αναλογικής πηγής πληροφορίας φαίνεται λογικό να υπολογισθεί κατ' αναλογία με την εντροπία διακριτής πηγής πληροφορίας (βλ. §1.2). Η μετατροπή της συνεχούς τυχαίας μεταβλητής A σε διακριτή πραγματοποιείται με υποδιαίρεση του πεδίου τιμών $[\ \alpha_{min}, \alpha_{max}\ ]$ σε διαστήματα πλάτους $\Delta\alpha$ στα οποία είναι πρακτικά σταθερή η συνάρτηση καταναμής πυκνότητας πιθανότητας $\pi_A(\alpha)$ (σχ. 1.12). Σαν σύμβολα πληροφορίας θεωρούνται οι τιμές α_i, $i = 1, 2, \ldots$, που εμφανίζονται με πιθανότητα $\pi_A(\alpha_i)\Delta\alpha$. Στο όριο $\Delta\alpha \to 0$ η εντροπία της διακριτοποιημένης πηγής πληροφορίας πρέπει να είναι η μέση πληροφορία που παρέχει η αναλογική πηγή :

$$H(A) = \lim_{\Delta\alpha\to 0}\left\{ -\sum_i \left[\pi_A(\alpha_i)\Delta\alpha\right]\log_e\left[\pi_A(\alpha_i)\Delta\alpha\right] \right\} =$$

$$= -\int \pi_A(\alpha)\log_e\left[\pi_A(\alpha)\right]d\alpha - \lim_{\Delta\alpha\to 0}\left\{ \log_e(\Delta\alpha) \right\} \qquad (1.47)$$

Είναι φανερό ότι ο δεύτερος όρος στο δεξιό μέλος της εξ.(1.47) τείνει προς το άπειρο. Επομένως η εντροπία της αναλογικής πηγής πληροφορίας είναι άπειρη. Αυτό δεν είναι παράδοξο αφού η πιθανότητα εμφάνισης οποιουδήποτε συμβόλου είναι απειροστή και κατά συνέπεια υπάρχει άπειρη αβεβαιότητα για την τιμή του μεγέθους στην έξοδο της αναλογικής πηγής. Ο πρώτος όρος στο δεξιό μέλος της εξ.(1.47)

περιγράφει επίσης μια ποσότητα πληροφορίας που παρέχει η αναλογική πηγή επιπλέον εκείνης που εκπροσωπεί ο δεύτερος όρος. Στον υπολογισμό αυτής της πρόσθετης ποσότητας πληροφορίας εμπλέκεται η κατανομή πυκνότητας πιθανότητας που αποτελεί ιδιαίτερο χαρακτηριστικό της αναλογικής πηγής. Δηλαδή, η εντροπία κάθε αναλογικής πηγής είναι μεν άπειρη αλλά προκύπτει σαν άθροισμα μιας άπειρης ποσότητας πληροφορίας, που είναι κοινή σε όλες τις αναλογικές πηγές, και μιας πεπερασμένης ποσότητας, που αντιστοιχεί στη συγκεκριμένη αναλογική πηγή (σχ. 1.13).



Σχ. 1.13 Μέση ποσότητα πληροφορίας στην έξοδο αναλογικής πηγής

Είναι επομένως λογικό να οριοθεί :

$$H(A) = -\int p_A(\alpha)\log_e\left[p_A(\alpha)\right]d\alpha \qquad (1.48)$$

σαν εντροπία της αναλογικής πηγής ενώ είναι σαφές ότι έτσι υπολογίζεται μόνο μέρος της ποσότητας πληροφορίας που παρέχει η αναλογική πηγή. Η έκφραση της εξ.(1.48) για την εντροπία της αναλογικής πηγής πληροφορίας παρουσιάζει τελικά εξαιρετική ομοιότητα με την αντίστοιχη έκφραση για διακριτή πηγή πληροφορίας. Υπάρχουν όμως και διαφορές που αποκαλύπτονται μέσα από τις παρακάτω ιδιότητες.

ΙΔΙΟΤΗΤΑ : Η εντροπία αναλογικής πηγής πληροφορίας μεταβάλλεται με κάθε μετασχηματισμό κατά το σχήμα :

$$H(B) = H(A) - E\left\{ \log_e\left[|J(A/B)| \right] \right\} =$$

$$= H(A) - \int n_A(\alpha) \log_e\left[|J(A/B)| \right] d\alpha \qquad (1.49)$$

όπου $J(A/B)$ είναι η Ιακωβιανή του μετασχηματισμού $A \to B$ (βλ. 1.IV). Είναι φανερό ότι η διαφοροποίηση της εντροπίας είναι η προσδοκητή τιμή του λογαρίθμου της Ιακωβιανής του μετασχηματισμού.

ΠΑΡΑΔΕΙΓΜΑ : Η έξοδος αναλογικής πηγής πληροφορίας ενισχύεται κατά σταθερό παράγοντα. Ο μετασχηματισμός περιγράφεται με τη σχέση $B = \kappa A$, όπου $\kappa > 0$ είναι ο σταθερός παράγων ενίσχυσης. Η Ιακωβιανή του μετασχηματισμού $A \to B$ είναι $J(A/B) = dA/dB = 1/\kappa$ και η εξ.(1.49) δίνει με τις προϋποθέσεις αυτές :

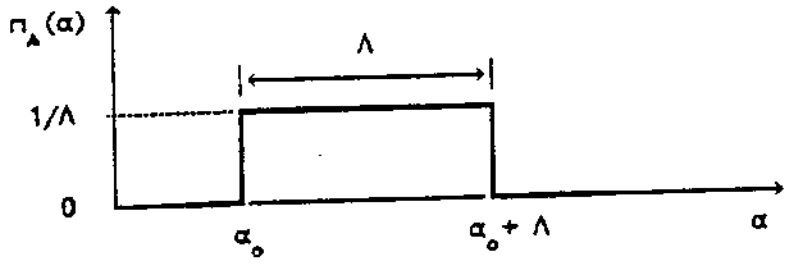
$$H(B) = H(A) + \log_e(\kappa) \qquad (1.50)$$

Η εξ.(1.50) υποδηλώνει αύξηση της μέσης πληροφορίας που παρέχει η αναλογική πηγή για ενίσχυση του σήματος εξόδου, δηλαδή για $\kappa > 1$, και μείωση της μέσης πληροφορίας για απόσβεση του σήματος εξόδου, δηλαδή για $\kappa < 1$. Αυτό είναι λογικό επειδή το πεδίο τιμών της εξόδου διαστέλλεται για $\kappa > 1$ ενώ συστέλλεται για $\kappa < 1$.

ΠΑΡΑΔΕΙΓΜΑ : Η έξοδος αναλογικής πηγής πληροφορίας μεταβάλλεται κατά σταθερό όρο. Ο μετασχηματισμός περιγράφεται με τη σχέση $B = A + \kappa$ με κ το σταθερό όρο που, με την προϋπόθεση $E(A) = 0$, εκπροσωπεί τη μέση τιμή της τυχαίας μεταβλητής B. Η Ιακωβιανή του μετασχηματισμού $A \to B$ είναι $J(A/B) = dA/dB = 1$ και η εξ.(1.49) δίνει $H(B) = H(A)$. Επομένως η εντροπία της αναλογικής πηγής πληροφορίας δεν επηρεάζεται από μεταβολές της μέσης τιμής της.

ΙΔΙΟΤΗΤΑ : Η εντροπία αναλογικής πηγής πληροφορίας δεν είναι μη αρνητικό μέγεθος. Υπενθυμίζεται ότι η εντροπία διακριτής πηγής πληροφορίας είναι μη αρνητικό μέγεθος.

ΠΑΡΑΔΕΙΓΜΑ : Εστω αναλογική πηγή πληροφορίας που εκπροσωπείται από τη συνεχή τυχαία μεταβλητή A με ομοιόμορφη κατανομή πυκνότητας πιθανότητας στο διάστημα $[\, \alpha_o, \alpha_o + \Lambda \,]$ (σχ. 1.14).



Σχ. 1.14 Συνεχής τυχαία μεταβλητή με ομοιόμορφη κατανομή πυκνότητας πιθανότητας.

Με εφαρμογή του ορισμού προκύπτει :

$$H(A) = -\int_{\alpha_o}^{\alpha_o+\Lambda} \frac{1}{\Lambda} \log_e\left(\frac{1}{\Lambda}\right) d\alpha = \log_e(\Lambda) \qquad (1.51)$$

και επομένως $H(A) \geq 0$ αν $\Lambda \geq 1$ ενώ $H(A) < 0$ αν $\Lambda < 1$.

ΙΔΙΟΤΗΤΑ : Το μέγιστο της εντροπίας αναλογικής πηγής πληροφορίας και η αντίστοιχη κατανομή πυκνότητας πιθανότητας εξαρτώνται από τις επιβαλλόμενες συνθήκες. Για το προσδιορισμό του μεγίστου εφαρμόζεται η μέθοδος των πολλαπλασιαστών Lagrange. Η συνάρτηση που πρέπει να μεγιστοποιηθεί γράφεται με τη μορφή :

$$H(A) = -\int p_A(\alpha) \log_e\left[p_A(\alpha)\right] d\alpha = \int F(\alpha, p_A)\, d\alpha \qquad (1.52)$$

ενώ οι επιβαλλόμενες συνθήκες περιγράφονται με τις σχέσεις :

$$\int F_i(\alpha, p_A)\, d\alpha = \lambda_i \quad ; \quad i = 1, 2, \ldots, v \qquad (1.53)$$

όπου $\lambda_1, \lambda_2, \ldots, \lambda_v$ είναι κάποιες σταθερές. Η συνάρτηση κατανομής πυκνότητας πιθανότητας που μεγιστοποιεί την εντροπία προσδιορίζεται από τη διαφορική εξίσωση :

$$\frac{\partial F}{\partial \pi_A} + \sum_{i=1}^{v} \kappa_i \frac{\partial F_i}{\partial \pi_A} = 0 \qquad (1.54)$$

όπου $\kappa_1, \kappa_2, \ldots, \kappa_v$ είναι προσδιοριστέες σταθερές. Οι τελευταίες προκύπτουν με αντικατάσταση της συνάρτησης π_A, που επιλύει την εξ.(1.54), στις ν συνθήκες (εξ.(1.53)).

ΠΑΡΑΔΕΙΓΜΑ : Εστω αναλογική πηγή πληροφορίας που εκπροσωπείται από συνεχή τυχαία μεταβλητή με (σταθερή) τυπική απόκλιση σ_A. Το μέγιστο της εντροπίας καθορίζεται από τις επιβαλλόμενες συνθήκες :

$$\int \pi_A(\alpha)\, d\alpha = 1, \quad \int \alpha^2 \pi_A(\alpha)\, d\alpha = \sigma_A^2 \qquad (1.55)$$

Επομένως $F_1(\alpha,\pi_A) = \pi_A(\alpha)$, $F_2(\alpha,\pi_A) = \alpha^2\pi_A(\alpha)$ και η εξ.(1.54) παίρνει εδώ τη μορφή :

$$\frac{\partial(-\pi_A \log_e \pi_A)}{\partial \pi_A} + \kappa_1 + \kappa_2\alpha^2 = 0 \qquad (1.56)$$

από την οποία προκύπτει αμέσως :

$$\pi_A(\alpha) = \exp\left\{ (\kappa_1 + \kappa_2\alpha^2)\ln e - 1 \right\} \qquad (1.57)$$

Με αντικατάσταση στις συνθήκες (εξ.(1.55)) υπολογίζονται μετά από μερικές πράξεις οι σταθερές κ_1, κ_2 :

$$\kappa_1 = \log_e\left(\frac{e}{\sigma_A\sqrt{2\pi}} \right)$$

$$\kappa_2 = -\frac{1}{2\sigma_A^2 \ln e} \qquad (1.58)$$

και στη συνέχεια από την εξ.(1.57) διαμορφώνεται η τελική έκφραση για την

καταναμή πυκνότητας πιθανότητας :

$$n_A(\alpha) = \frac{1}{\sigma_A\sqrt{2\pi}} \exp\left\{ - \frac{\alpha^2}{2\sigma_A^2} \right\} \qquad (1.59)$$

Επομένως για τη μεγιστοποίηση της εντροπίας με τις συνθήκες του παραδείγματος απαιτείται κανονική καταναμή πυκνότητας πιθανότητας με τυπική απόκλιση σ_A. Η έκφραση της εξ.(1.59) δείχνει ότι η μέση τιμή της τυχαίας μεταβλητής A είναι μηδέν. Αυτό δεν σημαίνει ότι η έξοδος της αναλογικής πηγής πληροφορίας έχει μέση τιμή μηδέν αλλά μόνο ότι δεν έχει τεθεί κάποια συνθήκη σχετική με τη μέση τιμή. Εξάλλου έχει ήδη αποδειχθεί ότι η εντροπία αναλογικής πηγής πληροφορίας δεν επηρεάζεται από μεταβολές της μέσης τιμής της εξόδου της. Αν συνδυασθούν οι εξ.(1.59),(1.48), προκύπτει η παρακάτω έκφραση για τη μέγιστη τιμή της εντροπίας με τις συνθήκες του παραδείγματος :

$$H(A) = \log_e\left(\sigma_A\sqrt{2\pi e} \right) \qquad (1.60)$$

Αλλά η τυπική απόκλιση της συνεχούς τυχαίας μεταβλητής που εκπροσωπεί αναλογική πηγή πληροφορίας αντιστοιχεί στο πλήθος συμβόλων του αλφαβήτου διακριτής πηγής πληροφορίας. Με την εξ.(1.60) επαναλαμβάνεται ουσιαστικά το συμπέρασμα της §1.2 ότι η μέγιστη τιμή της εντροπίας απλής πηγής πληροφορίας δίνεται από το λογάριθμο του πλήθους των συμβόλων της.

1.8 ΑΣΚΗΣΕΙΣ

1. Να υπολογισθεί η πληροφορία που συνοδεύει αριθμό κυκλοφορίας αυτοκινήτου της μορφής AAAXXXX, όπου A είναι γράμμα και X αριθμός.

2. Το μόριο DNA χρωματοσώματος περιέχει 3×10^6 κόμβους. Σε κάθε κόμβο είναι προσαρμοσμένη κάποια τριάδα των χημικών ουσιών A, C, G και U, π.χ. ACU. Η γενετική ταυτότητα του ανθρώπου διαμορφώνεται απο τη δομή των 48 χρωματοσωμάτων του. Να υπολογισθεί η ποσότητα πληροφορίας με την οποία έρχεται στον κόσμο κάθε

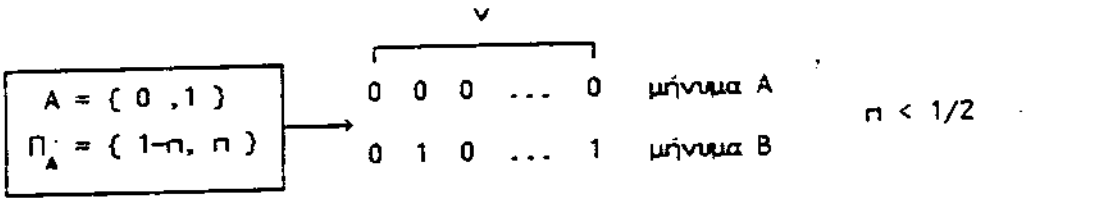
νεογέννητο.

3. Πηγή πληροφορίας έχει αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$ και κατανομή πιθανοτήτων $\Pi_A = \{ 0.3, 0.5, 0.2 \}$. Να υπολογισθεί η αυτοπληροφορία κάθε συμβόλου και η εντροπία της πηγής πληροφορίας. Για να βελτιωθεί η πιθανότητα ορθής μετάδοσης, κάθε σύμβολο εκπέμπεται τρείς φορές. Να υπολογισθεί η εντροπία και ο ρυθμός εκπομπής πληροφορίας στην περίπτωση αυτή.

4. Εστω πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2 \}$ και κατανομή πιθανοτήτων $\Pi_A = \{ 0.25, 0.75 \}$. Αλλη πηγή πληροφορίας με αλφάβητο $B = \{ \beta_1, \beta_2, \beta_3 \}$ σχετίζεται με την πηγή πληροφορίας A,Π_A μέσω των υπό συνθήκη πιθανοτήτων $\pi(\beta_1/\alpha_1) = 0.25$, $\pi(\beta_2/\alpha_1) = 0.35$, $\pi(\beta_3/\alpha_1) = 0.40$, $\pi(\beta_1/\alpha_2) = 0.10$, $\pi(\beta_2/\alpha_2) = 0.70$, $\pi(\beta_3/\alpha_2) = 0.20$. Να υπολογισθούν : η εντροπία $H(A)$, η εντροπία $H(B)$, η συνδετική εντροπία $H(AB)$ και οι υπό συνθήκη εντροπίες $H(A/B)$, $H(B/A)$.

5. Δίνονται τρεις διακριτές πηγές πληροφορίας με κοινό αλφάβητο $Q = \{ q_1, q_2, \ldots, q_\rho \}$ και κατανομή πιθανοτήτων $\Pi_\kappa = \{ \pi_\kappa(q_1), \pi_\kappa(q_2), \ldots, \pi_\kappa(q_\rho) \}$, $\kappa = A, B, \Gamma$, αντίστοιχα. Αν είναι γνωστό ότι ισχύει $\epsilon\pi_A(q_i) + (1-\epsilon)\pi_B(q_i) = \pi_\Gamma(q_i)$, $i = 1, 2, \ldots, \rho$, να αποδειχθεί ότι $\epsilon H(A) + (1-\epsilon)H(B) \leq H(\Gamma)$, όπου $H(A)$, $H(B)$, $H(\Gamma)$ είναι οι εντροπίες των τριών πηγών πληροφορίας.

6. Δυαδική πηγή πληροφορίας παράγει μήνυμα Α, που περιέχει ν μηδενικά, και μήνυμα Β, που περιέχει $\epsilon \geq 0$ μονάδες και $\nu-\epsilon$ μηδενικά, όπως φαίνεται στο παρακάτω σχήμα. Αν π_A, π_B είναι αντίστοιχα οι πιθανότητες των μηνυμάτων Α, Β, να επιλεγεί από τις σχέσεις $\pi_A > \pi_B$, $\pi_A = \pi_B$, $\pi_A < \pi_B$ εκείνη που είναι ορθή και να αιτιολογηθεί η επιλογή.



Κάθε μήνυμα ν ψηφίων που περιέχει $\epsilon = \pi\nu$ μονάδες και $\nu-\epsilon = (1-\pi)\nu$ μηδενικά ονομάζεται *ε-τυπικό μήνυμα*. Αν η πηγή πληροφορίας παράγει 10^6 μηνύματα ν ψηφίων, πόσα από αυτά αναμένεται να έχουν τη μορφή ε-τυπικού μηνύματος; (Εφαρμογή για $\nu = 20$ και $\pi = 0.3$).

7. Πηγή πληροφορίας με μνήμη πρώτης τάξης και αλφάβητο $A = \{ \alpha_1, \alpha_2 \}$ εκπροσωπείται από σύστημα Markov πρώτου βαθμού με μητρώο μεταβάσεων απλού βήματος :

$$\Pi = \begin{bmatrix} 1-\pi & \pi \\ \sigma & 1-\sigma \end{bmatrix}$$

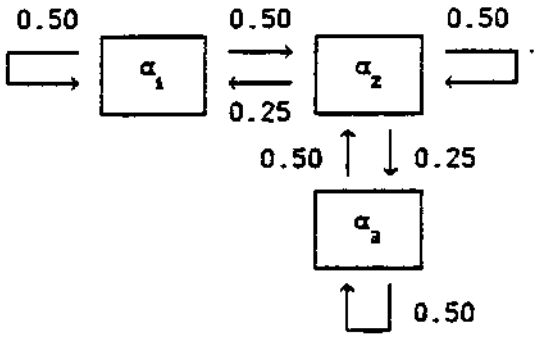
Να σχεδιασθεί το διάγραμμα καταστάσεων και να υπολογισθούν η οριακή κατανομή πιθανοτήτων, η οριακή εντροπία απλού βήματος και η οριακή εντροπία της πηγής πληροφορίας.

8. Πηγή πληροφορίας με μνήμη πρώτης τάξης έχει αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$, κατανομή πιθανοτήτων $\Pi_A = \{ 1/3, 16/27, 2/27 \}$ και μητρώο μεταβάσεων απλού βήματος :

$$\Pi = \begin{bmatrix} 0 & 4/5 & 1/5 \\ 1/2 & 1/2 & 0 \\ 1/2 & 2/5 & 1/10 \end{bmatrix}$$

Να σχεδιασθεί το διάγραμμα καταστάσεων, να εξετασθεί η κανονικότητα και η εργοδικότητα της πηγής και να υπολογισθεί η οριακή κατανομή πιθανοτήτων.

9. Πηγή πληροφορίας με μνήμη πρώτης τάξης έχει αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$ και κατανομή πιθανοτήτων $\Pi_A = \{ 1/8, 3/8, 1/2 \}$. Στο παρακάτω σχήμα δίνεται το διάγραμμα καταστάσεων του αντίστοιχου συστήματος Markov πρώτου βαθμού.



Να προσδιορισθούν το μητρώο μεταβάσεων απλού βήματος και το μητρώο μεταβάσεων

διπλού βήματος. Να υπολογισθούν η πιθανότητα $p_{32}(3)$, η οριακή κατανομή πιθανοτήτων, η εντροπία απλού βήματος, η εντροπία διπλού βήματος, η εντροπία της προσαρτημένης πηγής πληροφορίας και η οριακή εντροπία.

10. Να υπολογισθεί η εντροπία αναλογικής πηγής πληροφορίας A, $H_A(\alpha)$ με κατανομή πυκνότητας πιθανότητας :

$$p_A(\alpha) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left\{-\left(\frac{\alpha-\mu}{\sigma}\right)^2\right\}$$

όπου μ και σ είναι σταθερές.

11. Να υπολογισθεί το μέγιστο της εντροπίας αναλογικής πηγής πληροφορίας A, $H_A(\alpha)$ και η κατάλληλη κατανομή πυκνότητας πιθανότητας με τη συνθήκη η τυχαία μεταβλητή A να παίρνει μόνο θετικές τιμές με μέγιστη τιμή E.

12. Να υπολογισθεί το μέγιστο της εντροπίας αναλογικής πηγής πληροφορίας A, $H_A(\alpha)$ και η κατάλληλη κατανομή πυκνότητας πιθανότητας με τις συνθήκες (α) η τυχαία μεταβλητή A να παίρνει μη αρνητικές τιμές και (β) η μέση τιμή της να είναι η σταθερά $\mu > 0$.

1.Ι ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΠΙΘΑΝΟΤΗΤΩΝ

1.Ι.1 ΣΥΝΟΛΑ

ΟΡΙΣΜΟΣ : *Σύνολο* είναι κάθε συλλογή ευθαίρετων αντικειμένων. Τα μέλη της συλλογής χαρακτηρίζονται *στοιχεία* του συνόλου. Στη συνέχεια θα συμβολίζονται τα σύνολα με κεφαλαία γράμματα (π.χ. A, B, Γ, ...) και τα στοιχεία συνόλων με μικρά γράμματα (π.χ. α, β, γ, ...)

ΟΡΙΣΜΟΣ : *Κλάση* είναι κάθε σύνολο με στοιχεία που είναι επίσης σύνολα. Συμβολίζονται με κεφαλαία κεκλιμένα γράμματα (π.χ. *A*, *B*, *Γ*, ...).

ΟΡΙΣΜΟΣ : *Κενό* σύνολο 0 είναι το μοναδικό σύνολο χωρίς στοιχεία.

ΟΡΙΣΜΟΣ : *Πεπερασμένο* σύνολο είναι κάθε σύνολο με πεπερασμένο πλήθος στοιχείων.

ΟΡΙΣΜΟΣ : *Απειροσύνολο* είναι κάθε σύνολο με άπειρο πλήθος στοιχείων.

ΟΡΙΣΜΟΣ : *Αριθμήσιμο* σύνολο είναι κάθε σύνολο που αντιστοιχεί αμφιμονοσήμαντα σε κάποιο απόκομμα του συνόλου N των φυσικών αριθμών.

ΟΡΙΣΜΟΣ : Το σύνολο A είναι *υποσύνολο* του συνόλου B αν και μόνο αν $\forall\, \alpha \in A \Rightarrow \alpha \in B$. Η σχέση μεταξύ των συνόλων A, B συμβολίζεται $A \subset B$ ή $B \supset A$ και το σύνολο B χαρακτηρίζεται *υπερσύνολο* του συνόλου A.

ΟΡΙΣΜΟΣ : *Χώρος* Ω είναι το υπερσύνολο όλων των συνόλων.

ΟΡΙΣΜΟΣ : *Χώρος συνόλων* $S(\Omega)$ είναι η κλάση όλων των υποσυνόλων του χώρου Ω.

ΟΡΙΣΜΟΣ : *Συμπλήρωμα* συνόλου A είναι το σύνολο $A^c = \{ \alpha \,/\, \alpha \notin A \}$. Είναι φανερό ότι $(A^c)^c = A$.

ΠΟΡΙΣΜΑ : $\Omega^c = 0$ και $0^c = \Omega$.

ΟΡΙΣΜΟΣ : *Ένωση* συνόλων A και B είναι το σύνολο $A \cup B = \{ \gamma \,/\, \gamma \in A \text{ ή } \gamma \in B \}$.

ΟΡΙΣΜΟΣ : *Τομή* συνόλων A και B είναι το σύνολο $A \cap B = \{ \gamma \,/\, \gamma \in A \text{ και } \gamma \in B \}$.

ΘΕΩΡΗΜΑ : Οι σχέσεις $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$ περιγράφουν τους *νόμους De Morgan*.

ΟΡΙΣΜΟΣ : *Πεδίο Borel* B είναι κάθε κλάση, γενικά μη αριθμήσιμων, συνόλων με ιδιότητες :

(α) $\Omega \in B$
(β) Αν $A \in B$, τότε $A^c \in B$.
(γ) Αν $A, B \in B$, τότε $A \cup B \in B$.

ΠΟΡΙΣΜΑ : $0 \in B$.

1.1.2 ΧΩΡΟΙ ΠΙΘΑΝΟΤΗΤΑΣ

ΟΡΙΣΜΟΣ : *Γεγονός* είναι το αποτέλεσμα κάποιου πειράματος Ε . Διακρίνονται *απλά* και *σύνθετα* γεγονότα.

ΟΡΙΣΜΟΣ : *Δειγματικός Χώρος* Ω_E είναι το σύνολο των απλών γεγονότων ω πειράματος Ε . Στη συνέχεια απορρίπτεται ο κάτω δείκτης ε από το συμβολισμό του δειγματικού χώρου.

ΟΡΙΣΜΟΣ : *Παρατηρητό* γεγονός Α είναι κάθε υποσύνολο του δειγματικού χώρου Ω . Το σύνολο των παρατηρητών γεγονότων αποτελεί το πεδίο Borel $\mathcal{B}$ του πειράματος.

ΟΡΙΣΜΟΣ : *Μέτρο πιθανότητας* ή *πιθανότητα* Π(Α) παρατηρητού γεγονότος Α είναι αριθμός που αντιστοιχίζεται με δεδομένο νόμο σε κάθε παρατηρητό γεγονός από το πεδίο Borel πειράματος. Η πιθανότητα διαθέτει τις παρακάτω ιδιότητες :

(α) $0 \leq \Pi(A) \leq 1 \quad \forall A \in \mathcal{B}$
(β) $\Pi(\Omega) = 1$
(γ) $\Pi(\emptyset) = 0$
(δ) Αν $A \subset B$, τότε $\Pi(A) < \Pi(B)$.
(ε) $\Pi(A \cup B) = \Pi(A) + \Pi(B) - \Pi(A \cap B) \quad \forall A,B \in \mathcal{B}$
(στ) Αν $A,B \in \mathcal{B}$ είναι ξένα σύνολα, δηλαδή σύνολα χωρίς κοινά στοιχεία, $\Pi(A \cup B) = \Pi(A) + \Pi(B)$.

ΟΡΙΣΜΟΣ : Αν $A,B \in \mathcal{B}$, ο αριθμός $\Pi(A/B) = \Pi(A \cap B)/\Pi(B)$ είναι η *υπό συνθήκη πιθανότητα Α ως προς Β* .

ΟΡΙΣΜΟΣ : Δύο παρατηρητά γεγονότα $A,B \in \mathcal{B}$ θεωρούνται στατιστικά ανεξάρτητα αν ισχύει $\Pi(A \cap B) = \Pi(A)\Pi(B)$.

ΠΟΡΙΣΜΑ : Αν $A,B \in \mathcal{B}$ είναι στατιστικά ανεξάρτητα, τότε $\Pi(A/B) = \Pi(A)$ και $\Pi(B/A) = \Pi(B)$.

ΟΡΙΣΜΟΣ : *Χώρος πιθανότητας* είναι το διατεταγμένο σύνολο $(\Omega, \mathcal{B}, \Pi)$.

1.1.3 ΣΥΝΕΧΕΙΣ ΤΥΧΑΙΕΣ ΜΕΤΑΒΛΗΤΕΣ

ΟΡΙΣΜΟΣ : *Συνεχής τυχαία μεταβλητή* X είναι κάθε απεικόνιση του χώρου πιθανότητας (Ω, B, Π) στο σύνολο των πραγματικών αριθμών R, δηλαδή $X : \Omega \to R$, που διαθέτει την ιδιότητα $\Gamma_x = \{ \omega / \omega \in \Omega \text{ και } X(\omega) \leq x \} \in B \ \forall x \in R$. Είναι φανερό ότι η τυχαία μεταβλητή είναι συνάρτηση με πεδίο ορισμού το σύνολο Ω των απλών γεγονότων ω και πεδίο τιμών το σύνολο R των πραγματικών αριθμών x .

ΟΡΙΣΜΟΣ : *Κατανομή πιθανότητας* συνεχούς τυχαίας μεταβλητής X είναι η συνεχής συνάρτηση $\Pi_X(x) = \Pi(\Gamma_x)$ που περιγράφει την πιθανότητα $X \leq x$. Η κατανομή πιθανότητας έχει τις παρακάτω ιδιότητες :

(α) $\Pi_X(-\infty) = 0$
(β) $\Pi_X(\infty) = 1$
(γ) Είναι μη αρνητική, μονότονα αύξουσα και συνεχής από δεξιά συνάρτηση.

ΟΡΙΣΜΟΣ : *Κατανομή πυκνότητας πιθανότητας* συνεχούς τυχαίας μεταβλητής X είναι η συνάρτηση $\pi_X(x) = d\Pi_X(x)/dx$. Η κατανομή πυκνότητας πιθανότητας είναι μη αρνητική συνάρτηση και έχει τις παρακάτω ιδιότητες :

(α) $$\int_{-\infty}^{\infty} \pi_X(x)\, dx = 1$$

(β) $$\int_{a}^{b} \pi_X(x)\, dx = \Pi_X(b) - \Pi_X(a)$$

ΠΟΡΙΣΜΑ : $$\Pi_X(x) = \int_{-\infty}^{x} \pi_X(\lambda)\, d\lambda$$

Έστω οι τυχαίες μεταβλητές X, Y που εκπροσωπούν τα απλά πειράματα E_X, E_Y με χώρους πιθανότητας (Ω_X, B_X, Π_X) και (Ω_Y, B_Y, Π_Y), αντίστοιχα. Το σύνθετο πείραμα $E_X E_Y$ ορίζει το χώρο πιθανότητας $(\Omega_{XY}, B_{XY}, \Pi_{XY})$ με δειγματικό χώρο $\Omega_{XY} = \{ (\omega_X, \omega_Y) / \omega_X \in \Omega_X, \omega_Y \in \Omega_Y \}$.Είναι φανερό ότι B_{XY} συμπεριλαμβάνει τα

παρατηρητά γεγονότα $A \subseteq \Omega_{XY}$. Το μέτρο πιθανότητας Π_{XY} έχει τις γνωστές ιδιότητες :

(α) $0 \leq \Pi_{XY}(A) \leq 1 \quad \forall\, A \in \mathcal{B}_{XY}$

(β) $\Pi_{XY}(\Omega_{XY}) = 1,\ \Pi_{XY}(\emptyset) = 0$

(δ) Αν $A \subset B$, τότε $\Pi_{XY}(A) < \Pi_{XY}(B)$.

(ε) $\Pi_{XY}(A \cup B) = \Pi_{XY}(A) + \Pi_{XY}(B) - \Pi_{XY}(A \cap B) \quad \forall\, A,B \in \mathcal{B}_{XY}$

(στ) Αν $A,B \in \mathcal{B}_{XY}$ είναι ξένα σύνολα, δηλαδή σύνολα χωρίς κοινά στοιχεία, $\Pi_{XY}(A \cup B) = \Pi_{XY}(A) + \Pi_{XY}(B)$.

Αν $A \in \mathcal{B}_X$ και $B \in \mathcal{B}_Y$, τότε $AB \in \mathcal{B}_{XY}$ και μάλιστα $AB = (A\Omega_Y) \cap (\Omega_X B)$. Αν $A\Omega_Y$ και $\Omega_X B$ είναι στατιστικά ανεξάρτητα παρατηρητά γεγονότα του σύνθετου πειράματος $E_X E_Y$, τότε $\Pi_{XY}((A\Omega_Y) \cap (\Omega_X B)) = \Pi_{XY}(A\Omega_Y)\Pi_{XY}(\Omega_X B) = \Pi_X(A)\Pi_Y(B)$, επειδή $\Pi_{XY}(A\Omega_Y) = \Pi_X(A)$ και $\Pi_{XY}(\Omega_X B) = \Pi_Y(B)$.

Πίνακας 1.Ι.1

Συνεχείς τυχαίες μεταβλητές

X	$\pi_X(x)$	x
Ομοιόμορφη	$\frac{1}{b-a}$	$x \in [a, b]$
Εκθετική	$\lambda e^{-\lambda x}$	$x \in [0, \infty]$
Laplace	$\frac{\lambda}{2} e^{-\lambda \lvert x \rvert}$	$x \in R$
Κανονική (Gauss)	$(2\pi\sigma^2)^{-1/2} e^{-(x-\mu)^2/2\sigma^2}$	$x \in R$
Cauchy	$\frac{\lambda/\pi}{\lambda^2 + x^2}$	$x \in R$
Rayleigh	$\frac{x}{\lambda^2} e^{-x^2/2\lambda^2}$	$x \in [0, \infty]$
Maxwell	$\frac{\sqrt{2/\pi}}{\lambda^3} x^2 e^{-x^2/2\lambda^2}$	$x \in [0, \infty]$

ΟΡΙΣΜΟΣ : *Συνδετική κατανομή πιθανότητας* των συνεχών τυχαίων μεταβλητών X, Y είναι η συνάρτηση $\Pi_{XY}(x,y) = \Pi_{XY}(\Gamma_x \Gamma_y)$ με $\Gamma_x = \{ \omega_X / \omega_X \in \Omega_X$ και $X(\omega_X) \leq x \} \in \mathcal{B}_X \ \forall x \in R$ και $\Gamma_y = \{ \omega_Y / \omega_Y \in \Omega_Y$ και $Y(\omega_Y) \leq y \} \in \mathcal{B}_Y \ \forall y \in R$. Η συνάρτηση $\Pi_{XY}(x,y)$ έχει τις παρακάτω ιδιότητες :

(α) $\Pi_{XY}(-\infty,-\infty) = \Pi_{XY}(-\infty,y) = \Pi_{XY}(x,-\infty) = 0$

(β) $\Pi_{XY}(\infty,\infty) = 1$

(γ) $\Pi_{XY}(x,\infty) = \Pi_X(x)$, $\Pi_{XY}(\infty,y) = \Pi_Y(y)$. Οι συναρτήσεις $\Pi_X(x)$, $\Pi_Y(y)$ είναι οι *περιθωριακές κατανομές πιθανότητας* της $\Pi_{XY}(x,y)$.

(δ) Είναι μη αρνητική, αύξουσα και συνεχής από δεξιά συνάρτηση ως προς x και y .

ΟΡΙΣΜΟΣ : *Συνδετική κατανομή πυκνότητας πιθανότητας* των συνεχών τυχαίων μεταβλητών X, Y είναι η συνάρτηση $\pi_{XY}(x,y) = \partial^2 \Pi_{XY}(x,y)/\partial x \partial y$. Η συνάρτηση $\pi_{XY}(x,y)$ είναι μη αρνητική και έχει τις παρακάτω ιδιότητες :

(α) $$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \pi_{XY}(\lambda,\mu)\, d\lambda d\mu = 1$$

(β) $$\int_{-\infty}^{x}\int_{-\infty}^{y} \pi_{XY}(\lambda,\mu)\, d\lambda d\mu = \Pi_{XY}(x,y)$$

(γ) $$\int_{-\infty}^{\infty} \pi_{XY}(\lambda,y)\, d\lambda = \pi_Y(y). \quad \int_{-\infty}^{\infty} \pi_{XY}(x,\mu)\, d\mu = \pi_X(x)$$

Οι συναρτήσεις $\pi_X(x)$, $\pi_Y(y)$ είναι οι *περιθωριακές κατανομές πυκνότητας πιθανότητας* της $\pi_{XY}(x,y)$. Οι συνεχείς τυχαίες μεταβλητές είναι *στατιστικά ανεξάρτητες* αν ισχύει $\pi_{XY}(x,y) = \pi_X(x)\pi_Y(y)$.

ΟΡΙΣΜΟΣ : *Υπό συνθήκη κατανομή πιθανότητας* των συνεχών τυχαίων μεταβλητών X, Y είναι η συνάρτηση $\Pi_{XY}(x/y) = \Pi_{XY}(\Gamma_x \Gamma_y) / \Pi_Y(\Gamma_y)$ με $\Gamma_x = \{ \omega_X / \omega_X \in \Omega_X$ και $X(\omega_X) \leq x \} \in \mathcal{B}_X \ \forall x \in R$ και $\Gamma_y = \{ \omega_Y / \omega_Y \in \Omega_Y$ και $Y(\omega_Y) \leq y \} \in \mathcal{B}_Y \ \forall y \in R$. Ανάλογα ορίζεται και η συνάρτηση $\Pi_{XY}(y/x)$.

ΟΡΙΣΜΟΣ : *Υπό συνθήκη κατανομή πυκνότητας πιθανότητας* των συνεχών τυχαίων μεταβλητών X, Y είναι η συνάρτηση $\pi_{XY}(x/y) = \partial\Pi_{XY}(x/y)/\partial x$ ή $\pi_{XY}(y/x) = \partial\Pi_{XY}(y/x)/\partial y$. Είναι εύκολο να αποδειχθεί ότι $\pi_{XY}(x/y) = \pi_{XY}(x,y)/\pi_Y(y)$ και $\pi_{XY}(y/x) = \pi_{XY}(x,y)/\pi_X(x)$. Αν οι συνεχείς τυχαίες μεταβλητές X, Y είναι στατιστικά ανεξάρτητες, τότε $\pi_{XY}(x/y) = \pi_X(x)$ και $\pi_{XY}(y/x) = \pi_Y(y)$.

ΟΡΙΣΜΟΣ : *Ροπή ν-τάξεως* της συνεχούς τυχαίας μεταβλητής X είναι ο αριθμός $E\{X^\nu\} = \int_{-\infty}^{\infty} \lambda^\nu \pi_X(\lambda)\, d\lambda$ όπου ν είναι ακέραιος. Το σύμβολο $E\{\cdot\}$ χαρακτηρίζεται *μαθηματική προσδοκία*.

ΟΡΙΣΜΟΣ : *Μέση τιμή* μ_X της συνεχούς τυχαίας μεταβλητής X είναι η ροπή πρώτης τάξεως, δηλαδή $\mu_X = E\{X\}$.

ΟΡΙΣΜΟΣ : *Κεντρική ροπή ν-τάξεως* της συνεχούς τυχαίας μεταβλητής X είναι ο αριθμός $E\{(X-\mu_X)^\nu\} = \int_{-\infty}^{\infty} (\lambda - \mu_X)^\nu \pi_X(\lambda)\, d\lambda$ όπου ν είναι ακέραιος.

ΟΡΙΣΜΟΣ : *Μεταβλητότητα* σ_X^2 της συνεχούς τυχαίας μεταβλητής X είναι η κεντρική ροπή δεύτερης τάξεως, δηλαδή $\sigma_X^2 = E\{(X-\mu_X)^2\}$. Το μέγεθος σ_X χαρακτηρίζεται *τυπική απόκλιση*.

ΟΡΙΣΜΟΣ : *Συνδετική ροπή νξ-τάξεως* των συνεχών τυχαίων μεταβλητών X, Y είναι ο αριθμός $E\{X^\nu Y^\xi\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \lambda^\nu \mu^\xi \pi_{XY}(\lambda,\mu)\, d\lambda d\mu$, όπου ν,ξ είναι ακέραιοι.

ΟΡΙΣΜΟΣ : *Συνδετική κεντρική ροπή νξ-τάξεως* των συνεχών τυχαίων μεταβλητών X, Y είναι ο αριθμός $E\{(X-\mu_X)^\nu (Y-\mu_Y)^\xi\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} (\lambda-\mu_X)^\nu (\mu-\mu_Y)^\xi \pi_{XY}(\lambda,\mu)\, d\lambda d\mu$, όπου ν,ξ είναι ακέραιοι.

ΟΡΙΣΜΟΣ : *Συντελεστής συσχέτισης* ρ_{XY} των συνεχών τυχαίων μεταβλητών X, Y είναι ο αριθμός $E\{(X-\mu_X)(Y-\mu_Y)\}/\sigma_X\sigma_Y$. Οι συνεχείς τυχαίες μεταβλητές είναι *στατιστικά*

ασυσχέτιστες αν $\rho_{XY} = 0$ ή, ισοδύναμα, αν $E(XY) = E(X)E(Y)$.

ΘΕΩΡΗΜΑ : Αν $\{ X_v \}$ είναι ακολουθία στατιστικά ανεξάρτητων και όμοια κατανεμημένων συνεχών τυχαίων μεταβλητών με μέση τιμή μ και μεταβλητότητα σ^2, η συνεχής τυχαία μεταβλητή $X = X_1 + X_2 + \ldots X_v$ έχει μέση τιμή νμ και μεταβλητότητα $v\sigma^2$. Επιπλέον η κατανομή της τείνει προς την κανονική (βλ. πίνακα 1.I.1) καθώς $v \to \infty$ (Κεντρικό Οριακό θέωρημα).

Πίνακας 1.I.2

Διακριτές τυχαίες μεταβλητές

X, $x_i = i$	π_i	i
Ομοιόμορφη	1/v	$i \in \{ 0, 1, 2, \ldots, v-1 \}$
Δυαδική	$\pi_0 = \pi$, $\pi_1 = 1-\pi$, $0 \leq \pi \leq 1$	$i \in \{ 0, 1 \}$
Γεωμετρική	$\pi(1-\pi)^{i-1}$, $0 \leq \pi \leq 1$	$i \in \{ 1, 2, \ldots \}$
Poisson	$\lambda^i e^{-\lambda}/\lambda!$	$i \in \{ 0, 1, 2, \ldots \}$
Διωνυμική	$\binom{v}{i} \pi^i (1-\pi)^{v-i}$, $0 \leq \pi \leq 1$	$i \in \{ 0, 1, 2, \ldots, v \}$

1.I.4 ΔΙΑΚΡΙΤΕΣ ΤΥΧΑΙΕΣ ΜΕΤΑΒΛΗΤΕΣ

ΟΡΙΣΜΟΣ : *Διακριτή* τυχαία μεταβλητή είναι κάθε τυχαία μεταβλητή X με πεπερασμένο ή αριθμήσιμο πεδίο ορισμού $\Omega = \{ \omega_i, i = 1, 2, \ldots \}$ και αντίστοιχα πεπερασμένο ή αριθμήσιμο πεδίο τιμών $\{ X(\omega_i) = x_i \in R \,/\, \omega_i \in \Omega, i = 1, 2, \ldots \}$.

ΟΡΙΣΜΟΣ : *Κατανομή πιθανότητας* διακριτής τυχαίας μεταβλητής X είναι το σύνολο $\Pi_X = \{ \pi(x_i) = \Pi(\omega_i) = \pi_i \in R \,/\, \omega_i \in \Omega, i = 1, 2, \ldots \}$. Είναι φανερό ότι ισχύουν οι παρακάτω ιδιότητες :

(α) $0 \leq \pi_i \leq 1 \quad ; \quad i = 1, 2, \ldots$

(β) $\sum_i \pi_i = 1$

που προκύπτουν από τις γενικώτερες ιδιότητες του μέτρου πιθανότητας (βλ. §1.I.2).

ΟΡΙΣΜΟΣ : *Συνδετική κατανομή πιθανότητας* των διακριτών τυχαίων μεταβλητών X, Y είναι το σύνολο $\Pi_{XY} = \{ \pi(x_i, y_j) = \Pi_{XY}(\omega_{X_i}, \omega_{Y_j}) \in R \; / \; \omega_{X_i} \in \Omega_X, \; i = 1, 2, \ldots$ και $\omega_{Y_j} \in \Omega_Y, \; j = 1, 2, \ldots \}$ (βλ. §1.I.3) με ιδιότητες :

(α) $0 \leq \pi(x_i, y_j) \leq 1 \quad ; \quad i, j = 1, 2, \ldots$

(β) $\sum_i \sum_j \pi(x_i, y_j) = 1$

(γ) $\sum_i \pi(x_i, y_j) = \pi(y_j), \quad \sum_j \pi(x_i, y_j) = \pi(x_i)$.

Τα σύνολα $\Pi_X = \{ \pi(x_i), \; i = 1, 2, \ldots \}$ και $\Pi_Y = \{ \pi(y_i), \; i = 1, 2, \ldots \}$ είναι οι *περιθωριακές κατανομές πιθανότητας* της Π_{XY} . Οι διακριτές τυχαίες μεταβλητές X, Y είναι *στατιστικά ανεξάρτητες* αν ισχύει $\pi(x_i, y_j) = \pi(x_i)\pi(y_j)$, $i, j = 1, 2, \ldots$

ΟΡΙΣΜΟΣ : *Υπό συνθήκη κατανομή πιθανότητας* των διακριτών τυχαίων μεταβλητών X, Y είναι το σύνολο $\Pi_{X/Y} = \{ \pi(x_i/y_j) = \Pi_{XY}(\omega_{X_i}, \omega_{Y_j}) / \Pi_Y(\omega_{Y_j}) \in R \; / \; \omega_{X_i} \in \Omega_X,$ $\omega_{Y_j} \in \Omega_Y \; i, j = 1, 2, \ldots \}$. Ανάλογα ορίζεται και το σύνολο $\Pi_{Y/X}$. Είναι φανερό ότι $\pi(x_i/y_j) = \pi(x_i, y_j)/\pi(y_j)$ και $\pi(y_j/x_i) = \pi(x_i, y_j)/\pi(x_i)$. Αν οι διακριτές τυχαίες μεταβλητές X, Y είναι στατιστικά ανεξάρτητες, τότε $\pi(x_i/y_j) = \pi(x_i)$ και $\pi(y_j/x_i) = \pi(y_j)$.

ΟΡΙΣΜΟΣ : *Μέση τιμή* της διακριτής τυχαίας μεταβλητής X είναι ο αριθμός $\mu_X = \sum_i x_i \pi(x_i)$.

ΟΡΙΣΜΟΣ : *Μεταβλητότητα* της διακριτής τυχαίας μεταβλητής X είναι ο αριθμός

(α) $0 \leq \pi_i \leq 1$; $i = 1, 2, \ldots$

(β) $\sum_i \pi_i = 1$

που προκύπτουν από τις γενικώτερες ιδιότητες του μέτρου πιθανότητας (βλ. §1.I.2).

ΟΡΙΣΜΟΣ : *Συνδετική κατανομή πιθανότητας* των διακριτών τυχαίων μεταβλητών X, Y είναι το σύνολο $\Pi_{XY} = \{ \pi(x_i,y_j) = \Pi_{XY}(\omega_{X_i},\omega_{Y_j}) \in R \,/\, \omega_{X_i} \in \Omega_X,\ i = 1, 2, \ldots$ και $\omega_{Y_j} \in \Omega_Y,\ j = 1, 2, \ldots \}$ (βλ. §1.I.3) με ιδιότητες :

(α) $0 \leq \pi(x_i,y_j) \leq 1$; $i,j = 1, 2, \ldots$

(β) $\sum_i \sum_j \pi(x_i,y_j) = 1$

(γ) $\sum_i \pi(x_i,y_j) = \pi(y_j)$, $\sum_j \pi(x_i,y_j) = \pi(x_i)$.

Τα σύνολα $\Pi_X = \{ \pi(x_i),\ i = 1, 2, \ldots \}$ και $\Pi_Y = \{ \pi(y_i),\ i = 1, 2, \ldots \}$ είναι οι *περιθωριακές κατανομές πιθανότητας* της Π_{XY} . Οι διακριτές τυχαίες μεταβλητές X, Y είναι *στατιστικά ανεξάρτητες* αν ισχύει $\pi(x_i,y_j) = \pi(x_i)\pi(y_j)$, $i,j = 1, 2, \ldots$

ΟΡΙΣΜΟΣ : *Υπό συνθήκη κατανομή πιθανότητας* των διακριτών τυχαίων μεταβλητών X, Y είναι το σύνολο $\Pi_{X/Y} = \{ \pi(x_i/y_j) = \Pi_{XY}(\omega_{X_i},\omega_{Y_j})/\Pi_Y(\omega_{Y_j}) \in R \,/\, \omega_{X_i} \in \Omega_X,$ $\omega_{Y_j} \in \Omega_Y\ i,j = 1, 2, \ldots \}$. Ανάλογα ορίζεται και το σύνολο $\Pi_{Y/X}$. Είναι φανερό ότι $\pi(x_i/y_j) = \pi(x_i,y_j)/\pi(y_j)$ και $\pi(y_j/x_i) = \pi(x_i,y_j)/\pi(x_i)$. Αν οι διακριτές τυχαίες μεταβλητές X, Y είναι στατιστικά ανεξάρτητες, τότε $\pi(x_i/y_j) = \pi(x_i)$ και $\pi(y_j/x_i) = \pi(y_j)$.

ΟΡΙΣΜΟΣ : *Μέση τιμή* της διακριτής τυχαίας μεταβλητής X είναι ο αριθμός $\mu_X = \sum_i x_i \pi(x_i)$.

ΟΡΙΣΜΟΣ : *Μεταβλητότητα* της διακριτής τυχαίας μεταβλητής X είναι ο αριθμός

$\sigma_X^2 = \sum_i (x_i - \mu_X)^2 \pi(x_i)$. Το μέγεθος σ_X χαρακτηρίζεται *τυπική απόκλιση*.

1.Ι.5 ΣΤΟΧΑΣΤΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ

ΟΡΙΣΜΟΣ : *Στοχαστική διαδικασία* $X(t)$ είναι πεπερασμένο ή άριθμήσιμο σύνολο τυχαίων μεταβλητών $\{ X_i = X(t_i),\ i = 1, 2, \ldots \}$, που αντιστοιχεί σε πεπερασμένο ή αριθμήσιμο, αντίστοιχα, σύνολο $\{ t_i,\ i = 1, 2, \ldots \}$ τιμών παραμέτρου t , με καθορισμένες συνδετικές κατανομές πιθανότητας $\Pi_{X_1 X_2 \ldots}(x_1,t_1;\ x_2,t_2;\ \ldots)$.

ΟΡΙΣΜΟΣ : Η *διαδικασία Markov* $X(t)$, $t \in \{ t_1 \leqslant t_2 \leqslant \ldots \leqslant t_{v-1} \leqslant t_v \leqslant \ldots \}$ είναι στοχαστική διαδικασία με την ιδιότητα :

$$\Pi_{X_v X_{v-1} \ldots X_1}(x_v,t_v \,/\, x_{v-1},t_{v-1};\ \ldots;\ x_1,t_1) = \Pi_{X_v X_{v-1}}(x_v,t_v \,/\, x_{v-1},t_{v-1})$$

1.ΙΙ ΑΠΟΔΕΙΞΗ ΤΗΣ ΕΞ.(1.44)

Στο σύστημα Markov Α,Υ,Π εξελίσσεται αλυσίδα που τη χρονική στιγμή t διέρχεται από κάποια κατάσταση $\alpha_i \in A$. Η μετέπειτα εξέλιξη της αλυσίδας με βήμα μεγέθους $(\kappa+1)\tau$ προκύπτει με διαδοχή των φάσεων :

$$\begin{aligned} &\text{1η φάση} \quad \alpha(t) \;\; = \alpha_i \to \alpha_k = \alpha(t+\tau) \\ &\text{2η φάση} \quad \alpha(t+\tau) = \alpha_k \to \alpha_j = \alpha(t+\kappa\tau) \end{aligned} \quad :$$

Κατά την πρώτη φάση η αλυσίδα εξελίσσεται με βήμα μεγέθους τ, δηλαδή απλό βήμα, ενώ κατά τη δεύτερη φάση εξελίσσεται με βήμα μεγέθους $\kappa\tau$. Η ποσότητα πληροφορίας που αντιστοιχεί σε εξέλιξη με βήμα $(\kappa+1)\tau$ προκύπτει αντίστοιχα σαν άθροισμα των ποσοτήτων πληροφορίας που αντιστοιχούν στις δύο φάσεις :

$$H^{\kappa+1}(\alpha_i) = H(\alpha_i) + \sum_{k=1}^{\rho} \pi_{ik} H^{\kappa}(\alpha_k) \qquad (1)$$

και η μέση τιμή ως προς τις δυνατές καταστάσεις εκκίνησης είναι :

$$H^{\kappa+1}(A) = \sum_{i=1}^{\rho} v_i H^{\kappa+1}(\alpha_i) = \sum_{i=1}^{\rho} v_i H(\alpha_i) + \sum_{i=1}^{\rho} \sum_{k=1}^{\rho} v_i \pi_{ik} H^{\kappa}(\alpha_k)$$

$$= H(A) + \sum_{k=1}^{\rho} \left[\sum_{i=1}^{\rho} v_i \pi_{ik} \right] H^{\kappa}(\alpha_k) = H(A) + \sum_{k=1}^{\rho} v_k H^{\kappa}(\alpha_k) =$$

$$= H(A) + H^{\kappa}(A) \qquad (2)$$

όπου χρησιμοποιήθηκε και η εξ.(1.36). Η εξ.(2) με $\kappa = 1$ δίνει $H^2(A) = 2H(A)$ και επαγωγικά προκύπτει :

$$H^{\kappa}(A) = \kappa H(A) \qquad (3)$$

Επομένως $H^{\kappa+\lambda}(A) = (\kappa+\lambda)H(A) = \kappa H(A) + \lambda H(A) = H^{\kappa}(A) + H^{\lambda}(A)$ και η εξ.(1.44) έχει αποδειχθεί.

1.III ΑΠΟΔΕΙΞΗ ΤΗΣ ΕΞ.(1.46)

Η ταυτοανισότητα της εξ.(1.4) γράφεται με την ισοδύναμη μορφή :

$$\sum_{i=1}^{\rho} \pi_i \log_e \left(\frac{\tau_i}{\pi_i} \right) \leq 0 \qquad (1)$$

και για τις διδιάστατες καταναμές πιθανότητας $\pi(\alpha_i, \alpha_j)$, $\pi(\alpha_i)\pi(\alpha_j)$ επεκτείνεται στην ταυτοανισότητα :

$$\sum_{i=1}^{\rho}\sum_{j=1}^{\rho} \pi(\alpha_i,\alpha_j)\log_e\left[\frac{\pi(\alpha_i)\pi(\alpha_j)}{\pi(\alpha_i,\alpha_j)}\right] \leq 0 \qquad (2)$$

Στο πλαίσιο της θεωρίας πηγών πληροφορίας με μνήμη, $\pi(\alpha_i,\alpha_j) = \pi(\alpha_j/\alpha_i)\pi(\alpha_i)$ $= \pi_{ij}u_i$ και επομένως η εξ.(2) παίρνει τη μορφή :

$$\sum_{i=1}^{\rho}\sum_{j=1}^{\rho} \pi_{ij}u_i\log_e\left[\frac{u_j}{\pi_{ij}}\right] \leq 0 \Rightarrow$$

$$\sum_{j=1}^{\rho}\left[\sum_{i=1}^{\rho}\pi_{ij}u_i\right]\log_e(u_j) - \sum_{i=1}^{\rho}u_i\left[\sum_{j=1}^{\rho}\pi_{ij}\log_e(\pi_{ij})\right] \leq 0 \Rightarrow$$

$$\sum_{j=1}^{\rho}u_j\log_e(u_j) + \sum_{i=1}^{\rho}u_iH(\alpha_i) \leq 0 \Rightarrow$$

$$-H^{\infty}(A) + H(A) \leq 0 \Rightarrow$$

$$H(A) \leq H^{\infty}(A) \qquad (3)$$

και η εξ.(1.46) έχει αποδειχθεί αφού είναι προφανές ότι πέρα από την εξ.(3) ισχύει και $H(A), H^{\infty}(A) \leq \log_e\rho$.

1.Ιν ΙΑΚΩΒΙΑΝΗ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΥ

Αν U_v, V_v είναι v-διάστατοι διανυσματικοί χώροι (βλ. §5.III) επί του πεδίου (βλ. §5.II) $\{R, +, \cdot\}$, η *Ιακωβιανή του μετασχηματισμού* $U_v \to V_v$ είναι η ορίζουσα :

$$J(U_\nu/V_\nu) = \begin{vmatrix} \frac{\partial u_1}{\partial v_1} & \frac{\partial u_1}{\partial v_2} & \cdots & \frac{\partial u_1}{\partial v_\nu} \\ \frac{\partial u_2}{\partial v_1} & \frac{\partial u_2}{\partial v_2} & \cdots & \frac{\partial u_2}{\partial v_\nu} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \frac{\partial u_\nu}{\partial v_1} & \frac{\partial u_\nu}{\partial v_2} & \cdots & \frac{\partial u_\nu}{\partial v_\nu} \end{vmatrix} \qquad (1)$$

όπου $u_i, v_j \in R$, $i,j = 1, 2, \ldots, \nu$, είναι στοιχεία των διανυσμάτων ν-τάξεως $(u_1, u_2, \ldots, u_\nu) \in U_\nu$ και $(v_1, v_2, \ldots, v_\nu) \in V_\nu$. Οι παρακάτω ιδιότητες των Ιακωβιανών :

$$J(U_\nu/V_\nu)\,J(V_\nu/U_\nu) = 1 \qquad (2)$$

$$J(U_\nu/V_\nu)\,J(V_\nu/W_\nu) = J(U_\nu/W_\nu) \qquad (3)$$

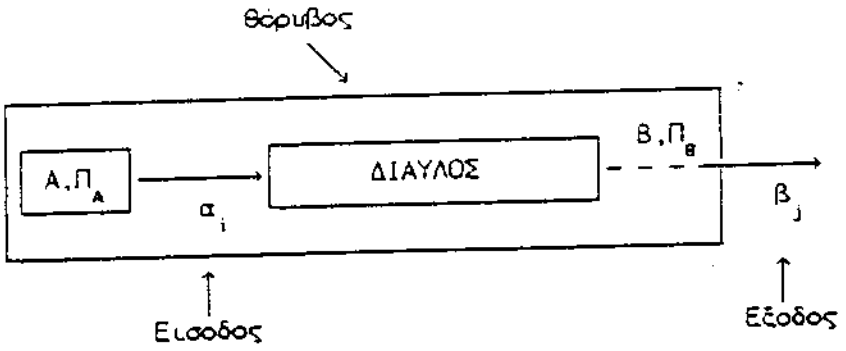
εκφράζουν αντίστοιχα τους μετασχηματισμούς $U_\nu \to V_\nu \to U_\nu$ και $U_\nu \to V_\nu \to W_\nu$.

Κεφάλαιο Δύο

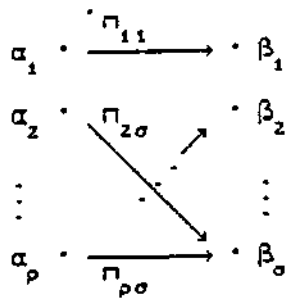
ΧΩΡΗΤΙΚΟΤΗΤΑ ΔΙΑΥΛΟΥ ΠΛΗΡΟΦΟΡΙΑΣ

2.1 ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Η συμβολή του διαύλου πληροφορίας στο σύστημα επικοινωνίας είναι απλά η διοχέτευση πληροφορίας από την εισοδο στην έξοδο του. Η πηγη πληροφορίας A,Π_A που προσαρμόζεται στην είσοδο του διαύλου πληροφορίας εμφανίζεται στην έξοδο του σαν πηγή πληροφορίας B,Π_B (σχ. 2.1), γενικά διαφορετική από την A,Π_A, και η διαφοροποίηση αυτή οφείλεται στην ιδια τη δομή του διαύλου πληροφορίας και στην επίδραση του περιβαλλοντος λειτουργίας.



Σχ. 2.1 Ο διαυλος πληροφορίας προεκτείνει την πηγη εισοδου A,Π_A στην πηγη εξόδου B,Π_B.



Σχ. 2.2 Διάγραμμα διαύλου

Η μετάδοση συμβόλων μέσα από το δίαυλο πληροφορίας περιγράφεται από το *μητρώο διαύλου* $\Pi(B/A)$ με στοιχεία τις υπό συνθήκη πιθανότητες $\pi_{ij} = \pi(\beta_j/\alpha_i)$ που συνδέουν το σύμβολο εξόδου β_j με το σύμβολο εισόδου α_i. Αν οι πηγές πληροφορίας A,Π_A και B,Π_B έχουν αντίστοιχα ρ και σ σύμβολα, το μητρώο διαύλου έχει ρ σειρές και σ στήλες :

$$\Pi(B/A) = \begin{bmatrix} \pi_{11} & \pi_{12} & \cdots & \pi_{1\sigma} \\ \pi_{21} & \pi_{22} & \cdots & \pi_{2\sigma} \\ \cdots & \cdots & \cdots & \cdots \\ \pi_{\rho 1} & \pi_{\rho 2} & \cdots & \pi_{\rho\sigma} \end{bmatrix} \qquad (2.1)$$

Εναλλακτικά η ροή συμβόλων μέσα από το δίαυλο πληροφορίας μπορεί να περιγραφεί με το *διάγραμμα διαύλου* (σχ. 2.2). Είναι φανερό ότι δύο ή περισσότερα σύμβολα εισόδου μπορεί να αντιστοιχούν σε ένα σύμβολο εξόδου αφού γενικά $\rho \neq \sigma$.

Τόσο το μητρώο διαύλου όσο και το διάγραμμα διαύλου περιγράφουν τη στοχαστική σύνδεση μεταξύ συμβόλων εισόδου και συμβόλων εξόδου. Όπως διαπιστώνεται παρακάτω, συνδέουν και την εντροπία της πηγής πληροφορίας A,Π_A με την εντροπία της πηγής πληροφορίας B,Π_B. Η εντροπία $H(A)$ της πηγής πληροφορίας A,Π_A καθορίζεται αποκλειστικά από τις πιθανότητες των συμβόλων $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ και επομένως το μητρώο $\Pi_R(A) = [\, \pi(\alpha_1), \pi(\alpha_2), \ldots, \pi(\alpha_\rho) \,]$ καθορίζει ουσιαστικά τη μέση ποσότητα πληροφορίας που προσάγει κάθε σύμβολο στην είσοδο του διαύλου πληροφορίας. Αντίστοιχα το μητρώο $\Pi_R(B) = [\, \pi(\beta_1), \pi(\beta_2), \ldots, \pi(\beta_\sigma) \,]$, με στοιχεία τις πιθανότητες των συμβόλων εξόδου, καθορίζει τη μέση ποσότητα πληροφορίας που φέρει κάθε σύμβολο στην έξοδο του διαύλου πληροφορίας, δηλαδή την εντροπία $H(B)$ της πηγής πληροφορίας B,Π_B. Είναι εύκολο να αποδειχθεί η

μητρωική εξίσωση :

$$\Pi_R(A)\ \Pi(B/A) = \Pi_R(B) \qquad (2.2)$$

που επιβεβαιώνει ότι η ροή πληροφορίας από την είσοδο μέχρι την έξοδο του διαύλου πληροφορίας ελέγχεται από το μητρώο διαύλου.

Με τις πιθανότητες των συμβόλων εισόδου $\pi(\alpha_1), \pi(\alpha_2), \ldots, \pi(\alpha_\rho)$ σχηματίζεται και το διαγώνιο μητρώο :

$$\Pi_D(A) = \begin{bmatrix} \pi(\alpha_1) & 0 & \ldots & 0 \\ 0 & \pi(\alpha_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \pi(\alpha_\rho) \end{bmatrix} \qquad (2.3)$$

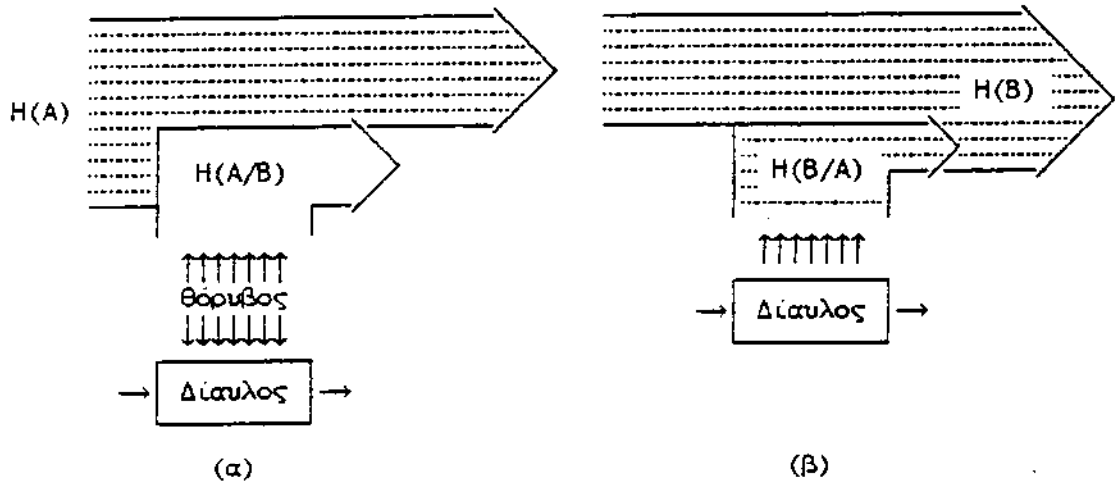
Αν αυτό πολλαπλασιασθεί με το μητρώο διαύλου, προκύπτει ρχσ μητρώο με στοιχεία τις συνδετικές πιθανότητες των συμβόλων εισόδου, εξόδου :

$$\Pi_D(A)\ \Pi(B/A) = \Pi(A,B) = \begin{bmatrix} \pi(\alpha_1,\beta_1) & \pi(\alpha_1,\beta_2) & \ldots & \pi(\alpha_1,\beta_\sigma) \\ \pi(\alpha_2,\beta_1) & \pi(\alpha_2,\beta_2) & \ldots & \pi(\alpha_2,\beta_\sigma) \\ \ldots & \ldots & \ldots & \ldots \\ \pi(\alpha_\rho,\beta_1) & \pi(\alpha_\rho,\beta_2) & \ldots & \pi(\alpha_\rho,\beta_\sigma) \end{bmatrix} \qquad (2.4)$$

Είναι φανερό ότι το μητρώο $\Pi(A,B)$ καθορίζει τη συνδετική εντροπία $H(AB)$ των πηγών πληροφορίας A,Π_A και B,Π_B, δηλαδή τη μέση πληροφορία ανά ζεύγος συμβόλων εισόδου – εξόδου. Η συνδετική εντροπία $H(AB)$ ονομάζεται κατά λογική ακολουθία *εντροπία συστήματος*.

Το μητρώο διαύλου, με στοιχεία τις υπό συνθήκη πιθανότητες $\pi_{ij} = \pi(\beta_j/\alpha_i)$, περιγράφει την αβεβαιότητα για το σύμβολο εξόδου με δεδομένο το σύμβολο εισόδου, δηλαδή την αβεβαιότητα που δημιουργείται στην είσοδο του διαύλου πληροφορίας για την έξοδο του. Η αβεβαιότητα στην έξοδο του διαύλου πληροφορίας για την είσοδο του, δηλαδή η αβεβαιότητα για το σύμβολο εισόδου με δεδομένο το σύμβολο εξόδου, περιγράφεται από το μητρώο $\Pi(A/B)$, με στοιχεία τις υπό συνθήκη πιθανότητες $\pi(\alpha_i/\beta_j)$. Και οι δύο μορφές αβεβαιότητας συνδέονται με τη λειτουργία του διαύλου πληροφορίας (σχ. 2.3).

Η πηγή πληροφορίας A,Π_A προσάγει τα σύμβολα α_i, $i = 1, 2, \ldots, \rho$ και την προσαρτημένη σ' αυτά πληροφορία, που κατά μέσο όρο είναι H(A) bits/σύμβολο, στην είσοδο του διαύλου πληροφορίας. Ο τελευταίος εμφανίζει στην έξοδο του τα σύμβολα β_j, $j = 1, 2, \ldots, \sigma$ και δημιουργεί αβεβαιότητα για το αντίστοιχο κάθε φορά σύμβολο εισόδου. Επομένως στην έξοδο του διαύλου πληροφορίας λείπει η ποσότητα πληροφορίας που απαιτείται για να αναγνωρισθεί με βεβαιότητα το σύμβολο εισόδου. Είναι φανερό ότι η μέση έλλειψη πληροφορίας για το σύμβολο εισόδου στην έξοδο του διαύλου πληροφορίας είναι η υπό συνθήκη εντροπία H(A/B).



Σχ. 2.3 Ροή πληροφορίας και μηχανισμοί απωλειών.
(α) Ο θόρυβος προκαλεί έλλειψη πληροφορίας H(A/B) στην έξοδο.
(β) Άγνοια του διαύλου ισοδυναμεί με έλλειψη πληροφορίας H(B/A) στην είσοδο.

Η μέση έλλειψη πληροφορίας για το σύμβολο εισόδου γίνεται αντιληπτή από παρατηρητή στην έξοδο σαν απώλεια πληροφορίας και αποδίδεται στην παρουσία θορύβου στο περιβάλλον του διαύλου πληροφορίας. Η υπό συνθήκη εντροπία H(A/B) ονομάζεται κατα λογική ακολουθία *εντροπία θορύβου*. Στο ισοζύγιο πληροφορίας του σχήματος 2.3α η εντροπία θορύβου εμφανίζεται σαν αρνητική πληροφορία που εισαγεται στο σύστημα καθ' όλη την έκταση του διαύλου πληροφορίας. Ο θόρυβος αντιμετωπιζεται ουσιαστικά σαν διανεμημένη πηγή πληροφορίας που προσάγει ανεπιθύμητη πληροφορία με αποτέλεσμα την υποβάθμιση, δηλαδή την απώλεια μέρους της χρήσιμης πληροφορίας που προσάγει η πηγή πληροφορίας A,Π_A. Αν το περιβάλλον είναι αθόρυβο ή ο δίαυλος πληροφορίας θωρακισμένος κατά του θορύβου, δεν δημιουργείται στην εξοδο αβεβαιότητα για το σύμβολο εισόδου. Επομένως

$\pi(\alpha_i/\beta_j) = 0$ ή 1 και $H(A/B) = 0$.

Ο δίαυλος πληροφορίας εμφανίζεται στην έξοδο του σαν πηγή πληροφορίας B,Π_B (σχ. 2.1) και παράγει τα σύμβολα β_j, $j = 1, 2, \ldots, \sigma$ με την προσαρτημένη σ' αυτά ποσότητα πληροφορίας, που κατά μέσο όρο είναι H(B) bits/σύμβολο. Παράλληλα ο δίαυλος πληροφορίας δημιουργεί στην είσοδο του αβεβαιότητα για το σύμβολο εξόδου β_j, $j = 1, 2, \ldots, \sigma$. Επομένως στην είσοδο του διαύλου πληροφορίας λείπει η ποσότητα πληροφορίας που απαιτείται για να καθορισθεί το σύμβολο εξόδου που αντιστοιχεί κάθε φορά στο σύμβολο εισόδου. Είναι φανερό ότι η μέση έλλειψη πληροφορίας ανά σύμβολο εξόδου στην είσοδο του διαύλου πληροφορίας είναι η υπό συνθήκη εντροπία H(B/A).

Η μέση έλλειψη πληροφορίας για το σύμβολο εξόδου γίνεται αντιληπτή από παρατηρητή στην είσοδο σαν απώλεια πληροφορίας και αποδίδεται στην άγνοια του για τη δομή και τη λειτουργία του διαύλου πληροφορίας. Η υπό συνθήκη εντροπία H(B/A) ονομάζεται κατά λογική ακολουθία *εντροπία διαύλου*. Στο ισοζύγιο πληροφορίας του σχήματος 2.3β η εντροπία διαύλου εμφανίζεται σαν πληροφορία που πηγάζει από το δίαυλο πληροφορίας και διατίθεται στην έξοδο του. Είναι φανερό όμως ότι δεν είναι διαθέσιμη στην είσοδο. Ο παρατηρητής στην είσοδο αντιλαμβάνεται την έλλειψη της σαν αβεβαιότητα για το σύμβολο εξόδου. Εξάλλου ο παρατηρητής στην έξοδο χρησιμοποιεί την πληροφορία H(B/A) χωρίς να είναι σε θέση να εκτιμήσει το μέγεθος της επειδή γι' αυτον ο δίαυλος πληροφορίας εμφανίζεται σαν πηγή πληροφορίας με εντροπία $H(B) = [\, H(A) - H(A/B) \,] + H(B/A)$. Αν η λειτουργία του διαύλου πληροφορίας είναι προβλέψιμη από την είσοδο του, τότε δεν υπάρχει αβεβαιότητα για το σύμβολο εξόδου, δηλαδή $\pi(\beta_j/\alpha_i) = 0$ ή 1 και επομένως $H(B/A) = 0$.

2.2 ΔΙΑΠΛΗΡΟΦΟΡΙΑ - ΧΩΡΗΤΙΚΟΤΗΤΑ

Παρά την προφανή χρησιμότητα των μεγεθών που ορισθηκαν στην §2.1, είναι φανερό ότι δεν υπάρχει ακόμη ένα μέγεθος που να χαρακτηρίζει και επομενως να εκπροσωπεί το δίαυλο πληροφορίας. Το βήμα αυτο πραγματοποιείται εδώ εισάγοντας την έννοια της διαπληροφορίας, που είναι ουσιαστικά ένα μεταβατικό μέγεθος, και μετά την έννοια της χωρητικότητας του διαύλου πληροφορίας.

ΟΡΙΣΜΟΣ : Διαπληροφορία ή αμοιβαία εντροπία διαύλου πληροφορίας είναι η μέση ποσότητα πληροφορίας που διοχετεύεται ανά σύμβολο πληροφορίας. Περιγράφεται μαθηματικά με την έκφραση :

$$I(A,B) = H(A) - H(A/B) \qquad (2.5)$$

και έχει τις παρακάτω ιδιότητες :

(α) $I(A,B) = I(B,A)$, δηλαδή είναι συμμετρική ως προς A,B,
(β) $I(A,B) \geq 0$, δηλαδή είναι μη αρνητικό μέγεθος, και
(γ) μεγιστοποιείται σε περιβάλλον απαλλαγμένο από θόρυβο.

Για την απόδειξη της ιδιότητας (α) χρησιμοποιούνται στην εξ.(2.5) οι εκφράσεις για την εντροπία εισόδου και την εντροπία θορύβου :

$$I(A,B) = -\sum_{i=1}^{\rho} n(\alpha_i)\log_c\left[n(\alpha_i)\right] + \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_c\left[n(\alpha_i/\beta_j)\right] =$$

$$= -\sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_c\left[n(\alpha_i)\right] + \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_c\left[\frac{n(\alpha_i,\beta_j)}{n(\beta_j)}\right] =$$

$$= \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma} n(\alpha_i,\beta_j)\log_c\left[\frac{n(\alpha_i,\beta_j)}{n(\alpha_i)n(\beta_j)}\right] \qquad (2.6)$$

Η έκφραση της εξ.(2.6) είναι προφανώς συμμετρική ως προς A,B και επομένως η εξ.(2.5) επεκτείνεται στην παρακάτω :

$$I(A,B) = H(A) - H(A/B) = H(B) - H(B/A) \qquad (2.7)$$

Με εφαρμογή της εξ.(1.21) προκύπτει επιπλέον :

$$I(A,B) = H(A) + H(B) - H(AB) \qquad (2.8)$$

Για την απόδειξη της ιδιότητας (β) χρησιμοποιείται η εξ.(1.22), που καθορίζει ότι $H(A/B) \leq H(A)$, οπότε $I(A,B) = H(A) - H(A/B) \geq 0$.

Αν δεν παρεισφρύει θόρυβος στο σύστημα επικοινωνίας, δεν δημιουργείται αβεβαιότητα για το σύμβολο στην είσοδο με δεδομένο το σύμβολο στην έξοδο του διαύλου πληροφορίας, οπότε $\pi(\alpha_i/\beta_j) = 0$ ή 1 και $H(A/B) = 0$. Επειδή η διαπληροφορία είναι μη αρνητικό μέγεθος και επιπλέον προκύπτει σαν διαφορά των μη αρνητικών μεγεθών $H(A)$, $H(A/B)$, η μέγιστη τιμή της $I(A,B) = H(A)$ αντιστοιχεί στην περίπτωση με $H(A/B) = 0$, δηλαδή στην εξιδανικευμένη περίπτωση που το περιβάλλον λειτουργίας του διαύλου πληροφορίας είναι απαλλαγμένο από θόρυβο ή, ισοδύναμα, ο δίαυλος πληροφορίας είναι τέλεια προστατευμένος από το περιβάλλον του.

ΟΡΙΣΜΟΣ : Χωρητικότητα διαύλου πληροφορίας είναι το μέγιστο της διαπληροφορίας σε περιβάλλον θορύβου :

$$C = \max_{\Pi_A} \left\{ I(A,B) \right\} \qquad (2.9)$$

Είναι φανερό ότι το μέγιστο αντιστοιχεί σε συγκεκριμένη κατανομή πιθανότητας των συμβόλων εισόδου. Δηλαδή, με κατάλληλη κατανομή πιθανοτήτων για τα σύμβολα εισόδου μεγιστοποιείται η ποσότητα πληροφορίας που διοχετεύεται στο δίαυλο πληροφορίας. Ο προσδιορισμός της κατανομής πιθανότητας Π_A που εξασφαλίζει τη βέλτιστη εκμετάλευση του διαύλου πληροφορίας είναι σημαντικό πρόβλημα στα συστήματα επικοινωνίας. Η χωρητικότητα, όπως και η διαπληροφορία, μετρώνται σε bits/σύμβολο ή και bits/sec αν είναι γνωστός ο ρυθμός προσαγωγής συμβόλων στην είσοδο του διαύλου πληροφορίας.

2.3 ΑΠΛΟΙ ΔΙΑΥΛΟΙ ΠΛΗΡΟΦΟΡΙΑΣ

Στη συνέχεια παρουσιάζονται μερικοί απλοί δίαυλοι πληροφορίας και υπολογίζεται η χωρητικότητα τους. Τέτοιοι δίαυλοι πληροφορίας είναι δυνατό να χρησιμοποιηθούν σαν δομικά στοιχεία συνθετώτερων συστημάτων επικοινωνίας.

2.3.1 ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ ΧΩΡΙΣ ΑΠΩΛΕΙΕΣ

Χαρακτηρίζεται από την παρουσία ενός μόνο μη μηδενικού στοιχείου σε κάθε στήλη του μητρώου διαύλου (σχ. 2.4). Είναι φανερό ότι για δεδομένο σύμβολο στην έξοδο του διαύλου πληροφορίας δεν υπάρχει αβεβαιότητα για το αντίστοιχο σύμβολο στην είσοδο του. Επομένως $\Pi(\alpha_i/\beta_j) = 0$ ή 1 και $H(A/B) = 0$. Η εξ.(2.5) καθορίζει :

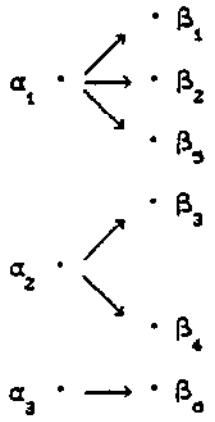
$$I(A,B) = H(A) \tag{2.10}$$

και επομένως :

$$C = \max\{ I(A,B) \} = \max\{ H(A) \} = \log_c \rho \tag{2.11}$$

Το μέγιστο προκύπτει στην περίπτωση που τα σύμβολα εισόδου είναι ισοπίθανα, δηλαδή $\Pi_A = \{ 1/\rho, 1/\rho, \ldots, 1/\rho \}$.

	β_1	β_2	β_3	β_4	β_5	β_6
α_1	1/8	3/8	0	0	1/2	0
α_2	0	0	2/3	1/3	0	0
α_3	0	0	0	0	0	1



Σχ. 2.4 Δίαυλος πληροφορίας χωρίς απώλειες.

2.3.2 ΚΑΘΟΡΙΣΤΙΚΟΣ ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Είναι ο δυαδικός του προηγουμένου διαύλου πληροφορίας αφού έχει ένα μόνο μη μηδενικό στοιχείο σε κάθε σειρά του μητρώου $\Pi(B/A)$ (σχ. 2.5). Είναι φανερό ότι για δεδομένο σύμβολο στην είσοδο του διαύλου πληροφορίας δεν υπάρχει αβεβαιότητα

για το αντίστοιχο σύμβολο στην έξοδο του. Επομένως $\Pi(\beta_j/\alpha_i) = 0$ ή 1 και $H(B/A) = 0$. Η εξ.(2.5) καθορίζει :

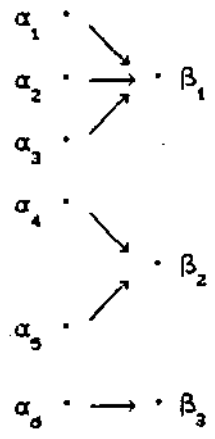
$$I(A,B) = H(B) \tag{2.12}$$

και επομένως :

$$C = \max\{ I(A,B) \} = \max\{ H(B) \} = \log_c \sigma \tag{2.13}$$

Το μέγιστο προκύπτει στην περίπτωση που τα σύμβολα εξόδου γίνονται ισοπίθανα, δηλαδή $\Pi_B = (1/\sigma, 1/\sigma, \ldots, 1/\sigma)$ και με την προϋπόθεση αυτή προσδιορίζεται η κατάλληλη κατανομή πιθανοτήτων για τα σύμβολα εισόδου.

	β_1	β_2	β_3
α_1	1	0	0
α_2	1	0	0
α_3	1	0	0
α_4	0	1	0
α_5	0	1	0
α_6	0	0	1



Σχ. 2.5 Καθαριστικός δίαυλος πληροφορίας.

2.3.3 ΙΔΑΝΙΚΟΣ ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Είναι η τομή των δύο προηγουμένων περιπτώσεων. Σε κάθε σειρά ή στήλη του μητρώου $\Pi(B/A)$ υπάρχει ένα μόνο μη μηδενικό στοιχείο (σχ. 2.6). Είναι φανερό ότι για δεδομένο σύμβολο στην είσοδο ή έξοδο του διαύλου πληροφορίας δεν υπάρχει αβεβαιότητα για το σύμβολο στην έξοδο ή είσοδο του, αντίστοιχα. Τα σύμβολα εξόδου είναι ισάριθμα με τα σύμβολα εισόδου και το μητρώο $\Pi(B/A)$ είναι μοναδιαίο. Η χωρητικότητα του ιδανικού διαύλου πληροφορίας προκύπτει από τις εξ.(2.11),(2.13) που συγχωνεύονται στην παρακάτω :

$$C = \max\left\{ H(A) \right\} = \max\left\{ H(B) \right\} = \log_e \rho = \log_e \sigma \qquad (2.14)$$

και η κατάλληλη καταναμή πιθανοτήτων για τα σύμβολα εισόδου είναι $\Pi_A = \{ 1/\rho, 1/\rho, \ldots, 1/\rho \}$.

	β_1	β_2	β_3
α_1	1	0	0
α_2	0	1	0
α_3	0	0	1

$\alpha_1 \cdot \longrightarrow \cdot \beta_1$

$\alpha_2 \cdot \longrightarrow \cdot \beta_2$

$\alpha_3 \cdot \longrightarrow \cdot \beta_3$

Σχ. 2.6 Ιδανικός δίαυλος πληροφορίας.

2.3.4 ΟΜΟΙΟΜΟΡΦΟΣ ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Έχει τα εξής χαρακτηριστικά : (α) όλες οι σειρές του μητρώου Π(B/A) είναι αναδιατάξεις κάποιας σειράς και (β) όλες οι στήλες του μητρώου Π(B/A) προκύπτουν επίσης με αναδιάταξη των στοιχείων οποιασδήποτε στήλης. Αν το μητρώο Π(B/A) είναι τετραγωνικό, όλες οι σειρές και οι στήλες του περιέχουν τα ίδια στοιχεία με οποιαδήποτε σειρά ή στήλη του (σχ. 2.7). Η εντροπία διαύλου είναι ανεξάρτητη από την καταναμή πιθανοτήτων των συμβόλων εισόδου. Αυτό αποδεικνύεται με εφαρμογή της εξ.(1.19) :

$$H(B/A) = -\sum_{i=1}^{\rho} \sum_{j=1}^{\sigma} \pi(\alpha_i, \beta_j) \log_e \left[\pi(\beta_j/\alpha_i) \right] =$$

$$= -\sum_{i=1}^{\rho} \left\{ \sum_{j=1}^{\sigma} \pi(\beta_j/\alpha_i) \log_e \left[\pi(\beta_j/\alpha_i) \right] \right\} \pi(\alpha_i) \qquad (2.15)$$

Αλλά το εσωτερικό άθροισμα στο δεξιό μέλος της εξ.(2.15) είναι σταθερό για κάθε σειρά του μητρώου Π(B/A), δηλαδή ανεξάρτητο του δείκτη i, και

επομένως :

$$H(B/A) = -\left[\sum_{j=1}^{\sigma} n(\beta_j/\alpha_i)\log_e\left[n(\beta_j/\alpha_i)\right]\right]\left[\sum_{i=1}^{\rho} n(\alpha_i)\right] =$$

$$= -\sum_{j=1}^{\sigma} n(\beta_j/\alpha_i)\log_e\left[n(\beta_j/\alpha_i)\right] \qquad (2.16)$$

Η διαπληροφορία του ομοιόμορφου διαύλου πληροφορίας προκύπτει με συνδυασμό των εξ.(2.7),(2.16) :

$$I(A,B) = H(B) + \sum_{j=1}^{\sigma} n(\beta_j/\alpha_i)\log_e\left[n(\beta_j/\alpha_i)\right] \qquad (2.17)$$

Η χωρητικότητα του προκύπτει από την εξ.(2.17) μεγιστοποιώντας την εντροπία εξόδου H(B) :

$$C = \log_e\sigma + \sum_{j=1}^{\sigma} n(\beta_j/\alpha_i)\log_e\left[n(\beta_j/\alpha_i)\right] \qquad (2.18)$$

και η κατάλληλη κατανομή πιθανοτήτων για τα σύμβολα εισόδου είναι εκείνη που καθιστά τα σύμβολα εξόδου ισοπίθανα.

2.3.5 ΔΥΑΔΙΚΟΣ ΣΥΜΜΕΤΡΙΚΟΣ ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Είναι ομοιόμορφος δίαυλος πληροφορίας με δύο σύμβολα εισόδου και δύο σύμβολα εξόδου (σχ. 2.8). Η χωρητικότητα του προκύπτει με εφαρμογή της εξ.(2.18) :

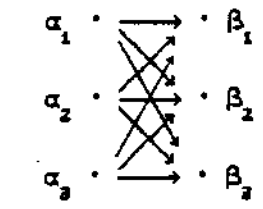
$$C = \log_e 2 + n\log_e n + (1-n)\log_e(1-n) \qquad (2.19)$$

όπου n είναι η πιθανότητα ορθής μετάδοσης κάθε συμβόλου εισόδου. Αν η βάση υπολογισμού των λογαρίθμων είναι 2, διαμορφώνεται η απλούστερη έκφραση :

$$C = 1 - H(\pi) \quad \text{bits/σύμβολο} \tag{2.20}$$

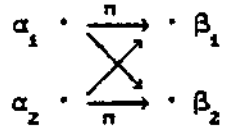
με $H(\pi)$ τη γνωστή (βλ. §1.2) συνάρτηση Shannon.

	β_1	β_2	β_3
α_1	1/2	1/4	1/4
α_2	1/4	1/4	1/2
α_3	1/4	1/2	1/4



Σχ. 2.7 Ομοιόμορφος δίαυλος πληροφορίας.

	β_1	β_2
α_1	π	$1-\pi$
α_2	$1-\pi$	π



Σχ. 2.8 Διαδικός συμμετρικός δίαυλος πληροφορίας.

2.3.6 Σ – ΔΙΑΥΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ

Λειτουργεί με δύο σύμβολα εισόδου και τρία σύμβολα εξόδου (σχ. 2.9). Το σύμβολο εξόδου β_2 εμφανίζεται όταν γίνεται σφάλμα κατά τη μετάδοση οποιουδήποτε συμβόλου εισόδου. Επομένως ο Σ – δίαυλος πληροφορίας προσφέρει τη δυνατότητα αποκάλυψης σφαλμάτων μετάδοσης. Εύκολα προκύπτει η παρακάτω απλή έκφραση για την εντροπία θορύβου με εφαρμογή της εξ. (1.19) :

$$H(A/B) = (1-\pi)H(A) \tag{2.21}$$

οπότε η εξ. (2.5) καθορίζει για τη διαπληροφορία :

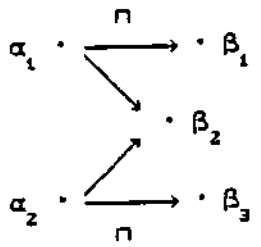
$$I(A,B) = \pi\, H(A) \tag{2.22}$$

Επομένως η χωρητικότητα του Σ - διαύλου πληροφορίας είναι :

$$C = n \max\left\{ H(A) \right\} = n\log_2 2 = n \text{ bits/σύμβολο} \qquad (2.23)$$

και αντιστοιχεί σε ισοπίθανα σύμβολα εισόδου.

	β_1	β_2	β_3
α_1	n	$1-n$	0
α_2	0	$1-n$	n



Σχ. 2.9 Σ - δίαυλος πληροφορίας.

2.4 ΤΕΧΝΙΚΗ MUROGA

Η χωρητικότητα συνθετώτερων διαύλων πληροφορίας προσδιορίζεται με την τεχνική Muroga που μεγιστοποιεί την έκφραση της διαπληροφορίας με τη βοήθεια πολλαπλασιαστών Lagrange. Η τεχνική Muroga πλεονεκτεί σε σύγκριση με την κατευθείαν εφαρμογή του ορισμού στο ότι μετατρέπει το πρόβλημα προσδιορισμού της χωρητικότητας σε πρόβλημα επίλυσης γραμμικού συστήματος εξισώσεων που αντιμετωπίζεται εύκολα με ηλεκτρονικό υπολογιστή.

Στη συνέχεια περιγράφεται χωρίς απόδειξη η τεχνική Muroga για δίαυλο πληροφορίας με ισάριθμα σύμβολα εισόδου - εξόδου. Το μητρώο διαύλου $\Pi(B/A)$ είναι τετραγωνικό με ρ σειρές και ρ στήλες. Με τα στοιχεία $n_{ij} = n(\beta_j/\alpha_i)$ διαμορφώνεται το παρακάτω γραμμικό σύστημα :

$$n_{11}X_1 + n_{12}X_2 + \ldots + n_{1\rho}X_\rho = \sum_{j=1}^{\rho} n_{1j}\log(n_{1j})$$

$$\pi_{21}X_1 + \pi_{22}X_2 + \ldots + \pi_{2\rho}X_\rho = \sum_{j=1}^{\rho} \pi_{2j}\log(\pi_{2j}) \qquad (2.24)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\pi_{\rho 1}X_1 + \pi_{\rho 2}X_2 + \ldots + \pi_{\rho\rho}X_\rho = \sum_{j=1}^{\rho} \pi_{\rho j}\log(\pi_{\rho j})$$

με αγνώστους τα βοηθητικά μεγέθη $X_1, X_2, \ldots, X_\rho$. Αφού επιλυθεί το σύστημα των εξ.(2.24), υπολογίζεται η χωρητικότητα του διαύλου πληροφορίας από την παρακάτω έκφραση :

$$C = \log_c\left(\sum_{i=1}^{\rho} 2^{x_i} \right) \qquad (2.25)$$

Οι πιθανότητες των συμβόλων εξόδου που εξασφαλίζουν πλήρη εκμετάλευση της χωρητικότητας του διαύλου πληροφορίας είναι :

$$\pi(\beta_i) = 2^{(x_i - C)} \quad ; \quad i = 1, 2, \ldots, \rho \qquad (2.26)$$

και η αντίστοιχη κατανομή πιθανότητας για τα σύμβολα εισόδου προκύπτει μέσω της εξ.(2.2). Η τεχνική Muroga, όπως διαπιστώνεται στο παράδειγμα που ακολουθεί, διευκολύνει σημαντικά τον υπολογισμό της χωρητικότητας ακόμη και σε διαύλους πληροφορίας με ολιγάριθμα σύμβολα εισόδου – εξόδου.

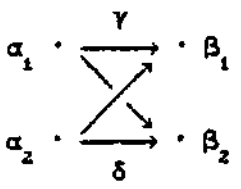
ΠΑΡΑΔΕΙΓΜΑ : Ο *γενικευμένος διαδυκός δίαυλος πληροφορίας* (σχ. 2.10) διαφοροποιείται από το δυαδικό συμμετρικό δίαυλο πληροφορίας (βλ. §2.3.5) κατά το ότι η πιθανότητα ορθής / εσφαλμένης μετάδοσης είναι διαφορετική για καθένα από τα δύο σύμβολα εισόδου. Αν οι πιθανότητες των συμβόλων εισόδου είναι $\pi(\alpha_1) = p$ και $\pi(\alpha_2) = 1 - p = q$, με κατευθείαν εφαρμογή του ορισμού προκύπτει η παρακάτω έκφραση για τη διαπληροφορία :

$$I(A,B) = H(p) + \gamma p\log_c\left(\frac{\gamma p}{\gamma p + (1-\delta)q} \right) + \delta q\log_c\left(\frac{\delta q}{(1-\gamma)p + \delta q} \right) +$$

$$+ (1-\gamma)p\log_e\left[\frac{(1-\gamma)p}{(1-\gamma)p + \delta q}\right] + (1-\delta)q\log_e\left[\frac{(1-\delta)q}{\gamma p + (1-\delta)q}\right] \qquad (2.27)$$

Για να προσδιορισθεί η χωρητικότητα του διαύλου πληροφορίας πρέπει να μεγιστοποιηθεί η έκφραση στο δεξιό μέλος της εξ.(2.27). Αυτό είναι κατ' αρχή δυνατό αλλά όχι και τόσο εύκολο παρόλο που πρόκειται για μάλλον απλό δίαυλο.

	β_1	β_2
α_1	γ	$1-\gamma$
α_2	$1-\delta$	δ



Σχ. 2.10 Γενικευμένος διαδυκός δίαυλος πληροφορίας.

Αν εφαρμοσθεί η τεχνική Muroga, διαμορφώνεται το παρακάτω γραμμικό σύστημα εξισώσεων :

$$\begin{aligned} \gamma X_1 + (1-\gamma)X_2 &= -H(\gamma) \\ (1-\delta)X_1 + \delta X_2 &= -H(\delta) \end{aligned} \qquad (2.28)$$

από το οποίο υπολογίζονται τα βοηθητικά μεγέθη X_1, X_2 :

$$\begin{aligned} X_1 &= \frac{\delta H(\gamma) - (1-\gamma)H(\delta)}{1-\gamma-\delta} \\ X_2 &= \frac{\gamma H(\delta) - (1-\delta)H(\gamma)}{1-\gamma-\delta} \end{aligned} \qquad (2.29)$$

Στη συνέχεια με εφαρμογή της εξ.(2.25) προκύπτει η χωρητικότητα του διαύλου πληροφορίας :

$$C = \frac{\gamma H(\delta) + \delta H(\gamma)}{1-\gamma-\delta} + \log_e\left[2^{\frac{H(\gamma)}{\gamma+\delta-1}} + 2^{\frac{H(\delta)}{\gamma+\delta-1}}\right] \qquad (2.30)$$

ενώ με εφαρμογή της εξ.(2.26) προκύπτουν οι κατάλληλες πιθανότητες για τα σύμβολα εξόδου :

$$\pi(\beta_1) = \frac{2^{\frac{H(\delta)}{\gamma+\delta-1}}}{2^{\frac{H(\gamma)}{\gamma+\delta-1}} + 2^{\frac{H(\delta)}{\gamma+\delta-1}}}$$

$$\pi(\beta_2) = \frac{2^{\frac{H(\gamma)}{\gamma+\delta-1}}}{2^{\frac{H(\gamma)}{\gamma+\delta-1}} + 2^{\frac{H(\delta)}{\gamma+\delta-1}}} \qquad (2.31)$$

Είναι φανερό ότι $\pi(\beta_1) + \pi(\beta_2) = 1$. Με εφαρμογή της εξ.(2.2) προκύπτουν τελικά οι κατάλληλες πιθανότητες για τα σύμβολα εισόδου :

$$p = \pi(\alpha_1) = \frac{\delta - \pi(\beta_2)}{\gamma + \delta - 1}$$

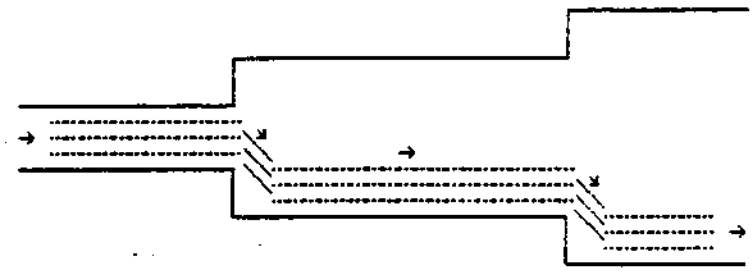
$$q = \pi(\alpha_2) = \frac{\gamma - \pi(\beta_1)}{\gamma + \delta - 1} \qquad (2.32)$$

και είναι φανερό ότι $p + q = \pi(\alpha_1) + \pi(\alpha_2) = 1$.

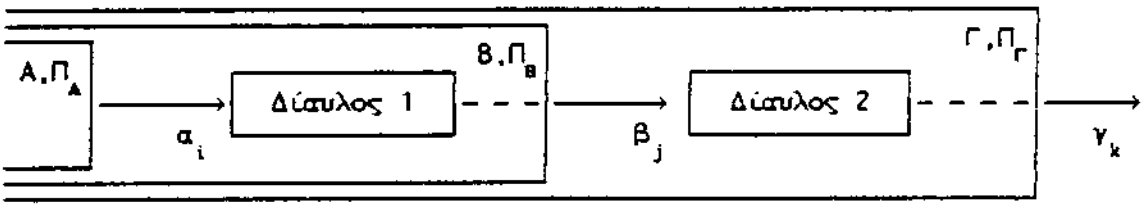
2.5 ΑΛΥΣΙΔΩΤΗ ΣΥΝΔΕΣΗ ΔΙΑΥΛΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

Αλυσίδα διαύλων πληροφορίας προκύπτει όταν αριθμός απλών διαύλων πληροφορίας διατάσσονται κατά τέτοιο τρόπο ώστε η έξοδος καθενός να είναι είσοδος του επομένου. Σε πραγματικά συστήματα επικοινωνιών η πληροφορία ρέει συνήθως μέσα από αλυσίδα διαύλων πληροφορίας (π.χ. πομπός, κυματοδηγός, κεραία εκπομπής, ατμόσφαιρα, κεραία λήψεως, δέκτης) και επομένως είναι λογικό να ενδιαφέρει τέτοια σύνδεση απλών διαύλων πληροφορίας.

Αν για τη ροή πληροφορίας μέσα από αλυσίδα διαύλων πληροφορίας χρησιμοποιηθεί η παρομοίωση της ροής κάποιου ρευστού μέσα από διαδοχή αγωγών διαφορετικής διατομής (σχ. 2.11), διαμορφώνεται αβίαστα η εντύπωση ότι γενικά δεν είναι δυνατή η βέλτιστη εκμετάλευση της χωρητικότητας κάθε απλού διαύλου πληροφορίας που συμμετέχει στην αλυσίδα. Η ανάλυση που ακολουθεί θα επιβεβαιώσει τη διαίσθηση.



Σχ. 2.11 Ροή ρευστού μέσα από αγωγούς διαφορετικής διατομής. Ενώ εξαντλείται η χωρητικότητα του πρώτου αγωγού, στους επόμενους υπάρχει ανεκμετάλευτος χώρος.



Σχ. 2.12 Αλυσίδα δύο απλών διαύλων πληροφορίας.

Εστω αλυσίδα δύο απλών διαύλων πληροφορίας (σχ. 2.12). Η πηγή πληροφορίας A,Π_A στην είσοδο της αλυσίδας προεκτείνεται στην πηγή πληροφορίας B,Π_B στην έξοδο του πρώτου απλού διαύλου πληροφορίας και τελικά στην πηγή πληροφορίας Γ,Π_Γ στην έξοδο του δεύτερου απλού διαύλου πληροφορίας. Η διαπληροφορία στον πρώτο απλό δίαυλο πληροφορίας είναι $I(A,B) = H(A) - H(A/B)$ και στην αλυσίδα των δύο απλών διαύλων πληροφορίας είναι $I(A,\Gamma) = H(A) - H(A/\Gamma)$. Αν η αλυσίδα δεν εξασφαλίζει πλήρη εκμετάλευση της χωρητικότητας κάθε απλού διαύλου πληροφορίας, όπως υποδεικνύει η διαίσθηση, πρέπει :

$$I(A,B) - I(A,\Gamma) = H(A/\Gamma) - H(A/B) \geq 0 \qquad (2.33)$$

και αυτό θα αποδειχθεί με εφαρμογή της εξ.(1.19). Εύκολα αποδεικνύεται ότι :

$$H(A/\Gamma) - H(A/B) = \sum_{i=1}^{\rho}\sum_{j=1}^{\sigma}\sum_{k=1}^{\tau} \pi(\alpha_i,\beta_j,\gamma_k)\log_e\left[\frac{\pi(\alpha_i/\beta_j)}{\pi(\alpha_i/\gamma_k)}\right] \qquad (2.34)$$

Επειδή καθένας από τους απλούς διαύλους πληροφορίας λειτουργεί ανεξάρτητα από τον άλλο, ισχύει :

$$\pi(\gamma_k/\beta_j,\alpha_i) = \pi(\gamma_k/\beta_j) \qquad (2.35)$$

Αλλά $\pi(\gamma_k/\beta_j,\alpha_i) = \pi(\gamma_k,\beta_j,\alpha_i)/\pi(\beta_j,\alpha_i)$ και $\pi(\gamma_k/\beta_j) = \pi(\gamma_k,\beta_j)/\pi(\beta_j)$ οπότε η εξ.(2.35) γράφεται με τη μορφή που ακολουθεί :

$$\frac{\pi(\alpha_i,\beta_j,\gamma_k)}{\pi(\beta_j,\gamma_k)} = \frac{\pi(\alpha_i,\beta_j)}{\pi(\beta_j)} \qquad (2.36)$$

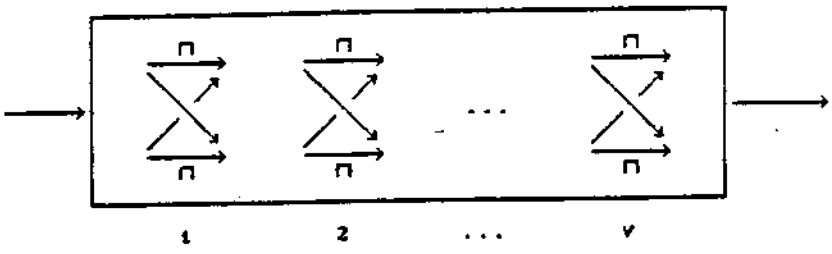
Η εξ.(2.36) οδηγεί στην παρακάτω :

$$\pi(\alpha_i/\beta_j,\gamma_k) = \pi(\alpha_i/\beta_j) \qquad (2.37)$$

που υποδεικνύει ότι καθένας απλός δίαυλος πληροφορίας λειτουργεί ανεξάρτητα από τον άλλο ακόμη και όταν η πληροφορία ρέει κατά την αντίθετη φορά. Με αντικατάσταση από την εξ.(2.37) στην εξ.(2.34) προκύπτει :

$$H(A/\Gamma) - H(A/B) = \sum_{j=1}^{\sigma}\sum_{k=1}^{\tau}\pi(\beta_j,\gamma_k)\left[\sum_{i=1}^{\rho}\pi(\alpha_i/\beta_j,\gamma_k)\log_e\left[\frac{\pi(\alpha_i/\beta_j,\gamma_k)}{\pi(\alpha_i/\gamma_k)}\right]\right] \qquad (2.38)$$

Αλλά το άθροισμα μεταξύ παρενθέσεων στο δεξιό μέλος της εξ.(2.38) είναι, σύμφωνα με την εξ.(1.7), μη αρνητικό. Επομένως επιβεβαιώνεται η εξ.(2.33) που υποδεικνύει ότι η διαπληροφορία στον πρώτο απλό δίαυλο πληροφορίας είναι μεγαλύτερη από τη διαπληροφορία στην αλυσίδα των δύο απλών διαύλων πληροφορίας. Αν $\pi(\alpha_i/\beta_j,\gamma_k) = \pi(\alpha_i/\gamma_k)$, τότε $I(A,B) - I(A,\Gamma) = H(A/\Gamma) - H(A/B) = 0$, δηλαδή παρά την αλυσιδωτή σύνδεση εξασφαλίζεται η βέλτιστη εκμετάλευση και των δύο απλών διαύλων πληροφορίας που συνιστούν την αλυσίδα.



Σχ. 2.13 Αλυσίδα ν δυαδικών συμμετρικών διαύλων πληροφορίας.

ΠΑΡΑΔΕΙΓΜΑ : Έστω αλυσίδα ν δυαδικών συμμετρικών διαύλων πληροφορίας (σχ. 2.13). Αν $p \geq 1/2$ είναι η πιθανότητα ορθής μετάδοσης οποιουδήποτε δυαδικού ψηφίου σε καθένα μέλος της αλυσίδας, αποδεικνύεται επαγωγικά ότι το μητρώο διαύλου της αλυσίδας είναι :

$$\Pi(B/A) = \begin{bmatrix} p_v & 1-p_v \\ 1-p_v & p_v \end{bmatrix} \tag{2.34}$$

με $p_v = (1 + \delta^v)/2$ και $\delta = 2p - 1$. Επειδή η αλυσίδα εμφανίζεται σαν δυαδικός συμμετρικός δίαυλος πληροφορίας (βλ. §2.3.5), η χωρητικότητα της είναι δυνατό να προσδιορισθεί με εφαρμογή της εξ.(2.19) :

$$C = \log_e 2 + p_v \log_e(p_v) + (1-p_v)\log_e(1-p_v) \tag{2.40}$$

Αν η βάση υπολογισμού των λογαρίθμων είναι 2, η εξ.(2.40) παίρνει τη μορφή που ακολουθεί :

$$C = 1 - H(p_v) \quad \text{bits/σύμβολο} \tag{2.41}$$

όπου $H(\cdot)$ είναι η συνάρτηση Shannon. Στο όριο $v \to \infty$, $\delta^v \to 0$, $p_v \to 1/2$ και :

$$\lim_{v \to \infty} C \to 1 - H(1/2) = 1 - 1 = 0 \tag{2.42}$$

δηλαδή η χωρητικότητα της αλυσίδας οριακά μηδενίζεται καθώς αυξάνει το μήκος της. Στην ιδανική περίπτωση με $p = 1$ ισχύει $p_v = 1$ και $C = 1 - H(1) = 1 - 0 = 1$ bit/σύμβολο ανεξάρτητα από το μήκος της αλυσίδας. Το αποτέλεσμα αυτό είναι λογικό επειδή σε κάθε μέλος της αλυσίδας θεωρήθηκε μηδενική πιθανότητα

σφάλματος.

2.6 ΑΝΑΛΟΓΙΚΗ ΡΟΗ ΠΛΗΡΟΦΟΡΙΑΣ

Αν στην είσοδο του διαύλου πληροφορίας προσαρμοσθεί αναλογική πηγή πληροφορίας A,π_A (βλ. §1.7), τότε και η έξοδος του εμφανίζεται, σύμφωνα με όσα αναφέρθηκαν στην §2.1, σαν αναλογική πηγή πληροφορίας, έστω B,π_B. Στο παράδειγμα της §1.7 η αναλογική πηγή πληροφορίας A,π_A εκπροσωπήθηκε από κανονική τυχαία μεταβλητή με (σταθερή) τυπική απόκλιση σ_A, δηλαδή :

$$\pi_A(\alpha) = \frac{1}{\sigma_A\sqrt{2\pi}} \exp\left\{ - \frac{\alpha^2}{2\sigma_A^2} \right\} \qquad (2.43)$$

Αν αυτή προσαρμοσθεί στην είσοδο του διαύλου πληροφορίας και επιπλέον το σύστημα επικοινωνίας θεωρηθεί γραμμικό για απλότητα, τότε και η έξοδος του διαύλου πληροφορίας θα εκπροσωπείται από κανονική τυχαία μεταβλητή με σταθερή τυπική απόκλιση, έστω σ_B, δηλαδή :

$$\pi_B(\beta) = \frac{1}{\sigma_B\sqrt{2\pi}} \exp\left\{ - \frac{\beta^2}{2\sigma_B^2} \right\} \qquad (2.44)$$

Επιπλέον η συνδετική κατανομή πυκνότητας πιθανότητας των μεταβλητών A,B θα είναι διδιάστατη κανονική :

$$\pi_{AB}(\alpha,\beta) = \frac{1}{2\pi\sigma_A\sigma_B\sqrt{1-\rho^2}} \exp\left\{ - \frac{1}{2(1-\rho^2)} \left(\frac{\alpha^2}{\sigma_A^2} + \frac{\beta^2}{\sigma_B^2} - \frac{2\rho\alpha\beta}{\sigma_A\sigma_B} \right) \right\} \qquad (2.45)$$

όπου $\rho = E(AB)/\sigma_A\sigma_B$ είναι ο συντελεστής συσχέτισης. Είναι λογικό να υπάρχει σημαντική συσχέτιση μεταξύ εισόδου και εξόδου αν ο δίαυλος πληροφορίας λειτουργεί ικανοποιητικά, δηλαδή, αν εξασφαλίζει αξιόπιστη ροή της πληροφορίας.

Κατ' αναλογία με την εξ.(1.48) ορίζεται η διαπληροφορία του διαύλου πληροφορίας:

$$I(A,B) = \int\int \pi_{AB}(\alpha,\beta)\ \log_e\left(\frac{\pi_{AB}(\alpha,\beta)}{\pi_A(\alpha)\pi_B(\beta)}\right) d\alpha d\beta \qquad (2.46)$$

και η εξ.(2.46) δεν είναι παρά προσαρμογή της εξ.(2.6) για αναλογική ροή πληροφορίας. Είναι φανερό ότι η έκφραση της διαπληροφορίας εξακολουθεί να είναι συμμετρική ως προς A,B. Με αντικατάσταση από τις εξ.(2.43)-(2.45) στην εξ.(2.46) προκύπτει :

$$I(A,B) = -\frac{1}{2}\log_e\left(1-\rho^2\right)\int\int \pi_{AB}(\alpha,\beta)\, d\alpha d\beta -$$

$$-\frac{\rho^2}{2(1-\rho^2)\ln e}\int\int \pi_{AB}(\alpha,\beta)\left(\frac{\alpha^2}{\sigma_A^2}+\frac{\beta^2}{\sigma_B^2}-\frac{2\alpha\beta}{\rho\sigma_A\sigma_B}\right) d\alpha d\beta \qquad (2.47)$$

Είναι εύκολο να αποδειχθεί ότι ο δεύτερος όρος στο δεξιό μέλος της εξ.(2.47) είναι μηδέν. Επιπλέον $\int\int \pi_{AB}(\alpha,\beta)\, d\alpha d\beta = 1$ και επομένως η εξ.(2.47) παίρνει την απλή μορφή που ακολουθεί :

$$I(A,B) = -\frac{1}{2}\log_e\left(1-\rho^2\right) \qquad (2.48)$$

Η εξ.(2.48) υποδεικνύει ότι η ροή πληροφορίας καθορίζεται από το συντελεστή συσχέτισης εισόδου - εξόδου. Αλλά η υποβάθμιση της συσχέτισης οφείλεται στην παρουσία θορύβου που αλλοιώνει το σήμα κατά τη διέλευση του μέσα από το δίαυλο. Αν για απλότητα ο θόρυβος θεωρηθεί αθροιστικός και λευκός, δηλαδή με ομοιόμορφη φασματική πυκνότητα ισχύος σε ευρεία ζώνη, τότε ο μετασχηματισμός του σήματος κατά τη διέλευση του μέσα από το δίαυλο περιγράφεται από την απλή σχέση :

$$B = A + \Theta \qquad (2.49)$$

όπου Θ είναι η τυχαία μεταβλητή που εκπροσωπεί το θόρυβο. Είναι λογικό να τεθούν οι συνθήκες $E(\Theta) = 0$ και $E(A\Theta) = E(A)E(\Theta) = 0$ που δείχνουν ότι ο θόρυβος έχει μέση τιμή μηδέν και ακόμη ότι σήμα και θόρυβος είναι στατιστικά ανεξάρτητα αφού προέρχονται από ξεχωριστές πηγές. Με τις προϋποθέσεις αυτές προκύπτει :

$$\rho = \frac{E(AB)}{\sigma_A\sigma_B} = \frac{E(A(A+\Theta))}{\sigma_A\sigma_B} = \frac{E(A^2)}{\sigma_A\sigma_B} + \frac{E(A\Theta)}{\sigma_A\sigma_B} = \frac{\sigma_A^2}{\sigma_A\sigma_B} = \frac{\sigma_A}{\sigma_B} \qquad (2.50)$$

Είναι εύκολο να αποδειχθεί ότι :

$$\sigma_B^2 = \sigma_A^2 + \sigma_\Theta^2 \qquad (2.51)$$

και με αντικατάσταση από τις εξ.(2.50),(2.51) στην εξ.(2.48) προκύπτει :

$$I(A,B) = \frac{1}{2}\log_e\left(1 + \frac{\sigma_A^2}{\sigma_\Theta^2}\right) \qquad (2.52)$$

Αλλά η μεταβλητότητα αναλογικού σήματος περιγράφει τη μέση ισχύ του, δηλαδή $\sigma_A^2 = S$ (ισχύς σήματος) και $\sigma_\Theta^2 = N$ (ισχύς θορύβου), και επομένως ο λόγος $\sigma_A^2/\sigma_\Theta^2 = S/N$ είναι η σηματοθορυβική σχέση, που συνήθως δίνεται σε dB. Η εξ.(2.52) διαμορφώνεται τελικά στην παρακάτω :

$$I(A,B) = \frac{1}{2}\log_e\left(1 + \frac{S}{N}\right) \qquad (2.53)$$

που δείχνει ότι η αναλογική ροή πληροφορίας ελέγχεται αποκλειστικά από τη σηματοθορυβική σχέση. Εφόσον η παροχή πληροφορίας στην είσοδο του διαύλου είχε ήδη μεγιστοποιηθεί, η έκφραση της εξ.(2.53) ισχύει και για τη χωρητικότητα του διαύλου πληροφορίας, που είναι το μέγιστο της διαπληροφορίας, δηλαδή :

$$C = \frac{1}{2}\log_e\left(1 + \frac{S}{N}\right) \qquad (2.54)$$

Το μέγεθος C μετράται σε bits/σύμβολο αν η βάση υπολογισμού του λογαρίθμου στην εξ.(2.54) είναι 2. Αν το αναλογικό σήμα υποστεί δειγματοληψία με ρυθμό Nyquist (βλ. §2.I), το πλήθος δειγμάτων ανά δευτερόλεπτο που διέρχονται μέσα από το δίαυλο είναι 2B, με B το εύρος ζώνης του σήματος. Θεωρώντας σαν σύμβολα πληροφορίας τα δείγματα του αναλογικού σήματος, που είναι διακριτά στο χρόνο αλλά συνεχή κατά την τιμή τους, ο ρυθμός ροής πληροφορίας μέσα από το δίαυλο

είναι :

$$C = B \log_2\left(1 + \frac{S}{N}\right) \tag{2.55}$$

και το μέγεθος C μετράται εδώ σε bits/sec. Ενδεικτικές τιμές της χωρητικότητας τηλεπικοινωνιακών διαύλων δίνονται στον πίνακα 2.1. Αν ο θόρυβος είναι λευκός με φασματική πυκνότητα ισχύος n W/Hz, τότε N = nB και η εξ.(2.55) παίρνει τη μορφή:

$$C = B \log_2\left(1 + \frac{S}{nB}\right) \tag{2.56}$$

Στο όριο $B \to \infty$ προκύπτει :

$$\lim_{B \to \infty} C \to 1.44 \frac{S}{n} \tag{2.57}$$

δηλαδή, ακόμη και αν χρησιμοποιηθεί όλο το φάσμα συχνοτήτων ο ρυθμός ροής πληροφορίας δεν ξεπερνά το άνω φράγμα που καθορίζει η εξ.(2.57). Περαιτέρω αύξηση του ρυθμού ροής της πληροφορίας είναι δυνατή μόνο με βελτίωση του λόγου S/n. Εξυπονοείται ότι σε πρακτικές εφαρμογές δεν είναι διαθέσιμο παρά ελάχιστο μέρος του φάσματος.

Πίνακας 2.1

Χωρητικότητα τηλεπικοινωνιακών διαύλων πληροφορίας.

Δίαυλος	S/N (dB)	B (KHz)	C (bits/sec)
Τηλέτυπο			$5.0 \cdot 10^1$
Τηλέφωνο	15	4	$2.0 \cdot 10^4$
AM ραδιόφωνο	20	20	$1.3 \cdot 10^5$
FM ραδιόφωνο	35	75	$8.7 \cdot 10^5$
Τηλεόραση	40	6000	$7.9 \cdot 10^7$
ISDN			$1.5 \cdot 10^8$
Οπτική Ινα			$4.0 \cdot 10^9$

Η ενέργεια που απαιτείται για μετάδοση πληροφορίας 1 bit υπολογίζεται από το

λόγο S/C που έχει διάσταση Watts/(bits/sec) = Joules/bit. Είναι φανερό ότι το μέγεθος S/C συνδέεται με το κόστος και γενικά τη δυνατότητα υλοποίησης του τηλεπικοινωνιακού συστήματος. Αν οι φασματικές πυκνότητες ισχύος σήματος και θορύβου είναι ομοιόμορφες, δηλαδή $S = sB$ και $N = nB$ με s, n σταθερές, η σηματοθορυβική σχέση S/N ταυτίζεται με το λόγο s/n. Η *πληροφοριακή πυκνότητα ενέργειας* S/C προκύπτει από την εξ.(2.55) :

$$S/C = n \frac{S/N}{\log_2\left(1 + S/N\right)} \tag{2.58}$$

Σε πολλές περιπτώσεις ο θόρυβος είναι θερμικό αποτέλεσμα και η φασματική πυκνότητα ισχύος του δίνεται από την απλή έκφραση :

$$n = kT \tag{2.59}$$

όπου $k = 1.37\times10^{-23}$ Joules/°K είναι η σταθερά Boltzmann και T η απόλυτη θερμοκρασία που μετράται σε βαθμούς Kelvin (°K). Ακόμη και αν ο θόρυβος έχει άλλη προέλευση είναι δυνατό να χρησιμοποιηθεί η απλή έκφραση της εξ.(2.59) εισάγοντας τη *θερμοκρασία θορύβου* :

$$T_e = \frac{n}{k} \tag{2.60}$$

Αν χρησιμοποιηθεί η εξ.(2.60) στην εξ.(2.58), διαμορφώνεται η τελική έκφραση για την πληροφοριακή πυκνότητα ενέργειας :

$$S/C = kT_e \frac{S/N}{\log_2\left(1 + S/N\right)} \tag{2.61}$$

και είναι φανερό ότι $S/C \to \infty$ καθώς $S/N \to \infty$. Επομένως η ενεργειακή απαίτηση για μετάδοση 1 bit αυξάνει με τη σηματοθορυβική σχέση. Από την άλλη πλευρά $S/C \to kT_e \ln 2$ καθώς $S/N \to 0$. Αν $S/N = 30$ dB και $T_e \simeq 300$ °K, η εξ.(2.61) καθορίζει ότι $S/C \simeq 4\cdot10^{-19}$ Joules/bit, δηλαδή ενέργεια 1 Joule επαρκεί για μετάδοση $2.5\cdot10^{18}$ bits ! Είναι φανερό λοιπόν ότι στο πλαίσιο των εφαρμογών της θεωρίας πληροφοριών η ενέργεια είναι δευτερεύον μέγεθος. Ποιός ενδιαφέρεται σήμερα για την κατανάλωση ρεύματος του προσωπικού υπολογιστή του ;

2.7 ΑΣΚΗΣΕΙΣ

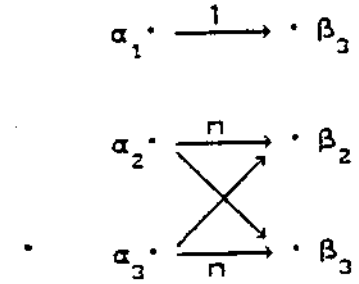
1. Εστω δίαυλος πληροφορίας με το παρακάτω μητρώο συνδετικών πιθανοτήτων των συμβόλων εισόδου, εξόδου :

$$\Pi(A,B) = \begin{bmatrix} 0.25 & 0.00 & 0.10 \\ 0.00 & 0.30 & 0.05 \\ 0.10 & 0.05 & 0.00 \\ 0.00 & 0.00 & 0.15 \end{bmatrix}$$

Να υπολογισθούν οι πιθανότητες των συμβόλων εισόδου, οι πιθανότητες των συμβόλων εξόδου, η εντροπία εισόδου H(A) και η εντροπία εξόδου H(B). Να προσδιορισθεί το μητρώο διαύλου Π(B/A) και να υπολογισθούν η εντροπία διαύλου H(B/A) και η εντροπία θορύβου H(A/B).

2. Να υπολογισθεί η χωρητικότητα (σε bits/sec) διαύλου πληροφορίας που διοχετεύει μηνύματα διάρκειας T sec. Η διακριτή πηγή πληροφορίας στην είσοδο του χρησιμοποιεί αλφάβητο ρ συμβόλων και εκπέμπει κ σύμβολα/sec. Να σχολιασθεί το αποτέλεσμα.

3. Δίνεται το παρακάτω διάγραμμα διαύλου :



Να προσδιορισθεί το μητρώο διαύλου Π(B/A). Αν $\pi(\alpha_1) = 0.3$, $\pi(\alpha_2) = 0.3$ και $\pi(\alpha_3) = 0.4$ είναι οι πιθανότητες των συμβόλων εισόδου, να προσδιορισθεί το μητρώο Π(A,B). Να υπολογισθεί η χωρητικότητα του διαύλου πληροφορίας.

4. Δίνονται τα παρακάτω μητρώα διαύλου. Να υπολογισθεί η χωρητικότητα των αντίστοιχων διαύλων πληροφορίας.

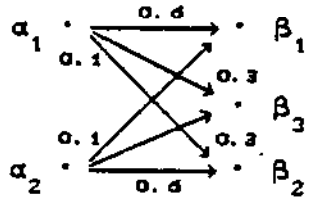
$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1/4 & 3/4 & 0 \\ 0 & 3/4 & 1/4 \end{bmatrix} \qquad \begin{bmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{bmatrix}$$

Στην τελευταία περίπτωση δίνονται και οι πιθανότητες των συμβόλων εισόδου $\pi(\alpha_1) = 3/4$, $\pi(\alpha_2) = 1/4$. Να υπολογισθεί η διαφορά μεταξύ διαπληροφορίας και χωρητικότητας και να αιτιολογηθεί.

5. Να υπολογισθεί η χωρητικότητα διαύλου πληροφορίας με μητρώο διαύλου :

$$\Pi(B/A) = \begin{bmatrix} 3/4 & 1/4 & 0 \\ 1/8 & 3/4 & 1/8 \\ 1/4 & 0 & 3/4 \end{bmatrix}$$

6. Δίνεται το παρακάτω διάγραμμα διαύλου. Να υπολογισθεί η χωρητικότητα του αντίστοιχου διαύλου πληροφορίας και να προσδιορισθεί η κατάλληλη καταναμή πιθανοτήτων των συμβόλων εισόδου.



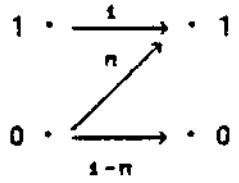
7. Δίνεται το παρακάτω μητρώο διαύλου :

$$\Pi(B/A) = \begin{bmatrix} \pi & 1-\pi & 0 & 0 \\ 1-\pi & \pi & 0 & 0 \\ 0 & 0 & \pi & 1-\pi \\ 0 & 0 & 1-\pi & \pi \end{bmatrix}$$

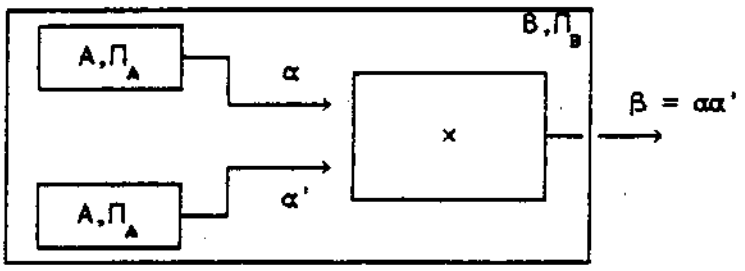
Να υπολογισθεί η χωρητικότητα $C(\pi)$ του αντίστοιχου διαύλου πληροφορίας και να σχεδιασθεί η συνάρτηση $C(\pi)$ στο διάστημα $[0, 1]$.

8. Να προσδιορισθεί η διαπληροφορία και η χωρητικότητα του *Z-διαύλου πληροφορίας*

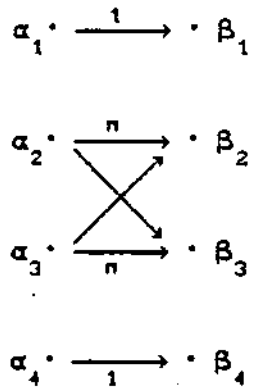
που περιγράφεται από το παρακάτω διάγραμμα διαύλου.



9. Ο παρακάτω δίαυλος πληροφορίας είναι ένας μείκτης. Στην είσοδο του προσαρμόζονται δύο επαναλήψεις της πηγής πληροφορίας $A = \{ 0, 1 \}$, $\Pi_A = \{ \pi, 1-\pi \}$ και στην έξοδο του εμφανίζεται το γινόμενο των δύο συμβόλων εισόδου. Να προσδιορισθεί το μητρώο διαύλου $\Pi(B/A)$ του μείκτη και να υπολογισθούν η χωρητικότητα, η εντροπία εισόδου και η εντροπία εξόδου. Εφαρμογή για $\pi = 0.7$.

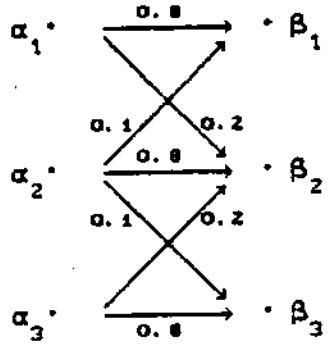


10. Δίνεται το παρακάτω διάγραμμα διαύλου. Να υπολογισθεί η χωρητικότητα $C(\pi)$ του αντίστοιχου διαύλου πληροφορίας και να σχεδιασθεί η συνάρτηση $C(\pi)$ στο διάστημα [0, 1].

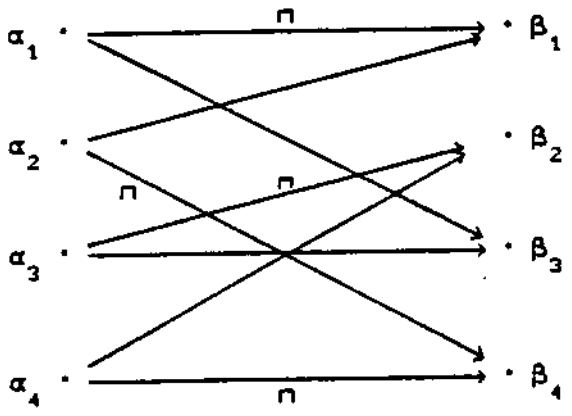


Να προσδιορισθεί η κατάλληλη καταναμή πιθανοτήτων των συμβόλων εισόδου για $\pi = 0$ ή $\pi = 0.5$ αν είναι γνωστό ότι $\pi(\alpha_1) = \pi(\alpha_4) = a$ και $\pi(\alpha_2) = \pi(\alpha_3) = b$.

11. Δίνεται το παρακάτω διάγραμμα διαύλου. Να υπολογίσθεί η χωρητικότητα του αντίστοιχου διαύλου πληροφορίας και η κατάλληλη κατανομή πιθανοτήτων των συμβόλων εισόδου. Λόγω συμμετρίας γίνεται δεκτό ότι $\pi(\alpha_1) = \pi(\alpha_2)$.



12. Το παρακάτω διάγραμμα διαύλου περιγράφει τη λειτουργία του *ορθογωνικού διαύλου πληροφορίας*. Αν τα σύμβολα εισόδου α_1, α_2, α_3, α_4 έχουν πιθανότητα π_1, π_2, π_3, π_4, αντίστοιχα, με $\pi_1 + \pi_2 + \pi_3 + \pi_4 = 1$, να υπολογισθούν οι πιθανότητες των συμβόλων εξόδου και η εντροπία συστήματος H(AB). Να προσδιορισθούν η κατανομή πιθανοτήτων για τα σύμβολα εισόδου και η πιθανότητα ορθής μετάδοσης π που εξασφαλίζουν πλήρη αξιοποίηση του διαύλου.



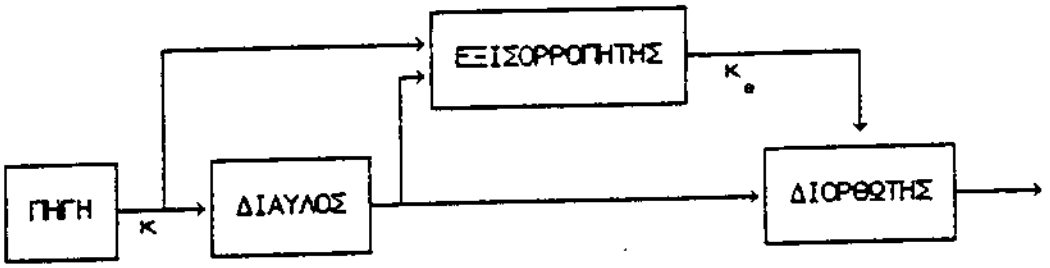
13. Ο *μ-αδικός συμμετρικός δίαυλος πληροφορίας* έχει πιθανότητες μετάδοσης :

$$\pi(\beta_i/\alpha_i) = \begin{cases} 1-\pi & \text{αν } i = j \\ \pi/(\mu-1) & \text{αν } i \neq j \end{cases}$$

όπου α_1, α_2, ... α_μ είναι τα σύμβολα εισόδου και β_1, β_2, ..., β_μ είναι τα σύμβολα εξόδου. Να σχεδιασθεί το διάγραμμα διαύλου και να σχολιασθεί η

λειτουργία του διαύλου πληροφορίας. Τι εκπροσωπεί η παράμετρος η : Να υπολογισθεί η χωρητικότητα C(η) και να σχεδιασθεί η συνάρτηση C(η) στο διάστημα [0, 1]. Να προσδιορισθεί η κατάλληλη κατανομή πιθανοτήτων των συμβόλων εισόδου.

14. Στο παρακάτω σχήμα περιγράφεται ιδανικό σύστημα επικοινωνίας που εξασφαλίζει τη διόρθωση όλων των σφαλμάτων μετάδοσης. Ο εξισορροπητής ελέγχει την είσοδο και την έξοδο του διαύλου πληροφορίας και παρέχει πληροφορία κ_e bits/sec στο διορθωτή που τη χρησιμοποιεί για να διορθώσει όλα τα σφάλματα μετάδοσης. Να υπολογισθεί η χωρητικότητα του διαύλου πληροφορίας αν είναι γνωστό ότι η διακριτή πηγή πληροφορίας στην είσοδο του χρησιμοποιεί αλφάβητο ρ συμβόλων και εκπέμπει κ σύμβολα/sec.



15. Για τη μετάδοση ψηφιακού μηνύματος μήκους Κ δυαδικών ψηφίων χρησιμοποιείται αναλογικός δίαυλος πληροφορίας με εύρος ζώνης Β. Αν S/N >> 1 είναι η σηματοθορυβική σχέση στην έξοδο του διαύλου πληροφορίας, να αποδειχθεί ότι ο ελάχιστος χρόνος για τη μετάδοση του ψηφιακού μηνύματος είναι :

$$T_{min} \simeq \frac{3K}{B(S/N)_{dB}}$$

όπου $(S/N)_{dB}$ υποδηλώνει τη σηματοθορυβική σχέση εκφρασμένη σε dB.

16. Η είσοδος διαύλου πληροφορίας περιγράφεται από διακριτή τυχαία μεταβλητή Α που παίρνει μόνο δύο ισοπίθανες τιμές, έστω ± α . Λόγω θορύβου η έξοδος του διαύλου πληροφορίας είναι συνεχής τυχαία μεταβλητή Β. Οι υπό συνθήκη κατανομές πυκνότητας πιθανότητας $\pi_{A|B}(\beta/\pm\alpha)$ είναι κανονικές με μέση τιμή ± α και τυπική απόκλιση σ . Να προσδιορισθεί η κατανομή πυκνότητας πιθανότητας $\pi_B(\beta)$ της εξόδου. Να δοθεί η έκφραση της χωρητικότητας του διαύλου σε μορφή που να μην επιδέχεται περαιτέρω απλούστευση.

17. Να αποδειχθεί ότι ισχύει (βλ. εξ:(2.47)) :

$$\iint \pi_{AB}(\alpha,\beta)\left(\frac{\alpha^2}{\sigma_A^2}+\frac{\beta^2}{\sigma_B^2}-\frac{2\alpha\beta}{\rho\sigma_A\sigma_B}\right)d\alpha d\beta = 0$$

18. Να αποδειχθεί η εξ.(2.51).

19. Τηλεπικοινωνιακός μηχανικός σχεδίασε σύστημα επικοινωνίας με χωρητικότητα διαύλου πληροφορίας 20 Mbits/sec, ισχύ σήματος στο δέκτη 1 mW και φασματική πυκνότητα ισχύος θορύβου 0.1 nW/Hz. Να ελεγχθεί η δυνατότητα υλοποίησης τέτοιου συστήματος.

20. Ο Mariner IV εκπέμπει εικόνα από τον Αρη στη Γη. Η ισχύς σήματος είναι S = 10 W, οι απώλειες μετάδοσης L = 200 dB και η φασματική πυκνότητα ισχύος του θορύβου $W = 0.5\times10^{-21}$ W/Hz. Η εικόνα αποτελείται από 200x200 στοιχεία με ένταση που μεταβάλλεται σε 64 επίπεδα. Να υπολογισθεί ο ελάχιστος χρόνος για αποστολή της εικόνας.

21. Να υπολογισθεί το απαιτούμενο εύρος ζώνης για τη μετάδοση σήματος εικόνας ασπρόμαυρης τηλεόρασης. Η σηματοθορυβική σχέση στην έξοδο του διαύλου πληροφορίας είναι τουλάχιστο 30 dB. Το μεταδιδόμενο σήμα προκύπτει με δειγματοληψία της τηλεοπτικής εικόνας σε 3×10^5 σημεία. Η τιμή του σήματος σε κάθε σημείο αντιστοιχεί σε κάποια απόχρωση του γκρίζου και θεωρείται για απλότητα ότι υπάρχουν 10 ισοπίθανες αποχρώσεις. Για την παραγωγή ζωντανής εικόνας απαιτείται ρυθμός μετάδοσης τουλάχιστο 30 εικόνων/sec. Αν η εικόνα είναι έγχρωμη, η μόνη διαφορά σε σχέση με την προηγούμενη περίπτωση είναι ότι η τιμή του σήματος σε κάθε σημείο της εικόνας αντιστοιχεί σε κάποια απόχρωση του κόκκινου, πράσινου ή γαλάζιου. Να υπολογισθεί το απαιτούμενο εύρος ζώνης συχνοτήτων για έγχρωμη εικόνα, αν θεωρηθεί ότι υπάρχουν 10 ισοπίθανες αποχρώσεις για κάθε χρώμα.

2.1 ΘΕΩΡΗΜΑ ΔΕΙΓΜΑΤΟΛΗΨΙΑΣ

Εστω δίαυλος επικοινωνίας που μεταδίδει αναλογικό σήμα με εύρος ζώνης B και διάρκεια T. Αν και δεν υπάρχει σήμα φραγμένο τόσο στο χρόνο όσο και στη συχνότητα, είναι δυνατό να θεωρηθεί σήμα με φάσμα περιορισμένο στη ζώνη [0, B] και ιστορία που εξαντλείται πρακτικά στο χρονικό διάστημα [0, T].

ΘΕΩΡΗΜΑ : Κάθε αναλογικό σήμα x(t) με εύρος ζώνης B Hz εκπροσωπείται από σειρά δειγμάτων του που λαμβάνονται με χρονικό βήμα 1/2B sec.

Η διαίσθηση υποδεικνύει ότι το αναλογικό σήμα δεν μεταβάλλεται σημαντικά σε χρονικό διάστημα συντομότερο από την ημιπερίοδο που αντιστοιχεί στη μέγιστη συχνότητα του. Επομένως δειγματοληψία με ρυθμό ταχύτερο από 2B δείγματα/sec, εξασφαλίζει ότι κάθε σημαντική πτυχή της ιστορίας του σήματος λαμβάνεται υπόψη. Στη συνέχεια περιγράφεται η μαθηματική απόδειξη του *θεωρήματος δειγματοληψίας*.

Εστω X(f) το φάσμα του σήματος x(t). Οι συναρτήσεις x(t), X(f) αποτελούν ζεύγος κατά το μετασχηματισμό *Fourier*, δηλαδή συνδέονται με τις παρακάτω ολοκληρωτικές εξισώσεις :

$$x(t) = \int_{-\infty}^{\infty} X(f)\, e^{2\pi i f t}\, df = \int_{-B}^{B} X(f)\, e^{2\pi i f t}\, df \qquad (1)$$

$$X(f) = \int_{-\infty}^{\infty} x(t)\, e^{-2\pi i f t}\, dt \simeq \int_{0}^{T} x(t)\, e^{-2\pi i f t}\, dt \qquad (2)$$

Στην εξ.(2) χρησιμοποιήθηκε και η παραδοχή $x(t) \simeq 0$ για $t \notin [0, T]$ παρόλο που αυτή δεν είναι απαραίτητη προϋπόθεση για την απόδειξη του θεωρήματος δειγματοληψίας. Αν $t = v/2B$, με v ακέραιο αριθμό, η εξ.(1) δίνει τα δείγματα του αναλογικού σήματος :

$$x_v = x(v/2B) = \int_{-B}^{B} X(f)\, e^{\pi i f v/B}\, df \qquad (3)$$

Το τελευταίο μέλος της εξ.(3) υποδεικνύει ότι τα δείγματα του αναλογικού σήματος

είναι ουσιαστικά οι συντελεστές του αναπτύγματος σε σειρά Fourier της συνάρτησης X(f) που θεωρείται περιοδική με θεμελιώδη περίοδο 2B. Αλλά το ανάπτυγμα περιοδικής συνάρτησης σε σειρά Fourier ταυτίζεται με τη συνάρτηση εφόσον διατηρούνται άπειροι όροι στο ανάπτυγμα. Επομένως η άπειρη σειρά δειγμάτων x_v που λαμβάνονται από το αναλογικό σήμα με ρυθμό 2B δείγματα/sec καθορίζουν το ανάπτυγμα Fourier της συνάρτησης X(f) που ταυτίζεται με το δύπλευρο φάσμα του αναλογικού σήματος στη ζώνη [-B, B]. Κατ' επέκταση καθορίζεται και η αρχική συνάρτηση x(t) αφού είναι καθορισμένο το φάσμα της.

Η εκπροσώπηση της συνάρτησης x(t) από τα δείγματα x_v πραγματοποιείται με το παρακάτω ανάπτυγμα :

$$x(t) = \sum_{-\infty}^{\infty} x_v \, \mathrm{sinc}(2Bt - v) \qquad (4)$$

όπου :

$$\mathrm{sinc}(\lambda) = \frac{\sin(\pi\lambda)}{\pi\lambda} \qquad (5)$$

Επειδή sinc(0) = 1 και sinc(λ) = 0 με λ ακέραιο και λ ≠ 0, η εξ.(4) καθορίζει ότι $x(v/2B) = x_v$. Επιπλέον κάθε όρος της σειράς στο δεξιό μέλος της εξ.(4) έχει μονόπλευρο φάσμα συχνοτήτων αμοιόμορφο και περιορισμένο στη ζώνη [0, B]. Επομένως η συνάρτηση x(t) έχει εύρος ζώνης B, όπως απαιτεί η διατύπωση του θεωρήματος δειγματοληψίας.

Η ισότητα μεταξύ των δύο μελών της εξ.(4) ισχύει μόνο στην περίπτωση σειράς απείρων όρων. Αν εισαχθεί η πρόσθετη παραδοχή ότι το σήμα είναι πρακτικά αμελητέο έξω από το χρονικό διάστημα [0, T], η εξ.(4) υποδεικνύει ότι το αναλογικό σήμα x(t) εκπροσωπείται από 2BT δείγματα του. Ο ελάχιστος ρυθμός δειγματοληψίας που εξασφαλίζει την ισχύ του θεωρήματος, δηλαδή 2B δείγματα/sec, είναι γνωστός σαν *ρυθμός Nyquist*.

Η ενέργεια του σήματος x(t), που είναι φραγμένο στο χρόνο και στη συχνότητα, προσδιορίζεται επίσης από τα 2BT δείγματα του :

$$E = \int_{-\infty}^{\infty} x^2(t)\, dt = (2B)^{-1} \sum_{v=1}^{2BT} x_v^2 \qquad (6)$$

Η εξ.(6) αποδεικνύεται εύκολα με εφαρμογή της παρακάτω ιδιότητας της συνάρτησης

sinc(·) :

$$\int_{-\infty}^{\infty} \text{sinc}(2Bt-\mu)\text{sinc}(2Bt-\nu)dt = \begin{cases} 0 & \mu \neq \nu \\ \mu/2B & \mu = \nu \end{cases} \quad \text{αν} \qquad (7)$$

με μ, ν ακέραιους αριθμούς. Αν τα δείγματα του αναλογικού σήματος x(t) θεωρηθούν σαν συντεταγμένες σημείου X σε χώρο 2BT διαστάσεων, τότε κάθε σήμα με εύρος ζώνης B και διάρκεια T αντιστοιχεί σε ένα σημείο του 2BT-διάστατου χώρου. Η απόσταση του σημείου X από την αρχή του συστήματος συντεταγμένων είναι $d^2 = x_1^2 + x_2^2 + \ldots + x_{2BT}^2$ και από την εξ.(6) διαπιστώνεται ότι :

$$d = (2BE)^{1/2} = (2BTS)^{1/2} \qquad (8)$$

όπου S = E/T είναι η ισχύς του σήματος. Η παρουσία θορύβου στο σύστημα επικοινωνίας έχει σαν αποτέλεσμα να λαμβάνεται στο δέκτη το σήμα x(t) + θ(t), όπου θ(t) εκπροσωπεί το θόρυβο. Ο τελευταίος είναι ανεπιθύμητο αναλογικό σήμα με εύρος ζώνης B, διάρκεια T και ισχύ N. Ενώ η είσοδος του διαύλου επικοινωνίας, δηλαδή το σήμα x(t), αντιστοιχεί σε συγκεκριμένο σημείο X του 2BT-διάστατου χώρου, η έξοδος του, σύμφωνα με την εξ.(8), αντιστοιχεί σε σημεία στο εσωτερικό σφαίρας με κέντρο το σημείο X και ακτίνα $(2BTN)^{1/2}$. Επομένως η παρουσία θορύβου στο σύστημα επικοινωνίας δημιουργεί αβεβαιότητα για τη θέση του εκπεμπόμενου σήματος στο 2BT-διάστατο χώρο.

Κεφάλαιο Τρία

ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΕ ΑΘΟΡΥΒΟ ΠΕΡΙΒΑΛΛΟΝ

3.1 ΟΡΟΛΟΓΙΑ ΚΑΙ ΤΑΞΙΝΟΜΗΣΗ ΚΩΔΙΚΩΝ

Η μεταφορά πληροφορίας πραγματοποιείται γενικά σε περιβάλλον θορύβου με αποτέλεσμα την εμφάνιση σφαλμάτων και την υποβάθμιση ή ματαίωση της επικοινωνίας. Το αντίδοτο είναι απλά η εκπομπή περισσότερης πληροφορίας από εκείνη που θα αρκούσε σε αθόρυβο περιβάλλον. Είναι φανερό ότι η πρόσθετη πληροφορία χρησιμοποιείται για την ανακάλυψη και διόρθωση σφαλμάτων. Σε κάθε μήνυμα ν συμβόλων υπάρχουν λοιπόν $\mu \leq \nu$ σύμβολα πληροφορίας και $\nu-\mu$ σύμβολα ελέγχου. Το σύστημα επικοινωνίας λειτουργεί γενικά με *περίσσεια* $\nu/\mu \geq 1$ και *ρυθμό πληροφορίας* ή *απόδοση* $\mu/\nu \leq 1$.

Με την περίσσεια εξασφαλίζεται κάποια προστασία της επικοινωνίας από σφάλματα. Είναι φανερό ότι τόσο περισσότερα σφάλματα ανακαλύπτονται και διορθώνονται όσο περισσότεροι έλεγχοι πραγματοποιούνται, δηλαδή όσο περισσότερα σύμβολα ελέγχου εμπυτεύονται στο μήνυμα. Η ασφάλεια της επικοινωνίας καθορίζεται λοιπόν από την περίσσεια και το αντιστάθμισμα για περισσότερη ασφάλεια είναι η απαίτηση μετάδοσης μακρύτερων μηνυμάτων. Από την άλλη πλευρά αύξηση της απόδοσης, δηλαδή του ρυθμού μετάδοσης της χρήσιμης πληροφορίας, είναι δυνατή μόνο με ελάττωση του πλήθους των συμβόλων ελέγχου με προφανές επακόλουθο να περνούν απαρατήρητα περισσότερα σφάλματα. Επομένως η σχεδίαση του συστήματος επικοινωνίας εμπλέκει

εκτός των άλλων και κάποιο συμβιβασμό μεταξύ απόδοσης και περίσσειας. Με την κωδικοποίηση επιδιώκεται να βελτιστοποιηθεί το σύστημα επικοινωνίας σε περιβάλλον θορύβου, δηλαδή ουσιαστικά να βρεθεί ο βέλτιστος συμβιβασμός μεταξύ απόδοσης και ασφάλειας.

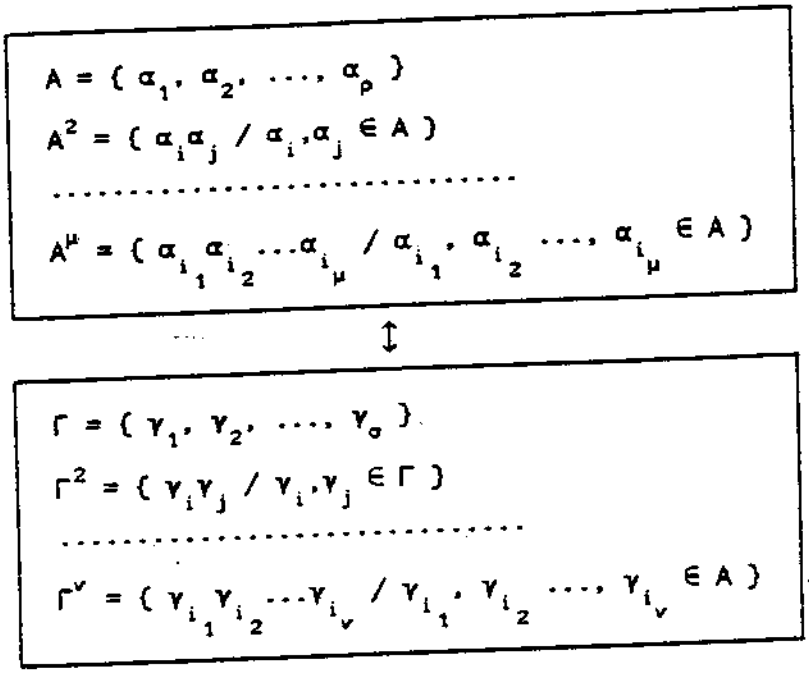
Δύο ακόμη παράγοντες που πρέπει να συνεκτιμώνται κατά τη σχεδίαση του συστήματος επικοινωνίας είναι η αξιοπιστία και το κόστος. Σε ορισμένες εφαρμογές η αξιοπιστία αποκτά απόλυτη προτεραιότητα αφού η αλλοίωση ενός μόνο συμβόλου μπορεί να επιφέρει δραματικά αποτελέσματα (π.χ. ανταλλαγή μηνυμάτων μεταξύ χειριστών πυρηνικών όπλων). Ορισμένο πλήθος σφαλμάτων γίνεται συνήθως ανεκτό σε απλούστερες εφαρμογές στις οποίες το χαμηλό κόστος λειτουργίας είναι ο σημαντικότερος παράγοντας. Η κωδικοποίηση είναι ουσιαστικά μιά έξυπνη τεχνική για να συμβιβαστούν οι απαιτήσεις απόδοσης, ασφάλειας, αξιοπιστίας και κόστους σε πραγματικά συστήματα επικοινωνίας.

ΟΡΙΣΜΟΣ : *Κώδικας* είναι κάθε απεικόνιση συμβόλων ή/και λέξεων από το αλφάβητο της πηγής πληροφορίας σε σύμβολα ή/και λέξεις από εναλλακτικό σύνολο συμβόλων, που ονομάζεται αντίστοιχα *κωδικό αλφάβητο*.

Αν $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_p \}$ είναι το αλφάβητο πηγής πληροφορίας A,Π_A και $\Gamma = \{ \gamma_1, \gamma_2, \ldots, \gamma_\sigma \}$ είναι το κωδικό αλφάβητο, τότε η κωδικοποίηση είναι απλά η αντιστοίχιση στοιχείων των συνόλων $A, A^2, \ldots, A^\mu$ με στοιχεία των συνόλων $\Gamma, \Gamma^2, \ldots, \Gamma^\nu$, όπου μ, ν ακέραιοι αριθμοί (σχ. 3.1).

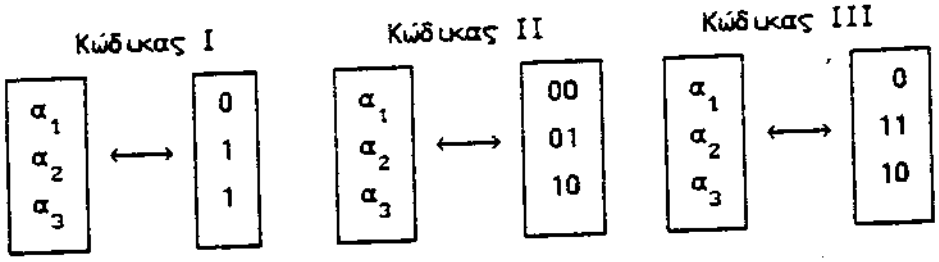
Το *κρυπτόγραμμα αντικατάστασης* προκύπτει στην απλή περίπτωση $A = \Gamma$. Τα κωδικά σύμβολα είναι τότε ίδια με τα σύμβολα πληροφορίας και το κλειδί του κώδικα είναι η απεικόνιση $A \leftrightarrow A$. Αν η πηγή πληροφορίας είναι η Αγγλική γλώσσα, που έχει 26 γράμματα, υπάρχουν $26! = 4.03 \cdot 10^{26}$ διαφορετικοί τρόποι για να κατασκευασθούν κρυπτογράμματα αντικατάστασης και για την αποκρυπτογράφηση απαιτείται ποσότητα πληροφορίας $\log_2(26!) = 88.4$ bits αφού όλα τα κλειδιά είναι ισοπίθανα για τον αποκρυπτογράφο. Είναι φανερό ότι κάθε κρυπτόγραμμα αντικατάστασης φέρει ποσότητα πληροφορίας ίση με το άθροισμα της ποσότητας πληροφορίας που φέρει το αντίστοιχο μήνυμα πληροφορίας και της ποσότητας πληροφορίας που αντιστοιχεί στην επιλογή κάποιου από τα 26! διαθέσιμα κλειδιά. Αν το μήνυμα πληροφορίας έχει μήκος ν γράμματα, η ποσότητα πληροφορίας του είναι 4.08ν bits αφού η εντροπία της Αγγλικής γλώσσας είναι 4.08 bits/σύμβολο (βλ. πίνακα 1.1). Είναι φανερό λοιπόν ότι το αντίστοιχο κρυπτόγραμμα αντικατάστασης φέρει πληροφορία (4.08ν + 88.4)

bits και πρέπει $4.08v + 88.4 \leq v\log_2(27)$ αφού χρησιμοποιείται και το κενό σαν σύμβολο πληροφορίας. Η παραπάνω ταυτοανισότητα υποδεικνύει ότι αν το κρυπτόγραμμα αντικατάστασης έχει μήκος $v \geq 131$ γράμματα, ο αποκρυπτογράφος διαθέτει αρκετή πληροφορία για να αναγνωρίσει το κλειδί του κώδικα.



Σχ. 3.1 *Η κωδικοποίηση είναι απεικόνιση του συνόλου* $A \cup A^2 \cup \ldots \cup A^\mu$ *στο σύνολο* $\Gamma \cup \Gamma^2 \cup \ldots \cup \Gamma^\nu$.

Αν $\Gamma = \{ 0, 1 \}$, τα σύμβολα/λέξεις πληροφορίας αντιστοιχίζονται σε διατάξεις δυαδικών ψηφίων. Η δυαδική κωδικοποίηση είναι η συνηθέστερη επιλογή των ψηφιακών συστημάτων επικοινωνίας.



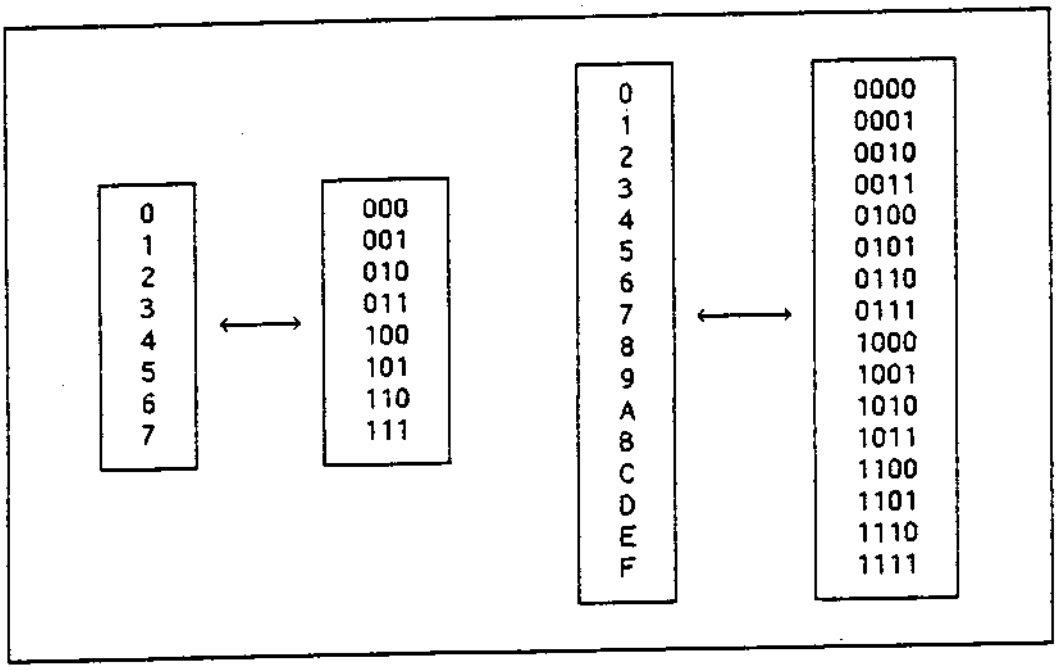
ΠΑΡΑΔΕΙΓΜΑ : Για την πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$ διατίθενται οι παραπάνω τρεις δυαδικοί κώδικες. Το κωδικό αλφάβητο είναι $\Gamma = \{ 0, 1 \}$. Ο κώδικας I αποτελεί απεικόνιση του συνόλου A στο σύνολο Γ ενώ ο κώδικας II απεικονίζει το σύνολο A στο σύνολο $\Gamma^2 = \{ 00, 01, 10, 11 \}$. Οι κωδικές λέξεις

είναι ισομήκεις, δηλαδή περιέχουν το ίδιο πλήθος δυαδικών ψηφίων, σε καθένα από τους κώδικες I, II. Στον κώδικα III χρησιμοποιούνται μερικά στοιχεία από την ένωση $\Gamma \cup \Gamma^2$ των συνόλων Γ, Γ^2 και οι κωδικές λέξεις δεν είναι ισομήκεις.

Το δυαδικό αλφάβητο είναι ιδιαίτερα χρήσιμο στην ψηφιακή μετάδοση πληροφορίας επειδή προσομοιώνεται εύκολα στα μοντέρνα τηλεπικοινωνιακά συστήματα. Ο ανθρώπινος εγκέφαλος σε αντίθεση με τα συστήματα τεχνητής νοημοσύνης προτιμά να χειρίζεται πολυπληθέστερα σύνολα συμβόλων. Οι γνωστότερες γλώσσες διαθέτουν αλφάβητο από 16 μέχρι 36 γράμματα. Επιπλέον το σύστημα αρίθμησης που χρησιμοποιείται σε καθημερινούς υπολογισμούς διαθέτει 10 αριθμούς. Για υπολογισμούς με ηλεκτρονικό υπολογιστή χρησιμοποιείται το δυαδικό σύστημα ή οι επεκτάσεις του σε οκταδικό και δεκαεξαδικό σύστημα (βλ. πίνακα 3.1).

Πίνακας 3.1

Δυαδικοί κώδικες για οκταδικό και δεκαεξαδικό σύστημα αρίθμησης



Η έβδομη επέκταση του δυαδικού αλφαβήτου προσφέρει τη δυνατότητα χρήσης $2^7 = 128$ διαφορετικών συμβόλων με κοινό παράδειγμα τον κώδικα ASCII 7-bits (βλ. πίνακα 3.2). Στις λέξεις του κώδικα ASCII 7-bits προστίθεται συνήθως και όγδοο δυαδικό ψηφίο ώστε το συνολικό πλήθος μονάδων στη λέξη να είναι άρτιο (ή περιττό). Με τον τρόπο αυτό γίνεται δυνατή η ανακάλυψη απλών σφαλμάτων αφού με την αλλοίωση κάποιου 0 σε 1 ή 1 σε 0 το πλήθος των μοναδων γίνεται περιττό (ή άρτιο).

Επομένως ο κώδικας ASCII 8-bits επιτρέπει κάποιο στοιχειώδη έλεγχο της ορθότητας των μεταδιδόμενων μηνυμάτων.

Ο περισσότερο γνωστός κώδικας με μη ισομήκεις λέξεις είναι ο κώδικας Morse (βλ. πίνακα 3.3), που αντιστοιχίζει γράμματα με μεγάλη πιθανότητα σε βραχείες κωδικές λέξεις και γράμματα με μικρή πιθανότητα σε μακρές κωδικές λέξεις. Αυτό γίνεται για να μειωθεί το μέσο μήκος των κωδικών λέξεων και επομένως να βελτιωθεί ο ρυθμός μετάδοσης και η απόδοση του συστήματος επικοινωνίας.

Πίνακας 3.2

Κώδικας ASCII 7-bits

Κωδική Λέξη	Σύμβολο	Κωδική Λέξη	Σύμβολο	Κωδική Λέξη	Σύμβολο	Κωδική Λέξη	Σύμβολο
000	NUL	040	SP	100	@	140	`
001	SOH	041	!	101	A	141	a
002	STX	042	"	102	B	142	b
003	ETX	043	#	103	C	143	c
004	EOT	044	$	104	D	144	d
005	ENQ	045	%	105	E	145	e
006	ACK	046	&	106	F	146	f
007	BEL	047	'	107	G	147	g
010	BS	050	(	110	H	150	h
011	HT	051	)	111	I	151	i
012	LF	052	*	112	J	152	j
013	VT	053	+	113	K	153	k
014	FF	054	,	114	L	154	l
015	CR	055	-	115	M	155	m
016	SO	056	.	116	N	156	n
017	SI	057	/	117	O	157	o
020	DLE	060	0	120	P	160	p
021	DC1	061	1	121	Q	161	q
022	DC2	062	2	122	R	162	r
023	DC3	063	3	123	S	163	s
024	DC4	064	4	124	T	164	t
025	NAK	065	5	125	U	165	u
026	SYN	066	6	126	V	166	v
027	ETB	067	7	127	W	167	w
030	CAN	070	8	130	X	170	x
031	EM	071	9	131	Y	171	y
032	SUB	072	:	132	Z	172	z
033	ESC	073	;	133	[	173	{
034	FS	074	<	134	\	174	|
035	GS	075	=	135	]	175	}
036	RS	076	>	136	^	176	~
037	US	077	?	137	_	177	DEL

Πίνακας 3.3

Κώδικας Morse

A	· −	J	· − − −	S	· · ·
B	− · · ·	K	− · −	T	−
C	− · − ·	L	· − · ·	U	· · −
D	− · ·	M	− −	V	· · · −
E	·	N	− ·	W	· − −
F	· · − ·	O	− − −	X	− · · −
G	− − ·	P	· − − ·	Y	− · − −
H	· · · ·	Q	− − · −	Z	− − · ·
I	· ·	R	· − ·		

Κάθε κώδικας πρέπει να εξασφαλίζει ευχερή αποκωδικοποίηση, δηλαδή ανάκτηση του μηνύματος πληροφορίας από το κωδικό μήνυμα. Οι τεχνικές κωδικοποίησης διακρίνονται γενικά σε δύο κατηγορίες, που περιγράφονται με τους παρακάτω ορισμούς.

ΟΡΙΣΜΟΣ : *Δομική κωδικοποίηση* είναι η αντιστοίχιση κάθε συμβόλου ή λέξης πληροφορίας σε προκαθορισμένη και σταθερή κωδική λέξη.

Οι *δομικοί κώδικες* είναι κώδικες με σταθερό κλειδί και συνήθως χρησιμοποιούν ισομήκεις λέξεις με συνέπεια να αναγνωρίζεται εύκολα η δομή των μηνυμάτων. Σχεδιάζονται με κριτήρια και αρχές που στηρίζονται στην άλγεβρα των πεπερασμένων πεδίων. Στην κατηγορία αυτή ανήκουν οι *κώδικες ομάδας* (βλ. §5.2) και οι *κυκλικοί κώδικες* (βλ. §§ 5.3, 5.4).

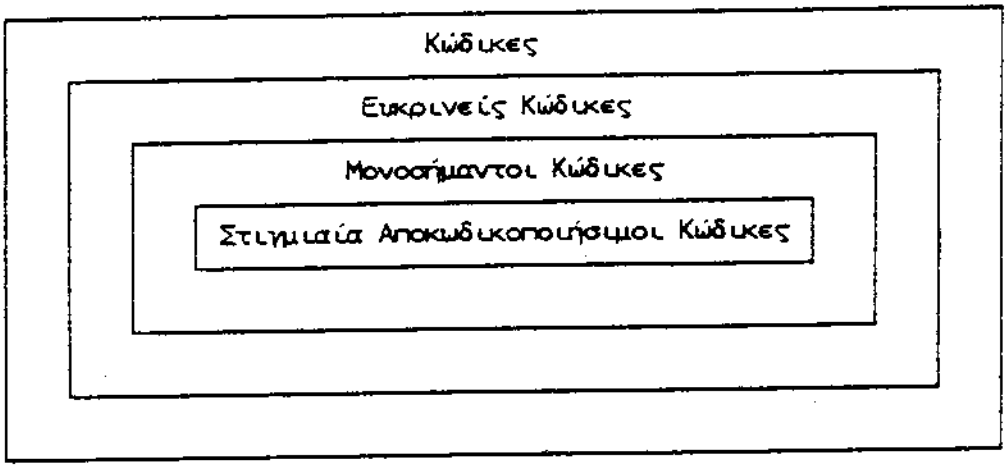
Στην §3.4 η κατηγορία των δομικών κωδίκων περιορίζεται στους κώδικες με ισομήκεις λέξεις. Οι *διαφορικοί κώδικες*, που ορίζονται εκεί, δεν χρησιμοποιούν ισομήκεις λέξεις αλλά σύμφωνα με τον παραπάνω ορισμό ανήκουν επίσης στους δομικούς κώδικες εφόσον έχουν σταθερό κλειδί.

ΟΡΙΣΜΟΣ : *Συνελικτική κωδικοποίηση* είναι η αντιστοίχιση συμβόλων ή λέξεων πληροφορίας σε μεταβλητές κωδικές λέξεις.

Ο κωδικοποιητής προετοιμάζει κωδικά σύμβολα ελέγχου και τα προσαρτά στα κωδικά σύμβολα που καθορίζει το κλειδί για κάθε σύμβολο πληροφορίας. Εφόσον τα ψηφία ελέγχου έχουν καθοριστεί λαμβάνοντας υπόψη το προηγούμενο τμήμα του μηνύματος πληροφορίας, η κωδική λέξη που προκύπτει εξαρτάται από τη θέση του συγκεκριμένου

συμβόλου στο μήνυμα πληροφορίας. Οι *συνελικτικοί κώδικες* (βλ. §5.5) δεν διαθέτουν σαφές θεωρητικό υπόβαθρο αλλά υλοποιούνται εύκολα και χρησιμοποιούνται εξίσου με τους δομικούς κώδικες.

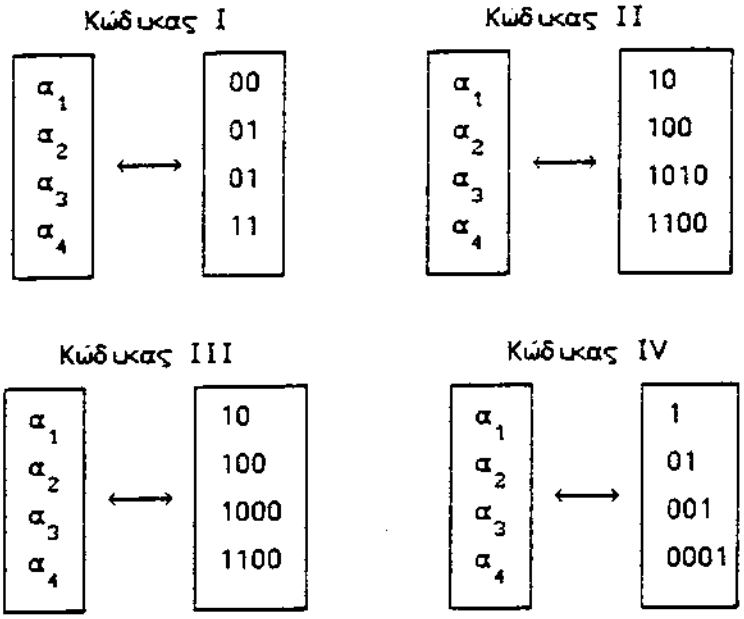
Με κριτήριο την ευχέρεια ή και τη δυνατότητα αποκωδικοποίησης οι κώδικες ταξινομούνται στις παρακάτω κατηγορίες.



ΟΡΙΣΜΟΣ : *Εικρινής κώδικας* είναι εκείνος που χρησιμοποιεί διαφορετική κωδική λέξη για κάθε σύμβολο ή λέξη πληροφορίας. Η εικρίνεια του κώδικα είναι η πρώτη προϋπόθεση γιά να υπάρχει δυνατότητα αποκωδικοποίησης.

ΟΡΙΣΜΟΣ : Ενας 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 καμμία κωδική λέξη να μην είναι πρόθεμα άλλης κωδικής λέξης.

ΠΑΡΑΔΕΙΓΜΑ : Για την πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \alpha_3 \alpha_4 \}$ διατίθενται οι παρακάτω δυαδικοί κώδικες. Ο κώδικας I δεν είναι εικρινής επειδή αντιστοιχίζει τα σύμβολα πληροφορίας α_2 και α_3 στην κωδική λέξη 01. Το μήνυμα πληροφορίας $\alpha_1\alpha_3\alpha_4\alpha_2\alpha_1$ μετατρέπεται κατά την κωδικοποίηση στο κωδικό μήνυμα 0001110100 αλλά κατά την αποκωδικοποίηση διαμορφώνονται τα μηνύματα πληροφορίας $\alpha_1\alpha_2\alpha_4\alpha_2\alpha_1$, $\alpha_1\alpha_3\alpha_4\alpha_2\alpha_1$, $\alpha_1\alpha_2\alpha_4\alpha_3\alpha_1$, $\alpha_1\alpha_3\alpha_4\alpha_3\alpha_1$. Οι κώδικες II, III, IV είναι εικρινείς επειδή οι κωδικές λέξεις που αντιστοιχούν στα σύμβολα πληροφορίας είναι διαφορετικές.



Ο κώδικας II δεν είναι μονοσήμαντος και αυτό διαπιστωνεται με το παράδειγμα που ακολουθεί. Τα μηνύματα πληροφορίας $\alpha_1\alpha_3\alpha_4\alpha_2\alpha_1$, $\alpha_3\alpha_1\alpha_4\alpha_2\alpha_1$ αντιστοιχούν στο κωδικό μήνυμα 101010110010010 . Είναι φανερό ότι δεν υπάρχει μονοσήμαντη αντιστοιχία μεταξύ μηνυμάτων πληροφορίας και κωδικών μηνυμάτων επειδή η κωδική λέξη 10 είναι πρόθεμα της κωδικής λέξης 1010 .

Η αποκωδικοποίηση μηνυμάτων που κατασκευάζονται με μονοσήμαντο κώδικα είναι γενικά δυνατή μετά την ολοκλήρωση του κωδικού μηνύματος. Συνήθως όμως είναι απαραίτητο να αποκωδικοποιείται το μήνυμα λέξη προς λέξη καθώς φθάνει στο δέκτη του συστήματος επικοινωνίας. Η ιδιότητα αυτή δεν χαρακτηρίζει ολους τους μονοσήμαντους κώδικες. Εστω το μήνυμα πληροφορίας $\alpha_2\alpha_1\alpha_3$ που με τον κώδικα III του παραδείγματος μετατρέπεται στο κωδικό μήνυμα 100101000 . Κατά την αποκωδικοποίηση είναι απαραίτητο να φθάσει το τέταρτο δυαδικό ψηφίο προκειμένου να γίνει αντιληπτό ότι συμπληρώθηκε η πρώτη κωδική λέξη. Παρόλο που η πρώτη κωδική λέξη ολοκληρώνεται με το τρίτο δυαδικό ψηφίο πρέπει να φθάσει και το τέταρτο δυαδικό ψηφίο ώστε να γίνει αντιληπτό ότι είχε τελειωσει η πρώτη κωδική λέξη. Είναι φανερό ότι πρόκειται για ανεπιθύμητη αδυναμια του κώδικα που υποβαθμίζει την επικοινωνία και επιδιώκεται γενικά η εξάλειψη της.

ΟΡΙΣΜΟΣ : *Στιγμιαία αποκωδικοποιήσιμος κώδικας* είναι κάθε μονοσήμαντος κωδικας που επιτρέπει αποκωδικοποίηση των μηνυμάτων λέξη προς λέξη χωρίς να απαιτείται εξέταση επόμενων κωδικών συμβόλων.

Ο κώδικας IV του παραδείγματος είναι στιγμιαία αποκωδικοποίησιμος αφού το τέλος κάθε κωδικής λέξης σημειώνεται με τη λήψη 1, που είναι γιά όλες τις κωδικές λέξεις το τελευταίο δυαδικό ψηφίο.

Ταχύτητα επικοινωνίας δεν εξασφαλίζεται μόνο με στιγμιαία αποκωδικοποίηση αλλά και με χρήση σύντομων κωδικών μηνυμάτων. Αν ο κώδικας αντιστοιχίζει στα σύμβολα πληροφορίας $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ τις κωδικές λέξεις $\zeta_1, \zeta_2, \ldots, \zeta_\rho$, που περιέχουν $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ σύμβολα του κωδικού αλφαβήτου, αντίστοιχα, τότε το μέσο μήκος κωδικών λέξεων ορίζεται με την έκφραση

$$\Lambda = \sum_{i=1}^{\rho} \lambda_i \pi_i \qquad (3.1)$$

όπου π_i είναι η πιθανότητα του συμβόλου πληροφορίας α_i, $i = 1, 2, \ldots, \rho$. Εύκολα διαπιστώνεται ότι το μέσο μήκος των κωδικών λέξεων ελαχιστοποιείται με την απλή τεχνική να αντιστοιχίζονται τα πιθανότερα σύμβολα πληροφορίας στις βραχύτερες κωδικές λέξεις. Επομένως, πρέπει $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_\rho$ αν $\pi_1 \geq \pi_2 \geq \ldots \geq \pi_\rho$.

ΟΡΙΣΜΟΣ : *Βέλτιστος κώδικας* είναι ο στιγμιαία αποκωδικοποίησιμος κώδικας με το ελάχιστο μέσο μήκος κωδικών λέξεων.

Ο ρυθμός μετάδοσης είναι το σημαντικώτερο κριτήριο γιά τη σχεδίαση του συστήματος επικοινωνίας σε αθόρυβο περιβάλλον. Επιδίωξη της κωδικοποίησης σε τέτοιο περιβάλλον πρέπει να είναι ο καθορισμός του βέλτιστου κώδικα.

3.2 ΘΕΩΡΗΜΑ KRAFT

ΘΕΩΡΗΜΑ : Εστω πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$, $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$ και κώδικας με αλφάβητο $\Gamma = \{ \gamma_1, \gamma_2, \ldots, \gamma_\sigma \}$, που διαμορφώνει κωδικές λέξεις μήκους $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ κωδικών συμβόλων, αντίστοιχα. Ικανή και αναγκαία συνθήκη γιά να υπάρχει στιγμιαία αποκωδικοποίησιμος κώδικας με τα συγκεκριμένα μήκη κωδικών λέξεων είναι να ισχύει η ταυτοανισότητα :

$$\sum_{i=1}^{\rho} \sigma^{-\lambda_i} \leq 1 \qquad (3.2)$$

Είναι απαραίτητο να τονισθεί ότι το θεώρημα Kraft εξασφαλίζει απλά την ύπαρξη στιγμιαία αποκωδικοποιήσιμου κώδικα με κωδικές λέξεις μήκους $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ που ικανοποιούν την εξ.(3.2) αλλά δεν υποδεικνύει οποιαδήποτε τεχνική για τον προσδιορισμό των κωδικών λέξεων και δεν υπονοεί ότι κάθε κώδικας με τα κατάλληλα μήκη κωδικών λέξεων είναι οπωσδήποτε στιγμιαία αποκωδικοποιήσιμος.

ΠΑΡΑΔΕΙΓΜΑ : Για την πηγή πληροφορίας $A = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ διατίθενται οι παρακάτω δυαδικοί κώδικες.

	Κώδικας I		Κώδικας II		Κώδικας III
α_1	⟷ 00	α_1	⟷ 0	α_1	⟷ 0
α_2	⟷ 10	α_2	⟷ 100	α_2	⟷ 10
α_3	⟷ 10	α_3	⟷ 110	α_3	⟷ 110
α_4	⟷ 11	α_4	⟷ 111	α_4	⟷ 11

Το αριστερό μέλος της εξ.(3.2) με $\sigma = 2$ είναι :

Κώδικας I : $4(1/4) = 1$

Κώδικας II : $1/2 + 3(1/8) = 7/8 < 1$

Κώδικας III : $1/2 + 2(1/4) + 1/8 = 9/8 > 1$

και επομένως οι κώδικες I και II ενδέχεται να είναι στιγμιαία αποκωδικοποιήσιμοι. Αντίθετα ο κώδικας III αποκλείεται να είναι στιγμιαία αποκωδικοποιήσιμος αφού δεν ικανοποιείται η εξ.(3.2). Αυτο επιβεβαιώνεται και με την παρατήρηση ότι ο κώδικας III δεν διαθέτει την προθεματική ιδιότητα. Επομένως δεν είναι ούτε μονοσήμαντος. Αλλά και ο κώδικας I ζεν είναι στιγμιαία αποκωδικοποιήσιμος παρόλο που ικανοποιεί την εξ.(3.2), αφού δεν είναι καν ευκρινής.

Η ταυτοανισότητα Kraft εξασφαλιζει την ύπαρξη στιγμιαία αποκωδικοποιήσιμου

κώδικα. Αλλά κάθε στιγμιαία αποκωδικοποιήσιμος κώδικας είναι και μονοσήμαντος. Αποδεικνύεται ότι η ταυτοανισότητα Kraft είναι ταυτόχρονα ικανή και αναγκαία συνθήκη γιά την ύπαρξη μονοσήμαντου κώδικα με δεδομένα μήκη κωδικών λέξεων.

3.3 ΠΡΩΤΟ ΘΕΩΡΗΜΑ SHANNON

Το θεώρημα Kraft αναφέρεται ουσιαστικά στα μήκη κωδικών λέξεων και όχι στις ίδιες τις κωδικές λέξεις. Είναι φανερό ότι χρειάζεται κάποιο κριτήριο γιά την αναγνώριση του βέλτιστου κώδικα μέσα από το πλήθος των στιγμιαία αποκωδικοποιήσιμων κωδίκων που ικανοποιούν την απαίτηση του θεωρήματος Kraft.

Γιά την πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$, $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$ που κωδικοποιείται με σύμβολα από το αλφάβητο $\Gamma = \{ \gamma_1, \gamma_2, \ldots, \gamma_\sigma \}$ σε λέξεις με μήκη $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ εισάγεται η εναλλακτική κατανομή πιθανοτήτων $T_A = \{ \tau_1, \tau_2, \ldots, \tau_\rho \}$, όπου :

$$0 \leq \tau_i = \frac{\sigma^{-\lambda_i}}{\sum_{i=1}^{\rho} \sigma^{-\lambda_i}} \leq 1 \qquad (3.3)$$

Είναι προφανές ότι $\tau_1 + \tau_2 + \ldots + \tau_\rho = 1$ όπως απαιτείται γιά κάθε κατανομή πιθανοτήτων. Εφαρμόζοντας την ταυτοανισότητα της εξ.(1.4) προκύπτει :

$$H(A) = -\sum_{i=1}^{\rho} \pi_i \log_e(\pi_i) \leq -\sum_{i=1}^{\rho} \pi_i \log_e(\tau_i) = -\sum_{i=1}^{\rho} \pi_i \log_e\left(\frac{\sigma^{-\lambda_i}}{\sum_{i=1}^{\rho} \sigma^{-\lambda_i}} \right) =$$

$$= \left(\log_e \sigma\right) \sum_{i=1}^{\rho} \pi_i \lambda_i + \left(\sum_{i=1}^{\rho} \pi_i \right) \log_e\left(\sum_{i=1}^{\rho} \sigma^{-\lambda_i} \right) \qquad (3.4)$$

Αλλά $\pi_1\lambda_1 + \pi_2\lambda_2 + \ldots + \pi_\rho\lambda_\rho = \Lambda$, $\pi_1 + \pi_2 + \ldots + \pi_\rho = 1$ και η εξ.(3.4) απλοποιείται στην παρακάτω :

$$H(A) \leq \Lambda \log_c \sigma + \log_c \left(\sum_{i=1}^{\rho} \sigma^{-\lambda_i} \right) \qquad (3.5)$$

Εφόσον ισχύει η ταυτοανισότητα Kraft, $\sigma^{-\lambda_1} + \sigma^{-\lambda_2} + \ldots + \sigma^{-\lambda_\rho} \leq 1$ και επομένως ο δεύτερος όρος στο δεξιό μέλος της εξ.(3.5) είναι αρνητικός. Αν παραλειφθεί, η ανισότητα ενισχύεται στην παρακάτω :

$$H(A) \leq \Lambda \log_c \sigma \qquad (3.6)$$

που γράφεται με την ισοδύναμη μορφή :

$$\Lambda \geq \frac{H(A)}{\log_c \sigma} \qquad (3.7)$$

Η εξ.(3.7) καθορίζει το κάτω φράγμα για το μεσο μήκος των κωδικών λέξεων με μήκη $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ που ικανοποιούν το θεώρημα Kraft. Κατά συνέπεια ο βέλτιστος κώδικας αναγνωρίζεται με κριτηριο την απόσταση του μέσου μήκους των κωδικών λέξεων από το κάτω φράγμα του.

Η ισότητα στην εξ.(3.7) ισχύει μονο στην ειδική περιπτωση $\sigma^{-\lambda_1} + \sigma^{-\lambda_2} + \ldots + \sigma^{-\lambda_\rho} = 1$ και $n_i = \tau_i = \sigma^{-\lambda_i}$, $i = 1, 2, \ldots, \rho$. Τα αντίστοιχα μήκη κωδικών λέξεων είναι :

$$\lambda_i = -\log_\sigma(n_i) \qquad (3.8)$$

και γίνονται αποδεκτά εφόσον είναι ακέραιοι αριθμοί. Γενικά η εξ.(3.8) οδηγεί σε πραγματικούς αριθμούς και για το λόγο αυτό το μέσο μήκος των κωδικών λέξεων είναι μεγαλύτερο απο το κατω φράγμα του ακόμη και στην περίπτωση του βέλτιστου κώδικα. Επιλέγονται λοιπόν σαν μήκη των κωδικών λέξεων οι ακέραιοι αριθμοί λ_i που είναι μεγαλύτεροι αλλά πλησιέστεροι προς την πραγματική ποσότητα $-\log_\sigma(n_i)$, δηλαδή :

$$-\log_\sigma(n_i) \leq \lambda_i \leq -\log_\sigma(n_i) + 1 \qquad (3.9)$$

Από την εξ.(3.9) διαμορφώνεται η διπλή ταυτοανισότητα :

$$-\sum_{i=1}^{\rho} n_i \log_\sigma(n_i) \leq \sum_{i=1}^{\rho} n_i \lambda_i \leq -\sum_{i=1}^{\rho} n_i \log_\sigma(n_i) + \sum_{i=1}^{\rho} n_i \qquad (3.10)$$

που καταλήγει στην παρακάτω :

$$\frac{H(A)}{\log_e \sigma} \leq \Lambda \leq \frac{H(A)}{\log_e \sigma} + 1 \qquad (3.11)$$

Η εξ.(3.11) είναι προέκταση της εξ.(3.7).

Αν αντί της πηγής πληροφορίας A,Π_A κωδικοποιείται η ν-οστή επέκταση της A^ν,Π_A^ν, η εξ.(3.11) γράφεται :

$$\frac{H(A)}{\log_e \sigma} \leq \frac{\Lambda_\nu}{\nu} \leq \frac{H(A)}{\log_e \sigma} + \frac{1}{\nu} \qquad (3.12)$$

και στο όριο $\nu \to \infty$:

$$\Lambda_\nu \to \frac{H(A^\nu)}{\log_e \sigma} \qquad (3.13)$$

Οι εξ.(3.7),(3.13) περιγράφουν το πρώτο θεώρημα Shannon, που είναι επίσης γνωστό σαν *θεώρημα κωδικοποίησης σε περιβάλλον χωρίς θόρυβο*. Είναι απαραίτητο να υπενθυμισθεί ότι μέχρι το σημείο αυτό έχει αγνοηθεί η ύπαρξη θορύβου στο σύστημα επικοινωνίας και αναζητήθηκε απλά η βελτιστοποίηση του κώδικα της πηγής πληροφορίας.

ΘΕΩΡΗΜΑ : Έστω πηγή πληροφορίας με αλφάβητο ρ συμβόλων και κώδικας με αλφάβητο σ συμβόλων. Το μέσο μήκος των κωδικών λέξεων προσεγγίζει όσο είναι επιθυμητό στο κάτω φράγμα του κωδικοποιώντας ανώτερες επεκτάσεις της πηγής πληροφορίας. Το αντίτιμο για τέτοια βελτιστοποίηση του κώδικα είναι η δυσκολία κωδικοποίησης και η αύξηση του χρόνου που απαιτείται για την κωδικοποίηση, μετάδοση και αποκωδικοποίηση του μηνύματος πληροφορίας.

Το πρώτο θεώρημα Shannon διατυπώνει ουσιαστικά τη θεωρητική δυνατότητα σχεδίασης

κώδικα με μέσο μήκος λέξεων ίσο με το κάτω φράγμα του. Αλλά το αντίτιμο σε δυσκολία, κόστος και χρόνο περιορίζει τη χρησιμότητα του βελτιστοποιημένου κώδικα.

3.4 ΑΠΛΟΙ ΚΩΔΙΚΕΣ

Με κριτήριο το πλήθος συμβόλων ανά λέξη διακρίνονται *δομικοί* και *διαφορικοί* κώδικες. Οι δομικοί κώδικες χρησιμοποιούν ισομήκεις λέξεις (π.χ. κώδικας ASCII) με προφανή συνέπεια να είναι απλή υπόθεση η διάσπαση μακρών μηνυμάτων σε λέξεις και στη συνέχεια η αποκωδικοποίηση. Οι διαφορικοί κώδικες (π.χ. κώδικας Morse) αντιστοιχίζουν μακρές κωδικές λέξεις σε σύμβολα πληροφορίας με μικρή πιθανότητα και βραχείες κωδικές λέξεις σε σύμβολα πληροφορίας με μεγάλη πιθανότητα. Είναι φανερό ότι με την τεχνική αυτή γίνεται οικονομία κωδικών συμβόλων με συνέπεια να βελτιώνεται η απόδοση του κώδικα.

Οι διαφορικοί κώδικες υπερτερούν σε απόδοση των δομικών κωδίκων όταν τα σύμβολα πληροφορίας έχουν σημαντικά διαφορετικές πιθανότητες. Το πρόβλημα με τους διαφορικούς κώδικες εντοπίζεται στην αναγνώριση του πέρατος κάθε λέξης σε μακρά μηνύματα, δηλαδή στη δυνατότητα στιγμιαίας αποκωδικοποίησης. Αν τα σύμβολα πληροφορίας είναι ισοπίθανα οι διαφορικοί κώδικες εκφυλίζονται σε δομικούς κώδικες.

Στη συνέχεια περιγράφονται μερικοί απλοί διαφορικοί κώδικες. Αν και είναι μάλλον ξεπερασμένοι, η παρουσίαση τους έχει κυρίως εκπαιδευτική αλλά και ιστορική σκοπιμότητα.

3.4.1 ΚΩΔΙΚΑΣ SHANNON

Ο δυαδικός κώδικας Shannon διαμορφώνεται σε τέσσερα βήματα :

(α) Τα σύμβολα πληροφορίας $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ διατάσσονται κατά ελαττούμενη

πιθανότητα :

$$\begin{array}{ccccccc} \alpha_1 & & \alpha_2 & & \cdots & & \alpha_\rho \\ \updownarrow & & \updownarrow & & & & \updownarrow \\ \pi_1 & \geq & \pi_2 & \geq & \cdots & \geq & \pi_\rho \end{array}$$

(β) Σε κάθε σύμβολο πληροφορίας α_i αντιστοιχίζεται αριθμός ϵ_i κατά το παρακάτω σχήμα :

$$\alpha_1 \longleftrightarrow \epsilon_1 = 0$$

$$\alpha_2 \longleftrightarrow \epsilon_2 = \pi_1 + \epsilon_1 = \pi_1$$

$$\alpha_3 \longleftrightarrow \epsilon_3 = \pi_2 + \epsilon_2 = \pi_1 + \pi_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\alpha_\rho \longleftrightarrow \epsilon_\rho = \pi_{\rho-1} + \epsilon_{\rho-1} = \pi_1 + \pi_2 + \cdots \pi_{\rho-1}$$

(γ) Το μήκος λ_i της κωδικής λέξης που αντιστοιχεί στο σύμβολο πληροφορίας α_i είναι ο ελάχιστος ακέραιος που ικανοποιεί την ταυτοανισότητα :

$$2^{\lambda_i}\pi_i \geq 1 \qquad (3.14)$$

(δ) Οι δεκαδικοί αριθμοί ϵ_i, $i = 1, 2, \ldots, \rho$, μετατρέπονται σε δυαδικούς αριθμούς και από τους τελευταίους διατηρούνται μόνο λ_i σημαντικά ψηφία που αποτελούν αντίστοιχα τις κωδικές λέξεις για τα σύμβολα πληροφορίας α_i, $i = 1, 2, \ldots, \rho$.

ΠΑΡΑΔΕΙΓΜΑ : Εστω πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4 \}$, $\Pi_A = \{ 0.5, 0.3, 0.1, 0.1 \}$. Τα σύμβολα πληροφορίας είναι ήδη διατεταγμένα κατά ελαττούμενη πιθανότητα. Επομένως το βήμα (α) της διαδικασίας κωδικοποίησης έχει πραγματοποιηθεί. Στο βήμα (β) προσδιορίζονται οι αριθμοί ϵ_1, ϵ_2, ϵ_3, ϵ_4 :

$$\epsilon_1 = 0 \qquad = 0.0 \qquad 0.\underline{0}0000\ldots$$

$$\epsilon_2 = 0.5 + \epsilon_1 = 0.5 \qquad 0.\underline{1}0000\ldots$$

$$\epsilon_3 = 0.3 + \epsilon_2 = 0.8 \qquad 0.\underline{11}001\ldots$$

$$\epsilon_4 = 0.1 + \epsilon_3 = 0.9 \qquad 0.\underline{111}00\ldots$$

και μάλιστα δίνονται δύπλα σε δυαδική μορφή επειδή αυτό θα είναι απαραίτητο στο βήμα (δ). Το μήκος των κωδικών λέξεων προκύπτει με εφαρμογή της εξ.(3.14) :

$$2^{\lambda_1}(0.5) \geq 1 \Rightarrow \lambda_1 = 1$$

$$2^{\lambda_2}(0.3) \geq 1 \Rightarrow \lambda_2 = 2$$

$$2^{\lambda_3}(0.1) \geq 1 \Rightarrow \lambda_3 = 4$$

$$2^{\lambda_4}(0.1) \geq 1 \Rightarrow \lambda_4 = 4$$

Επομένως το κλειδί του κώδικα είναι :

α_1	$\longleftrightarrow$ 0
α_2	$\longleftrightarrow$ 10
α_3	$\longleftrightarrow$ 1100
α_4	$\longleftrightarrow$ 1110

και οι κωδικές λέξεις προέρχονται από τα υπογραμμισμένα ψηφία της δυαδική μορφής των αριθμών ϵ_1, ϵ_2, ϵ_3, ϵ_4. Το μέσο μήκος των κωδικών λέξεων είναι $\Lambda = 1(0.5) + 2(0.3) + 4(0.1) + 4(0.1) = 1.9$ ψηφία/λέξη και επειδή κάθε δυαδικό ψηφίο αντιστοιχεί σε 1 bit, $\Lambda = 1.9$ bits/λέξη. Η εντροπία της πηγής πληροφορίας είναι $H(A) = -0.5\log_2(0.5) - 0.3\log_2(0.3) - 0.1\log_2(0.1) - 0.1\log_2(0.1) = 1.685$ bits/σύμβολο και $\Lambda = 1.9$ bits/σύμβολο $> H(A)/\log_2\sigma = 1.685/\log_2 2 = 1.685$ bits/σύμβολο, όπως απαιτεί η εξ.(3.7).

3.4.2 ΚΩΔΙΚΑΣ SHANNON–FANO

Ο κώδικας διαμορφώνεται σε πέντε βήματα :

(α) Τα σύμβολα πληροφορίας $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ διατάσσονται κατά ελαττούμενη πιθανότητα :

$$\begin{array}{ccccccc} \alpha_1 & & \alpha_2 & & \ldots & & \alpha_\rho \\ \updownarrow & & \updownarrow & & & & \updownarrow \\ \Pi_1 & \geq & \Pi_2 & \geq & \ldots & \geq & \Pi_\rho \end{array}$$

(β) Επιλέγεται συγκεκριμένη διάταξη και για τα κωδικά σύμβολα, έστω η $\gamma_1, \gamma_2, \ldots, \gamma_\sigma$, που δεν διαταράσσεται κατά τις διαδικασίες κωδικοποίησης και αποκωδικοποίησης.

(γ) Τα σύμβολα πληροφορίας συγχωνεύονται με γειτονικά σύμβολα ώστε να σχηματισθούν σ ομάδες συμβόλων. Οι πιθανότητες των συμβόλων που συμμετέχουν σε κάθε ομάδα αθροίζονται και το αποτέλεσμα επιδιώκεται να είναι κατά το δυνατό πλησιέστερα στον αριθμό $1/\sigma$. Επομένως οι σ ομάδες συμβόλων εκπροσωπούν ουσιαστικά σ σύνθετα σύμβολα που είναι κατά το δυνατό ισοπίθανα.

(δ) Στα σύμβολα της 1ης ομάδας προσδίνεται σαν πρώτο κωδικό σύμβολο το γ_1, στα σύμβολα της 2ης ομάδας προσδίνεται σαν πρώτο κωδικό σύμβολο το γ_2 κ.ο.κ.

(ε) Κάθε ομάδα συμβόλων υποδιαιρείται σε σ υπο–ομάδες συμβόλων που είναι κατά το δυνατό ισοπίθανες. Στα σύμβολα των υπο–ομάδων προσδίνεται δεύτερο κωδικό σύμβολο με την προκαθορισμένη διάταξη $\gamma_1, \gamma_2, \ldots, \gamma_\sigma$. Οι υποδιαιρέσεις συνεχίζονται μέχρι να προκύψουν υπο–ομάδες με ένα μόνο σύμβολο.

ΠΑΡΑΔΕΙΓΜΑ : Εστω πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8 \}$. $\Pi_A = \{ 0.25, 0.25, 0.125, 0.125, 0.0625, 0.0625, 0.0625, 0.0625 \}$. Τα σύμβολα πληροφορίας είναι ήδη διατεταγμένα κατά ελαττούμενη πιθανότητα. Επομένως το βήμα (α) της διαδικασίας κωδικοποίησης έχει πραγματοποιηθεί. Στο βήμα (β) επιλέγεται για τα σύμβολα του δυαδικού κώδικα Shannon–Fano η διάταξη 0, 1. Η κατασκευή του κώδικα περιγράφεται στον πίνακα 3.4 .

Πίνακας 3.4

Δυαδικός κώδικας Shannon-Fano

Σύμβολα	Πιθανότητες	1ο Βήμα	2ο Βήμα	3ο Βήμα	4ο Βήμα
α_1	0.25	0	00	00	00
α_2	0.25	0	01	01	01
α_3	0.125	1	10	100	100
α_4	0.125	1	10	101	101
α_5	0.0625	1	11	110	1100
α_6	0.0625	1	11	110	1101
α_7	0.0625	1	11	111	1110
α_8	0.0625	1	11	111	1111

Το μέσο μήκος των κωδικών λέξεων είναι $\Lambda = 2(0.25) + 2(0.25) + 3(0.125) + 3(0.125) + 4(0.0625) + 4(0.0625) + 4(0.0625) + 4(0.0625) = 2.75$ bits/λέξη. Για την εντροπία της πηγής πληροφορίας προκύπτει $H(A) = 2.75$ bits/σύμβολο και επομένως $\Lambda = H(A)/\log_2\sigma$, δηλαδή ο κώδικας αυτός είναι, σύμφωνα με το πρώτο θεώρημα Shannon, βέλτιστος. Στο επόμενο παράδειγμα η τεχνική Shannon-Fano διαμορφώνει μη βέλτιστο κώδικα.

ΠΑΡΑΔΕΙΓΜΑ : Εστω πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7 \}$. $\Pi_A = \{ 0.4, 0.2, 0.12, 0.08, 0.08, 0.08, 0.04 \}$. Τα σύμβολα πληροφορίας είναι ήδη διατεταγμένα κατά ελαττούμενη πιθανότητα. Επομένως το βήμα (α) της διαδικασίας κωδικοποίησης έχει πραγματοποιηθεί. Στο βήμα (β) επιλέγεται για τα σύμβολα του δυαδικού κώδικα Shannon-Fano η διάταξη 0, 1. Η κατασκευή του κώδικα περιγράφεται στον πίνακα 3.5 .

Το μέσο μήκος των κωδικών λέξεων είναι $\Lambda = 2.52$ bits/λέξη, η εντροπία της πηγής πληροφορίας είναι $H(A) = 2.42$ bits/σύμβολο και επομένως $\Lambda > H(A)/\log_2\sigma$ $(\sigma = 2)$, δηλαδή ο κώδικας αυτός, σύμφωνα με το πρώτο θεώρημα Shannon, δεν είναι βέλτιστος. Είναι φανερό ότι ο πρώτος διαμερισμός μπορεί να πραγματοποιηθεί μεταξύ των συμβόλων πληροφορίας α_1, α_2 οπότε προκύπτει εναλλακτικός κώδικας Shannon-Fano, που μάλιστα προκύπτει ότι έχει μικρότερο μέσο μήκος κωδικών

λέξεων.

Πίνακας 3.5

Δυαδικός κώδικας Shannon-Fano

Σύμβολα	Πιθανότητες	1ο Βήμα	2ο Βήμα	3ο Βήμα	4ο Βήμα
α_1	0.40	0	00	00	00
α_2	0.20	0	01	01	01
α_3	0.12	1	10	100	100
α_4	0.08	1	10	101	101
α_5	0.08	1	11	110	110
α_6	0.08	1	11	111	1110
α_7	0.04	1	11	111	1111

3.4.3 ΚΩΔΙΚΑΣ HUFFMANN

Ο κώδικας διαμορφώνεται σε πέντε βήματα :

(α) Τα σύμβολα πληροφορίας $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ διατάσσονται κατά ελαττούμενη πιθανότητα :

$$\begin{array}{ccccccc} \alpha_1 & & \alpha_2 & & \cdots & & \alpha_\rho \\ \updownarrow & & \updownarrow & & & & \updownarrow \\ \pi_1 & \geq & \pi_2 & \geq & \cdots & \geq & \pi_\rho \end{array}$$

(β) Επιλέγεται συγκεκριμένη διάταξη και για τα κωδικά σύμβολα, έστω η $\gamma_1, \gamma_2, \ldots, \gamma_\sigma$, που δεν διαταράσσεται κατά τις διαδικασίες κωδικοποίησης και αποκωδικοποίησης.

(γ) Ομαδοποιούνται τα τελευταία σ σύμβολα πληροφορίας σε ένα σύνθετο σύμβολο με πιθανότητα ίση με το άθροισμα των πιθανοτήτων των μελών της ομάδας. Προκύπτουν

έτσι ρ − σ + 1 σύμβολα που επαναδιατάσσονται κατά ελαττούμενη πιθανότητα. Η διαδικασία επαναλαμβάνεται μερικές φορές και σε κάθε επανάληψη το πλήθος συμβόλων μειώνεται κατά σ − 1. Τελική επιδίωξη είναι να απομείνουν μετά από Ν επαναλήψεις σ σύμβολα που αντιστοιχίζονται στα κωδικά σύμβολα κατά τη διάταξη του βήματος (β). Αφού σε κάθε επανάληψη μειώνεται το πλήθος των συμβόλων κατά σ − 1 και μετά από Ν επαναλήψεις απομένουν σ σύμβολα, το αρχικό πλήθος συμβόλων πρέπει να είναι Ρ = σ + Ν(σ − 1). Αν ρ < Ρ, προστίθενται στο τέλος της διάταξης των συμβόλων πληροφορίας Ρ − ρ πλασματικά σύμβολα με μηδενική πιθανότητα.

Πίνακας 3.6

Τετραδικός κώδικας Huffmann

	Αρχική Διάταξη		1η Μείωση		2η Μείωση		3η Μείωση	
Σύμβολα	Πιθαν.	Λέξη	Πιθαν.	Λέξη	Πιθαν.	Λέξη	Πιθαν.	Λέξη
α_1	0.25	1	0.25	1	0.25	1	0.37	0
α_2	0.15	3	0.15	3	0.23	2	0.25	1
α_3	0.12	00	0.12	00	0.15	3	0.23	2
α_4	0.10	01	0.10	01	0.12	00	0.15	3
α_5	0.08	02	0.08	02	0.10	01		
α_6	0.06	20	0.07	03	0.08	02		
α_7	0.06	21	0.06	20	0.07	03		
α_8	0.06	22	0.06	21				
α_9	0.05	23	0.06	22				
α_{10}	0.04	030	0.05	23				
α_{11}	0.03	031						
α_{12}	0.00	032						
α_{13}	0.00	033						

(δ) Στα σ (σύνθετα) σύμβολα που διαμορφώνονται τελικά προσδίνονται τα κωδικά σύμβολα με τη διάταξη του βήματος (β) σαν πρώτο σύμβολο των αντίστοιχων κωδικών λέξεων που θα διαμορφωθούν σταδιακά.

(ε) Επιστρέφοντας βήμα με βήμα προς την αρχική διάταξη συμβόλων πληροφορίας.

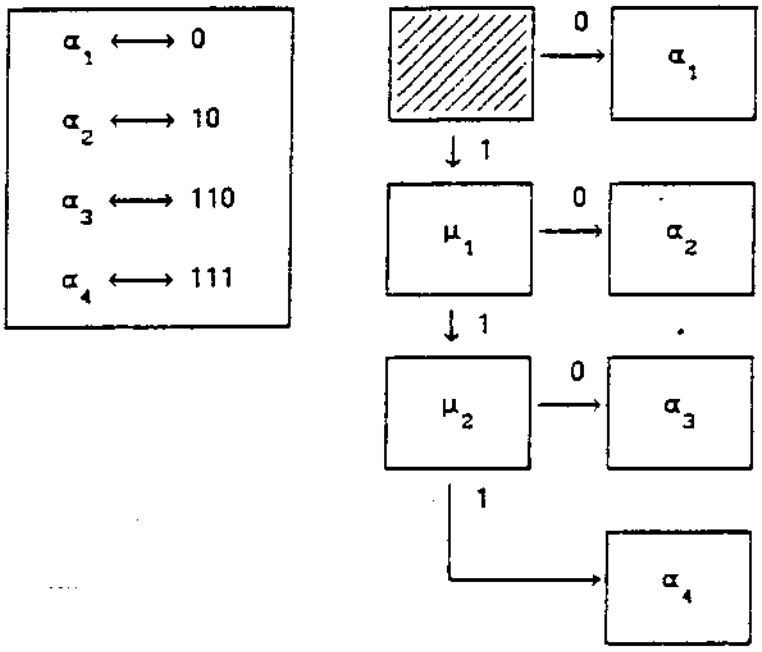
προσδίνονται τα κωδικά σύμβολα με τη διάταξη του βήματος (β) σαν επόμενο σύμβολο των κωδικών λέξεων που αντιστοιχίζονται στα μέλη κάθε σύνθετου συμβόλου. Η διαδικασία αυτή διευκρινίζεται με το παράδειγμα που ακολουθεί.

ΠΑΡΑΔΕΙΓΜΑ : Εστω η πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11} \}$, $\Pi_A = \{ 0.25, 0.15, 0.12, 0.10, 0.08, 0.06, 0.06, 0.06, 0.05, 0.04, 0.03 \}$. Ο τετραδικός κώδικας Huffmann χρησιμοποιεί τα σύμβολα 0, 1, 2, 3 που στη συνέχεια θεωρούνται με τη διάταξη αυτή. Ο κώδικας παράγεται με τη διαδικασία μειώσεων που περιγράφεται στον πίνακα 3.6 . Με κάθε βήμα το πλήθος συμβόλων μειώνεται κατά 3 και τελικά απομένουν 4 σύμβολα. Επειδή $\rho = 11 \neq 4 + 3N$ για ακέραιο N, προστίθενται στη διάταξη των συμβόλων πληροφορίας 2 πλασματικά σύμβολα με αποτέλεσμα $P = \rho + 2 = 13 = 4 + 3N$ με $N = 3$. Επομένως απαιτούνται 3 βήματα για να μειωθεί το αρχικό πλήθος 13 συμβόλων στο τελικό πλήθος 4 συμβόλων.

3.4.4 ΔΕΝΔΡΟΔΙΑΓΡΑΜΜΑ ΑΠΟΦΑΣΗΣ

Η αποκωδικοποίηση διαφορικών κωδίκων που διαθέτουν την προθεματική ιδιότητα υλοποιείται με το *πεπερασμένο αυτόματο* ή *δενδροδιάγραμμα απόφασης*. Η λειτουργία του γίνεται κατανοητή με το παρακάτω απλό παράδειγμα.

ΠΑΡΑΔΕΙΓΜΑ : Εστω δυαδικός κώδικας τεσσάρων λέξεων και το αντίστοιχο δενδροδιάγραμμα απόφασης (σχ. 3.2). Το αυτόματο βρίσκεται αρχικά στην κατάσταση που αντιστοιχεί στο σκιασμένο τετράγωνο. Με την άφιξη του πρώτου κωδικού ψηφίου, που είναι 0 ή 1, το αυτόματο περνά αντίστοιχα στην τελική κατάσταση α_1 ή στη μεταβατική κατάσταση μ_1. Από κάθε τελική κατάσταση το αυτόματο περνά αμέσως στην αρχική κατάσταση και αναμένει την άφιξη του επόμενου κωδικού ψηφίου. Αν το αυτόματο βρεθεί στην κατάσταση μ_1, με την άφιξη του δεύτερου κωδικού ψηφίου, που είναι επίσης 0 ή 1, περνά αντίστοιχα στην τελική κατάσταση α_2 ή στη μεταβατική κατάσταση μ_2. Από την κατάσταση μ_2 περνά στην τελική κατάσταση α_3 ή στην τελική κατάσταση α_4 με την άφιξη του τρίτου κωδικού ψηφίου, που πρέπει να είναι αντίστοιχα 0 ή 1. Κάθε φορά που το αυτόματο περνά σε κάποια τελική κατάσταση γίνεται αποκωδικοποίηση της αντίστοιχης κωδικής λέξης που έχει συμπληρωθεί. Η αποκωδικοποίηση είναι στιγμιαία επειδή έγινε δεκτό ότι ο κώδικας διαθέτει την προθεματική ιδιότητα.



Σχ. 3.2 Δενδροδιάγραμμα απόφασης.

3.5 ΑΣΚΗΣΕΙΣ

1. Να εξεταοθεί η δυνατότητα στιγμιαίας αποκωδικοποίησης κώδικα με λέξεις μήκους 1, 2, ..., ν, ... συμβόλων.

2. Να εξεταοθεί η δυνατότητα στιγμιαίας αποκωδικοποίησης τετραδικού κώδικα με λέξεις όπως στον παρακάτω πίνακα.

Πλήθος	Μήκος
2	1
3	2
4	3
...	...
ν+1	ν
...	...

3. Στον *κώδικα κόμμα* το τέλος κάθε κωδικής λέξης σημειώνεται με την εμφάνιση του σημείου στίξης (,). Οι μακρύτερες κωδικές λέξεις δεν έχουν υποχρεωτικά το κόμμα στην τελευταία θέση τους και αναγνωρίζονται απλά από το μεγαλύτερο μήκος τους. Να εξεταοθεί η δυνατότητα στιγμιαίας αποκωδικοποίησης του κώδικα κόμμα.

4. Εστω πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$ και καταναμή πιθανοτήτων $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$. Η ν-οστή επέκταση της, δηλαδή η πηγή πληροφορίας A^ν, Π_A^ν, υφίσταται δυαδική κωδικοποίηση και κάθε σύμβολο πληροφορίας $\alpha_i^\nu = \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_\nu} \in A^\nu$, που έχει πιθανότητα εμφάνισης $\pi_i^\nu = \pi_{i_1} \pi_{i_2} \ldots \pi_{i_\nu} \in \Pi_A^\nu$, αντιστοιχίζεται σε κωδική λέξη μήκους λ_i^ν δυαδικών ψηφίων. Αν ισχύει :

$$-\log_2(\pi_i^\nu) \leq \lambda_i^\nu \leq 1 - \log_2(\pi_i^\nu)$$

για $i = 1, 2, \ldots, \rho^\nu$, να αποδειχθεί ότι το μέσο μήκος των κωδικών λέξεων :

$$\Lambda_\nu = \sum_{i=1}^{\rho^\nu} \pi_i^\nu \lambda_i^\nu$$

ικανοποιεί τη διπλή ταυτοανισότητα :

$$\nu H(A) \leq \Lambda_\nu \leq \nu H(A) + 1 .$$

5. Η έξοδος του κωδικοποιητή της προηγούμενης άσκησης παρέχει πληροφορία $-\log_2(\pi_i^\nu)/\lambda_i^\nu$ bits/δυαδικό ψηφίο, $i = 1, 2, \ldots, \rho^\nu$. Επομένως η μέση πληροφορία ανά δυαδικό ψηφίο είναι :

$$H_\nu = \sum_{i=1}^{\rho^\nu} \pi_i^\nu \left[- \frac{\log_2(\pi_i^\nu)}{\lambda_i^\nu} \right]$$

Να αποδειχθεί ότι ισχύει η διπλή ταυτοανισότητα :

$$1 + \frac{1}{\nu \log_2(\pi_{max}^\nu)} \leq H_\nu \leq 1$$

όπου $\pi_{max}^\nu = \max \{ \pi_i^\nu ; i = 1, 2, \ldots, \rho^\nu \}$. Τι παρατηρείται στο όριο $\nu \to \infty$;

6. Έστω πηγή πληροφορίας με αλφάβητο $A = \{ \alpha_1, \alpha_2, \ldots, \alpha_\rho \}$ και κατανομή πιθανοτήτων $\Pi_A = \{ \pi_1, \pi_2, \ldots, \pi_\rho \}$. Κάθε μήνυμα ν συμβόλων $\alpha_i^\nu = \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_\nu}$ είναι ουσιαστικά σύμβολο της πηγής πληροφορίας A^ν, Π_A^ν, δηλαδή της ν-οστής επέκτασης της πηγής πληροφορίας A, Π_A. Το *ε-τυπικό* μήνυμα ν συμβόλων α_c^ν περιέχει ν_i φορές το σύμβολο $\alpha_i \in A$, $i = 1, 2, \ldots, \rho$, όπου ν_i ικανοποιεί τη διπλή ταυτοανισότητα :

$$(1-\epsilon)\nu\pi_i \leq \nu_i < (1+\epsilon)\nu\pi_i$$

με $\epsilon > 0$ και $\nu_1 + \nu_2 + \ldots + \nu_\rho = \nu$. Να αποδειχθεί ότι η πιθανότητα του ε-τυπικού συμβόλου, έστω π_c^ν, ικανοποιεί τη διπλή ταυτοανισότητα :

$$2^{-\nu(1+\epsilon)H(A)} \leq \pi_c^\nu \leq 2^{-\nu(1-\epsilon)H(A)}$$

όπου H(A) είναι η εντροπία της πηγής πληροφορίας A, Π_A. Αν για την κωδικοποίηση των ε-τυπικών συμβόλων χρησιμοποιούνται λ_c^ν δυαδικά ψηφία, να αποδειχθεί ότι πρέπει να ισχύει επιπλέον η διπλή ταυτοανισοτητα:

$$(1+\epsilon)\nu H(A) \leq \lambda_c^\nu \leq (1+\epsilon)\nu H(A) + 1 .$$

7. Έστω η πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8 \}$, $\Pi_A = \{ 0.22, 0.16, 0.15, 0.13, 0.12, 0.09, 0.08, 0.05 \}$. Να προσδιορισθούν οι δυαδικοί κώδικες Shannon, Shannon-Fano, Huffmann και να υπολογισθεί το μέσο μήκος των κωδικών λέξεων για κάθε κώδικα.

8. Να προσδιορισθεί ο δυαδικός κώδικας Shannon-Fano για την τριαδική πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3 \}$, $\Pi_A = \{ 1/3^\kappa, 1/3^{\kappa+1}, 1 - 1/3^\kappa - 1/3^{\kappa+1} \}$, όπου κ είναι θετικός ακέραιος. Να υπολογισθεί το μέσο μήκος των κωδικών λέξεων.

9. Έστω πηγή πληροφορίας $A = \{ \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \}$, $\Pi_A = \{ 0.4, 0.2, 0.2, 0.1, 0.1 \}$. Να προσδιορισθεί ο δυαδικός κώδικας Huffmann με τη μικρότερη μεταβλητότητα μήκους των κωδικών λέξεων.

10. Πηγή πληροφορίας με αλφάβητο $\{ \alpha, \beta \}$ και κατανομη πιθανοτητων $\{ 1 - 1/2^\kappa, 1/2^\kappa \}$, όπου κ θετικός ακέραιος, κωδικοποιείται κατά Shannon και Huffmann. Να

σχολιασθεί το μήκος των κωδικών λέξεων. Να υπολογισθεί το μέσο μήκος κωδικών λέξεων για κάθε κώδικα. Τι παρατηρείται στο όριο $x \to \infty$;

11. Δίνεται παρακάτω ο δυαδικός κώδικας Shannon-Fano για το Αγγλικό αλφάβητο. Να σχεδιασθεί το δενδροδιάγραμμα απόφασης του αποκωδικοποιητή.

A	1111	N	1100
B	101000	O	1110
C	01010	P	110111
D	11010	Q	1101100101
E	100	R	1011
F	01011	S	0110
G	00001	T	001
H	0001	U	01000
I	0111	V	1101101
J	1101100110	W	101001
K	11011000	X	1101100111
L	10101	Y	00000
M	01001	Z	1101100100

Κεφάλαιο Τέσσερα

ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΘΟΡΥΒΟΥ

4.1 ΚΡΙΤΗΡΙΑ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ

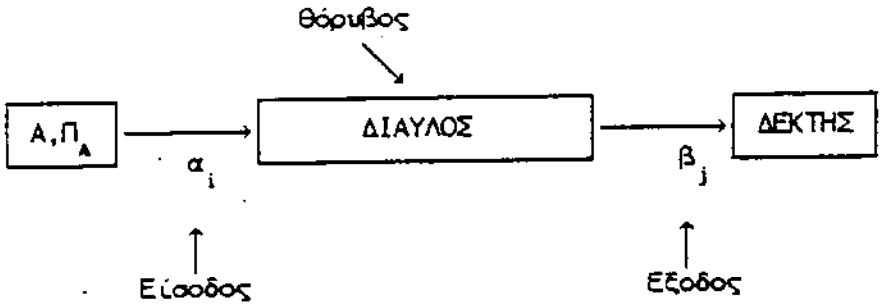
Στο προηγούμενο κεφάλαιο εξετάσθηκε η κωδικοποίηση σε αθόρυβο περιβάλλον που δεν προκαλεί αλλοίωση του μεταδιδόμενου κωδικού μηνύματος. Βελτιστοποίηση του συστήματος επικοινωνίας σε τέτοιο εξιδανικευμένο περιβάλλον είναι απλά η μεγιστοποίηση του ρυθμού μετάδοσης, δηλαδή της απόδοσης του κώδικα, και με το πρώτο θεώρημα Shannon αποδείχθηκε ότι το μέσο μήκος κωδικών λέξεων μπορεί να προσεγγίσει όσο είναι επιθυμητό το κάτω φράγμα του αν και με κάποιο κόστος.

Η παρουσία θορύβου στο σύστημα επικοινωνίας υποβαθμίζει την αξιοπιστία του προκαλώντας την εμφάνιση σφαλμάτων κατά τη μετάδοση της πληροφορίας. Στην έξοδο του διαύλου πληροφορίας (σχ. 4.1) δημιουργείται επομένως αβεβαιότητα για το σύμβολο εισόδου. Στην αποκωδικοποίηση του λαμβανόμενου μηνύματος εμπλέκεται κάποια πιθανότητα σφάλματος που εξαρτάται γενικά από τις διάφορες παραμέτρους του συστήματος επικοινωνίας. Η βελτιστοποίηση του συστήματος επικοινωνίας σε περιβάλλον θορύβου περιλαμβάνει και την ελαχιστοποίηση της πιθανότητας εσφαλμένης αποκωδικοποίησης.

Με το δεύτερο θεώρημα Shannon (βλ. §4.3) θα διαμορφωθεί το συμπέρασμα ότι είναι δυνατή η βέλτιστη λειτουργία του διαύλου πληροφορίας ακόμη και με την παρουσία

θορύβου. Δηλαδή η πιθανότητα εσφαλμένης αποκωδικοποίησης μπορεί να ελαττωθεί όσο είναι επιθυμητό και ταυτόχρονα ο ρυθμός μετάδοσης της πληροφορίας να προσεγγίζει όσο είναι επιθυμητό τη χωρητικότητα του διαύλου πληροφορίας.

Έστω ότι στην έξοδο του διαύλου πληροφορίας φθάνει το σύμβολο β_j, $j = 1, 2, \ldots, \rho$. Η αβεβαιότητα για το σύμβολο εισόδου α_i , $i = 1, 2, \ldots, \rho$ καθορίζεται από το δίαυλο πληροφορίας μέσω των υπό συνθήκη πιθανοτήτων $\pi(\beta_j/\alpha_i)$ αλλά και από την πηγή πληροφορίας μέσω της κατανομής πιθανοτήτων $\Pi_A = (\pi(\alpha_i) / i = 1, 2, \ldots, \rho)$. Η αντιστοίχιση της εξόδου β_j στην είσοδο α_i χαρακτηρίζεται *κανόνας απόφασης* και εμπλέκει κάποια πιθανότητα σφάλματος η_E που είναι ουσιαστικά η πιθανότητα εσφαλμένης αποκωδικοποίησης για το συγκεκριμένο κανόνα απόφασης. Στη συνέχεια θα εξετασθούν δύο κανόνες απόφασης και θα υπολογισθεί η αντίστοιχη πιθανότητα εσφαλμένης αποκωδικοποίησης.



Σχ. 4.1 Γενικά $\beta_j \neq \alpha_i$ λόγω σφαλμάτων που προκαλεί ο θόρυβος.

Ο *κανόνας του τέλειου παρατηρητή* αντιστοιχίζει στο σύμβολο εξόδου β_j εκείνο το σύμβολο εισόδου α' που ικανοποιεί τη συνθήκη :

$$\pi(\alpha'/\beta_j) \geq \pi(\alpha_i/\beta_j) \quad ; \quad i = 1, 2, \ldots, \rho \tag{4.1}$$

δηλαδή η υπό συνθήκη πιθανότητα $\pi(\alpha_i/\beta_j)$ μεγιστοποιείται όταν $\alpha_i = \alpha'$. Η πιθανότητα εσφαλμένης αποκωδικοποίησης κατά τη λήψη του συμβόλου β_j είναι :

$$\pi(E/\beta_j) = 1 - \pi(\alpha'/\beta_j) = \sum_{\alpha_i \neq \alpha'} \pi(\alpha_i/\beta_j) \tag{4.2}$$

και η μέση τιμή της ως προς τα σύμβολα εξόδου είναι η πιθανότητα εσφαλμένης αποκωδικοποίησης η_E που αντιστοιχεί στον κανόνα του τέλειου παρατηρητή :

$$\pi_\varepsilon = \sum_{j=1}^{\rho} \pi(E/\beta_j)\pi(\beta_j) = \sum_{j=1}^{\rho} \left[1 - \pi(\alpha'/\beta_j) \right]\pi(\beta_j) =$$

$$= 1 - \sum_{j=1}^{\rho} \pi(\alpha'/\beta_j)\pi(\beta_j) = 1 - \sum_{j=1}^{\rho} \pi(\beta_j/\alpha')\pi(\alpha') \qquad (4.3)$$

Αν τα σύμβολα εισόδου είναι ισοπίθανα, $\pi(\alpha') = 1/\rho$ και η πιθανότητα σφάλματος υπολογίζεται από την απλοποιημένη έκφραση :

$$\pi_\varepsilon = 1 - \frac{1}{\rho} \sum_{j=1}^{\rho} \pi(\beta_j/\alpha') \qquad (4.4)$$

Αποδεικνύεται ότι ο κανόνας του τέλειου παρατηρητή διαμορφώνει την ελάχιστη πιθανότητα εσφαλμένης αποκωδικοποίησης.

Εναλλακτικά πραγματοποιείται αποκωδικοποίηση με τον *κανόνα της μέγιστης πιθανοφάνειας* που αντιστοιχίζει στο σύμβολο εξόδου β_j εκείνο το σύμβολο εισόδου α' που ικανοποιεί τη συνθήκη :

$$\pi(\beta_j/\alpha') \geq \pi(\beta_j/\alpha_i) \quad ; \quad i = 1, 2, \ldots, \rho \qquad (4.5)$$

δηλαδή η υπό συνθήκη πιθανότητα $\pi(\beta_j/\alpha_i)$ μεγιστοποιείται όταν $\alpha_i = \alpha'$. Ο κανόνας της μέγιστης πιθανοφάνειας εφαρμόζεται επειδή είναι απλούστερος του προηγούμενου αλλά και γιά τον πρακτικό λόγο ότι δεν είναι δυνατός ο υπολογισμός των υπό συνθήκη πιθανοτήτων $\pi(\alpha_i/\beta_j)$ όταν οι πιθανότητες εισόδου $\pi(\alpha_i)$, $i = 1, 2, \ldots, \rho$ είναι άγνωστες στο δέκτη. Ο κανόνας της μέγιστης πιθανοφάνειας δεν οδηγεί σε βέλτιστη πιθανότητα σφάλματος. Στην ειδική περίπτωση ισοπίθανων συμβόλων εισόδου προκύπτει :

$$\pi(\beta_j/\alpha_i) = \pi(\alpha_i/\beta_j) \frac{\pi(\beta_j)}{1/\rho} = \rho\pi(\beta_j)\pi(\alpha_i/\beta_j) \qquad (4.6)$$

και επομένως :

$$\pi(\beta_j/\alpha') \geq \pi(\beta_j/\alpha_i) \iff$$

$$p(\beta_j)P(\alpha' /\beta_j) \geq p(\beta_j)P(\alpha_i/\beta_j) \longleftrightarrow$$

$$P(\alpha' /\beta_j) \geq P(\alpha_i/\beta_j) \qquad (4.7)$$

δηλαδή οι δύο κανόνες χρησιμοποιούν το ίδιο κριτήριο απόφασης. Η πιθανότητα εσφαλμένης αποκωδικοποίησης δίνεται, όπως είναι ήδη γνωστό, από την εξ.(4.4).

ΠΑΡΑΔΕΙΓΜΑ : Έστω δίαυλος πληροφορίας με μητρώο διαύλου :

$$\Pi(B/A) = \begin{bmatrix} 3/4 & 3/16 & 1/16 & 0 \\ 0 & 3/4 & 3/16 & 1/16 \\ 0 & 0 & 3/4 & 1/4 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Εφαρμόζοντας τον κανόνα της μέγιστης πιθανοφάνειας προκύπτει το σχήμα αποκωδικοποίησης :

β_j	$\longleftrightarrow$	α'
β_1	$\longleftrightarrow$	α_1
β_2	$\longleftrightarrow$	α_2
β_3	$\longleftrightarrow$	α_3
β_4	$\longleftrightarrow$	α_4

και η πιθανότητα σφάλματος για ισοπίθανα σύμβολα εισόδου είναι :

$$P_E = 1 - (1/4)\sum_{j=1}^{4} P(\beta_j/\alpha') = 1 - (1/4)(3/4 + 3/4 + 3/4 + 1) = 0.187 \quad \text{ή} \quad 18.7\ \%$$

Με την υπόθεση ισοπίθανων συμβόλων εισόδου το μητρώο Π(A/B) είναι :

$$\Pi(A/B) = \begin{bmatrix} 1 & 1/5 & 1/16 & 0 \\ 0 & 4/5 & 3/16 & 1/21 \\ 0 & 0 & 3/4 & 4/21 \\ 0 & 0 & 0 & 16/21 \end{bmatrix}$$

και ο κανόνας του τέλειου παρατηρητή οδηγεί στο σχήμα αποκωδικοποίησης :

β_j	$\longleftrightarrow$	α'
β_1	$\longleftrightarrow$	α_1
β_2	$\longleftrightarrow$	α_2
β_3	$\longleftrightarrow$	α_3
β_4	$\longleftrightarrow$	α_4

που είναι όμοιο με το αντίστοιχο σχήμα του κανόνα της μέγιστης πιθανοφάνειας. Επομένως οι δύο κανόνες είναι ισοδύναμοι, όπως αναμένεται γενικά για ισοπίθανα σύμβολα εισόδου.

Αν το μητρώο διαύλου είναι :

$$\Pi(B/A) = \begin{bmatrix} 3/4 & 3/16 & 1/16 & 0 \\ 0 & 1/4 & 3/4 & 0 \\ 0 & 3/4 & 0 & 1/4 \\ 0 & 0 & 1/4 & 3/4 \end{bmatrix}$$

το σχήμα αποκωδικοποίησης γίνεται :

β_j	$\longleftrightarrow$	α'
β_1	$\longleftrightarrow$	α_1
β_2	$\longleftrightarrow$	α_3
β_3	$\longleftrightarrow$	α_2
β_4	$\longleftrightarrow$	α_4

και είναι το ίδιο για τους δύο κανόνες απόφασης με την προϋπόθεση ισοπίθανων συμβόλων εισόδου. Η αντίστοιχη πιθανότητα εσφαλμένης αποκωδικοποίησης είναι :

$$\Pi_\Sigma = 1 - (1/4)(3/4 + 3/4 + 3/4 + 3/4) = 1/4 \quad \text{ή} \quad 25\ \%$$

4.2 ΦΡΑΓΜΑ FANO

Η παρουσία θορύβου στο σύστημα επικοινωνίας προκαλεί στο δέκτη αβεβαιότητα για το σύμβολο εκπομπής που ισοδυναμεί με απώλεια πληροφορίας κατά τη μετάδοση. Η μέση τιμή της απώλειας πληροφορίας λόγω θορύβου είναι η εντροπία θορύβου H(A/B) που ορίσθηκε στην §2.1. Η σχέση της πιθανότητας σφάλματος η_ε με την εντροπία θορύβου H(A/B) του συστήματος επικοινωνίας, που λειτουργεί σε περιβάλλον θορύβου, περιγράφεται με την ταυτοανισότητα :

$$H(A/B) \leq H(\eta_\varepsilon) + \eta_\varepsilon \log_e(\rho-1) \qquad (4.8)$$

που χαρακτηρίζεται *φράγμα Fano*. Η φυσική σημασία της εξ.(4.8) αποκαλύπτεται με τον παρακάτω συλλογισμό.

Η εντροπία θορύβου H(A/B) είναι ουσιαστικά μιά πρόσθετη ποσότητα πληροφορίας που απαιτείται στο δέκτη προκειμένου να αρθεί η αβεβαιότητα για το σύμβολο εκπομπής. Το άνω φράγμα αυτής της πρόσθετης πληροφορίας, που απαιτείται για ορθή αποκωδικοποίηση, δίνεται στο δεξιό μέλος της εξ.(4.8) σαν άθροισμα δύο όρων. Ο πρώτος όρος, $H(\eta_\varepsilon)$, εκπροσωπεί τη μέση πληροφορία που απαιτείται για τη δυαδική απόφαση ύπαρξης ή μη σφάλματος κατά τη μετάδοση του συμβόλου πληροφορίας. Ο δεύτερος όρος, $\eta_\varepsilon \log_e(\rho-1)$, εκπροσωπεί τη μέση πληροφορία που απαιτείται για να καθορισθεί ποιό από τα υπόλοιπα $(\rho-1)$ σύμβολα έχει σταλεί εφόσον έχει διαπιστωθεί σφάλμα. Επειδή η χωρητικότητα του διαύλου πληροφορίας συνδέεται με την εντροπία θορύβου, η εξ.(4.8) συνδέει ουσιαστικά την πιθανότητα εσφαλμένης αποκωδικοποίησης η_ε με τη χωρητικότητα του διαύλου πληροφορίας στο σύστημα επικοινωνίας.

Η απόδειξη της εξ.(4.8) ξεκινά από την εξ.(1.19) :

$$H(A/B) = \sum_{j=1}^{\rho} H(A/\beta_j)n(\beta_j) = -\sum_{i=1}^{\rho}\sum_{j=1}^{\rho} n(\alpha_i/\beta_j)\log_e\left[n(\alpha_i/\beta_j)\right]n(\beta_j) \qquad (4.9)$$

Αν θεωρηθεί ότι ορθή αποκωδικοποίηση πραγματοποιείται κατά το σχήμα $\beta_i \leftrightarrow \alpha_i$, $i = 1, 2, \ldots, \rho$, τότε είναι δυνατό να διαμορφωθεί η παρακάτω έκφραση για την εντροπία θορύβου :

$$H(A/B) = -\sum_{j=1}^{\rho}\left[n(\alpha_j/\beta_j)\log_e\left[n(\alpha_j/\beta_j)\right] + \sum_{\substack{i=1\\ i\neq j}}^{\rho} n(\alpha_i/\beta_j)\log_e\left[n(\alpha_i/\beta_j)\right] \right] n(\beta_j) =$$

$$-\sum_{j=1}^{\rho}\left[\left[1 - n(E/\beta_j)\right]\log_e\left[1 - n(E/\beta_j)\right] + n(E/\beta_j)\log_e\left[n(E/\beta_j)\right] + \right.$$

$$\left. n(E/\beta_j)\sum_{\substack{i=1\\ i\neq j}}^{\rho}\left[\frac{n(\alpha_i/\beta_j)}{n(E/\beta_j)} \right]\log_e\left[\frac{n(\alpha_i/\beta_j)}{n(E/\beta_j)} \right] \right] n(\beta_j) \qquad (4.10)$$

όπου $n(E/\beta_j)$ είναι η πιθανότητα αφάλματος όταν στο δέκτη λαμβάνεται το σύμβολο β_j :

$$n(E/\beta_j) = 1 - n(\alpha_j/\beta_j) = \sum_{\substack{i=1\\ i\neq j}}^{\rho} n(\alpha_i/\beta_j) \qquad (4.11)$$

Είναι φανερό ότι :

$$\sum_{\substack{i=1\\ i\neq j}}^{\rho}\left[\frac{n(\alpha_i/\beta_j)}{n(E/\beta_j)} \right] = 1 \qquad (4.12)$$

και επομένως :

$$-\sum_{\substack{i=1\\ i\neq j}}^{\rho}\left[\frac{n(\alpha_i/\beta_j)}{n(E/\beta_j)} \right]\log_e\left[\frac{n(\alpha_i/\beta_j)}{n(E/\beta_j)} \right] \leq \log_e(\rho-1) \qquad (4.13)$$

Η εξ.(4.10) παίρνει τη μορφή που ακολουθεί :

$$H(A/B) \leq \sum_{j=1}^{\rho}\left[H(n(E/\beta_j)) + n(E/\beta_j)\log_e(\rho-1) \right] n(\beta_j) =$$

$$H(n(E/B)) + n(E)\log_e(\rho-1) \qquad (4.14)$$

Αλλά η εξ.(1.22) υποδεικνύει ότι $H(\pi(E/B)) \leq H(\pi(E))$ και με την αντικατάσταση $\pi(E) = \pi_E$ προκύπτει η εξ.(4.8) που περιγράφει το φράγμα Fano.

Η ισότητα στην εξ.(4.13) ισχύει στην περίπτωση :

$$\pi(\alpha_i/\beta_j) = \frac{\pi(E/\beta_j)}{\rho - 1}, \quad i \neq j \tag{4.15}$$

που υποδεικνύει ότι το μέγιστο της αβεβαιότητας που προκαλεί ο θόρυβος αντιστοιχεί στην περίπτωση που τα $(\rho-1)$ σχήματα εσφαλμένης αποκωδικοποίησης $\beta_j \leftrightarrow \alpha_i$, $i \neq j$, είναι ισοπίθανα.

4.3 ΔΕΥΤΕΡΟ ΘΕΩΡΗΜΑ SHANNON

ΘΕΩΡΗΜΑ : Εστω πηγή πληροφορίας χωρίς μνήμη με αλφάβητο ρ συμβόλων και εντροπία Η, δίαυλος πληροφορίας με χωρητικότητα C και αυθαίρετος αριθμός $\epsilon > 0$. Αν $0 \leq H \leq C$, υπάρχει κώδικας που αντιστοιχίζει τα σύμβολα πληροφορίας σε κωδικές λέξεις ν ψηφίων και εξασφαλίζει πιθανότητα εσφαλμένης αποκωδικοποίησης $\pi_E \leq \epsilon$. Αν $\alpha_1, \alpha_2, \ldots, \alpha_\rho$ είναι τα σύμβολα εισόδου, $\beta_1, \beta_2, \ldots, \beta_\rho$ είναι τα σύμβολα εξόδου και $\beta_i \leftrightarrow \alpha_i$, $i = 1, 2, \ldots, \rho$ είναι το σχήμα ορθής αποκωδικοποίησης, η πιθανότητα ορθής αποκωδικοποίησης είναι $\pi(\alpha_i/\beta_i) = \pi_0 = 1-\pi_E \geq 1-\epsilon$. Δηλαδή, η μεν πιθανότητα εσφαλμένης αποκωδικοποίησης προσεγγίζει την τιμή 0 η δε πιθανότητα ορθής αποκωδικοποίησης προσεγγίζει την τιμή 1 όσο είναι επιθυμητό. Το πλήθος ψηφίων ανά κωδική λέξη επιλέγεται από τη σχέση $\rho \geq 2^{\nu H}$. Αν $0 < C < H$, δεν υπάρχει κώδικας για τη δεδομένη πηγή πληροφορίας που να εξασφαλίζει αυθαίρετα μικρή πιθανότητα σφάλματος.

Το δεύτερο θεώρημα Shannon, που είναι γνωστό και σαν *θεώρημα κωδικοποίησης σε περιβάλλον θορύβου*, υποδεικνύει ότι η χωρητικότητα του διαύλου πληροφορίας είναι η σημαντικώτερη παράμετρος του συστήματος επικοινωνίας και εγγυάται την ύπαρξη αυθαίρετα αξιόπιστου κώδικα για μετάδοση πληροφορίας με ρυθμό που προσεγγίζει αυθαίρετα τη χωρητικότητα. Είναι φανερό, όμως, ότι το θεώρημα δεν παρέχει μέθοδο για τον προσδιορισμό του βέλτιστου κώδικα.

Η απόδειξη του δεύτερου θεωρήματος Shannon είναι περίπλοκη και μακρά. Θα δοθεί εδώ μόνο η απόδειξη για την ειδική περίπτωση του δυαδικού συμμετρικού διαύλου πληροφορίας. Κατά την αποδεικτική διαδικασία προκύπτει ότι για ροή κωδικοποιημένης πληροφορίας με ρυθμό που προσεγγίζει τη χωρητικότητα και με πιθανότητα εσφαλμένης αποκωδικοποίησης που προσεγγίζει το μηδέν απαιτούνται μακρές κωδικές λέξεις. Δηλαδή ο βέλτιστος κώδικας είναι συνήθως δύσχρηστος. Το δεύτερο θεώρημα Shannon δεν λύνει επομένως όλα τα προβλήματα αλλά εγγυάται απλά τη δυνατότητα σχεδίασης αξιόπιστου κώδικα για σύστημα επικοινωνίας που είναι εκτεθειμένο σε θόρυβο.

Έστω ότι ρ σύμβολα πληροφορίας κωδικοποιούνται σε δυαδικές ν-άδες. Το πλήθος των δυαδικών ν-άδων είναι 2^v και πρέπει προφανώς να υπερβαίνει το πλήθος των συμβόλων πληροφορίας, δηλαδή $2^v \geq \rho$ ή :

$$v \geq \log_2 \rho \tag{4.16}$$

Αν εφαρμοσθεί η τεχνική τυχαίας κωδικοποίησης Shannon, η επιλογή των ρ δυαδικών ν-άδων που εκπροσωπούν τα σύμβολα πληροφορίας γίνεται τυχαία και επομένως η πιθανότητα να εκπροσωπεί μια δυαδική ν-άδα κάποιο σύμβολο πληροφορίας είναι $\rho/2^v$.

Έστω ότι ο δυαδικός συμμετρικός δίαυλος πληροφορίας λειτουργεί με πιθανότητα σφάλματος $q \leq 0.5$ σε κάθε δυαδικό ψηφίο. Η πιθανότητα ορθής μετάδοσης είναι $p = 1 - q$. Κατά τη μετάδοση των κωδικών λέξεων γίνονται κατά μέσο όρο $vq < v/2$ σφάλματα ανά λέξη, δηλαδή κατά μέσο όρο λιγότερα από τα μισά ψηφία αλλοιώνονται σε κάθε κωδική λέξη. Το πλήθος των δυαδικών ν-άδων που διαφοροποιούνται από κάποια κωδική λέξη κατά ξ ψηφία είναι $\binom{v}{\xi}$, δηλαδή όσοι και οι συνδυασμοί ν πραγμάτων ανά ξ. Επομένως το πλήθος των δυαδικών ν-άδων που διαφοροποιούνται από κάποια κωδική λέξη κατά vq ψηφία ή λιγότερα είναι :

$$N = \binom{v}{0} + \binom{v}{1} + \ldots + \binom{v}{vq} = \sum_{i=0}^{vq} \binom{v}{i} \tag{4.17}$$

και τόσες δυαδικές ν-άδες σχετίζονται στην έξοδο του διαύλου με την υπόψη κωδική λέξη επειδή διαφοροποιούνται από αυτή σε λιγότερα από τα μισά ψηφία. Είναι

εύκολο να αποδειχθεί ότι $\begin{bmatrix} v \\ i \end{bmatrix} < \begin{bmatrix} v \\ i+1 \end{bmatrix}$ επειδή $0 \leq i < vq \leq v/2 < (v+1)/2$. Δηλαδή οι όροι του αθροίσματος στην εξ.(4.17) αυξάνουν με το δείκτη i και επομένως διαμορφώνεται η ανισότητα :

$$N < (vq+1)\begin{bmatrix} v \\ vq \end{bmatrix} = \frac{(vq+1)v!}{(vq)!(v-vq)!} \qquad (4.18)$$

Με εφαρμογή της προσέγγισης Stirling $v! \cong \sqrt{2\pi}\, e^{-v} v^{v+1/2}$ προκύπτει τελικά :

$$N < \frac{(vq+1)q^{-vq}p^{-vp}}{(2\pi vpq)^{1/2}} \qquad (4.19)$$

Κάθε κωδική λέξη που προσάγεται στην είσοδο του δυαδικού συμμετρικού διαύλου πληροφορίας μπορεί να σχετισθεί με N δυαδικές v-άδες στην έξοδο του. Από αυτές μια είναι ίδια με την κωδική λέξη και N-1 διαφοροποιούνται σε λιγότερα από τα μισά ψηφία. Επομένως η πιθανότητα να είναι μια δυαδική v-άδα στην έξοδο του δυαδικού συμμετρικού διαύλου πληροφορίας εσφαλμένη μορφή κάποιας κωδικής λέξης δίνεται από την ανισότητα :

$$p_E = p(N-1)/2^v < \frac{p(vq+1)2^{-vC}}{(2\pi vpq)^{1/2}} \qquad (4.20)$$

επειδή $q^{-vq} = 2^{-v\log_2 q}$, $p^{-vp} = 2^{-v\log_2 p}$ και $C = 1 + p\log_2 p + q\log_2 q$ bits/σύμβολο είναι η χωρητικότητα του δυαδικού συμμετρικού διαύλου πληροφορίας. Είδαμε η τεχνική τυχαίας κωδικοποίησης δεν προσφέρει τη δυνατότητα διόρθωσης σφαλμάτων. η εξ.(4.20) περιγράφει την πιθανότητα εσφαλμένης αποκωδικοποίησης και στο όριο $v \to \infty$ προκύπτει :

$$\lim_{v\to\infty}(p_E) = \frac{p}{\sqrt{2\pi p}} \lim_{v\to\infty}\left\{ \frac{vq+1}{\sqrt{vq}}\, 2^{-vC} \right\} =$$

$$= \frac{p}{\sqrt{2\pi p}} \lim_{v\to\infty}\left\{ \left(\sqrt{vq} + \frac{1}{\sqrt{vq}}\right) \frac{1}{(1+1)^{vC}} \right\} =$$

$$= \frac{\rho}{\sqrt{2\pi\rho}} \lim_{v\to\infty} \left\{ \left(\sqrt{vq} + \frac{1}{\sqrt{vq}} \right) \frac{1}{(1 + vC + \ldots)} \right\} <$$

$$< \frac{\rho}{\sqrt{2\pi\rho}} \lim_{v\to\infty} \left\{ \frac{1}{vC} \left(\sqrt{vq} + \frac{1}{\sqrt{vq}} \right) \right\} = 0 \quad .$$

Το πρώτο μέρος του θεωρήματος έχει επομένως αποδειχθεί.

Ο δίαυλος πληροφορίας διοχετεύει δυαδικά ψηφία και έχει χωρητικότητα C bits/δυαδικό ψηφίο. Η χωρητικότητα του διαύλου ανά ν-άδα δυαδικών ψηφίων είναι νC bits/ δυαδική ν-άδα. Η τεχνική τυχαίας κωδικοποίησης διαμορφώνει αλφάβητο από ρ ισοπίθανες δυαδικές ν-άδες και επομένως η εντροπία της πηγής πληροφορίας, όπως αυτή προεκτείνεται στην έξοδο του κωδικοποιητή, είναι $H(A) = \log_2\rho$ bits/ δυαδική ν-άδα. Αλλά $H(A) \leq vC$ και επομένως το μέγιστο πλήθος συμβόλων πληροφορίας είναι $\rho_{max} = 2^{vC}$.

Έστω ότι το πλήθος των συμβόλων πληροφορίας είναι :

$$\rho = \rho_{max}/v = 2^{vC}/v \qquad (4.21)$$

Η εντροπία της πηγής πληροφορίας γίνεται αντίστοιχα $H(A) = \log_2(2^{vC}/v)$ bits/ δυαδική ν-άδα ή :

$$H(A) = \frac{\log_2(2^{vC}/v)}{v} = C - \frac{\log_2 v}{v} \text{ bits/δυαδικό ψηφίο} \qquad (4.22)$$

και στο όριο $v \to \infty$ τείνει στη χωρητικότητα του διαύλου πληροφορίας. Επομένως είναι δυνατή πλήρης εκμετάλευση της χωρητικότητας αλλά τονίζεται πάλι ότι αυτό έχει προκύψει εδώ μόνο για την ειδική περίπτωση του δυαδικού συμμετρικου διαύλου πληροφορίας.

Αν το πλήθος των συμβόλων πληροφορίας είναι :

$$\rho = 2^{v(C+\varepsilon)} \qquad (4.23)$$

δηλαδή μεγαλύτερο από το μέγιστο επιτρεπτό αριθμό $\rho_{max} = 2^{vC}$, η εντροπία της

πηγής πληροφορίας υπερβαίνει τη χωρητικότητα :

$$H(A) = \log_2 \rho = vC + v\epsilon > vC \qquad (4.24)$$

Αλλά η διαπληροφορία είναι εξ ορισμού μικρότερη της χωρητικότητας :

$$I(A,B) = H(A) - H(A/B) \leq vC \qquad (4.25)$$

Αν συνδυασθούν οι εξ.(4.24),(4.25), διαπιστώνεται ότι :

$$H(A/B) > v\epsilon \qquad (4.26)$$

και με εφαρμογή της εξ.(4.8), που περιγράφει το θεώρημα Fano, προκύπτει :

$$v\epsilon < H(A/B) \leq H(\pi_E) + \pi_E \log_2(\rho-1) < 1 + \pi_E \log_2 \rho = 1 + \pi_E v(C + \epsilon)$$

Στο όριο $v \to \infty$:

$$\pi_E > \frac{\epsilon}{C + \epsilon} \qquad (4.27)$$

δηλαδή η πιθανότητα σφάλματος δεν τείνει στο μηδέν. Επομένως επαληθεύεται και το δεύτερο μέρος του θεωρήματος που αφορά στην περίπτωση $H > C$.

4.4 ΑΠΟΚΑΛΥΨΗ ΣΦΑΛΜΑΤΩΝ

Το δεύτερο θεώρημα Shannon μεταθέτει το ενδιαφέρον στη διαμόρφωση τεχνικών αποκάλυψης και διόρθωσης σφαλμάτων που συμβαίνουν κατά τη μετάδοση κωδικών μηνυμάτων στο δίαυλο πληροφορίας.

4.4.1 ΕΛΕΓΧΟΣ ΙΣΟΤΗΤΑΣ

Έστω κώδικας που αντιστοιχίζει τα σύμβολα πληροφορίας σε δυαδικές v-άδες με $v-1$

ψηφία πληροφορίας και 1 ψηφίο ελέγχου. Η τιμή του ψηφίου ελέγχου μπορεί να καθοριοθεί με το κριτήριο άρτιας / περιττής ισότητας, δηλαδή το ψηφίο ελέγχου παίρνει τιμή 0 ή 1 ώστε το συνολικό πλήθος μονάδων στη δυαδική ν-άδα να είναι άρτιο / περιττό, αντίστοιχα.

ΠΑΡΑΔΕΙΓΜΑ : Στη δυαδική 7-άδα 0101110 προσαρμόζεται όγδοο ψηφίο ελέγχου. Αν εφαρμοσθεί το κριτήριο άρτιας ισότητας, το ψηφίο ελέγχου πρέπει να είναι 0 ώστε στη δυαδική 8-άδα 01011100 να υπάρχει άρτιο πλήθος μονάδων. Με το κριτήριο περιττής ισότητας διαμορφώνεται η δυαδική 8-άδα 01011101 που περιέχει περιττό πλήθος μονάδων.

Με το κριτήριο απλής ισότητας είναι δυνατό να αποκαλυφθούν απλά σφάλματα. Είναι φανερό ότι η δυαδική 8-άδα 01011100 που διαμορφώθηκε με το κριτήριο άρτιας ισότητας στο παραπάνω παράδειγμα μπορεί να μετατραπεί με διπλό σφάλμα στη δυαδική 8-άδα 01101100 που ικανοποιεί επίσης το κριτήριο άρτιας ισότητας παρόλο που τα δυαδικά ψηφία στην τρίτη και τέταρτη θέση έχουν αλλοιωθεί. Επομένως με ένα ψηφίο ελέγχου δεν είναι δυνατό να αποκαλυφθούν διπλά σφάλματα. Αν συμβεί και τρίτο σφάλμα, το κριτήριο απλής ισότητας ενεργοποιείται αλλά δεν είναι δυνατό να αποκαλυφθεί ο ακριβής αριθμός σφαλμάτων. Γενικά το κριτήριο απλής ισότητας ενεργοποιείται μόνο για περιττό πλήθος σφαλμάτων και δεν καθορίζει ούτε τον ακριβή αριθμό σφαλμάτων ούτε τη θέση των αλλοιωμένων ψηφίων.

Είναι φανερό ότι προσθέτοντας ψηφία ελέγχου αυξάνει η πιθανότητα αλλοίωσης της κωδικής λέξης κατά τη μετάδοση. Αν p, q = 1 − p είναι αντίστοιχα η πιθανότητα ορθής / εσφαλμένης μετάδοσης κάθε δυαδικού ψηφίου, το πλήθος σφαλμάτων κατά τη μετάδοση δυαδική ν-άδας περιγράφεται με διακριτή τυχαία μεταβλητή που ακολουθεί διωνυμική κατανομή. Η πιθανότητα να αλλοιωθούν ξ δυαδικά ψηφία κατά τη μετάδοση της δυαδικής ν-άδας δίνεται από την παρακάτω έκφραση :

$$\Pi(\xi/\nu) = \binom{\nu}{\xi} p^{\nu-\xi} q^{\xi} \quad ; \quad \xi = 0,\ 1,\ \ldots,\ \nu \qquad (4.28)$$

όπου $\binom{\nu}{\xi} = \nu!/\xi!(\nu-\xi)!$ είναι οι συνδυασμοί ν πραγμάτων ανά ξ. Με εφαρμογή της εξ.(4.28) προκύπτει η πιθανότητα απλού σφάλματος στη δυαδική 7-άδα $\Pi(1/7) = \binom{7}{1} p^{6} q$. Με προσθήκη ενός ψηφίου ελέγχου προκύπτει δυαδική 8-άδα και η πιθανότητα να συμβεί απλό σφάλμα σε κάποιο από τα επτά ψηφία πληροφορίας και επιπλέον σφάλμα στο μοναδικό ψηφίο ελέγχου, είναι μικρότερη από

$\Pi(2/8) = \binom{8}{2} p^6 q^2$. Αν q = 0.01, η σχετική αύξηση της πιθανότητας εσφαλμένης μετάδοσης της κωδικής λέξης είναι $\Pi(2/8)/\Pi(1/7) = 0.04$ ή **4 %** . Αλλά στη δυαδική 8-άδα υπάρχει η ελκυστική δυνατότητα αποκάλυψης απλού σφάλματος ή περιττού πλήθους σφαλμάτων και η αύξηση της πιθανότητας σφάλματος κατά **4 %** εκπροσωπεί σχετικά ασήμαντο τίμημα.

Είναι φανερό ότι με περισσότερα ψηφία ελέγχου θα υπάρχει δυνατότητα αποκάλυψης πολλαπλών σφαλμάτων. Αν δεν υπάρχουν ψηφία ελέγχου, η μόνη δυνατότητα για τη βελτίωση της αξιοπιστίας της επικοινωνίας είναι να επαναληφθεί η εκπομπή του μηνύματος. Η τακτική αυτή, εκτός από χρονοβόρα, σε πολλές εφαρμογές δεν είναι καν εφικτή.

4.4.2 ΔΙΔΙΑΣΤΑΤΟΣ ΕΛΕΓΧΟΣ ΙΣΟΤΗΤΑΣ ΣΕ ΟΡΘΟΓΩΝΙΚΟ ΚΩΔΙΚΑ

Ο Σ-δίαυλος (βλ. §2.3.6) εμφανιζει στην έξοδο του ιδιαίτερο σύμβολο κάθε φορά που γίνεται σφαλμα μετάδοσης. Στην τυπική λειτουργία $\beta_1, \beta_3 \in \{ 0, 1 \}$ και β_2= " ". Επομένως εσφαλμένη μετάδοση του μηνύματος 011100101 θα μπορούσε να είναι 01 100101 που δείχνει απλό σφάλμα στο τρίτο ψηφίο. Διόρθωση του σφάλματος είναι δυνατή μόνον αν στο τελος του μηνύματος προστεθεί ψηφίο ελέγχου και εφαρμοσθεί το κριτήριο απλής, έστω άρτιας, ισότητας. Για το συγκεκριμένο παράδειγμα είναι :

0111001011 η είσοδος
01 1001011 έξοδος με απλό σφάλμα και
0111001011 η διορθωμένη έξοδος

επειδή το πλήθος των μονάδων πρέπει να είναι άρτιο. Γενικά, αν ν δυαδικά ψηφία μεταφέρουν πληροφορία και προστεθεί ένα ψηφίο ελέγχου, προκύπτει *περίσσεια* $(\nu+1)/\nu = 1 + 1/\nu$. Ο *ρυθμός πληροφορίας* ορίζεται σαν ποσοστό των ψηφίων πληροφορίας στο συνολο των δυαδικών ψηφίων της κωδικής λέξης και είναι το αντιστροφο μέγεθος της περίσσειας. Στο συγκεκριμένο παράδειγμα ο ρυθμός πληροφορίας είναι $\nu/(\nu+1) \simeq 1 - 1/\nu$ με την προϋπόθεση $\nu \gg 1$.

Ο έλεγχος ισοτητας μπορεί να επεκταθεί σε δύο διαστάσεις οπότε δημιουργείται η

δυνατότητα διόρθωσης δυπλών σφαλμάτων. Η τεχνική αυτή, που είναι γνωστή σαν *ορθογωνική κωδικοποίηση*, προσαρμόζεται στη λειτουργία του Σ-διαύλου. Η διαδικασία κατασκευής του ορθογωνικού κώδικα περιγράφεται με τα παρακάτω βήματα που συνοδεύονται και με συγκεκριμένο παράδειγμα.

(i) Χρησιμοποιούνται μ κωδικές λέξεις ν δυαδικών ψηφίων που διατάσσονται η μια κάτω από την άλλη. Διαμορφώνεται έτσι ένα ορθογωνικό πλέγμα μν δυαδικών ψηφίων.

Κωδική λέξη		Πλέγμα δυαδικών ψηφίων ν					
1		1	0	1	1	0	1
2		0	1	0	0	0	1
3	μ	1	0	0	1	1	0
4		0	1	1	1	0	0
5		0	0	1	1	1	0

(ii) Σε κάθε σειρά και στήλη του πλέγματος προστίθεται ψηφίο ελέγχου. Το επεκτεταμένο πλέγμα περιέχει επομένως (μ+1)(ν+1) δυαδικά ψηφία.

Κωδική λέξη		Επεκτεταμένο πλέγμα δυαδικών ψηφίων ν+1						
1		1	0	1	1	0	1	0
2		0	1	0	0	0	1	0
3	μ+1	1	0	0	1	1	0	1
4		0	1	1	1	0	0	1
5		0	0	1	1	1	0	1
		0	0	1	0	0	0	1

Εξοδος Σ - διαύλου

1		1	0	1	1	0		0
2		0	1		0	0		0
3	μ+1	1	0	0	1	1	0	1
4		0	1		1	.	0	1
5		0	0	1	1	1	0	1
		0	0	1	0	0	0	1

(iii) Στην έξοδο του Σ-διαύλου εμφανίζονται κενά στις θέσεις των σφαλμάτων.

(iv) Εφαρμόζοντας έλεγχο ισότητας κατά τις δύο διαστάσεις του πλέγματος είναι δυνατό να διορθωθούν μέχρι και δυτλά σφάλματα σε κάθε κωδική λέξη. Η διαδικασία διόρθωσης εκκινεί από τη σειρά / στήλη που εμφανίζει απλό σφάλμα. Στο συγκεκριμένο παράδειγμα διορθώνεται αρχικά το απλό σφάλμα στην πρώτη σειρά, μετά το σφάλμα που απομένει στην έκτη στήλη κ.λπ.

Αν p, q = 1 − p είναι οι πιθανότητες ορθής και εσφαλμένης μετάδοσης, αντίστοιχα, οποιουδήποτε δυαδικού ψηφίου, σε κάθε κωδική λέξη ν+1 ψηφίων συμβαίνουν κατά μέσο όρο (ν+1)q σφάλματα και στο πλέγμα που συγκροτείται από μ+1 κωδικές λέξεις στην έξοδο του Σ-διαύλου θα υπάρχουν κατά μέσο όρο (μ+1)(ν+1)q κενά. Εφόσον κάθε σειρά του πλέγματος περιέχει ένα ψηφίο ελέγχου, είναι δυνατό να διορθωθούν απλά σφάλματα. Επομένως σε κάθε σειρά απομένουν μετά τον έλεγχο ισότητας κατά μέσο όρο $(\nu+1)q - (\nu+1)p^{\nu}q \simeq \nu(\nu+1)q^2 < (\nu+1)^2q^2$ σφάλματα. Αν q_1 είναι η πιθανότητα σφάλματος σε κάθε δυαδικό ψηφίο μετά το έλεγχο ισότητας που διορθώνει απλά σφάλματα σε κάθε σειρά, το μέσο πλήθος κενών σε κάθε σειρά είναι $(\nu+1)q_1 < (\nu+1)^2q^2$, δηλαδή :

$$q_1 < (\nu+1)q^2 \tag{4.29}$$

Η ύπαρξη ενός ψηφίου ελέγχου σε κάθε σειρά έχει σαν αποτέλεσμα να απομένουν κατά μέσο όρο $(\mu+1)(\nu+1)q_1 < (\mu+1)(\nu+1)^2q^2$ κενά στο πλέγμα.

Επεκτείνοντας τον παραπάνω συλλογισμό, διαπιστώνεται ότι η ύπαρξη ενός ψηφίου ελέγχου σε κάθε στήλη έχει σαν αποτέλεσμα να διορθώνονται απλά σφάλματα σε κάθε στήλη, δηλαδή να απομένουν σε κάθε στήλη κατά μέσο όρο $(\mu+1)q_1 - (\mu+1)(1-q_1)^{\mu}q_1 \simeq \mu(\mu+1)q_1^2 < (\mu+1)^2q_1^2$ κενά. Αν q_2 είναι η πιθανότητα σφάλματος σε κάθε δυαδικό ψηφίο μετά τον έλεγχο ισότητας που διορθώνει απλά σφάλματα σε κάθε στήλη, το μέσο πλήθος σφαλμάτων σε κάθε στήλη είναι $(\mu+1)q_2 < (\mu+1)^2q_1^2$, δηλαδή :

$$q_2 < (\mu+1)q_1^2 < (\mu+1)(\nu+1)^2q^4 \tag{4.30}$$

Στο πλέγμα απομένουν τελικά κατά μέσο όρο $(\nu+1)(\mu+1)q_2 < (\mu+1)^2(\nu+1)^3q^4$ κενά.

Αν q = 0.01 και μ = ν = 9, η παραπάνω ανάλυση δείχνει ότι η πιθανότητα σφάλματος

σε κάθε δυαδικό ψηφίο του πλέγματος είναι :

$q = 0.01$ χωρίς έλεγχο ισότητας
$q_1 < 0.001$ με έλεγχο ισότητας σε κάθε σειρά
$q_2 < 0.00001$ με έλεγχο ισότητας σε κάθε σειρά και στήλη

Επομένως με διδιάστατο έλεγχο ισότητας βελτιώνεται η πιθανότητα σφάλματος σε κάθε δυαδικό ψηφίο τουλάχιστο 1000 φορές. Το τίμημα είναι ελάττωση του ρυθμού πληροφορίας κατά $1 - \mu\nu/(\mu+1)(\nu+1)$, δηλαδή για το συγκεκριμένο παράδειγμα κατά 0.19 ή περίπου 20 % .

4.5 ΔΙΟΡΘΩΣΗ ΣΦΑΛΜΑΤΩΝ

Η απλούστερη τεχνική διόρθωσης σφαλμάτων στηρίζεται στην αρχή της ελάχιστης απόστασης μεταξύ της εσφαλμένης δυαδικής ν-άδας και της αντίστοιχης κωδικής λέξης.

ΟΡΙΣΜΟΣ : *Απόσταση Hamming* μεταξύ των δυαδικών ν-άδων $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\nu)$ και $\beta = (\beta_1, \beta_2, \ldots, \beta_\nu)$ είναι το μέγεθος $D(\alpha,\beta) = (\alpha_1 \oplus \beta_1) + (\alpha_2 \oplus \beta_2) + \ldots + (\alpha_\nu \oplus \beta_\nu)$, όπου $\oplus$ είναι το σύμβολο της δυαδικής πρόσθεσης ($0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$).

Οι ιδιότητες της απόστασης Hamming είναι :

- $D(\alpha,\beta) = 0$ αν $\alpha = \beta$
- $D(\alpha,\beta) = D(\beta,\alpha) > 0$ αν $\alpha \neq \beta$
- $D(\alpha,\beta) + D(\beta,\gamma) \geq D(\alpha,\gamma)$

όπου α, β, γ είναι δυαδικές ν-άδες. Είναι φανερό ότι η απόσταση Hamming υποδηλώνει το πλήθος των δυαδικών ψηφίων που διαφοροποιούνται στις δυαδικές ν-άδες. Αν $D(\alpha,\beta) = 0$, οι δυαδικές ν-άδες είναι ίδιες.

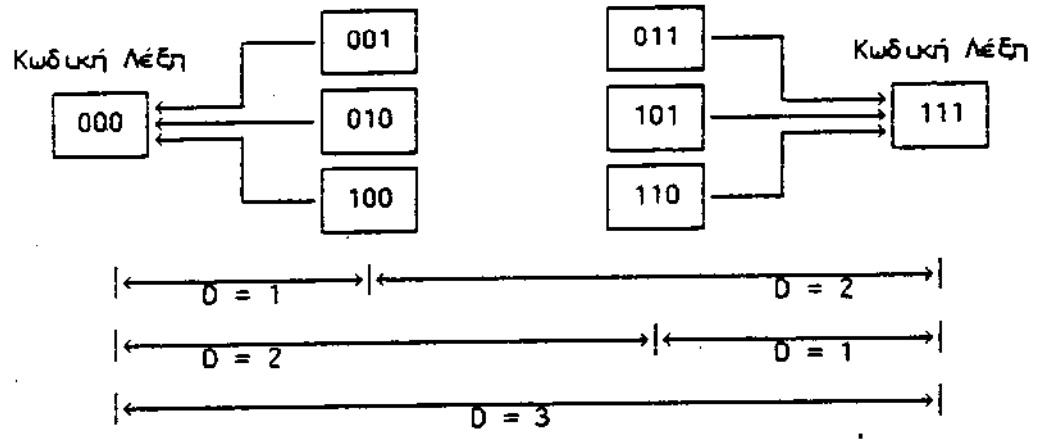
ΠΑΡΑΔΕΙΓΜΑ : Η απόσταση Hamming μεταξύ δυαδικών τριάδων είναι από 0 έως 3 όπως διαπιστώνεται από τον πίνακα 4.1.

Πίνακας 4.1

Απόσταση Hamming δυαδικών τριάδων

α	β	D(α,β)
000	000	0
111	111	0
110	111	1
110	101	2
010	101	3

Έστω ότι κατασκευάζεται δυαδικός κώδικας με ελάχιστη απόσταση Hamming μεταξύ κωδικών λέξεων $D_{min} = 3$. Αν γίνει δεκτό ότι κατά τη μετάδοση συμβαίνουν μόνο απλά σφάλματα, τότε κάθε δυαδική ν-άδα που δεν είναι κωδική λέξη αναγνωρίζεται σαν εσφαλμένη μορφή εκείνης της κωδικής λέξης από την οποία απέχει απόσταση Hamming D = 1. Ο κώδικας επιτρέπει τη διόρθωση απλών σφαλμάτων χωρίς να αναγνωρίζεται το αλλοιωμένο ψηφίο. Στην περίπτωση δυαδικών τριάδων υπάρχουν μόνο δύο κωδικές λέξεις με απόσταση Hamming $D_{min} = 3$. Η διαδικασία διόρθωσης απλών σφαλμάτων σε δυαδικές τριάδες περιγράφεται στο διάγραμμα που ακολουθεί (σχ. 4.2).



Σχ. 4.2 Διόρθωση δυαδικών τριάδων με απλό σφάλμα.

Με επέκταση του παραπάνω συλλογισμού διαπιστώνεται εύκολα ότι είναι δυνατό να διορθώνονται σ εσφαλμένα ψηφία σε κωδικές λέξεις με ελάχιστη απόσταση Hamming :

$$D_{min} \geq 2\sigma + 1 \qquad (4.31)$$

Το πλήθος των δυαδικών ν-άδων που είναι δυνατό να χρησιμοποιηθούν σαν κωδικές

λέξεις με αμοιβαία απόσταση όπως απαιτεί η εξ.(4.31) προσδιορίζεται με τον εξής απλό συλλογισμό. Υπάρχουν συνολικά 2^v δυαδικές ν-άδες. Το πλήθος των δυαδικών ν-άδων που διαφοροποιούνται από κάποια δυαδική ν-άδα αναφοράς σε σ ψηφία ή λιγότερα είναι $N = \binom{v}{0} + \binom{v}{1} + \ldots + \binom{v}{\sigma}$. Αν λοιπόν χρησιμοποιηθούν ρ δυαδικές ν-άδες σαν κωδικές λέξεις και σε κάθε μία από αυτές αντιστοιχούν N δυαδικές ν-άδες με απόσταση Hamming από την κωδική λέξη $D \leq \sigma$, πρέπει $\rho N \leq 2^v$:

$$\rho \leq \frac{2^v}{\sum_{i=0}^{\sigma} \binom{v}{i}} \qquad (4.32)$$

Η εξ.(4.32) περιγράφει την αναγκαία αλλά όχι και ικανή συνθήκη για τη δυνατότητα διόρθωσης σ αλλοιωμένων ψηφίων σε κωδικές λέξεις ν ψηφίων που αντιστοιχούν σε ρ σύμβολα πληροφορίας. Αν $v = 4$ και $\sigma = 1$, η εξ.(4.32) καθορίζει $\rho \leq 3.2$. Είναι όμως εύκολο να διαπιστωθεί ότι υπάρχουν μόνο δύο δυαδικές τετράδες με ελάχιστη απόσταση Hamming $D_{min} = 3$, που απαιτείται για διόρθωση απλών σφαλμάτων.

4.6 ΚΩΔΙΚΑΣ HAMMING

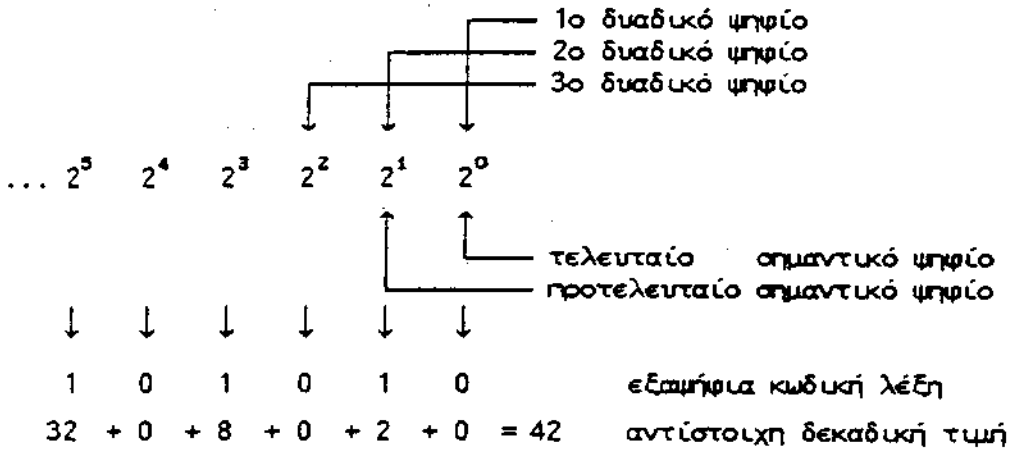
Η τεχνική κωδικοποίησης Hamming επιτρέπει την αναγνώριση της θέσης των αλλοιωμένων ψηφίων. Για την κατανόηση της τεχνικής δίνονται στο σχ. 4.3 οι απαραίτητες έννοιες.

Οι κώδικες Hamming με μ ψηφία πληροφορίας και ν-μ ψηφία ελέγχου ανά κωδική λέξη, δομούνται σε τέσσερα βήματα :

(i) Μέσω των ψηφίων ελέγχου συγκροτείται το *σύνδρομο*, δηλαδή ένας αριθμός ελέγχου με ν-μ δυαδικά ψηφία. Η δεκαδική τιμή του συνδρόμου αντιστοιχεί στη θέση του αλλοιωμένου ψηφίου. Επομένως το σύνδρομο πρέπει να παίρνει τόσες τιμές όσες είναι απαραίτητο για να περιγράφουν τα ενδεχόμενα (α) απλό σφάλμα σε οποιοδήποτε από τα μ ψηφία πληροφορίας, (β) απλό σφάλμα σε οποιοδήποτε από τα ν-μ ψηφία ελέγχου και (γ) κανένα σφάλμα μετάδοσης. δηλαδή :

$$2^{\nu-\mu} \geq \mu + (\nu-\mu) + 1 = \nu + 1 \qquad (4.33)$$

(ii) Οι ν θέσεις δυαδικών ψηφίων σε κάθε κωδική λέξη αριθμούνται από 1 μέχρι ν ξεκινώντας από το τελευταίο σημαντικό ψηφίο (σχ. 4.3). Τα ν−μ ψηφία ελέγχου συμβολίζονται $E_0, E_1, \ldots, E_{\nu-\mu-1}$ και τοποθετούνται στις θέσεις με τακτικό αριθμό $2^0 = 1, 2^1 = 2, \ldots, 2^{\nu-\mu-1}$, αντίστοιχα. Τα ψηφία πληροφορίας, που συμβολίζονται $\Pi_0, \Pi_1, \ldots, \Pi_{\mu-1}$ τοποθετούνται στις ενδιάμεσες κενές θέσεις, δηλαδή στην 3η, 5η, 6η, 7η, 9η, ... Στις ανώτερες θέσεις τοποθετούνται τα περισσότερο σημαντικά ψηφία.



α	...	10	9	8	7	6	5	4	3	2	1
β	...	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001
γ	...	Π_5	Π_4	E_3	Π_3	Π_2	Π_1	E_2	Π_0	E_1	E_0

α : τακτικός αριθμός θέσης (δεκαδική μορφή)
β : τακτικός αριθμός θέσης (δυαδική μορφή)
γ : ψηφία πληροφορίας Π_i, $i = 0, 1, 2, \ldots, \mu-1$
ψηφία ελέγχου E_i, $i = 0, 1, 2, \ldots, \nu-\mu-1$

Σχ. 4.3 Δομή κωδικών λέξεων

(iii) Αν εφαρμοσθεί άρτια ισότητα, τα ψηφία ελέγχου παίρνουν τέτοιες τιμές ώστε το πλήθος των μονάδων στις θέσεις που το καθένα ελέγχει να είναι άρτιο. Στον πίνακα 4.2 δίνονται οι θέσεις για τις οποίες είναι υπεύθυνο κάθε ψηφίο ελέγχου. Παρατηρείται ότι το ψηφίο ελέγχου E_i, $i = 0, 1, 2, \ldots, \nu-\mu-1$, ελέγχει όλες τις

θέσεις με δυαδικό τακτικό αριθμό που έχει μονάδα στην 2^i-οστή θέση του. Μερικές από τις εξισώσεις ελέγχου δίνονται παρακάτω :

$$E_0 \oplus \Pi_0 \oplus \Pi_1 \oplus \Pi_3 \oplus \Pi_4 \oplus \ldots = Z_0$$

$$E_1 \oplus \Pi_0 \oplus \Pi_2 \oplus \Pi_3 \oplus \Pi_5 \oplus \ldots = Z_1 \qquad (4.34)$$

$$E_2 \oplus \Pi_1 \oplus \Pi_2 \oplus \Pi_3 \oplus \Pi_7 \oplus \ldots = Z_2$$

και εφόσον ικανοποιούνται τα κριτήρια άρτιας ισότητας (ορθή μετάδοση) πρέπει $Z_0 = Z_1 = Z_2 = 0$.

Πίνακας 4.2

Ελεγχόμενες θέσεις από ψηφία ελέγχου E_0, E_1, E_2

Τακτικός Αριθμός Θέσης		Ψηφίο Ελέγχου		
Δεκαδική Μορφή	Δυαδική Μορφή	E_0	E_1	E_2
1	0001	X		
2	0010		X	
3	0011	X	X	
4	0100			X
5	0101	X		X
6	0110		X	X
7	0111	X	X	X
8	1000			
9	1001	X		
10	1010		X	
11	1011	X	X	
12	1100			X
13	1101	X		X
14	1110		X	X
15	1111	X	X	X

(iv) Με τα ψηφία Z_0, Z_1, Z_2, ... διαμορφώνεται ο αριθμός ελέγχου $\Sigma = \ldots Z_2 Z_1 Z_0$. (σύνδρομο) και η δεκαδική τιμή του δείχνει τη θέση του αλλοιωμένου ψηφίου. Αν

$\Sigma = 0$, δεν έχει γίνει σφάλμα κατά τη μετάδοση της κωδικής λέξης.

ΠΑΡΑΔΕΙΓΜΑ : Εστω 16 σύμβολα πληροφορίας που εκπροσωπούνται από τις 16 δυαδικές τετράδες. Η εξ.(4.33) υποδεικνύει ότι απαιτούνται 3 ψηφία ελέγχου για την κατασκευή του κώδικα Hamming. Επομένως οι κωδικές λέξεις θα είναι δυαδικές 7-άδες. Είναι γνωστό ότι υπάρχουν $2^7 = 128$ δυαδικές 7-άδες και από αυτές θα χρησιμοποιηθούν μόνο 16 για να εκπροσωπούν τα σύμβολα πληροφορίας. Τα ψηφία ελέγχου E_0, E_1 ,E_2 θα τοποθετηθούν στην 1η, 2η, 4η θέση, αντίστοιχα, ενώ τα ψηφία πληροφορίας Π_0, Π_1, Π_2, Π_3 θα τοποθετηθούν στην 3η, 5η, 6η, 7η θέση, αντίστοιχα.Επομένως η κωδική λέξη έχει τη μορφή $\Pi_3\Pi_2\Pi_1E_2\Pi_0E_1E_0$. Τα ψηφία ελέγχου προσδιορίζονται από τις εξ.(4.34) με $Z_0 = Z_1 = Z_2 = 0$. Εστω λοιπόν η λέξη πληροφορίας $\Pi_3\Pi_2\Pi_1\Pi_0 = 0010$. Τα ψηφία ελέγχου ικανοποιούν τις εξισώσεις :

$$E_0 = \Pi_0 \oplus \Pi_1 \oplus \Pi_3 = 0 \oplus 1 \oplus 0 = 1$$

$$E_1 = \Pi_0 \oplus \Pi_2 \oplus \Pi_3 = 0 \oplus 0 \oplus 0 = 0 \qquad (4.35)$$

$$E_2 = \Pi_1 \oplus \Pi_2 \oplus \Pi_3 = 1 \oplus 0 \oplus 0 = 1$$

και επομένως η κωδική λέξη είναι 0011001. Αν στην έξοδο του διαύλου φθάσει η δυαδική 7-άδα 0111001, οι εξ.(4.34) υποδεικνύουν ότι :

$$Z_0 = E_0 \oplus \Pi_0 \oplus \Pi_1 \oplus \Pi_3 = 1 \oplus 0 \oplus 1 \oplus 0 = 0$$

$$Z_1 = E_1 \oplus \Pi_0 \oplus \Pi_2 \oplus \Pi_3 = 0 \oplus 0 \oplus 1 \oplus 0 = 1 \qquad (4.36)$$

$$Z_2 = E_2 \oplus \Pi_1 \oplus \Pi_2 \oplus \Pi_3 = 1 \oplus 1 \oplus 1 \oplus 0 = 1$$

και επομένως το σύνδρομο είναι $\Sigma = 110$ ή $\Sigma = 6$ που δείχνει ότι έγινε σφάλμα στην 6η θέση. Επομένως η ορθή δυαδική 7-άδα είναι 0011001.

4.7 ΑΣΚΗΣΕΙΣ

1. Δίνεται το παρακάτω μητρώο διαύλου :

$$\Pi(B/A) = \begin{bmatrix} 0.5 & 0.3 & 0.2 \\ 0.2 & 0.3 & 0.5 \\ 0.3 & 0.3 & 0.4 \end{bmatrix}$$

Αν τα σύμβολα εισόδου είναι ισοπίθανα, να καθορισθεί το σχήμα αποκωδικοποίησης που αντιστοιχεί στο κριτήριο του τέλειου παρατηρητή και στο κριτήριο της μέγιστης πιθανοφάνειας. Να υπολογισθεί η πιθανότητα εσφαλμένης αποκωδικοποίησης σε κάθε περίπτωση.

2. Η πιθανότητα ξ σφαλμάτων κατά τη μετάδοση δυαδικών ν-άδων περιγράφεται με τη διωνυμική κατανομή :

$$\Pi(\xi/\nu) = \begin{pmatrix} \nu \\ \xi \end{pmatrix} p^{\nu-\xi}(1-p)^{\xi} \quad ; \quad \xi = 0, 1, \ldots, \nu$$

όπου p είναι η πιθανότητα ορθής μετάδοσης οποιουδήποτε δυαδικού ψηφίου. Να υπολογισθεί το μέσο πλήθος σφαλμάτων κατά τη μετάδοση των δυαδικών ν-άδων.

3. Δυαδικός συμμετρικός δίαυλος πληροφορίας χρησιμοποιείται γιά τη μετάδοση χαρακτήρων ASCII, δηλαδή δυαδικων 8-άδων. Αν η πηγή πληροφορίας στην είσοδο παράγει μόνο τα κεφαλαία γράμματα του Αγγλικού αλφαβήτου και η πιθανότητα σφάλματος κατά τη μετάδοση οποιουδήποτε δυαδικού ψηφίου είναι 2 %, να εκτιμηθεί η πιθανότητα εσφαλμένης μετάδοσης κάθε συμβόλου πληροφορίας.

4. Να υπολογισθεί το μέγιστο δυνατό πλήθος κωδικών λέξεων σε κώδικα διόρθωσης απλού σφάλματος με λέξεις μήκους πέντε δυαδικών ψηφίων.

5. Το παρακάτω πλέγμα δυαδικών ψηφίων εμφανίζεται στην έξοδο Σ-διαύλου πληροφορίας που τροφοδοτείται από ορθογωνικό κωδικοποιητή. Να διορθωθούν τα σφάλματα και να γίνει αποκωδικοποίηση με την υπόθεση ότι για την κατασκευή των κωδικών λέξεων χρησιμοποιήθηκε κώδικας Hamming.

1	1		1	1	1	1	1
1	0		1		0	1	1
0	1	1	1		0	1	1
0		0	0	1	1		1
1	1	1	1	0	1		0
1	1	1		0	0	1	0
	1	0	0	0	1	1	0
1		1	0	0	0	1	

6. Να σχεδιασθεί κώδικας Hamming με 5-ψήφιες λέξεις και δυνατότητα διόρθωσης απλών σφαλμάτων. Αν η πιθανότητα σφάλματος κατά τη μετάδοση οποιουδήποτε δυαδικού ψηφίου είναι 1 %, να υπολογισθεί η πιθανότητα εσφαλμένης αποκωδικοποίησης

7. Τα μηνύματα 1111111, 1001111, 011100010111110 έχουν κωδικοποιηθεί κατά Hamming. Να διορθωθούν τυχόντα σφάλματα και να αποκωδικοποιηθούν.

8. Να σχεδιασθεί κώδικας Hamming με δύο ψηφία ελέγχου. Να σχολιασθεί η μορφή των κωδικοποιημένων μηνυμάτων.

9. Το κωδικό μήνυμα 11101010000000111011010100 κατασκευάσθηκε με κώδικα Hamming. Ο παρακάτω πίνακας, που είναι το κλειδί του αρχικού δυαδικού κώδικα, υποδεικνύει ότι κάθε κωδική λέξη περιέχει 5 δυαδικά ψηφία. Να αποκαλυφθεί το μήνυμα πληροφορίας αφού διορθωθούν σφάλματα.

A	00000	I	01111	Q	10011	Y	11100
B	10000	J	11111	R	00011	Z	01100
C	01000	K	00111	S	11011	$	10100
D	00100	L	01011	T	10111	&	11000
E	00010	M	01101	U	10001	#	11110
F	00001	N	01110	V	10010	%	11101
G	01010	O	00101	W	11001	=	10110
H	00110	P	01001	X	10101	"	11010

Κεφάλαιο Πέντε

ΑΛΓΕΒΡΙΚΗ ΚΩΔΙΚΟΠΟΙΗΣΗ

5.1 ΕΙΣΑΓΩΓΗ

Η ανάπτυξη κωδίκων που προσφέρουν τη δυνατότητα διόρθωσης πολλαπλών σφαλμάτων εμπλέκει σύνθετες μαθηματικές τεχνικές από την άλγεβρα των πεπερασμένων πεδίων (Galois) και τη θεωρία πρώτων πολυωνύμων. Στοιχεία για τα δύο αυτά μαθηματικά θέματα παρουσιάζονται σε παραρτήματα στο τέλος του κεφαλαίου. Είναι προφανές ότι όσα αναφέρονται εκεί αποτελούν την ελάχιστη βάση για τη μελέτη της δομής των αλγεβρικών κωδίκων.

Η αλγεβρική κωδικοποίηση αναπτύσσεται με εξαιρετική ταχύτητα και ήδη έχει διογκωθεί τόσο ώστε το κεφάλαιο αυτό να δίνει μόνο την ελάχιστη εικόνα της περιοχής.

5.2 ΚΩΔΙΚΕΣ ΟΜΑΔΑΣ

Είναι δομικοί κώδικες. Αν χρησιμοποιείται το δυαδικό αλφάβητο $\Delta_1 = \{ 0, 1 \}$ και το μήκος των κωδικών λέξεων είναι v, τότε από το σύνολο των 2^v δυαδικών v-άδων

επιλέγονται 2^{μ} ($\mu \leq \nu$) κωδικές λέξεις. Σε κάθε κωδική λέξη υπάρχουν μ ψηφία πληροφορίας και ν−μ ψηφία ελέγχου. Ο κώδικας λειτουργεί με *περίσσεια* ν/μ και *ρυθμό πληροφορίας* (*απόδοση*) μ/ν.

Το κωδικό αλφάβητο Δ_1, εφοδιασμένο με τις πράξεις της άλγεβρας Bool :

$$\begin{array}{ll} 0 \oplus 1 = 1 & 0 \cdot 1 = 0 \\ 1 \oplus 0 = 1 & 1 \cdot 0 = 0 \\ 1 \oplus 1 = 0 & 1 \cdot 1 = 1 \\ 0 \oplus 0 = 0 & 0 \cdot 0 = 0 \end{array} \qquad (5.1)$$

ικανοποιεί όλες τις προυποθέσεις του ορισμού ενός πεδίου (βλ. §5.II). Το απλούστατο αυτό πεδίο είναι γνωστό σαν πεδίο Galois και συμβολίζεται GF(2).

Το σύνολο Δ_ν των δυαδικών ν−άδων αποτελεί αβελιανή ομάδα ως προς τη δυαδική πρόσθεση $\oplus$ επειδή ικανοποιεί τις προϋποθέσεις που αναφέρονται στην §5.I. Αυτό είναι εύκολο να ελεγχθεί στην απλή περίπτωση δυαδικών τριάδων Δ_3 = { 000, 001, 010, 100, 011, 101, 110, 111 } :

(i) Αν $\alpha,\beta \in \Delta_3$, τότε $\alpha \oplus \beta$ ($= \beta \oplus \alpha$) $\in \Delta_3$ (π.χ., για $\alpha = 010$ και $\beta = 100$, $\alpha \oplus \beta = 110 = \beta \oplus \alpha \in \Delta_3$).

(ii) Αν $\alpha, \beta, \gamma \in \Delta_3$, τότε $(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma)$ (π.χ., για $\alpha = 111$, $\beta = 110$ και $\gamma = 101$, $(\alpha \oplus \beta) \oplus \gamma = 100 = \alpha \oplus (\beta \oplus \gamma)$).

(iii) Το σύνολο Δ_3 διαθέτει ουδέτερο στοιχείο. Αυτό είναι η ν−άδα που περιέχει μόνο μηδενικά (π.χ., 001 ⊕ 000 = 000 ⊕ 001 = 001).

(iv) Κάθε ν−άδα ταυτίζεται με την αντίστροφη (αντίθετη) της (π.χ., 011 ⊕ 011 = 000).

Είναι προφανές ότι το σύνολο Δ_3 είναι κλειστό ως προς το βαθμωτό πολλαπλασιασμό με στοιχεία του δυαδικού συνόλου Δ_1 . Δηλαδή, αν $\alpha \in \Delta_3$ και $\kappa \in \Delta_1$, τότε $\kappa \cdot \alpha \in \Delta_3$ (π.χ., από το στοιχείο $101 \in \Delta_3$ προκύπτουν τα στοιχεία $101 = 1 \cdot 101$ και

$000 = 0 \cdot 101$ που ανήκουν στο συνόλο Δ_3) .

Οι δυαδικές ν-άδες είναι δυνατό να θεωρηθούν σαν διανύσματα ν-τάξεως. Κατ' επέκταση των παραπάνω το σύνολο Δ_ν είναι κλειστό ως προς τη δυαδική πρόσθεση $\oplus$ και το βαθμωτό πολλαπλασιασμό με στοιχεία του συνόλου Δ_1 . Κατά συνέπεια τα διανύσματα ν-τάξεως ορίζουν διανυσματικό χώρο, έστω V_ν, επί του πεδίου GF(2) και ισχύουν όλες οι ιδιότητες που αναφέρονται στην §5.III για διανυσματικούς χώρους. Οι ιδιότητες αυτές επαναλαμβάνονται εδώ προσαρμοσμένες στην ορολογία των δομικών κωδίκων :

(i) Κάθε γραμμικός συνδυασμός κωδικών λέξεων είναι κωδική λέξη.

(ii) Οι κωδικές λέξεις $X_1, X_2, \ldots, X_\mu$ είναι γραμμικά ανεξάρτητες αν υπάρχουν μ δυαδικά ψηφία $\kappa_1, \kappa_2, \ldots, \kappa_\mu$, που δεν είναι όλα μηδέν, ώστε $\kappa_1 \cdot X_1 \oplus \kappa_2 \cdot X_2 \oplus \ldots \oplus \kappa_\mu \cdot X_\mu = 0$.

(iii) Είναι προφανές ότι υπάρχουν λιγότερες από 2^ν γραμμικά ανεξάρτητες κωδικές λέξεις μήκους ν δυαδικών ψηφίων. Η *διάσταση* του κώδικα, δηλαδή το μέγιστο πλήθος των γραμμικά ανεξάρτητων κωδικών λέξεων, είναι ν. Αυτό διαπιστώνεται θεωρώντας τις παρακάτω ν κωδικές λέξεις μήκους ν δυαδικών ψηφίων :

$$\begin{array}{c} \\ \nu \end{array} \overset{\nu}{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \ldots 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \ldots 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \ldots 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \ldots 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \ldots 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & 0 \ldots 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \ldots 0 & 1 \end{bmatrix}}$$

που αντιστοιχούν στα μοναδιαία διανύσματα κατά τους άξονες ν-διάστατου Ευκλείδιου χώρου.

(iv) Αν κάθε κωδική λέξη προκύπτει σαν γραμμικός συνδυασμός των ανεξάρτητων κωδικών λέξεων $X_1, X_2, \ldots, X_\mu$, τότε οι τελευταίες αποτελούν *βάση* του κώδικα. Αν

$X_\lambda = (\kappa_{\lambda 1}, \kappa_{\lambda 2}, \ldots, \kappa_{\lambda v})$, $\lambda = 1, 2, \ldots, \mu$, το μxν μητρώο

$$K = \begin{bmatrix} \kappa_{11} & \kappa_{12} & \ldots & \kappa_{1v} \\ \kappa_{21} & \kappa_{22} & \ldots & \kappa_{2v} \\ \kappa_{31} & \kappa_{32} & \ldots & \kappa_{3v} \\ \ldots & \ldots & \ldots & \ldots \\ \kappa_{\mu 1} & \kappa_{\mu 2} & \ldots & \kappa_{\mu v} \end{bmatrix} \qquad (5.2)$$

ονομαζεται *γεννήτρια* του κώδικα. Κάθε κωδική λέξη είναι γραμμικός συνδυασμός σειρών του μητρώου K. Εφόσον οι τελεστέες είναι διανύσματα ν-τάξεως, διαμορφώνεται ο παρακάτω συνοπτικός ορισμός.

ΟΡΙΣΜΟΣ : *Κώδικας ομάδας* ή *διαδικός γραμμικός κώδικας* είναι ο διανυσματικός χώρος επί του πεδίου GF(2) που διατρέχουν οι σειρές κάποιας γεννήτριας μxν ($\mu \leq v$), με ν και μ το πλήθος δυαδικών ψηφίων σε κάθε κωδική λέξη και τη διάσταση του κώδικα, αντίστοιχα. Αν $\mu = v$, τότε ο κώδικας είναι ουσιαστικά ο διανυσματικός χώρος V_v, ενώ στην περίπτωση $\mu < v$ ο κώδικας είναι κάποιος υπο-χώρος του V_v, που μπορεί να συμβολίζεται με V_v^μ ώστε να υποδεικνύεται με τον άνω δείκτη και η διαστάση του. Εύκολα διαπιστώνεται ότι ο κώδικας V_v^μ περιλαμβάνει 2^μ κωδικές λέξεις.

ΠΑΡΑΔΕΙΓΜΑ : Ο δυαδικός γραμμικός κώδικας V_3 με κωδικές λέξεις $\Delta_3 = \{ 000, 001, 010, 100, 011, 101, 110, 111 \}$ διαμορφώνεται από τη γεννήτρια :

$$K = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (5.3)$$

Είναι φανερό ότι οι σειρές του μητρώου K είναι γραμμικά ανεξάρτητα διανύσματα 3ης-τάξεως και ακόμη ότι κάθε κωδική λέξη είναι κάποιος γραμμικός συνδυασμός των σειρών της γεννήτριας (π.χ. $110 = 1 \cdot 100 \oplus 1 \cdot 010 \oplus 0 \cdot 001$).

Προκειμένου να υπάρχει δυνατότητα διόρθωσης σφαλμάτων, απλών ή πολλαπλών, σε κάθε κωδική λέξη υπάρχουν εκτός από ψηφία πληροφορίας και ψηφία ελέγχου. Εστω ότι στις λέξεις του κώδικα V_v^μ υπάρχουν μ ψηφία πληροφορίας και ν-μ ψηφία

ελέγχου. Με απλές πράξεις επί των σειρών ή/και αναδιατάξεις στηλών η γεννήτρια του κώδικα είναι δυνατό να γραφεί με την παρακάτω *συστηματική* μορφή :

$$K = [\, I_\mu \mid P \,] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 \ldots & 0 & \rho_{11} & \rho_{12} \cdots & \rho_{1,\nu-\mu} \\ 0 & 1 & 0 \ldots & 0 & \rho_{21} & \rho_{22} \cdots & \rho_{2,\nu-\mu} \\ 0 & 0 & 1 \ldots & 0 & \rho_{31} & \rho_{32} \cdots & \rho_{3,\nu-\mu} \\ \multicolumn{4}{c|}{\ldots\ldots\ldots\ldots} & \multicolumn{3}{c}{\ldots\ldots\ldots\ldots\ldots\ldots} \\ 0 & 0 & 0 \ldots & 1 & \rho_{\mu 1} & \rho_{\mu 2} \cdots & \rho_{\mu,\nu-\mu} \end{array}\right] \qquad (5.4)$$

όπου I_μ είναι μχμ μοναδιαίο μητρώο και P είναι μχ(ν−μ) μητρώο. Αν η κωδική λέξη γραφεί με τη μορφή $X = [\, \Pi \mid E \,]$ όπου $\Pi = [\, \pi_1\ \pi_2\ \pi_3 \ldots \pi_\mu \,]$ και $E = [\, \epsilon_1\ \epsilon_2\ \epsilon_3 \ldots \epsilon_{\nu-\mu} \,]$ περιέχουν αντίστοιχα τα ψηφία πληροφορίας και τα ψηφία ελέγχου, είναι φανερό ότι $X = \Pi K$ ή $[\, \Pi \mid E \,] = \Pi\, [\, I_\mu \mid P \,]$ και τελικά $E = \Pi P$:

$$[\, \epsilon_1\ \epsilon_2\ \epsilon_3 \ldots \epsilon_{\nu-\mu} \,] = [\, \pi_1\ \pi_2\ \pi_3 \ldots \pi_\mu \,] \left[\begin{array}{ccc} \rho_{11} & \rho_{12} \cdots & \rho_{1,\nu-\mu} \\ \rho_{21} & \rho_{22} \cdots & \rho_{2,\nu-\mu} \\ \rho_{31} & \rho_{32} \cdots & \rho_{3,\nu-\mu} \\ \multicolumn{3}{c}{\ldots\ldots\ldots\ldots\ldots\ldots} \\ \rho_{\mu 1} & \rho_{\mu 2} \cdots & \rho_{\mu,\nu-\mu} \end{array}\right] \qquad (5.5)$$

δηλαδή τα ψηφία ελέγχου προσδιορίζονται πολλαπλασιάζοντας τη σειρά των ψηφίων πληροφορίας Π με στήλες του μητρώου P. Ο κώδικας που διαμορφώνεται με τον τρόπο αυτό χαρακτηρίζεται *συστηματικός κώδικας ομάδας* επειδή η γεννήτρια του είχε συστηματική μορφή. Αλλά η τελευταία προκύπτει από γεννήτρια με μη συστηματική μορφή μετά από στοιχειώδεις πράξεις επί των σειρών ή/και αναδιατάξεις των στηλών. Εφόσον οι δύο μορφές είναι ισοδύναμες και οι αντίστοιχοι κώδικες θα είναι ισοδύναμοι, δηλαδή οι κωδικές λέξεις έχουν τα ίδια ψηφία αλλά ενδεχομένως σε διαφορετικές θέσεις. Είναι φανερό λοιπόν ότι κάθε κώδικας ομάδας είναι ισοδύναμος με συστηματικό κώδικα ομάδας.

Σύμφωνα με όσα αναφέρονται στην §5.III, το σύνολο των δυαδικών ν−άδων που είναι ορθογώνιες προς τις σειρές της γεννήτριας αποτελεί επίσης υπο−χώρο του V_ν που χαρακτηρίζεται σαν μηδενικός χώρος του V_ν^μ , συμβολίζεται με ${}^0V_\nu^\mu$ και έχει διάσταση ν−μ. Επομένως ${}^0V_\nu^\mu$ ($= V_\nu^{\nu-\mu}$) είναι επίσης κάποιος κώδικας ομάδας που

περιλαμβάνει $2^{\nu-\mu}$ κωδικές λέξεις. Αντιστρέφοντας τα παραπάνω, το σύνολο των δυαδικών ν-άδων που είναι ορθογώνιες προς τις σειρές της γεννήτριας του κώδικα $V_\nu^{\nu-\mu}$ αποτελεί τον κώδικα ${}^{\perp}V_\nu^{\nu-\mu} = V_\nu^{\nu-(\nu-\mu)} = V_\nu^{\mu}$. Ο κώδικας $V_\nu^{\nu-\mu}$ χαρακτηρίζεται *διαδικός* του κώδικα V_ν^{μ} και αντίστροφα.

ΠΑΡΑΔΕΙΓΜΑ : Εστω ο κώδικας ομάδας V_3^2 = { 000 110 101 011 }. Εύκολα διαπιστώνεται ότι η γεννήτρια του κώδικα είναι το 2x3 μητρώο :

$$K = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \qquad (5.6)$$

και επομένως η διάσταση του κώδικα είναι 2, όπως ήδη δηλώθηκε με τον άνω δείκτη στο συμβολισμό V_3^2. Το σύνολο { 000 111 } των δυαδικών τριάδων που είναι ορθογώνιες προς τις σειρές του μητρώου K αποτελεί, σύμφωνα με όσα προαναφέρθηκαν, τον κώδικα ομάδας V_3^1 με διάσταση 1. Η γεννήτρια του τελευταίου είναι το μητρώο [1 1 1] και είναι προφανές ότι ο κώδικας V_3^2 περιλαμβάνει όλες τις κωδικές λέξεις που είναι ορθογώνιες προς τη μοναδική σειρά του μητρώου [1 1 1] (π.χ. 110 · 111 = 1·1 ⊕ 1·1 ⊕ 0·1 = 0).

Αν X είναι λέξη του κώδικα V_ν^{μ} και H είναι η γεννήτρια του κώδικα $V_\nu^{\nu-\mu}$, που είναι (ν−μ)xν μητρώο, τότε η ορθογωνικότητα μεταξύ X και οποιασδήποτε σειράς του μητρώου H περιγράφεται με τη σχέση $X \cdot H^T = 0$, όπου H^T είναι το ανάστροφο του H, δηλαδή νx(ν−μ) μητρώο. Εχει ήδη αποδειχθεί ότι X = ΠK και επομένως $\Pi K \cdot H^T = 0$ για κάθε κωδική λέξη, οπότε πρέπει $K \cdot H^T = 0$. Αλλά $K = [\, I_\mu \mid P \,]$ και εύκολα διαπιστώνεται ότι $H = [\, -P^T \mid I_{\nu-\mu} \,]$. Το αρνητικό πρόσημο μπορεί να αγνοηθεί αφού η δυαδική αφαίρεση ισοδυναμεί με δυαδική πρόσθεση. Το μητρώο H χαρακτηρίζεται *μητρώο ελέγχου ισότητας* επειδή, όπως διαπιστώνεται από τα παραδείγματα που ακολουθούν, καθορίζει τις εξισώσεις με τις οποίες προσδιορίζονται τα ψηφία ελέγχου και πραγματοποιούνται οι έλεγχοι για αποκάλυψη σφαλμάτων.

ΠΑΡΑΔΕΙΓΜΑ : Εστω συστηματικός κώδικας ομάδας V_7^4 με γεννήτρια :

$$K = [\, I_4 \mid P \,] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \qquad (5.7)$$

Η τυπική κωδική λέξη έχει τη δομή $X = [\, \Pi \mid E \,] = [\, \pi_1\ \pi_2\ \pi_3\ \pi_4\ \epsilon_1\ \epsilon_2\ \epsilon_3 \,]$. Τα ψηφία ελέγχου προκύπτουν από τις εξισώσεις :

$$\begin{aligned} \epsilon_1 &= \pi_1 \oplus \pi_2 \oplus \pi_3 \\ \epsilon_2 &= \pi_2 \oplus \pi_3 \oplus \pi_4 \\ \epsilon_3 &= \pi_1 \oplus \pi_2 \oplus \pi_4 \end{aligned} \qquad (5.8)$$

που διαμορφώνονται πολλαπλασιάζοντας τη σειρά $[\, \pi_1\ \pi_2\ \pi_3\ \pi_4 \,]$ με στήλες του μητρώου P.

ΠΑΡΑΔΕΙΓΜΑ : Θεωρείται εδώ ο δυαδικός του κώδικα ομάδας του προηγουμένου παραδείγματος, δηλαδή ο κώδικας ομάδας V_7^3 με γεννήτρια :

$$H = [\, P^T \mid I_3 \,] = \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \qquad (5.9)$$

Αν X είναι λέξη του κώδικα V_7^4, πρέπει $X \cdot H^T = 0$ και επομένως προκύπτουν οι παρακάτω εξισώσεις για τα ψηφία ελέγχου :

$$\begin{aligned} \pi_1 \oplus \pi_2 \oplus \pi_3 \oplus \epsilon_1 &= 0 \\ \pi_2 \oplus \pi_3 \oplus \pi_4 \oplus \epsilon_2 &= 0 \\ \pi_1 \oplus \pi_2 \oplus \pi_4 \oplus \epsilon_3 &= 0 \end{aligned} \qquad (5.10)$$

που είναι ισοδύναμες με τις εξ.(5.8) του προηγουμένου παραδείγματος.

Για τη διόρθωση σφαλμάτων σε κωδικές ομάδας χρησιμοποιείται το *σύνδρομο* του σφάλματος, δηλαδή ένας αριθμός που εξαρτάται από το σφάλμα και όχι από την κωδική λέξη στην οποία αυτό συνέβη. Έστω X κάποια λέξη του κώδικα ομάδας V_ν^μ. Αν κατά τη μετάδοση συμβεί απλό σφάλμα, τότε στο δέκτη του συστήματος επικοινωνίας λαμβάνεται η δυαδική ν–άδα $X \oplus \Lambda$, όπου Λ είναι δυαδική ν–άδα με 1 στη θέση του σφάλματος και 0 σε όλες τις άλλες θέσεις. Είναι φανερό ότι :

$$(X \oplus \Lambda)\cdot H^T = \Lambda\cdot H^T \neq 0 \qquad (5.11)$$

Τα στοιχεία της σειράς $\Lambda\cdot H^T = [\ \kappa_1\ \kappa_2\ \ldots\ \kappa_{\nu-\mu}\ ]$ ορίζουν το σύνδρομο $\Sigma = \kappa_1\ \kappa_2\ \ldots\ \kappa_{\nu-\mu}$ που υποδεικνύει τη θέση όπου συνέβη σφάλμα. Κάθε μοναδιαίο ψηφίο στο σύνδρομο αντιστοιχεί σε έλεγχο ισότητας που αποτυγχάνει. Αν εξετασθούν οι ελεγχόμενες θέσεις για κάθε αποτυχημένο έλεγχο ισότητας εντοπίζεται το ψηφίο που έχει αλλοιωθεί κατά τη μετάδοση.

ΠΑΡΑΔΕΙΓΜΑ : Εστω ο κώδικας του προηγουμένου παραδείγματος. Αν στην έξοδο του διαύλου πληροφορίας ληφθεί η κωδική λέξη 1010111, διαμορφώνεται το σύνδρομο $\Sigma = 100$ από την εξίσωση :

$$[\ 1\ 0\ 0\ ] = [\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ ] \cdot \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]^T \qquad (5.12)$$

Το σύνδρομο υποδεικνύει ότι απέτυχε ο πρώτος έλεγχος ισότητας. Η πρώτη από τις εξ.(5.10) δείχνει ότι το σφάλμα μπορεί να έχει γίνει σε κάποια από τις θέσεις π_1, π_2, π_3, ϵ_1. Αλλά από τις υπόλοιπες εξ.(5.10) διαπιστώνεται ότι τα ψηφία π_1, π_2, π_3 είναι σωστά, οπότε εντοπίζεται το σφάλμα στη θέση του ψηφίου ϵ_1. Επομένως η ορθή κωδική λέξη είναι 1010011.

Εύκολα διαπιστώνεται ότι το σύνδρομο Σ έχει ίδια διάταξη ψηφίων με κάποια στήλη του μητρώου ελέγχου ισότητας Η. Οι στήλες του μητρώου Η είναι επομένως όλες οι δυνατές μορφές συνδρόμου απλού σφάλματος. Αν δεν υπάρχει σφάλμα, δηλαδή $\Lambda = [\ 0\ 0\ \ldots\ 0\ ]$, τότε $\Sigma = 00\ldots0$. Το σύνδρομο απλού σφάλματος έχει συνολικά $\nu+1$ τιμές, δηλαδή ν τιμές για την αποκάλυψη σφάλματος σε κάποια από τα ν ψηφία της κωδικής λέξης και μία ακόμη (το μηδέν) για την περίπτωση να έχει μεταδοθεί η κωδική λέξη χωρίς αλλοίωση.

Το γινόμενο $X\cdot H^T$, με $X \in V_\nu^\mu$, αποτελεί ουσιαστικά κάποιο γραμμικό συνδυασμό σειρών του μητρώου ελέγχου ισότητας Η. Δεδομένου ότι $X\cdot H^T = 0$ για κάθε κωδική λέξη Χ, οι σειρές του μητρώου Η είναι γραμμικά εξαρτημένες. Αν D_{min} είναι το ελάχιστο βάρος Hamming των κωδικών λέξεων, δηλαδή το ελάχιστο πλήθος μη μηδενικών ψηφίων σε κάθε λέξη, τότε D_{min} σειρές του μητρώου Η είναι γραμμικά

εξαρτημένες ή, ισοδύναμα, δεν υπάρχουν περισσότερες από $D_{min} - 1$ γραμμικά ανεξάρτητες σειρές. Η δομή του μητρώου $H = [\, P^T \mid I_{v-\mu} \,]$ υποδεικνύει ότι η τάξη σειρών του, δηλαδή το πλήθος των γραμμικά ανεξάρτητων σειρών του, είναι το πολύ $v-\mu$. Επομένως πρέπει $v-\mu \geq D_{min} - 1$, ή :

$$D_{min} \leq v - \mu + 1 \tag{5.13}$$

δηλαδή το ελάχιστο βάρος Hamming των λέξεων του κώδικα V_v^μ είναι φραγμένο από πάνω. Αν προστεθεί ένα επιπλέον ψηφίο ελέγχου σε κάθε λέξη του κώδικα, τότε προκύπτει ο επεκτεταμένος κώδικας V_{v+1}^μ. Η ελάχιστη απόσταση Hamming μεταξύ των κωδικών λέξεων γίνεται $D_{min} + 1$ αν το πρόσθετο ψηφίο ελέγχου προκύπτει με άρτιο έλεγχο ισότητας. Το μητρώο ελέγχου ισότητας του επεκτεταμένου κώδικα έχει τη μορφή :

$$H_e = \left[\begin{array}{ccc:c} & H & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hdashline 1 & 1 \ \ldots \ 1 & & 1 \end{array}\right] \tag{5.14}$$

και η τελευταία σειρά αφορά σε έλεγχο ισότητας επί όλων των ψηφίων της δυαδικής (v+1)-άδας που χρησιμοποιείται σαν κωδική λέξη.

Πίνακας 5.1

Κανονική διάταξη δυαδικών v-άδων

	X_1	X_2	X_3	X_4	...
Λ_1	$X_1 \oplus \Lambda_1$	$X_2 \oplus \Lambda_1$	$X_3 \oplus \Lambda_1$	$X_4 \oplus \Lambda_1$	...
Λ_2	$X_1 \oplus \Lambda_2$	$X_2 \oplus \Lambda_2$	$X_3 \oplus \Lambda_2$	$X_4 \oplus \Lambda_2$	...
Λ_3	$X_1 \oplus \Lambda_3$	$X_2 \oplus \Lambda_3$	$X_3 \oplus \Lambda_3$	$X_4 \oplus \Lambda_4$	...
Λ_4	$X_1 \oplus \Lambda_4$	$X_2 \oplus \Lambda_4$	$X_3 \oplus \Lambda_4$	$X_4 \oplus \Lambda_4$	...
...	...	...	...	...	...

Η διόρθωση σφαλμάτων σε κώδικα ομάδας V_v^μ μπορεί να πραγματοποιηθεί και με τη βοήθεια της *κανονικής διάταξης* των δυαδικών v-άδων (βλ. πίνακα 5.1) που κατασκευάζεται με τα εξής βήματα. Στην πρώτη σειρά τοποθετούνται όλες οι κωδικές λέξεις. Στη συνέχεια επιλέγεται κάποια δυαδική v-άδα, έστω Λ_1, που δεν έχει

χρησιμοποιηθεί μέχρι τότε και διαμορφώνονται τα στοιχεία της δεύτερης σειράς προσθέτοντας σε κάθε κωδική λέξη τη δυαδική ν-άδα Λ_1. Για την τρίτη σειρά επιλέγεται κάποια δυαδική ν-άδα, έστω Λ_2, που δεν έχει χρησιμοποιηθεί μέχρι τότε και διαμορφώνονται τα στοιχεία της σειράς προσθέτοντας στις κωδικές λέξεις τη δυαδική ν-άδα Λ_2. Η διαδικασία αυτή συνεχίζεται μέχρι να εμφανισθούν στην κανονική διάταξη όλες οι δυαδικές ν-άδες. Η κανονική διάταξη αναγνωρίζεται σαν το μητρώο παρασυνόλων που ορίσθηκε στην § 5.Ι. Οι σειρές της κανονικής διάταξης αντιστοιχούν στα παρασύνολα με οδηγούς τα στοιχεία Λ_1, Λ_2, ...

Είναι φανερό ότι προσθέτοντας τους οδηγούς Λ_1, Λ_2, ... στην κωδική λέξη, έστω, X_1, προκύπτουν αλλοιωμένες (εσφαλμένες) μορφές της και μάλιστα οι θέσεις που καταλαμβάνονται από 1 σε κάθε οδηγό είναι οι θέσεις όπου γίνονται τα σφάλματα. Επομένως κάθε στήλη της κανονικής διάταξης περιέχει στην κορυφή μια κωδική λέξη και από κάτω τις εσφαλμένες μορφές της. Αν οι οδηγοί επιλέγονται έτσι ώστε να έχουν το ελάχιστο βάρος Hamming, τότε σε κάθε στήλη της κανονικής διάταξης εμφανίζονται οι πιθανότερες αλλοιωμένες μορφές της κωδικής λέξης που βρίσκεται στην κορυφή της. Το σχήμα αποκωδικοποίησης είναι απλό. Η λαμβανόμενη δυαδική ν-άδα αναγνωρίζεται μέσα στην κανονική διάταξη και, εφόσον δεν βρίσκεται στην πρώτη σειρά, θεωρείται οτι προέρχεται από την κωδική λέξη που βρίσκεται στην κορυφή της ίδιας στήλης.

Πίνακας 5.2

Κανονική διάταξη δυαδικών 5-άδων

	X_1	X_2	X_3	X_4
00000	00000	01111	10011	11100
10000	10000	11111	00011	01100
01000	01000	00111	11011	10100
00100	00100	01011	10111	11000
00010	00010	01101	10001	11110
00001	00001	01110	10010	11101
01010	01010	00101	11001	10110
00110	00110	01001	10101	11010

ΠΑΡΑΔΕΙΓΜΑ : Εστω κώδικας που χρησιμοποιεί τις δυαδικές 5-άδες 00000, 01111, 10011, 11100. Υπάρχουν 32 δυαδικές 5-άδες και η κανονική διάταξη (βλ. πίνακα 5.2) θα έχει 8 σειρές με οδηγούς τις δυαδικές 5-άδες 10000, 01000,

00100, 00010, 00001 που αντιστοιχούν σε απλό σφάλμα και τις δυαδικές 5-άδες 01010, 00110 που αντιστοιχούν σε διπλά σφάλματα. Είναι φανερό ότι υπάρχουν περισσότερες από 2 δυνατότητες διπλού σφάλματος και επομένως υπάρχει κάποια ελευθερία στην επιλογή των δύο τελευταίων οδηγών της κανονικής διάταξης. Κριτήριο για την επιλογή τους θα μπορούσε να είναι ότι αντιστοιχούν στις πιθανότερες περιπτώσεις διπλού σφάλματος. Με βάση την παραπάνω κανονική διάταξη, αν ληφθεί η δυαδική 5-άδα 01101, που βρίσκεται στην τρίτη σήλη, αναγνωρίζεται σαν αλλοιωμένη μορφή της κωδικής λέξης 01111. Εύκολα διαπιστώνεται ότι η απόσταση Hamming μεταξύ της εσφαλμένης 5-άδας 01101 και κάποιας κωδικής λέξης γίνεται ελάχιστη για την κωδική λέξη 01111.

Η πιθανότητα ορθής αποκωδικοποίησης με χρήση της κανονικής διάταξης δίνεται, στην περίπτωση δυαδικού συμμετρικού διαύλου πληροφορίας από την έκφραση :

$$P_o = \gamma_0 p^v + \gamma_1 (1-p) p^{v-1} + \gamma_2 (1-p)^2 p^{v-2} + \ldots \qquad (5.15)$$

όπου γ_0, γ_1, γ_2, ... είναι το πλήθος οδηγών με βάρος Hamming 0, 1, 2, ..., αντίστοιχα, και p είναι η πιθανότητα ορθής μετάδοσης κάθε δυαδικού ψηφίου. Για τον κώδικα του προηγουμένου παραδείγματος $\gamma_0 = 1$, $\gamma_1 = 5$, $\gamma_2 = 2$ και αν $p = 0.9$, προκύπτει πιθανότητα ορθής αποκωδικοποίησης $P_o = 0.9332$. Επομένως η πιθανότητα εσφαλμένης αποκωδικοποίησης είναι $P_E = 1 - P_o = 0.0669$.

5.2.1 ΚΩΔΙΚΕΣ HAMMING

Οι δυαδικοί κώδικες Hamming είναι κώδικες ομάδας της μορφής $v = 2^\kappa - 1$, $\mu = 2^\kappa - \kappa - 1$ όπου κ θετικός ακέραιος. Αν $\kappa = 3$, τότε προκύπτει ο κώδικας V_7^4. Επειδή τα ψηφία ελέγχου είναι τοποθετημένα σε κατάλληλες θέσεις (βλ. §4.6), η δεκαδική τιμή του συνδρόμου υποδεικνύει τη θέση του σφάλματος.

5.2.2 ΚΩΔΙΚΕΣ HADAMARD

Προκύπτουν επιλέγοντας σαν κωδικές λέξεις τις σειρές ενός μητρώου Hadamard. Το τελευταίο είναι $v \times v$ δυαδικό μητρώο με την ιδιότητα κάθε σειρά του να διαφέρει

από οποιαδήποτε άλλη σειρά σε v/2 θέσεις. Μιά σειρά του μητρώου Hadamard περιέχει μόνο μηδενικά ενώ όλες οι άλλες περιέχουν v/2 μηδενικά και v/2 μονάδες. Το απλούστερο μητρώο Hadamard είναι :

$$M_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{5.16}$$

και τα συνθετώτερα μέλη της οικογένειας προκύπτουν με την αναδρομική σχέση :

$$M_{2v} = \begin{bmatrix} M_v & M_v \\ M_v & \bar{M}_v \end{bmatrix} \tag{5.17}$$

όπου $\bar{M}_v$ είναι το συμπληρωματικό του M_v που προκύπτει εναλλάσσοντας 0 και 1. Σαν παράδειγμα δίνονται τα μητρώα M_4, $\bar{M}_4$:

$$M_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \bar{M}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \tag{5.18}$$

Οι σειρές των μητρώων M_4, $\bar{M}_4$ συνιστούν κώδικα ομάδας με $v = 4$, $\mu = 3$ και $D_{min} = 2$. Γενικά οι κώδικες Hadamard έχουν παραμέτρους της μορφής $v = 2^x$, $\mu = \kappa + 1$, $D_{min} = 2^{x-1}$ όπου κ θετικός ακέραιος.

5.2.3 ΚΩΔΙΚΑΣ GOLAY

Είναι ο κώδικας ομάδας V_{23}^{12} με $D_{min} = 7$.

5.3 ΚΥΚΛΙΚΟΙ ΚΩΔΙΚΕΣ

Είναι κώδικες ομάδας εφοδιασμένοι με την *κυκλική ιδιότητα* : αν η δυαδική v-άδα

$$\kappa_1 \quad \kappa_2 \quad \kappa_3 \quad \ldots \quad \kappa_\nu$$

είναι κωδική λέξη, τότε και οι δυαδικές ν-άδες που προκύπτουν με κυκλική μετάθεση των κωδικών ψηφίων

$$\kappa_\nu \quad \kappa_1 \quad \kappa_2 \quad \ldots \quad \kappa_{\nu-1}$$

$$\kappa_{\nu-1} \quad \kappa_\nu \quad \kappa_1 \quad \ldots \quad \kappa_{\nu-2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\kappa_2 \quad \kappa_3 \quad \kappa_4 \quad \ldots \quad \kappa_1$$

είναι κωδικές λέξεις. Η ενδιαφέρουσα δομή των κυκλικών κωδίκων προσφέρεται για εφαρμογές σε σύγχρονα συστήματα επικοινωνιών.

Η σχεδίαση κυκλικών κωδίκων στηρίζεται στη θεωρία πρώτων πολυωνύμων. Ενώ στους κώδικες ομάδας θεωρήθηκε ότι κάθε δυαδική ν-άδα που χρησιμοποιείται σαν κωδική λέξη αντιστοιχεί σε διάνυσμα ν-τάξεως, οι λέξεις κυκλικού κώδικα αντιστοιχίζονται σε (ν-1)-βαθμού πολυώνυμα, που έχουν ν όρους. Αυτό πραγματοποιείται εύκολα θεωρώντας ότι τα κωδικά ψηφία είναι συντελεστές των δυνάμεων της (αυθαίρετης) ανεξάρτητης μεταβλητής x. Η τυπική κωδική λέξη $X = \kappa_1\kappa_2 \ldots \kappa_\nu$ αντιστοιχεί στο πολυώνυμο :

$$X(x) = \kappa_1 x^{\nu-1} + \kappa_2 x^{\nu-2} + \ldots + \kappa_{\nu-1}x + \kappa_\nu \qquad (5.19)$$

Όπως αποδεικνύεται στην §5.V, το σύνολο P_ν των (ν-1)-βαθμού, δυαδικών πολυωνύμων και η δυαδική πρόσθεση ⊕ αποτελούν ομάδα. Η υπο-ομάδα των (ν-1)-βαθμού, δυαδικών πολυωνύμων που προκύπτουν με κυκλική μετάθεση των συντελεστών του πολυωνύμου X(x) διαμορφώνεται με τη διαδικασία της παρακάτω εξίσωσης :

$$x^i X(x) = (x^\nu + 1)F(x) \oplus X_i(x) \qquad (5.20)$$

Είναι προφανές ότι $X_i(x)$ είναι (ν-1)-βαθμού, δυαδικό πολυώνυμο αφού προκύπτει σαν υπόλοιπο της διαίρεσης $x^i X(x)/(x^\nu + 1)$. Αν $i = 0$, η εξ.(5.20) δίνει το αρχικό πολυώνυμο :

$$X_0(x) = X(x) = \kappa_1 x^{\nu-1} + \kappa_2 x^{\nu-2} + \ldots + \kappa_{\nu-1} x + \kappa_\nu \qquad (5.21)$$

ενώ για $i = 1$ προκύπτει το πολυώνυμο (βλ. §5.IV) :

$$X_1(x) \equiv xX(x) \quad [\mathrm{mod}(x^\nu + 1)] = \kappa_2 x^{\nu-1} + \kappa_3 x^{\nu-2} + \ldots + \kappa_\nu x + \kappa_1 \qquad (5.22)$$

Είναι φανερό ότι οι συντελεστές του πολυωνύμου $X_1(x)$ προκύπτουν από εκείνους του πολυωνύμου $X(x)$ με κυκλική μετάθεση κατά μία θέση. Εύκολα γενικεύεται αυτή η παρατήρηση : το πολυώνυμο $X_i(x) \equiv x^i X(x) \quad [\mathrm{mod}(x^\nu + 1)]$ προκύπτει από το πολυώνυμο $X_0(x) = X(x)$ με κυκλική μετάθεση των συντελεστών του κατά i θέσεις. Επομένως τα πολυώνυμα $X_i(x)$, $i = 0, 1, 2, \ldots, \nu-1$, αντιστοιχίζονται σε λέξεις κυκλικού κώδικα με ν δυαδικά ψηφία ανά λέξη.

Στη συνέχεια εισάγεται η συνήθης για κώδικα ομάδας υπόθεση ότι σε κάθε δυαδική ν-άδα που χρησιμοποιείται σαν κωδική λέξη υπάρχουν μ ψηφία πληροφορίας και $\nu-\mu$ ψηφία ελέγχου. Δηλαδή η κωδική λέξη $X = \kappa_1 \kappa_2 \ldots \kappa_\nu$ προέρχεται από τη λέξη πληροφορίας $\Pi = \pi_1 \pi_2 \ldots \pi_\mu$, $\mu \leq \nu$, και αντιστοιχεί στο $(\nu-1)$-βαθμού, δυαδικό πολυώνυμο $X(x) = \Pi(x)K(x)$, όπου ο παράγων $\Pi(x) = \pi_1 x^{\mu-1} + \pi_2 x^{\mu-2} + \ldots + \pi_{\mu-1} x + \pi_\mu$ χρησιμοποιεί σαν συντελεστές των δυνάμεων της μεταβλητής x τα ψηφία πληροφορίας. Ο παράγων $K(x)$ είναι $(\nu-\mu)$-βαθμού, δυαδικό πολυώνυμο και πρέπει να επιλεγεί έτσι ώστε να ικανοποιείται η κυκλική ιδιότητα που περιγράφεται με την εξ.(5.20) :

$$x^i \Pi(x)K(x) = (x^\nu + 1)F(x) \oplus X_i(x) \qquad (5.23)$$

Αλλά $X_i(x) = \Pi_i(x)K(x)$ και επομένως το πολυώνυμο $K(x)$ είναι διαιρέτης του $(x^\nu + 1)F(x)$. Επιλέγεται λοιπόν το πολυώνυμο $K(x)$ σαν διαιρέτης του πολυωνύμου $x^\nu + 1$ και μάλιστα σαν ένας από τους $(\nu-\mu)$-βαθμού διαιρέτες. Κάθε επιλογή οδηγεί σε κυκλικό κώδικα και το πολυώνυμο $K(x)$ ονομάζεται, όπως είναι φυσικό, *γεννήτρια* του κυκλικού κώδικα.

ΠΑΡΑΔΕΙΓΜΑ : Έστω κυκλικός κώδικας με $\nu = 7$ και $\mu = 4$. Εύκολα διαπιστώνεται ότι $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$ και επομένως διατίθενται σαν γεννήτριες τα πολυώνυμα $x^3 + x^2 + 1$ και $x^3 + x + 1$. Έστω $K(x) = x^3 + x^2 + 1$. Οι κωδικές λέξεις προκύπτουν πολλαπλασιάζοντας το πολυώνυμο $\Pi(x) = \pi_1 x^3 + \pi_2 x^2 + \pi_3 x + \pi_4$ με τη γεννήτρια $K(x)$. Οι κωδικές λέξεις που διαμορφώνονται με τον τρόπο

αυτό δίνονται στον πίνακα 5.3 .

Πίνακας 5.3

Κυκλικός κώδικας V_7^4 με γεννήτρια $K(x) = x^3 + x^2 + 1$

Λέξη πληροφορίας	Κωδική Λέξη	Λέξη πληροφορίας	Κωδική Λέξη
1 0000	0000000	9 1000	1101000
2 0001	0001101	10 1001	1100101
3 0010	0011010	11 1010	1110010
4 0011	0010111	12 1011	1111111
5 0100	0110100	13 1100	1011100
6 0101	0111001	14 1101	1010001
7 0110	0101110	15 1110	1000110
8 0111	0100011	16 1111	1001011

Είναι φανερό ότι ο κυκλικός κώδικας χρησιμοποιεί τα μ ψηφία πληροφορίας για να προσδιορίσει τα ν κωδικά ψηφία. Τα ψηφία πληροφορίας δεν εμφανίζονται όμως στην κωδική λέξη και η δομή της τελευταίας δεν επιτρέπει τη διακριση μεταξύ ψηφίων πληροφορίας και ψηφίων ελέγχου. Αυτή η αδυναμία θεραπεύεται εισάγοντας τους *συστηματικούς κυκλικούς κώδικες* με την παρακάτω μέθοδο κωδικοποίησης.

Έστω η λέξη πληροφορίας $\Pi = \pi_1\pi_2 \ldots \pi_\mu$, $\mu \leq \nu$, που κατά τα γνωστά αντιστοιχεί στο πολυώνυμο $\Pi(x) = \pi_1 x^{\mu-1} + \pi_2 x^{\mu-2} + \ldots + \pi_{\mu-1}x + \pi_\mu$. Το πολυώνυμο $x^{\nu-\mu}\Pi(x) = \pi_1 x^{\nu-1} + \pi_2 x^{\nu-2} + \ldots + \pi_{\mu-1}x^{\nu-\mu+1} + \pi_\mu x^{\nu-\mu}$, διαιρούμενο με τη γεννήτρια $K(x)$, δίνει πηλίκο $F(x)$ και υπόλοιπο $E(x) = \epsilon_1 x^{\nu-\mu-1} + \epsilon_2 x^{\nu-\mu-2} + \ldots + \epsilon_{\nu-\mu-1}x + \epsilon_{\nu-\mu}$ δηλαδή :

$$x^{\nu-\mu}\Pi(x) = F(x)K(x) \oplus E(x) \tag{5.24}$$

Επειδή η δυαδική πρόσθεση ισοδυναμεί με δυαδική αφαίρεση, η εξ.(5.24) γράφεται ως εξής :

$$x^{\nu-\mu}\Pi(x) \oplus E(x) = F(x)K(x) \tag{5.25}$$

και επομένως το πολυώνυμο $x^{\nu-\mu}\Pi(x) + E(x) = \pi_1 x^{\nu-1} + \pi_2 x^{\nu-2} + \ldots + \pi_{\mu-1}x^{\nu-\mu+1} + \pi_\mu x^{\nu-\mu} + \epsilon_1 x^{\nu-\mu-1} + \epsilon_2 x^{\nu-\mu-2} + \ldots + \epsilon_{\nu-\mu-1}x + \epsilon_{\nu-\mu}$ είναι πολλαπλάσιο της

γεννήτριας $K(x)$. Κατά συνέπεια οι συντελεστές του διαμορφώνουν λέξη του κυκλικού κώδικα και μάλιστα αυτή έχει τη μορφή $\pi_1\pi_2 \ldots \pi_\mu\epsilon_1\epsilon_2 \ldots \epsilon_{\nu-\mu}$, δηλαδή οι πρώτες μ θέσεις καταλαμβάνονται από τα ψηφία πληροφορίας και οι επόμενες ν−μ θέσεις από τα ψηφία ελέγχου.

ΠΑΡΑΔΕΙΓΜΑ : Εστω η λέξη πληροφορίας 0011 του προηγουμένου παραδείγματος ($\nu = 7$, $\mu = 4$). Είναι φανερό ότι $\Pi(x) = \pi_1x^3 + \pi_2x^2 + \pi_3x + \pi_4 = x + 1$ και επομένως $x^{\nu-\mu}\Pi(x) = x^4 + x^3$. Σαν γεννήτρια του κυκλικού κώδικα θεωρήθηκε το πολυώνυμο $K(x) = x^3 + x^2 + 1$. Η διαίρεση $x^{\nu-\mu}\Pi(x)/K(x)$ δίνει πηλίκο $F(x) = x$ και υπόλοιπο $E(x) = x$. Επειδή $E(x) = \epsilon_1x^2 + \epsilon_2x + \epsilon_3$, προκύπτει $\epsilon_1 = 0$, $\epsilon_2 = 1$, $\epsilon_3 = 0$ και επομένως η κωδική λέξη είναι 0011010. Παρατηρείται αμέσως ότι τα πρώτα τέσσερα ψηφία συνιστούν τη λέξη πληροφορίας 0011. Στο προηγούμενο παράδειγμα η ίδια λέξη πληροφορίας είχε κωδικοποιηθεί σαν 0010111 και δεν ήταν δυνατό να αναγνωριοθούν ψηφία πληροφορίας και ψηφία ελέγχου.

Η αποκωδικοποίηση κυκλικών κωδίκων είναι σχετικά απλή υπόθεση. Εστω ότι εκπέμπεται η δυαδική ν−άδα X και λαμβάνεται η δυαδική ν−άδα Y. Αυτές αντιστοιχούν στα πολυώνυμα $X(x)$ και $Y(x) = X(x) \oplus \Lambda(x) = \Pi(x)K(x) \oplus \Lambda(x)$, όπου $\Lambda(x)$ είναι το πολυώνυμο που εκπροσωπεί τυχόντα σφάλματα. Αν $Y(x) \equiv 0 \pmod{K(x)}$, δηλαδή $Y(x)$ είναι πολλαπλάσιο της γεννήτριας $K(x)$, η δυαδική ν−άδα Y αναγνωρίζεται σαν κωδική λέξη παρόλο που μπορεί $\Lambda(x) \neq 0$. Γενικά όμως $Y(x) \equiv \Lambda(x) \pmod{K(x)}$, δηλαδή το πολυώνυμο $\Lambda(x)$ προκύπτει σαν υπόλοιπο της διαίρεσης $Y(x)/K(x)$. Στην περίπτωση απλού σφάλματος στη θέση i είναι φανερό ότι $\Lambda(x) = x^i$. Επειδή η εξίσωση $Y(x) = X(x) + \Lambda(x)$ ισοδυναμεί με την $Y(x) \oplus \Lambda(x) = X(x)$, αρκεί να προστεθούν τα πολυώνυμα $Y(x)$, $\Lambda(x)$ για να προσδιορισθεί η κωδική λέξη που είχε σταλεί.

5.3.1 ΚΥΚΛΙΚΟΙ ΚΩΔΙΚΕΣ HAMMING

Είναι κυκλικοί κώδικες με $\nu = 2^\kappa - 1$, $\nu - \mu = \kappa$ όπου κ θετικός ακέραιος που εκπροσωπεί το πλήθος των ψηφίων ελέγχου.

5.3.2 ΚΥΚΛΙΚΟΣ ΚΩΔΙΚΑΣ GOLAY

Ο κώδικας Golay είχε εισαχθεί στην §5.2.3 σαν κώδικας ομάδας με $v = 23$, $\mu = 12$ και $D_{min} = 7$. Ο κυκλικός κώδικας Golay διατηρεί αυτά τα χαρακτηριστικά και προκύπτει από τη γεννήτρια $K(x) = x^{11} + x^9 + x^7 + x^5 + x^5 + x + 1$.

5.3.3 ΚΥΚΛΙΚΟΙ ΚΩΔΙΚΕΣ BCH

Οι κυκλικοί κώδικες BCH (Bose–Chaudhuri–Hocquenhem) έχουν χαρακτηριστικά $v = 2^\kappa - 1$, $v-\mu \leq \lambda\kappa$, $D_{min} = 2\lambda + 1$, όπου λ,κ θετικοί ακέραιοι. Η γεννήτρια τέτοιων κωδίκων είναι κάποιος από τους παράγοντες του πολυωνύμου $x^{2^\kappa - 1} + 1$, που συνήθως προσφέρονται σε πίνακες.

5.4 ΥΛΟΠΟΙΗΣΗ ΚΥΚΛΙΚΩΝ ΚΩΔΙΚΩΝ

Κάθε κυκλικός κώδικας V_v^μ γεννάται από παράγοντα του πολυωνύμου $x^v + 1$. Η γεννήτρια του κυκλικού κώδικα είναι $(v-\mu)$–βαθμού, ενικό, δυαδικό πολυώνυμο (βλ. §5.V) και μάλιστα πρώτο πολυώνυμο, δηλαδή πολυώνυμο που διαιρείται μόνο από το ίδιο και φυσικά το τετριμμένο πολυώνυμο 1. Η τελευταία απαίτηση επιβάλλεται με σκοπό να αποκτήσει ο κώδικας την αναγκαία δομή για ευχερή υλοποίηση της διάταξης κωδικοποίησης/αποκωδικοποίησης. Στον πίνακα 5.4 δίνονται όλα τα πολυώνυμα μέχρι και 3ου–βαθμού, παρατίθενται οι παράγοντες τους και αναγνωρίζονται τα πρώτα πολυώνυμα που προσφέρονται για γεννήτριες κυκλικών κωδίκων.

Αν $K(x)$ είναι η γεννήτρια του κυκλικού κώδικα V_v^μ, οι κωδικές λέξεις εκπροσωπούνται από $(v-1)$–βαθμού, modulo–$K(x)$, δυαδικά πολυώνυμα. Οπως αποδεικνύεται στην §5.V το σύνολο P_v των $(v-1)$–βαθμού, δυαδικών πολυωνύμων, εφοδιασμένο με τη δυαδική πρόσθεση $\oplus$, αποτελεί την ομάδα $\{ P_v, \oplus \}$. Ο κυκλικός κώδικας V_v^μ, δηλαδή το σύνολο των $(v-1)$–βαθμού, modulo–$K(x)$, δυαδικών κωδικών πολυωνύμων, έχει τις παρακάτω ιδιότητες:

(i) Αν $X(x), \Psi(x) \in V_\nu^\mu$, τότε και $X(x) \otimes \Psi(x) \in V_\nu^\mu$, δηλαδή, $\{ V_\nu^\mu, \otimes \}$ είναι υπο-ομάδα της $\{ P_\nu, \otimes \}$. Υπενθυμίζεται ότι κάθε κυκλικός κώδικας είναι κώδικας ομάδας.

(ii) Αν $X(x) \in V_\nu^\mu$, τότε και $X_i(x) \equiv x^i X(x) \ [\mathrm{mod}(x^\nu + 1)] \in V_\nu^\mu$, $i = 0, 1, \ldots, \nu-1$.

Το σύνολο V_ν^μ χαρακτηρίζεται σαν *κυκλική υπο-ομάδα* της ομάδας $\{ P_\nu, \otimes \}$. Κατ' επέκταση της ιδιότητας (ii), αν $\kappa \in \Delta_1$ και $X(x) \in V_\nu^\mu$, τότε και $\kappa x^i \circledast X(x) \in V_\nu^\mu$, όπου με το σύμβολο $\circledast$ εκπροσωπείται η πράξη του modulo-2 & modulo-$(x^\nu + 1)$ πολλαπλασιασμού (βλ. §5.V), δηλαδή τα πολυώνυμα κx^i, $X(x)$ πολλαπλασιάζονται με το συνήθη τρόπο modulo-2 και το γινόμενο ελαττώνεται σε $(\nu-1)$-βαθμού, δυαδικό πολυώνυμο χρησιμοποιώντας την εξίσωση $x^\nu = 1$. Με συνδυασμό των ιδιοτήτων (i) και (ii) διαπιστώνεται ότι, αν $X(x) \in V_\nu^\mu$ και $\Psi(x) \in P_\nu$, δηλαδή $\Psi(x) = \kappa_1 x^{\nu-1} + \kappa_2 x^{\nu-2} + \ldots + \kappa_{\nu-1} x + \kappa_\nu$ με $\kappa_1, \kappa_2, \ldots, \kappa_\nu \in \Delta_1$, τότε και $X(x) \circledast \Psi(x) \in V_\nu^\mu$.

Πίνακας 5.4

Δυαδικά πολυώνυμα μέχρι και 3ου-βαθμού

Βαθμός	Πολυώνυμο	Παράγοντες	Πρώτο Πολυώνυμο
0	1	1	1
1	x	1, x	x
1	$x + 1$	1, $x + 1$	$x + 1$
2	x^2	1, x, x^2	
2	$x^2 + 1$	1, $x + 1$, $x^2 + 1$	
2	$x^2 + x$	1, x, $x + 1$, $x^2 + x$	
2	$x^2 + x + 1$	1, $x^2 + x + 1$	$x^2 + x + 1$
3	x^3	1, x, x^2, x^3	
3	$x^3 + 1$	1, $x + 1$, $x^2 + x + 1$, $x^3 + 1$	
3	$x^3 + x$	1, x, $x + 1$, $x^2 + 1$, $x^3 + x$	
3	$x^3 + x + 1$	1, $x^3 + x + 1$	$x^3 + x + 1$
3	$x^3 + x^2$	1, x, x^2, $x + 1$, $x^3 + x^2$	
3	$x^3 + x^2 + 1$	1, $x^3 + x^2 + 1$	$x^3 + x^2 + 1$
3	$x^3 + x^2 + x$	1, x, $x^2 + x + 1$, $x^3 + x^2 + x$	
3	$x^3 + x^2 + x + 1$	1, $x + 1$, $x^2 + 1$, $x^3 + x^2 + x + 1$	

ΟΡΙΣΜΟΣ : Ιδανικό I του συνόλου P_v είναι κάθε υποσύνολο του με τις ιδιότητες : (i) $\{ I, \otimes \}$ είναι υπο-ομάδα της $\{ P_v, \otimes \}$ και (ii) αν $X(x) \in I$ και $A(x) \in P_v$, τότε και $X(x) \otimes A(x) \in I$.

Το σύνολο των κωδικών πολυωνύμων V_v^μ με τις μέχρι τώρα ιδιότητες αποτελεί, κατά τον παραπάνω ορισμό, ιδανικό του συνόλου των (v−1)-βαθμιού, δυαδικών πολυωνύμων P_v. Δηλαδή κάθε κυκλική υπο-ομάδα του συνόλου P_v αποτελεί ιδανικό του.

ΛΗΜΜΑ : Αν $X(x), \Psi(x) \in I$, όπου I είναι κάποιο ιδανικό του P_v, τότε ο Μέγιστος Κοινός Διαιρέτης (ΜΚΔ) τους, έστω $Z(x)$, γράφεται με τη μορφή $Z(x) = A(x) \otimes X(x) \oplus B(x) \otimes \Psi(x)$ και επομένως $Z(x) \in I$.

ΛΗΜΜΑ : Κάθε πολυώνυμο που ανήκει στο ιδανικό I του συνόλου P_v είναι πολλαπλάσιο του μοναδικού πολυωνύμου ελάχιστου βαθμού του I. Το πολυώνυμο αυτό ονομάζεται *γεννήτρια* του ιδανικού I.

Έστω $K(x)$ η γεννήτρια του ιδανικού I. Αν $X(x) \in I$, τότε ο ΜΚΔ των $K(x)$ και $X(x)$, έστω $\Psi(x)$, ανήκει στο ιδανικό I σύμφωνα με το πρώτο λήμμα. Αν $K(x)$ δεν διαιρεί ακριβώς το πολυώνυμο $X(x)$, τότε ο ΜΚΔ τους θα είναι πολυώνυμο βαθμού κατώτερου εκείνου του $K(x)$. Αλλά αυτό δεν συμβιβάζεται με την υπόθεση ότι $K(x)$ είναι το ελάχιστου βαθμού πολυώνυμο του ιδανικού I. Επομένως το (αυθαίρετο) πολυώνυμο $X(x)$ του I είναι πολλαπλάσιο του $K(x)$. Αν δύο πολυώνυμα $K_1(x), K_2(x)$ είναι ελάχιστου βαθμού μέλη του ιδανικού I, τότε καθένα είναι πολλαπλάσιο του άλλου και επομένως ταυτίζονται. Δηλαδή υπάρχει μόνο μία γεννήτρια για το ιδανικό I.

ΛΗΜΜΑ : Έστω ιδανικό I του συνόλου P_v. Η γεννήτρια του $K(x)$ είναι παράγοντας του πολυωνύμου $x^v + 1$.

Σύμφωνα με το πρώτο λήμμα, ο ΜΚΔ των πολυωνύμων $K(x)$ και $x^v + 1$, έστω $\Lambda(x)$, γράφεται με τη μορφή $\Lambda(x) = A(x) \otimes K(x) \oplus B(x) \otimes (x^v + 1) = A(x) \otimes K(x) \equiv A(x)K(x)$ $[\mathrm{mod}(x^v + 1)]$ και $\Lambda(x) \in I$. Έχει ήδη γίνει δεκτό ότι το πολυώνυμο $\Lambda(x)$ διαιρεί ακριβώς τη γεννήτρια $K(x)$ του ιδανικού I. Αλλά, σύμφωνα με το δεύτερο λήμμα, η γεννήτρια $K(x)$ του ιδανικού I διαιρεί ακριβώς το πολυώνυμο $\Lambda(x)$ αφού $\Lambda(x) \in I$. Επομένως $\Lambda(x) = K(x)$ και μάλιστα $K(x)$ διαιρεί ακριβώς το πολυώνυμο $x^v + 1$.

ΘΕΩΡΗΜΑ : Κάθε κυκλικός κώδικας V_v^μ αποτελεί ιδανικό του συνόλου P_v με

γεννήτρια κάποιο από τους (ν−μ)-βαθμού διαιρέτες του πολυωνύμου $x^{\nu} + 1$.

Η παραγοντοποίηση του πολυωνύμου $x^{\nu} + 1$ ισοδυναμεί με τον προσδιορισμό των ριζών της εξίσωσης $x^{\nu} + 1 = 0$ ή, στο πλαίσιο της modulo-2 αριθμητικής, της εξίσωσης :

$$x^{\nu} - 1 = 0 \qquad (5.26)$$

Είναι γνωστό ότι η εξ.(5.26) επιλύεται για $x_\lambda = \exp(2\pi j\lambda/\nu)$, $\lambda = 0, 1, \ldots, \nu-1$. Μερικές από τις ν-τάξεως ρίζες της μονάδας διαθέτουν την ελκυστική ιδιότητα να παράγουν με ύψωση σε δύναμη όλες τις υπόλοιπες ρίζες. Τέτοιες ρίζες, που ονομάζονται *πρωταρχικές*, συνδέονται, όπως θα φανεί παρακάτω, με τη δυνατότητα διόρθωσης σφαλμάτων σε κυκλικούς κώδικες. Είναι φανερό ότι η ρίζα $x_1 = \exp(2\pi j/\nu)$ είναι πρωταρχική αφού $x_1^{\lambda} = (\exp(2\pi j/\nu))^{\lambda} = \exp(2\pi j\lambda/\nu) = x_\lambda$, $\lambda = 0, 1, \ldots, \nu-1$. Αλλά και κάθε ρίζα $x_\lambda = \exp(2\pi j\lambda/\nu)$ με λ πρώτο ακέραιο σε σχέση με ν είναι πρωταρχική ν-τάξεως ρίζα της μονάδας. Αυτό αποδεικνύεται με τον συλλογισμό που ακολουθεί. Αφού όλες οι ν-τάξεως ρίζες της μονάδας προκύπτουν από την $x_\lambda = \exp(2\pi j\lambda/\nu)$ με ύψωση σε δύναμη, πρέπει :

$$\left(e^{2\pi j\lambda/\nu}\right)^{\mu_1} \neq \left(e^{2\pi j\lambda/\nu}\right)^{\mu_2} \quad \text{για } \mu_1 \neq \mu_2 \qquad (5.27)$$

όπου $\mu_1, \mu_2 = 0, 1, \ldots, \nu-1$. Η εξ.(5.27) γράφεται με την ισοδύναμη μορφή :

$$\exp(2\pi j\lambda(\mu_1-\mu_2)/\nu) \neq 1 \quad \text{για } \mu_1 \neq \mu_2 \qquad (5.28)$$

και ισχύει αν $\lambda(\mu_1-\mu_2)/\nu$ δεν είναι ακέραιος. Εφόσον $\lambda < \nu$ και $|\mu_1-\mu_2| < \nu$, αρκεί λ και ν να μην έχουν κοινούς διαιρέτες. Επομένως πρωταρχική, ν-τάξεως ρίζα της μονάδας προκύπτει για λ πρώτο ακέραιο σε σχέση με ν.

ΛΗΜΜΑ : Κάθε λ-βαθμού, πρώτο (μη παραγοντοποιήσιμο), ενικό, δυαδικό πολυώνυμο K(x) παράγει πολυωνυμικό πεδίο $F_\lambda(x)$ που εκπροσωπεί το πεδίο Galois $GF(2^\lambda)$. Το σύνολο $F_\lambda(x)$ αποτελείται από (λ−1)-βαθμού, δυαδικά πολυώνυμα, είναι κλειστό ως προς τη δυαδική πρόσθεση ⊕ και το modulo-2 & modulo-K(x) πολλαπλασιασμό ⊛ . Είναι προφανές ότι το σύνολο $F_\lambda(x)$ διαθέτει $2^\lambda - 1$ μη μηδενικά στοιχεία. Όλα τα μη μηδενικά στοιχεία του $F_\lambda(x)$ είναι ρίζες της εξίσωσης

$$x^{2^\lambda-1} - 1 = 0 \qquad (5.29)$$

και αντίστροφα. Κατά συνέπεια μερικά στοιχεία του συνόλου $F_\lambda(x)$, που χαρακτηρίζονται *πρωταρχικά*, παράγουν με ύψωση σε δύναμη όλα τα υπόλοιπα.

Πίνακας 5.5

Στοιχεία $F_3(x)$

2ου-βαθμού Πολυώνυμα	Δυαδικές 3-άδες
0	000
1	001
x	010
x + 1	011
x^2	100
$x^2 + 1$	101
$x^2 + x$	110
$x^2 + x + 1$	111

ΠΑΡΑΔΕΙΓΜΑ : Από τον πίνακα 5.4 επιλέγεται το 3ου-βαθμού, πρώτο, ενικό, δυαδικό πολυώνυμο $K(x) = x^3 + x + 1$. Το πεδίο $\{ F_3(x), \odot, \circledast \}$ περιέχει όλα τα 2ου-βαθμού, δυαδικά πολυώνυμα (βλ. πίνακα 5.5) και είναι κλειστό ως προς τις πράξεις $\odot$, $\circledast$. Η τελευταία ισοδυναμεί με το συνήθη πολλαπλασιασμό με μόνη διαφορά ότι το γινόμενο ελαττώνεται σε 2ου-βαθμού πολυώνυμο χρησιμοποιώντας την εξίσωση $K(x) = 0$, δηλαδή για το παράδειγμα την εξίσωση $x^3 = x + 1$.

Είναι εύκολο να αποδειχθεί ότι όλα τα μη μηδενικά στοιχεία του συνόλου $F_3(x)$ είναι 7ης-τάξεως ρίζες της μονάδας, δηλαδή ρίζες του πολυωνύμου $x^7 + 1$. Ενδεικτικά ελέγχεται το πολυώνυμο $x + 1$:

$$(x + 1)^7 + 1 = (x + 1)^2 \circledast (x + 1)^2 \circledast (x + 1)^2 \circledast (x + 1) + 1 =$$

$$(x^2 + 1) \circledast (x^2 + 1) \circledast (x^2 + 1) \circledast (x + 1) + 1 = (x^4 + 1) \circledast (x^3 + x^2 + x + 1) + 1 =$$

$$(x^2 + x + 1) \circledast x^2 + 1 = x^4 + x^3 + x^2 + 1 = x^2 + x + x + 1 + x^2 + 1 = 0 \qquad (5.30)$$

Επιπλέον μπορεί να αποδειχθεί ότι κάθε μη μηδενικό στοιχείο του συνόλου $F_3(x)$

είναι πρωταρχικό. Ενδεικτικά ελέγχεται το στοιχείο x που πρέπει με ύψωση σε δύναμη να παράγει όλα τα στοιχεία του συνόλου $F_8(x)$:

$$x^0 = 1$$

$$x^1 = x$$

$$x^2 = x^2$$

$$x^3 = x + 1$$

$$x^4 = x^2 + x$$

$$x^5 = x^2 \otimes (x + 1) = x^3 + x^2 = x^2 + x + 1$$

$$x^6 = (x + 1) \otimes (x + 1) = x^2 + 1$$

ΘΕΩΡΗΜΑ : Εστω κυκλικός κώδικας V_ν^μ με γεννήτρια $K(x)$ κάποιο $(\nu-\mu)$-βαθμού, πρώτο, ενικό, δυαδικό πολυώνυμο. Αν $\nu + 1 = 2^{\nu-\mu}$, η γεννήτρια $K(x)$ παράγει το πολυωνυμικό πεδίο $F_{2^{\nu-\mu}}(x)$ με στοιχεία όλα τα $(\nu-\mu-1)$-βαθμού, δυαδικά πολυώνυμα $E(x) = \epsilon_1 x^{\nu-\mu-1} + \epsilon_2 x^{\nu-\mu-2} + \ldots + \epsilon_{\nu-\mu-1} x + \epsilon_{\nu-\mu}$ και υπάρχει η δυνατότητα αποκάλυψης απλού σφάλματος.

Η γεννήτρια είναι παράγων του πολυωνύμου $x^{2^{\nu-\mu}-1} + 1 = x^\nu + 1$. Τα στοιχεία του πολυωνυμικού πεδίου $F_{2^{\nu-\mu}}(x)$ είναι $(\nu-\mu)$-τάξεως ρίζες της μονάδας και μάλιστα το στοιχείο x είναι πρωταρχική ρίζα. Επομένως κάθε στοιχείο $E(x)$ αντιστοιχεί σε κάποια μορφή του συνδρόμου απλού σφάλματος $\Lambda(x) = x^i$, $i = 0, 1, 2, \ldots, \nu-1$. Το στοιχείο $E(x) = 0$ αντιστοιχεί στο σύνδρομο $\Lambda(x) = 0$ που υποδεικνύει ότι δεν έγινε σφάλμα κατά τη μετάδοση της κωδικής λέξης. Τα κωδικά πολυώνυμα παράγονται με τη διαδικασία της εξ.(5.25) και ο κώδικας είναι προφανώς κυκλικός κώδικας Hamming.

ΘΕΩΡΗΜΑ : Αν $K_1(x)$, $K_2(x)$ είναι γεννήτριες των ιδανικών I_1, I_2 του συνόλου P_ν και $K_1(x)K_2(x) = x^\nu + 1$, τότε $X_1(x) \otimes X_2(x) = 0$ για $X_1(x) \in I_1$, $X_2(x) \in I_2$.

Αν $X_1(x) \in I_1$, $X_2(x) \in I_2$, τότε $X_1(x) = A(x)K_1(x)$, $X_2(x) = B(x)K_2(x)$ και

επομένως $X_1(x)X_2(x) = A(x)B(x)(x^v + 1)$, δηλαδή $X_1(x)X_2(x) \equiv 0 \ [\mathrm{mod}(x^v + 1)]$. Η ισοδύναμα $X_1(x) \circledast X_2(x) = 0$.

Αν $X_1(x) = \kappa_0 + \kappa_1 x + \ldots + \kappa_{v-1}x^{v-1}$ και $X_2(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{v-1}x^{v-1}$ με $\kappa_i, \lambda_i \in \Delta_1$, $i = 0, 1, \ldots, v-1$, τότε ο συντελεστής του όρου x^i στο γινόμενο $X_1(x) \circledast X_2(x)$ δίνεται από το άθροισμα :

$$\sum_{j=0}^{v-1} \kappa_j \lambda_{i-j} = 0 \qquad (5.31)$$

με την παραδοχή $\lambda_{v+i} = \lambda_i$. Η εξ.(5.31) πρέπει να ισχύει για $i = 0, 1, \ldots, v-1$ αν $X_1(x) \in I_1$ και $X_2(x) \in I_2$.

ΘΕΩΡΗΜΑ : Αν $K_1(x)$, $K_2(x)$ είναι γεννήτριες των ιδανικών I_1, I_2 του συνόλου P_v και $K_1(x)K_2(x) = x^v + 1$, τότε η εξίσωση $X(x) \circledast K_{1,2}(x) = 0$ με $X(x) \in P_v$ εξυπονοεί ότι $X(x) \in I_{2,1}$, αντίστοιχα.

Αν $X(x) \in P_v$ και $X(x) \circledast K_2(x) = 0$, τότε $X(x)K_2(x) = A(x)(x^v + 1)$ και επομένως $X(x) = A(x)(x^v + 1)/K_2(x) = A(x)K_1(x)$, δηλαδή $X(x) \in I_1$.

Στη συνέχεια εφαρμόζονται τα θεωρήματα αυτά στην περίπτωση κυκλικού κώδικα V_v^μ. Η γεννήτρια του κώδικα είναι $(v-\mu)$-βαθμού, πρώτο, ενικό, δυαδικό πολυώνυμο, έστω $K_1(x)$. Ο κυκλικός κώδικας V_v^μ είναι ιδανικό, έστω I_1, του συνόλου P_v. Η γεννήτρια του κώδικα είναι και γεννήτρια του ιδανικού. Αν I_2 είναι ιδανικό του συνόλου P_v με γεννήτρια $K_2(x) = (x^v + 1)/K_1(x)$, τότε $K_2(x)$ είναι μ-βαθμού, ενικό, δυαδικό πολυώνυμο, δηλαδή $K_2(x) = \kappa_0 + \kappa_1 x + \ldots + \kappa_{\mu-1}x^{\mu-1} + \kappa_\mu x^\mu$ και $\kappa_0 = \kappa_\mu = 1$ (γιατί ;). Το (αυθαίρετο) πολυώνυμο $X(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{v-1}x^{v-1}$ του συνόλου P_v είναι κωδικό πολυώνυμο, δηλαδή εκπροσωπεί λέξη του κυκλικού κώδικα V_v^μ, αν ανήκει στο ιδανικό I_1 και προϋπόθεση γι' αυτό είναι να ισχύει η εξίσωση $X(x) \circledast K_2(x) = 0$ ή, με εφαρμογή της εξ.(5.31) :

$$\sum_{j=0}^{\mu} \kappa_j \lambda_{i-j} = 0 \qquad (5.32)$$

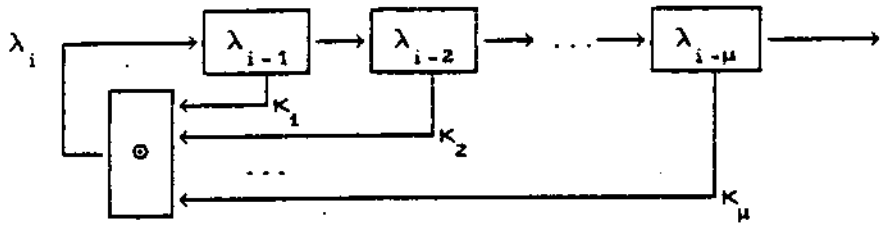
Η εξ.(5.32) αναγνωρίζεται σαν αναδρομική σχέση :

$$\lambda_i = \kappa_1\lambda_{i-1} \oplus \kappa_2\lambda_{i-2} \oplus \ldots \oplus \kappa_\mu\lambda_{i-\mu} \qquad (5.33)$$

με την οποία προσδιορίζεται το ψηφίο λ_i όταν δίνονται μ προηγούμενα ψηφία $\lambda_{i-1}, \lambda_{i-2}, \ldots, \lambda_{i-\mu}$. Εξυπονείται ότι ο κωδικοποιητής εμφανίζει διαδοχικά τα δυαδικά ψηφία της κωδικής λέξης στην έξοδο του και επομένως ο δείκτης i συνδέεται με τη χρονική στιγμή παραγωγής του δυαδικού ψηφίου λ_i. Είναι φανερό ότι η αναδρομική σχέση της εξ.(5.33) αντιστοιχεί στο πολυώνυμο $K_2(x)$. Συγκεκριμένα τα ψηφία $\lambda_i, \lambda_{i-1}, \lambda_{i-2}, \ldots, \lambda_{i-\mu}$ αντιστοιχίζονται στους όρους του πολυωνύμου $K_2(x)$ κατά το σχήμα :

$$\begin{array}{ccccccccccc} K_2(x) = & \kappa_0 & + \kappa_1 x & + \kappa_2 x^2 & + \ldots + & \kappa_{\mu-1} x^{\mu-1} & + \kappa_\mu x^\mu \\ & \uparrow & \uparrow & \uparrow & & \uparrow & \uparrow \\ 0 = & \kappa_0\lambda_i & \oplus \kappa_1\lambda_{i-1} & \oplus \kappa_2\lambda_{i-2} & \oplus \ldots \oplus & \kappa_{\mu-1}\lambda_{i-\mu+1} & \oplus \kappa_\mu\lambda_{i-\mu} \end{array} \qquad (5.34)$$

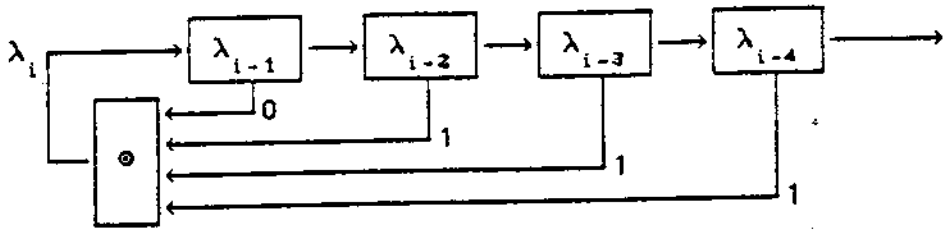
και η εξ.(5.34) αναγνωρίζεται σαν ισοδύναμη της εξ.(5.33) επειδή $\kappa_0 = 1$. Είναι φανερό ότι πολλαπλασιασμός επί x στο πολυώνυμο $K_2(x)$ αντιστοιχεί σε μετάθεση κατά μία θέση στην εξ.(5.34). Η αναδρομική σχέση της εξ.(5.34), δηλαδή ο μηχανισμός παραγωγής των κωδικών λέξεων, υλοποιείται με *καταχωρητή μ–θέσεων* (σχ.5.1). Τα ψηφία πληροφορίας $\pi_1\pi_2\ldots\pi_\mu$ τοποθετούνται στις μ θέσεις του καταχωρητή. Οι κλάδοι ανάδρασης προσάγουν τα δυαδικά ψηφία των μ θέσεων του καταχωρητή στην είσοδο του αθροιστή. Η έξοδος του αθροιστή, δηλαδή το δυαδικό ψηφίο $\lambda_i = \kappa_1\lambda_{i-1} \oplus \kappa_2\lambda_{i-2} \oplus \ldots \oplus \kappa_\mu\lambda_{i-\mu}$ προσάγεται στην είσοδο του καταχωρητή και καταλαμβάνει την πρώτη θέση εκτοπίζοντας το δυαδικό ψηφίο στην τελευταία θέση. Με ν επαναλήψεις της διαδικασίας παράγονται στην έξοδο του καταχωρητή μ ψηφία πληροφορίας ακολουθούμενα από ν–μ ψηφία ελέγχου σε αντίστροφη διάταξη αφού πρώτα παράγονται τα λιγότερο σημαντικά ψηφία της κωδικής λέξης.



Σχ. 5.1 Καταχωρητής μ–θέσεων

ΠΑΡΑΔΕΙΓΜΑ : Έστω ο κυκλικός κώδικας V_7^4 με γεννήτορα $K(x) = x^3 + x^2 + 1$. Το πολυώνυμο $(x^7 + 1)/K(x) = x^4 + x^3 + x^2 + 1$ αντιστοιχεί στην αναδρομική σχέση

$\lambda_i = \lambda_{i-2} \oplus \lambda_{i-3} \oplus \lambda_{i-4}$ που υλοποιείται με τον παρακάτω καταχωρητή 4-θέσεων (σχ. 5.2).



Σχ. 5.2 Καταχωρητής 4-θέσεων για το πολυώνυμο $x^4 + x^3 + x^2 + 1$

Έστω η λέξη πληροφορίας 0011. Αν τοποθετηθούν τα ψηφία 0,0,1,1 στις τέσσερεις θέσεις του καταχωρητή, τότε $\lambda_{i-1} = 0$, $\lambda_{i-2} = 0$, $\lambda_{i-3} = 1$, $\lambda_{i-4} = 1$ και επομένως $\lambda_i = 0 \oplus 1 \oplus 1 = 0$. Κατά τον πρώτο κύκλο ανάδρασης προσάγεται στην πρώτη θέση του καταχωρητή το ψηφίο 0 και εκτοπίζεται από την τέταρτη θέση το ψηφίο 1. Αν πραγματοποιηθούν 7 κύκλοι ανάδρασης, τότε το περιεχόμενο των τεσσάρων θέσεων και η έξοδος του καταχωρητή δίνονται στον πίνακα 5.6 .

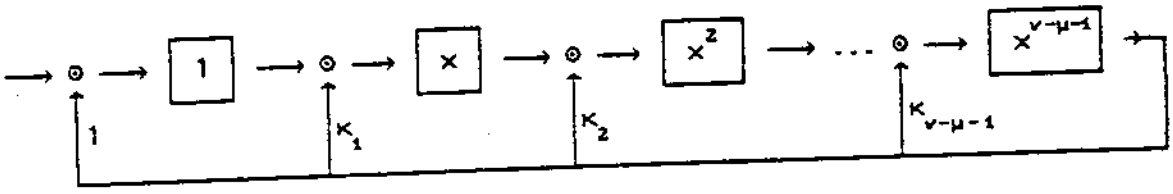
Πίνακας 5.6

Περιεχόμενο και έξοδος του καταχωρητή

Θέση 1	Θέση 2	Θέση 3	Θέση 4	Εξοδος $\Pi_1\ \Pi_2\ \Pi_3\ \Pi_4\ \epsilon_1\ \epsilon_2\ \epsilon_3$
0	0	1	1	
0	0	0	1	$1 = \Pi_4$
1	0	0	0	$1 = \Pi_3$
0	1	0	0	$0 = \Pi_2$
1	0	1	0	$0 = \Pi_1$
1	1	0	1	$0 = \epsilon_3$
0	1	1	0	$1 = \epsilon_2$
0	0	1	1	$0 = \epsilon_1$

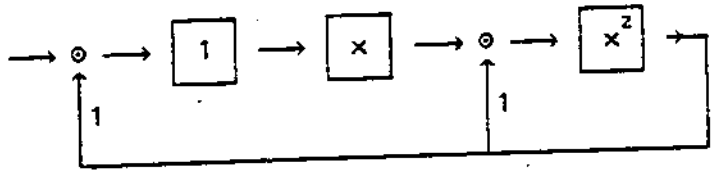
Ο καταχωρητής μ-θέσεων αντιστοιχεί στο πολυώνυμο $K_2(x) = (x^\nu + 1)/K_1(x)$ και διαθέτει μία θέση για κάθε ψηφίο πληροφορίας. Ο κυκλικός κώδικας V_ν^μ υλοποιείται και με τον καταχωρητή (ν-μ)-θέσεων (σχ .5.3) που αντιστοιχεί στη γεννήτρια $K_1(x) = \kappa_0 + \kappa_1 x + \ldots + \kappa_{\nu-\mu} x^{\nu-\mu}$ με $\kappa_0 = \kappa_{\nu-\mu} = 1$ και διαθέτει μία θέση για κάθε ψηφίο ελέγχου. Ο κλάδος ανάδρασης υλοποιεί την εξίσωση $K_1(x) = 0$, δηλαδή την

εξίσωση $x^{\nu-\mu} = 1 + \kappa_1 x + \ldots + \kappa_{\nu-\mu-1} x^{\nu-\mu-1}$. Αν στην είσοδο του καταχωρητή προσαχθεί η δυαδική ν-άδα που εκπροσωπείται από το πολυώνυμο $x^{\nu-\mu}\Pi(x)$, μετά από ν βήματα (και μ αναδράσεις) ο καταχωρητής (ν−μ)−θέσεων περιέχει τα δυαδικά ψηφία ελέγχου $\epsilon_1, \epsilon_2, \ldots, \epsilon_{\nu-\mu}$. Επομένως τροφοδοτώντας το πολυώνυμο $x^{\nu-\mu}\Pi(x)$ στον καταχωρητή (ν−μ)−θέσεων, που αντιστοιχεί στη γεννήτρια $K_1(x)$, υπολογίζεται το υπόλοιπο της διαίρεσης $x^{\nu-\mu}\Pi(x)/K_1(x)$. Η κωδική λέξη διαμορφώνεται προσθέτοντας τα ψηφία ελέγχου $\epsilon_1\epsilon_2\ldots\epsilon_{\nu-\mu}$ στο τέλος της λέξης πληροφορίας $\pi_1\pi_2\ldots\pi_\mu$.



Σχ. 5.3 Καταχωρητής (ν−μ)−θέσεων

ΠΑΡΑΔΕΙΓΜΑ : Εστω ο κυκλικός κώδικας V_7^4 με γεννήτρια $K(x) = x^3 + x^2 + 1$. Ο αντίστοιχος καταχωρητής 3-θέσεων (σχ. 5.4) υποδέχεται στην είσοδο του τη δυαδική 4-άδα των ψηφίων πληροφορίας $\pi_4\pi_3\pi_2\pi_1$, με πρώτο από δεξιά το σημαντικώτερο ψηφίο, και μετά από 7 βήματα (και 3 αναδράσεις) διαμορφώνονται στο εσωτερικό του τα ψηφία ελέγχου $\epsilon_3\epsilon_2\epsilon_1$. Το περιεχόμενο των τριών θέσεων του καταχωρητή σε κάθε βήμα της διαδικασίας δίνεται στον πίνακα 5.7 . Στην είσοδο προσάγεται η λέξη πληροφορίας 0011 που αντιστρέφεται και επεκτείνεται στη δυαδική 7-άδα 0001100.



Σχ. 5.4 Καταχωρητής 3-θέσεων

Θέση	6	5	4	3	2	1	0
		↓					
Ψηφίο	0	1	1	1	0	1	0

Σχ. 5.5 Το σύνδρομο υποδεικνύει σφάλμα στην 5η θέση.

Πίνακας 5.7

Διαδικασία κωδικοποίησης

Είσοδος	θέση 1	θέση 2	θέση 3
0001100			
000110	0		
00011	0	0	
0001	1	0	0
000	1	1	0
00	0	1	1
0	1	0	0
	0 ↑ ϵ_3	1 ↑ ϵ_2	0 ↑ ϵ_1

Πίνακας 5.8

Διαδικασία αποκωδικοποίησης

Είσοδος	θέση 1	θέση 2	θέση 3
0101110			
010111	0		
01011	1	0	
0101	1	1	0
010	1	1	1
01	1	1	0
0	1	1	1
	1 ↑ ϵ_3	1 ↑ ϵ_2	0 ↑ ϵ_1

Επομένως η κωδική λέξη είναι 0011010. Κατά την αποκωδικοποίηση χρησιμοποιείται και πάλι ο καταχωρητής 3–θέσεων. Η λαμβανόμενη δυαδική 7–άδα προσάγεται στην είσοδο του καταχωρητή και μετά από 7 βήματα διαμορφώνεται στο εσωτερικό του καταχωρητή το σύνδρομο σφάλματος. Αν λοιπόν ληφθεί η δυαδική 7–άδα 0111010, οι θέσεις του καταχωρητή αποκτούν το περιεχόμενο του πίνακα 5.8 και τελικά διαμορφώνεται το σύνδρομο $\Lambda(x) = x + 1 = x^5$ που υποδεικνύει ότι έγινε σφάλμα

στην 5η θέση (σχ. 5.5).

Επομένως η ορθή δυαδική 7-άδα είναι, μετά την αντιστροφή, 0011010. Τα ψηφία ελέγχου δεν χρειάζονται πλέον και η λέξη πληροφορίας είναι η δυαδική 4-άδα 0011.

5.5 ΣΥΝΕΛΙΚΤΙΚΟΙ ΚΩΔΙΚΕΣ

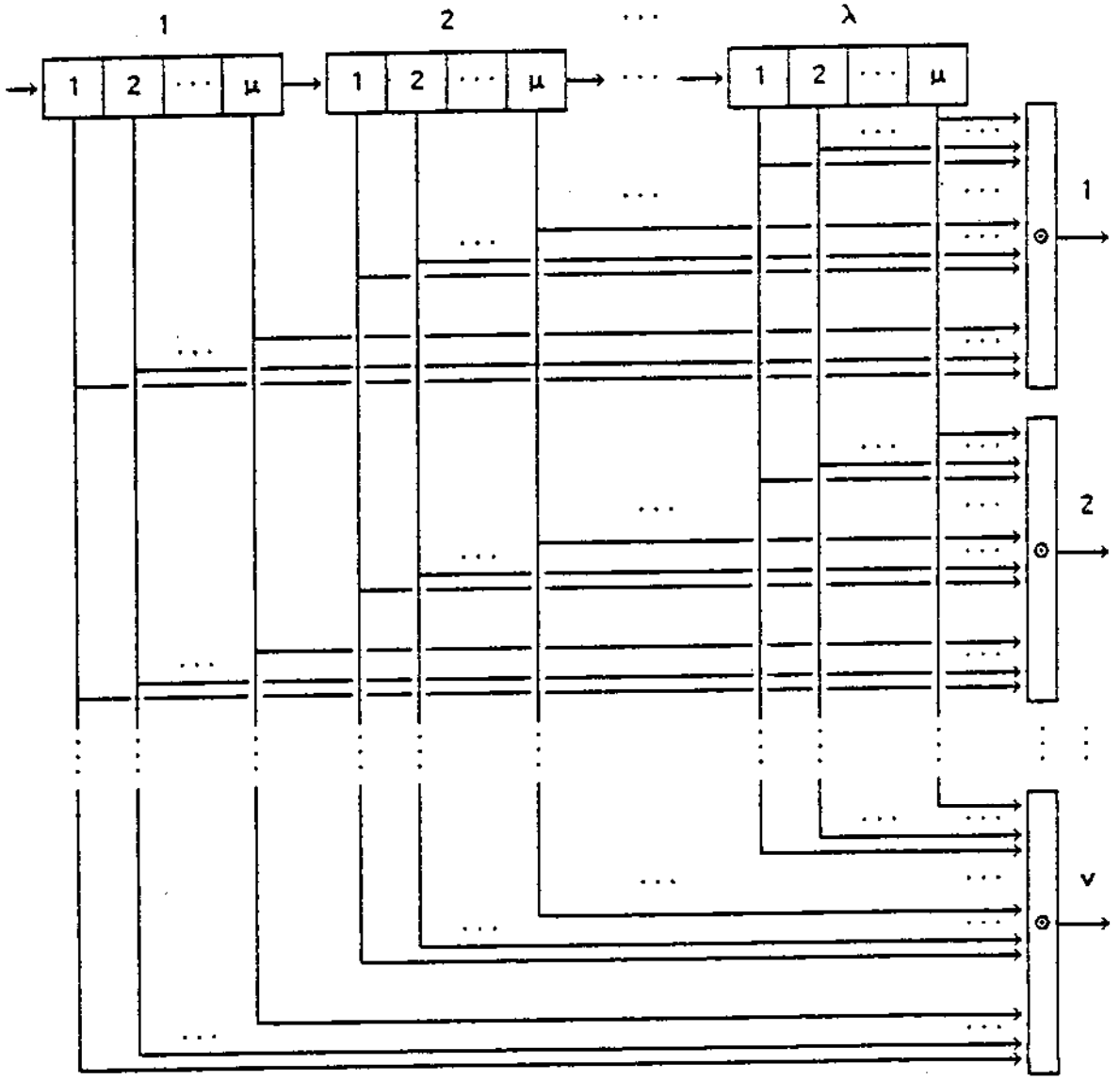
Η χρήση καταχωρητών στη σχεδίαση κωδίκων εξελίχθηκε ταχύτερα από την αντίστοιχη αλγεβρική θεωρία και απέκτησε ιδιαίτερη δυναμική με αποτέλεσμα την εμφάνιση συνθετώτερων τεχνικών κωδικοποίησης. Οι *συνελικτικοί κώδικες* εκμεταλεύονται τις ελκυστικές ιδιότητες των καταχωρητών και χρησιμοποιούνται εξίσου με τους δομικούς κώδικες παρόλο που στερούνται αντίστοιχης θεωρητικής θεμελίωσης.

Η συνελικτική κωδικοποίηση διαφοροποιείται σημαντικά από τη δομική κωδικοποίηση. Η κωδική λέξη που αντιστοιχίζεται σε σύμβολο ή λέξη πληροφορίας διαμορφώνεται από το περιεχόμενο των θέσεων του καταχωρητή, δηλαδή από προηγούμενο τμήμα του μηνύματος πληροφορίας. Επομένως δεν υπάρχει συγκεκριμένο κλειδί και κάθε σύμβολο ή λέξη πληροφορίας, ανάλογα με τη θέση στο μήνυμα πληροφορίας, είναι δυνατό να εκπροσωπείται από διαφορετική κωδική λέξη.

Ο συνελικτικός κώδικας υλοποιείται με πολλαπλό γραμμικό καταχωρητή (σχ. 5.6). Στη συνήθη περίπτωση δυαδικής κωδικοποίησης κάθε κωδική λέξη έχει μ ψηφία πληροφορίας και ν-μ ψηφία ελέγχου. Ο καταχωρητής έχει γενικά λ τμήματα (bytes) μ θέσεων (bits/byte), δηλαδή συνολικά λμ θέσεις (bits), και ν αθροιστές με ισάριθμες απολήξεις. Η παράμετρος λ ονομάζεται *περιοριστικό μέγεθος* του κώδικα. Ο καταχωρητής τροφοδοτείται με δυαδικές μ-άδες, που αντιστοιχούν σε σύμβολα ή λέξεις πληροφορίας σύμφωνα με κάποιο κλειδί, και εκτοπίζει ένα δυαδικό ψηφίο από κάθε απόληξη, δηλαδή συνολικά ν δυαδικά ψηφία που συνθέτουν την κωδική λέξη προς μετάδοση. Ο λόγος μ/ν είναι ο *ρυθμός λειτουργίας* του συνελικτικού κώδικα.

Ο συνελικτικός κώδικας εκπροσωπείται είτε από το διάγραμμα του καταχωρητή, που δείχνει τη ροή δυαδικών ψηφίων από τις λμ θέσεις καταχώρησης στους ν αθροιστές, είτε από τη *γεννήτρια* $K = \{ \kappa_{ij} \}$, που είναι λμxν μητρώο με στοιχεία $\kappa_{ij} = 1$ ή 0 αν το περιεχόμενο της θέσης καταχώρησης i χρησιμοποιείται ή όχι, αντίστοιχα,

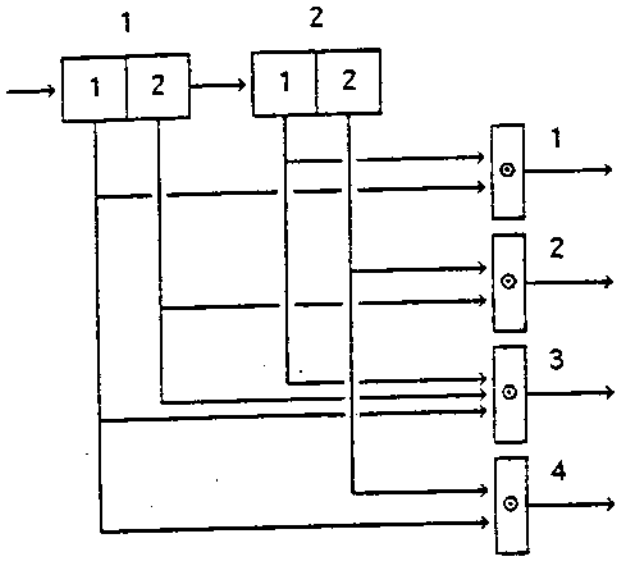
στην είσοδο του αθροιστή j .



Σχ. 5.6 Συνελικτικός κωδικοποιητής.

ΠΑΡΑΔΕΙΓΜΑ : Εστω συνελικτικός κώδικας με καταχωρητή όπως στο σχήμα 5.7. Είναι φανερό ότι μ = 2 bits/byte, λ = 2 bytes και v = 4 bits . Το περιοριστικό μέγεθος του κώδικα είναι λ = 2 bytes και ο ρυθμός λειτουργίας μ/v = 1/2 . Η γεννήτρια του συνελικτικού κώδικα είναι το μητρώο :

$$K = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \qquad (5.35)$$



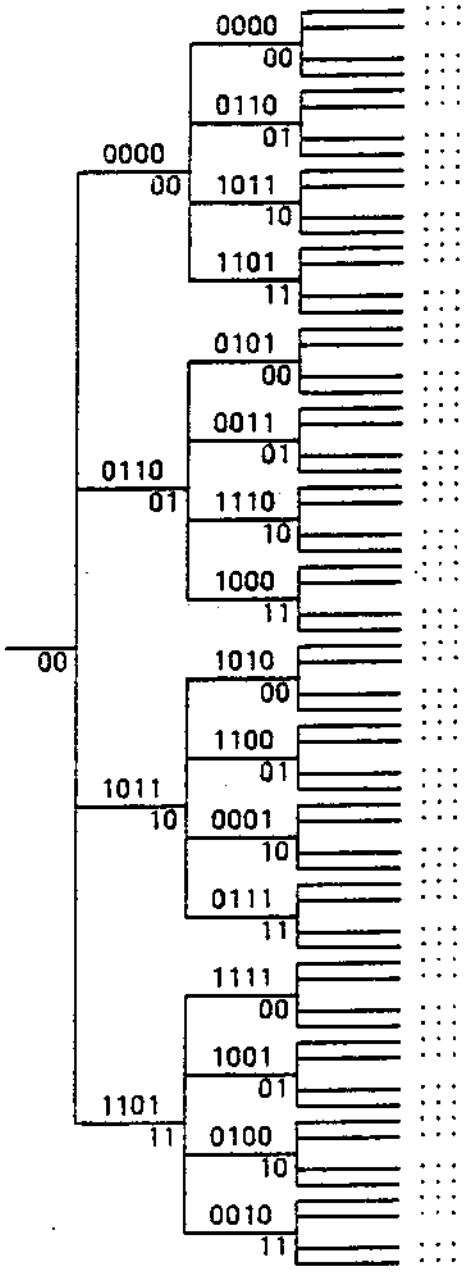
Σχ. 5.7 Συνελικτικός κώδικας με ρυθμό λειτουργίας 1/2 .

Στην είσοδο του καταχωρητή προσάγονται οι δυαδικές 2-άδες 00, 01, 10, 11, που αντιστοιχούν σε τεταδικό αλφάβητο πληροφορίας. Στην έξοδο του καταχωρητή διαμορφώνονται δυαδικές 4-άδες.

Η λειτουργία του συνελικτικού κωδικοποιητή περιγράφεται εναλλακτικά με *δενδροδιάγραμμα*, *διάγραμμα trellis* ή *διάγραμμα καταστάσεων*. Στη συνέχεια περιγράφονται τα τρία διαγράμματα, που είναι προφανώς ισοδύναμα, σε συνδυασμό με το παραπάνω παράδειγμα.

Το δενδροδιάγραμμα έχει τη μορφή κλάδων μεταξύ κόμβων. Κάθε κόμβος αντιστοιχεί στο περιεχόμενο του πρώτου τμήματος του καταχωρητή. Αρχικά όλα τα τμήματα του καταχωρητή περιέχουν μηδενικά. Είναι φανερό ότι με κάθε εισαγωγή δυαδικής μ-άδας στον κωδικοποιητή το περιεχόμενο του πρώτου τμήματος του καταχωρητή μεταβάλλεται, τα επόμενα τμήματα του καταχωρητή αποκτούν το περιεχόμενο του αμέσως προηγούμενου τμήματος και ο κωδικοποιητής εμφανίζει στην έξοδο κάποια δυαδική ν-άδα. Επομένως κάθε κλάδος του δενδροδιαγράμματος ψύεται από τον κόμβο που αντιστοιχεί στο αρχικό περιεχόμενο του καταχωρητή, καταλήγει στον κόμβο που αντιστοιχεί στο νέο περιεχόμενο του καταχωρητή και φέρει σαν ιδιαίτερο χαρακτηριστικό (ψύλλωμα) την αντίστοιχη δυαδική ν-άδα εξόδου.

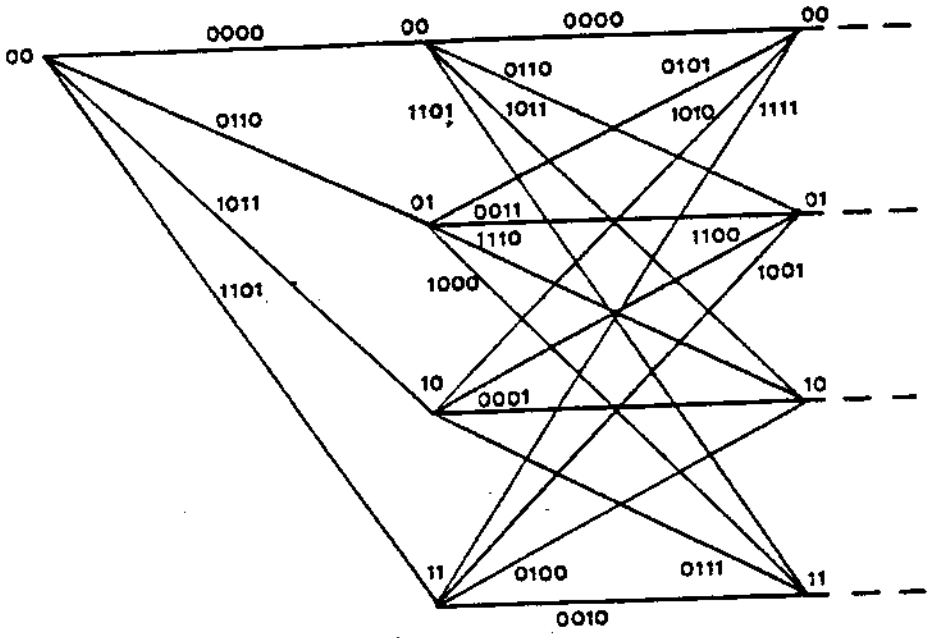
Το δενδροδιάγραμμα για τον κωδικοποιητή του παραδείγματος (σχ. 5.8) έχει κλάδους που φέρουν από πάνω τη δυαδική 4-άδα εξόδου και κάτω δεξιά την αντίστοιχη



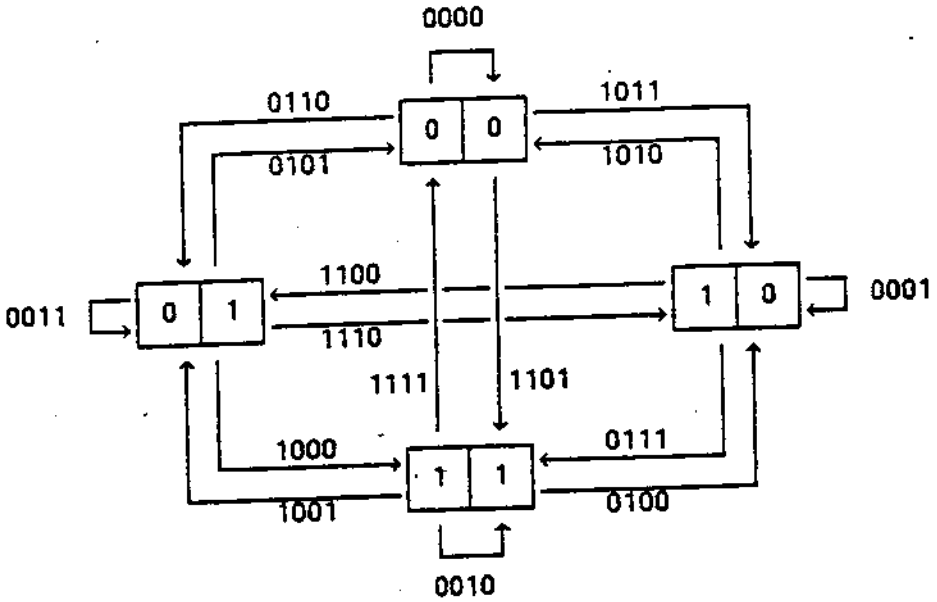
Σχ. 5.8 Δενδροδιάγραμμα του συνελικτικού κωδικοποιητή $\mu = 2$, $\lambda = 2$, $v = 4$.

δυαδική 2-άδα εισόδου που καταλαμβάνει τις θέσεις του πρώτου τμήματος του καταχωρητή. Αρχικά υπάρχει μόνον ο κόμβος 00. Στη δεύτερη γενεά προκύπτουν οι κόμβοι 00, 01, 10, 11 και στην τρίτη γενεά προκύπτουν τέσσερεις κόμβοι 00, τέσσερεις κόμβοι 01, τέσσερεις κόμβοι 10 και τέσσερεις κόμβοι 11. Σε κάθε νέα γενεά τετραπλασιάζεται το πλήθος των κλάδων και των κόμβων. Αν συγχωνευθούν οι όμοιοι κόμβοι σε κάθε γενεά, προκύπτει το διάγραμμα trellis (σχ. 5.9). Το διάγραμμα καταστάσεων (σχ. 5.10) περιγράφει τις μεταβολές του περιεχομένου του πρώτου τμήματος του καταχωρητή. Υπάρχουν προφανώς τέσσερεις καταστάσεις, που

αντιστοιχούν σε περιεχόμενο 00, 01, 10, 11. Μετάβαση από κατάσταση σε κατάσταση συνοδεύεται με εμφάνιση δυαδικής 4-άδας στην έξοδο του κωδικοποιητή, που δηλώνεται δίπλα στον αντίστοιχο κλάδο.



Σχ. 5.9 Διάγραμμα trellis του συνελικτικού κωδικοποιητή μ = 2, λ = 2, ν = 4.



Σχ. 5.10 Διάγραμμα καταστάσεων του συνελικτικού κωδικοποιητή μ = 2, λ = 2, ν = 4.

5.6 ΑΣΚΗΣΕΙΣ

1. Κατάσκοπος μετέδωσε το κωδικό μήνυμα 0011001100010110010011010101011011 . Αν είναι γνωστό ότι χρησιμοποίησε συστηματικό κώδικα ομάδας V_8^5 με μητρώο ελέγχου ισότητας :

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} .$$

να αναγνωρισθούν οι κωδικές λέξεις, να διορθωθούν τυχόντα σφάλματα και να αποκαλυφθεί το μήνυμα πληροφορίας. Να χρησιμοποιηθεί στο τελευταίο βήμα ο παρακάτω πίνακας.

A	00000	I	01111	Q	10011	Y	11100
B	10000	J	11111	R	00011	Z	01100
C	01000	K	00111	S	11011	$	10100
D	00100	L	01011	T	10111	&	11000
E	00010	M	01101	U	10001	#	11110
F	00001	N	01110	V	10010	%	11101
G	01010	O	00101	W	11001	=	10110
H	00110	P	01001	X	10101	"	11010

2. Απακρυπτογράφος λαμβάνει το μήνυμα πληροφορίας 11101. Αν είναι γνωστό ότι χρησιμοποιήθηκε συστηματικός κώδικας ομάδας V_5^2 με γεννήτρια :

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

να ελεγχθεί η ορθότητα του μηνύματος και να αποκαλυφθεί το μήνυμα πληροφορίας.

3. Δίνεται η γεννήτρια συστηματικού κώδικα ομάδας V_7^4 :

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

Να κωδικοποιηθεί το μήνυμα πληροφορίας 1110. Να αποκωδικοποιηθούν τα κωδικά μηνύματα 1010011 και 0110101 αφού διορθωθούν τυχόντα σφάλματα.

4. Δίνεται η γεννήτρια συστηματικού κώδικα ομάδας V_6^3 :

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

Να προσδιορισθούν όλες οι κωδικές λέξεις. Να υπολογισθεί η πιθανότητα εσφαλμένης αποκωδικοποίησης με την προϋπόθεση ότι η μετάδοση πραγματοποιείται σε δυαδικό συμμετρικό δίαυλο πληροφορίας με πιθανότητα σφάλματος σε κάθε δυαδικό ψηφίο 1 % .

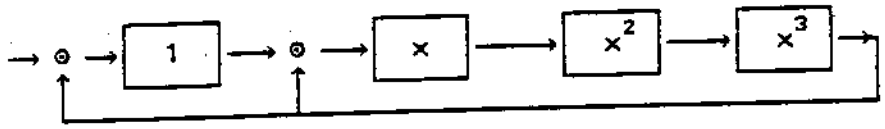
5. Να διαμορφωθούν όλες οι λέξεις κυκλικού κώδικα ομάδας V_7^4 με γεννήτρια $K(x) = x^3 + x + 1$.

6. Να σχεδιασθούν οι καταχωρητές τριών και τεσσάρων θέσεων που υλοποιούν τον κωδικοποιητή της προηγούμενης άσκησης.

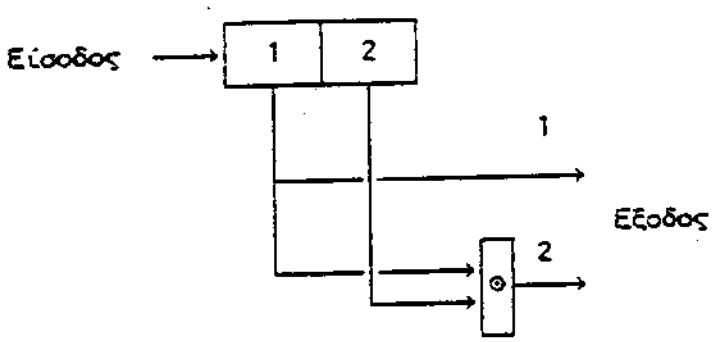
7. Να αποδειχθεί ότι το δυαδικό πολυώνυμο $x^4 + x + 1$ είναι πρώτο πολυώνυμο.

8. Έστω κυκλικός κώδικας ομάδας V_{12}^8 με γεννήτρια $K(x) = x^4 + x + 1$. Να κωδικοποιηθεί το μήνυμα πληροφορίας 10100111 . Να αποκωδικοποιηθεί το κωδικό μήνυμα 001111100111 .

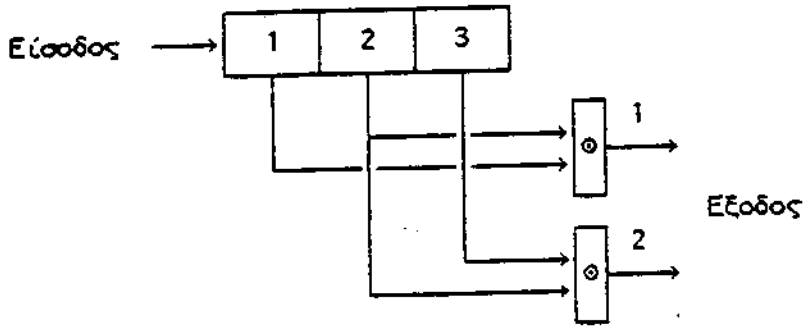
9. Να κωδικοποιηθεί το μήνυμα πληροφορίας 10100111 με τον παρακάτω καταχωρητή τεσσάρων θέσεων που υλοποιεί τον κωδικοποιητή της προηγούμενης άσκησης.



10. Να σχεδιασθεί το δενδροδιάγραμμα, το διάγραμμα trellis και το διάγραμμα καταστάσεων του συνελικτικού κώδικα 1/2 που υλοποιείται από τον παρακάτω καταχωρητή.



11. Να σχεδιασθεί το δενδροδιάγραμμα, το διάγραμμα trellis και το διάγραμμα καταστάσεων του συνελικτικού κώδικα 1/2 που υλοποιείται από τον παρακάτω καταχωρητή.



5.1 ΟΜΑΔΕΣ

ΟΡΙΣΜΟΣ : Ομάδα G = (A, #) ορίζουν κάθε μη κενό σύνολο A και νόμος εσωτερικής συνθέσεως (πράξη) # που υπόκεινται στις παρακάτω αρχές :

(i) Το σύνολο είναι κλειστό ως προς την πράξη. Δηλαδή, αν $\alpha,\beta \in A$, τότε και $\alpha\#\beta \in A$.

(ii) Η πράξη είναι προσεταιριστική. Δηλαδή, αν $\alpha,\beta,\gamma \in A$, τότε $\alpha\#(\beta\#\gamma) = (\alpha\#\beta)\#\gamma$.

(iii) Το σύνολο διαθέτει ουδέτερο στοιχείο για τη συγκεκριμένη πράξη. Αν ο είναι το ουδέτερο στοιχείο, τότε $\alpha\#o = o\#\alpha = \alpha \quad \forall\, \alpha \in A$.

(iv) Για κάθε στοιχείο του συνόλου υπάρχει και το αντίστροφο του ως προς τη

συγκεκριμένη πράξη. Δηλαδή, αν $\tilde{\alpha} \in A$ είναι το αντίστροφο του $\alpha \in A$, τότε $\alpha\#\tilde{\alpha} = o = \tilde{\alpha}\#\alpha$.

Αν επιπλέον η πράξη είναι αντιμεταθετική, δηλαδή $\alpha\#\beta = \beta\#\alpha$ $\forall\ \alpha,\beta \in A$, η αντιμεταθετική ομάδα χαρακτηρίζεται *αβελιανή*. Η ομάδα χαρακτηρίζεται *πεπερασμένη*, αν το σύνολο A έχει πεπερασμένο πλήθος στοιχείων. Το πλήθος των στοιχείων του A είναι η *τάξη* της ομάδας.

ΠΑΡΑΔΕΙΓΜΑ : Το σύνολο των πραγματικών αριθμών R και η πρόσθεση + ορίζουν αβελιανή ομάδα με ουδέτερο στοιχείο το 0. Αντίστροφος κάθε πραγματικού αριθμού α είναι ο πραγματικός αριθμός $-\alpha$, που για τη συγκεκριμένη πράξη χαρακτηρίζεται *αντίθετος*.

ΟΡΙΣΜΟΣ : Αν G = (A, #) είναι ομάδα και A' είναι μη κενό υποσύνολο του A με στοιχεία που ικανοποιούν τις αρχές (i)-(iv), τότε G' = (A', #) είναι *υπο-ομάδα* της G. Είναι φανερό οτι το ουδέτερο στοιχείο περιέχεται σε κάθε υπο-ομάδα.

ΠΑΡΑΔΕΙΓΜΑ : Το σύνολο των ακεραίων αριθμών Z και η πρόσθεση + ορίζουν ομάδα, έστω G. Το υπο-σύνολο του Z που περιέχει τα πολλαπλάσια του 3, δηλαδή τους ακεραίους ... −6, −3, 0, 3, 6, ..., και η πρόσθεση + ορίζουν υπο-ομάδα της G.

ΟΡΙΣΜΟΣ : Εστω πεπερασμένη ομάδα G με νμ στοιχεία και υπο-ομάδα της G' με στοιχεία $\gamma_1, \gamma_2, \ldots, \gamma_\nu$. Είναι φανερό ότι ένα από αυτά, έστω το γ_1, είναι το ουδέτερο στοιχείο. Τα στοιχεία της ομάδας G διατάσσονται σε μ σειρές ν στοιχείων διαμορφώνοντας έτσι το μxν μητρώο παρασυνόλων :

$$\begin{bmatrix} & \gamma_1 & \gamma_2 & \cdots & \gamma_\nu \\ \delta_1 & = \gamma_1\#\delta_1 & \gamma_2\#\delta_1 & \cdots & \gamma_\nu\#\delta_1 \\ \delta_2 & = \gamma_1\#\delta_2 & \gamma_2\#\delta_2 & \cdots & \gamma_\nu\#\delta_2 \\ \cdots & \cdots & \cdots & & \\ \delta_{\mu-1} & = \gamma_1\#\delta_{\mu-1} & \gamma_2\#\delta_{\mu-1} & \cdots & \gamma_\nu\#\delta_{\mu-1} \end{bmatrix}$$

όπου δ_i είναι στοιχείο της ομάδας που δεν έχει χρησιμοποιηθεί στις προηγούμενες i σειρές. Κάθε σειρά του μητρώου ονομάζεται *δεξιό παρασύνολο* της υπο-ομάδας G' και τα στοιχεία $\delta_1, \delta_2, \ldots, \delta_{\mu-1}$ που χρησιμοποιούνται στην πρώτη θέση κάθε σειράς ονομάζονται *οδηγοί παρασυνόλων*. Εξυπονοείται ότι είναι δυνατό να διαμορφωθούν και αριστερά παρασύνολα με στοιχεία της μορφής $\delta_i \# \gamma_k$. Τα αντίστοιχα μητρώα ταυτίζονται αν η πράξη # είναι αντιμεταθετική.

ΘΕΩΡΗΜΑ : Κάθε στοιχείο της ομάδας G εμφανίζεται σε ένα μόνο παρασύνολο.

Έστω ότι το στοιχείο $\alpha \in A$ της ομάδας $G = (A, \#)$ ανήκει στα παρασύνολα με οδηγούς δ_i, δ_k. Χωρίς περιορισμό της γενικότητας μπορεί να γίνει δεκτό ότι $i > k$. Προφανώς $\alpha = \gamma_m \# \delta_i = \gamma_n \# \delta_k$ και επομένως $\delta_i = (\tilde{\gamma}_m \# \gamma_n) \# \delta_k = \gamma_l \# \delta_k$. Η τελευταία σχέση δείχνει ότι ο οδηγός του i+1 παρασυνόλου έχει χρησιμοποιηθεί στο k+1 παρασύνολο που, σύμφωνα με την υπόθεση, προηγείται. Αυτό όμως δεν συμβιβάζεται με τη διαδικασία κατασκευής του μητρώου παρασυνόλων. Άρα η αρχική υπόθεση οδηγεί σε άτοπο και το θεώρημα έχει αποδειχθεί.

ΘΕΩΡΗΜΑ : Δύο στοιχεία α, β ομάδας G ανήκουν στο ίδιο παρασύνολο αν και μόνον αν το στοιχείο $\tilde{\alpha} \# \beta$ ανήκει στην υπο-ομάδα G' .

Αν α, β ανήκουν στο παρασύνολο με οδηγό το στοιχείο δ_i, τότε $\alpha = \gamma_m \# \delta_i$ και $\beta = \gamma_n \# \delta_i$. Επομένως $\tilde{\alpha} \# \beta = (\tilde{\gamma}_m \# \tilde{\delta}_i) \# (\gamma_n \# \delta_i) = \tilde{\gamma}_m \# \gamma_n = \gamma_l$. δηλαδή είναι στοιχείο της υπο-ομάδας G' και το ευθύ μέρος του θεωρήματος έχει αποδειχθεί. Εύκολα προκύπτει και το αντίστροφο.

5.II ΠΕΔΙΑ

ΟΡΙΣΜΟΣ : Πεδίο $F = (A, \#, @)$ ορίζουν μη κενό σύνολο A και νόμοι εσωτερικής συνθέσεως (πράξεις) #, @ που υπόκεινται στις παρακάτω αρχές :

(i) Το σύνολο είναι κλειστό ως προς τις πράξεις. Δηλαδή, αν $\alpha, \beta \in A$, τότε $\alpha \# \beta \in A$ και $\alpha @ \beta \in A$.

(ii) Οι πράξεις είναι αντιμεταθετικές και προσεταιριστικές. Δηλαδή, αν

$\alpha,\beta,\gamma \in A$, τότε $\alpha\#\beta = \beta\#\alpha$, $\alpha\theta\beta = \beta\theta\alpha$, $(\alpha\#\beta)\#\gamma = \alpha\#(\beta\#\gamma)$ και $(\alpha\theta\beta)\theta\gamma = \alpha\theta(\beta\theta\gamma)$.

(iii) Για καθε πράξη υπάρχει ουδέτερο στοιχείο. Αν ο και π είναι το ουδέτερο στοιχείο για την πράξη # και θ, αντίστοιχα, τότε $\alpha\#o = o\#\alpha = \alpha$ και $\alpha\theta\pi = \pi\theta\alpha = \alpha$, $\forall\, \alpha \in A$.

(iv) Το σύνολο περιέχει το αντίστροφο κάθε στοιχείου ως προς τις δύο πράξεις. Αν $\tilde{\alpha}$ και $\hat{\alpha}$ είναι το αντίστροφο του $\alpha \in A$ ως προς # και θ, αντίστοιχα, τότε $\alpha\#\tilde{\alpha} = \tilde{\alpha}\#\alpha = o$ και $\alpha\theta\hat{\alpha} = \hat{\alpha}\theta\alpha = \pi$.
(v) Ισχύει η επιμεριστική ιδιότητα $\alpha\theta(\beta\#\gamma) = (\alpha\theta\beta)\#(\alpha\theta\gamma)$ όπου $\alpha,\beta,\gamma \in A$.

ΠΟΡΙΣΜΑ : Αν $F = \{ A, \#, \theta \}$ είναι πεδίο, τότε $\{ A, \# \}$ και $\{ A, \theta \}$ είναι αβελιανές ομάδες.

ΠΑΡΑΔΕΙΓΜΑ : Το σύνολο των πραγματικών αριθμών R, η πρόσθεση + και ο πολλαπλασιασμός · ορίζουν πεδίο. Ουδέτερο στοιχείο για την πρόσθεση είναι το μηδέν και για τον πολλαπλασιασμό η μονάδα. Αντίστροφος του πραγματικού αριθμού, έστω 4, είναι για την πρόσθεση ο πραγματικός αριθμός −4 ενώ για τον πολλαπλασιασμό είναι ο πραγματικός αριθμός 0.25 . Προφανώς ισχύουν η αντιμεταθετική, προσεταιριστική και επιμεριστική ιδιότητα.

5.III ΔΙΑΝΥΣΜΑΤΙΚΟΙ ΧΩΡΟΙ

ΟΡΙΣΜΟΣ : Διάνυσμα ν−τάξεως επί του πεδίου $F = \{ A, \#, \theta \}$ είναι κάθε διάταξη ν στοιχείων του συνόλου A. Δηλαδή, αν $x_1, x_2, \ldots, x_\nu \in A$, τότε $X = (x_1, x_2, \ldots, x_\nu)$ είναι ένα διάνυσμα ν−τάξεως επί του πεδίου F.

ΟΡΙΣΜΟΣ : Διανυσματικός χώρος V_ν επί του πεδίου F είναι κάθε σύνολο διανυσμάτων ν−τάξεως $X = (x_1, x_2, \ldots, x_\nu)$ επί του πεδίου F που υπόκεινται στις αρχές :

(i) $\{ V_\nu, \# \}$ αποτελεί αβελιανή ομάδα. Η πράξη # μεταξύ δύο διανυσμάτων $X,\Psi \in V_\nu$ παράγει το διάνυσμα $X\#\Psi \in V_\nu$, όπου $X\#\Psi = (x_1\#\psi_1, x_2\#\psi_2, \ldots, x_\nu\#\psi_\nu)$ και προφανώς $X\#\Psi = \Psi\#X$, $(X\#\Psi)\#Z = X\#(\Psi\#Z)$ με $Z \in V_\nu$. Ουδέτερο στοιχείο είναι το διάνυσμα ν−τάξεως $O = (o, o, \ldots, o)$, όπου o είναι το ουδέτερο στοιχείο της

αβελιανής ομάδας (A, #). Αντίστροφο του διανύσματος $X = (x_1, x_2, \ldots, x_\nu)$ είναι το διάνυσμα $\tilde{X} = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_\nu)$ όπου $\tilde{x}$ είναι το αντίστροφο του στοιχείου x της αβελιανής ομάδας (A, #).

(ii) Η πράξη @ μεταξύ διανύσματος $X = (x_1, x_2, \ldots, x_\nu) \in V_\nu$ και στοιχείου $\kappa \in A$, που χαρακτηρίζεται σαν βαθμωτό γινόμενο, παράγει διάνυσμα $\kappa@X = (\kappa@x_1, \kappa@x_2, \ldots, \kappa@x_\nu) \in V_\nu$. Το βαθμωτό γινόμενο έχει την αντιμεταθετική, προσεταιριστική και επιμεριστική ιδιότητα, δηλαδή αν $X,\Psi \in V_\nu$ και $\kappa,\lambda \in A$, τότε $\kappa@X = X@\kappa$, $\kappa@(\lambda@X) = (\kappa@\lambda)@X$ και $\kappa@(X\#\Psi) = (\kappa@X)\#(\kappa@\Psi)$. Αν η είναι το ουδέτερο στοιχείο της αβελιανής ομάδας (A, @), τότε $\eta@X = X@\eta = X \ \forall \ X \in V_\nu$. Ακόμη αν $\hat{\kappa}$ είναι το αντίστροφο του στοιχείου κ της αβελιανής ομάδας (A, @), τότε $\kappa@(\hat{\kappa}@X) = (\hat{\kappa}@\kappa)@X = X \in V_\nu$.

(iii) Η πράξη @ μεταξύ διανυσμάτων, που χαρακτηρίζεται σαν εσωτερικό γινόμενο, παράγει στοιχείο του συνόλου A, δηλαδή αν $X,\Psi \in V_\nu$, τότε $X@\Psi = (x_1@\psi_1)\#(x_2@\psi_2)\#\ldots(x_\nu@\psi_\nu) \in A$. Αν $X@\Psi = o$, τα διανύσματα X,Ψ είναι ορθογώνια.

ΠΑΡΑΔΕΙΓΜΑ : Διάνυσμα 3ης-τάξεως επί του πεδίου (R, +, ·) αποτελεί οποιαδήποτε διάταξη τριών πραγματικών αριθμών, έστω η (5, 4, 0.5). Το σύνολο όλων των διανυσμάτων 3ης-τάξεως αποτελεί 3-διάστατο διανυσματικό χώρο επί του πεδίου (R, +, ·). Το εσωτερικό γινόμενο έχει τη μορφή $X\cdot\Psi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3$, όπου $X = (x_1, x_2, x_3)$ και $\Psi = (\psi_1, \psi_2, \psi_3)$ είναι διανύσματα 3ης-τάξεως με στοιχεία πραγματικούς αριθμούς. Αν $X = (1, 4, 7)$, $\Psi = (3, 2, 1)$, τότε $X\cdot\Psi = 18$. Τα διανύσματα 3ης-τάξεως $X = (1, 4, 7)$, $\Psi = (-2, 4, -2)$ είναι ορθογώνια αφού $X\cdot\Psi = 0$. Είναι φανερό ότι ο διανυσματικός χώρος V_3 αντιστοιχεί στον τριδιάστατο Ευκλείδιο χώρο. Οι τριάδες πραγματικών αριθμών που ορίζουν ένα στοιχείο του διανυσματικού χώρου αντιστοιχούν στις Καρτεσιανές συντεταγμένες (x, y, z) σημείου του τριδιάστατου Ευκλείδιου χώρου.

ΟΡΙΣΜΟΣ : Αν V_ν είναι ν-διάστατος διανυσματικός χώρος επί του πεδίου (A, #, @) και V'_ν είναι μη κενό υποσύνολο του V_ν με στοιχεία που ικανοποιούν τις αρχές (i)-(iii), τότε το σύνολο των διανυσμάτων ν-τάξεως V'_ν αποτελεί διανυσματικό *υπο-χώρο* του V_ν επί του πεδίου (A, #, @).

ΠΑΡΑΔΕΙΓΜΑ : Τα διανύσματα 3ης-τάξεως (α, β, 0) με $\alpha,\beta \in R$ ανήκουν σε διανυσματικό υπο-χώρο του V_3, έστω V'_3. Από γεωμετρική άποψη τα διανύσματα του υπο-χώρου αντιστοιχούν σε σημεία επί του επιπέδου z = 0, δηλαδή ενώ ο

διανυσματικός χώρος V_3 αντιστοιχεί στον τριδιάστατο Ευκλείδιο χώρο, ο διανυσματικός υπο-χώρος V'_3 αντιστοιχεί σε διδιάστατο επίπεδο.

Είναι ήδη φανερό ότι η έννοια της διάστασης είναι διαφορετική στη γραμμική άλγεβρα και στη γεωμετρία. Η διάκριση αυτή έγινε σωστηλά δεκτή χρησιμοποιώντας τον όρο *διάνυσμα ν-τάξεως* αντί του όρου *ν-διάστατο διάνυσμα*. Στο παράδειγμα γίνεται σαφές ότι ένα διάνυσμα 3ης-τάξεως που ανήκει στο διανυσματικό υπο-χώρο V'_3 αντιστοιχεί σε διδιάστατο και όχι τριδιάστατο διάνυσμα του Ευκλείδιου χώρου. Προκειμένου να οριστεί η έννοια της διάστασης διανυσματικού χώρου είναι απαραίτητο να περιγραφεί η γραμμική εξάρτηση - ανεξαρτησία διανυσμάτων ν-τάξεως. Σε ό,τι ακολουθεί θεωρούνται διανυσματικοί χώροι επί του πεδίου $\{ R, +, \cdot \}$.

ΟΡΙΣΜΟΣ : Γραμμικός συνδυασμός μ διανυσμάτων ν-τάξεως $X_1, X_2, \ldots, X_\mu$ είναι το διάνυσμα ν-τάξεως $X = \kappa_1 X_1 + \kappa_2 X_2 + \ldots + \kappa_\mu X_\mu$, όπου $\kappa_1, \kappa_2, \ldots, \kappa_\mu \in R$. Τα διανύσματα $X_1, X_2, \ldots, X_\mu$ θεωρούνται γραμμικά ανεξάρτητα αν η σχέση $\kappa_1 X_1 + \kappa_2 X_2 + \ldots + \kappa_\mu X_\mu = 0$ ισχύει μόνο εφόσον $\kappa_1 = \kappa_2 = \ldots = \kappa_\mu = 0$. Αντίθετα, αν υπάρχουν πραγματικοί αριθμοί $\kappa_1, \kappa_2, \ldots, \kappa_\mu$, που δεν είναι όλοι μηδέν, τέτοιοι ώστε $\kappa_1 X_1 + \kappa_2 X_2 + \ldots + \kappa_\mu X_\mu = 0$, τότε τα διανύσματα $X_1, X_2, \ldots, X_\mu$ θεωρούνται γραμμικά εξαρτημένα και επομένως οποιοδήποτε από αυτά είναι δυνατό να γραφεί σαν γραμμικός συνδυασμός των υπολοίπων.

ΘΕΩΡΗΜΑ : Το σύνολο των γραμμικών συνδυασμών δοθέντων διανυσμάτων $X_1, X_2, \ldots, X_\mu$ αποτελεί διανυσματικό χώρο.

Είναι εύκολο να αποδειχθεί ότι οι γραμμικοί συνδυασμοί των διανυσμάτων $X_1, X_2, \ldots, X_\mu$ ικανοποιούν τις αρχές (i)-(iii) του ορισμού διανυσματικού χώρου.

ΟΡΙΣΜΟΣ : Ο διανυσματικός χώρος που περιέχει όλους τους γραμμικούς συνδυασμούς των διανυσμάτων $X_1, X_2, \ldots, X_\mu$ ορίζεται σαν *διανυσματικός χώρος που διατρέχουν τα διανύσματα* $X_1, X_2, \ldots, X_\mu$. Τα διανύσματα $X_1, X_2, \ldots, X_\mu$ αποτελούν τη *γεννήτρια* του εν λόγω διανυσματικού χώρου.

ΟΡΙΣΜΟΣ : *Βάση* διανυσματικού χώρου είναι κάθε γεννήτρια του που συνίσταται από γραμμικά ανεξάρτητα διανύσματα.

ΠΑΡΑΔΕΙΓΜΑ : Τα διανύσματα 3ης-τάξεως $E_1 = (1, 0, 0)$, $E_2 = (0, 1, 0)$, $E_3 = (0, 0, 1)$ διατρέχουν το διανυσματικό χώρο V_3. Το διάνυσμα $X = (4, 3, 7)$

γράφεται $X = 4E_1 + 3E_2 + 7E_3$ και ανάλογη έκφραση είναι δυνατό να γραφεί για κάθε διάνυσμα του V. Είναι επιπλέον προφανές ότι τα διανύσματα E_1, E_2, E_3 είναι γραμμικά ανεξάρτητα και επομένως αποτελούν βάση του διανυσματικού χώρου V_3.

ΘΕΩΡΗΜΑ : Στο διανυσματικό χώρο που διατρέχουν τα διανύσματα X_1, X_2, ..., X_μ υπάρχουν $\lambda \leq \mu$ γραμμικά ανεξάρτητα διανύσματα.

ΟΡΙΣΜΟΣ : Διάσταση διανυσματικού χώρου είναι το μέγιστο πλήθος των γραμμικά ανεξάρτητων διανυσμάτων που περιέχει. Η διάσταση, έστω μ, του διανυσματικού χώρου V_ν μπορεί να συμπεριληφθεί στο συμβολισμό του σαν άνω δείκτης, οπότε διαμορφώνεται το σύμβολο V_ν^μ.

ΘΕΩΡΗΜΑ : Αν δύο σύνολα γραμμικά ανεξάρτητων διανυσμάτων διατρέχουν τον ίδιο διανυσματικό χώρο, τότε τα σύνολα αυτά περιέχουν ισάριθμα διανύσματα.

ΘΕΩΡΗΜΑ : Ο διανυσματικός χώρος V_ν^ν που συνίσταται από όλα τα διανυσμάτα ν-τάξεως έχει διάσταση ν.

Αυτό διαπιστώνεται θεωρώντας τα *καταστατικά* διανύσματα ν-τάξεως

$$E_1 = (1, 0, 0, \ldots, 0)$$

$$E_2 = (0, 1, 0, \ldots, 0)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$E_\nu = (0, 0, 0, \ldots, 1)$$

Κάθε διάνυσμα ν-τάξεως, έστω $X = (X_1, X_2, \ldots, X_\nu)$, γράφεται με τη μορφή $X = X_1E_1 + X_2E_2 + \ldots + X_\nu E_\nu$, δηλαδή σαν γραμμικός συνδυασμός των καταστατικών διανυσμάτων. Επομένως το σύνολο V_ν^ν όλων των διανυσμάτων ν-τάξεως είναι ο διανυσματικός χώρος που διατρέχουν τα καταστατικά διανύσματα ν-τάξεως E_1, E_2, ..., E_ν και, αφού αυτά είναι γραμμικά ανεξάρτητα, ο διανυσματικός χώρος V_ν^ν έχει διάσταση ν.

ΠΟΡΙΣΜΑ : Κάθε διανυσματικός χώρος V_ν^μ με $\mu \leq \nu$ είναι διανυσματικός υπο-χώρος του V_ν^ν.

ΟΡΙΣΜΟΣ : Έστω διανυσματικός υπο-χώρος V_ν^μ, $\mu \leq \nu$, του V_ν^ν. *Μηδενικός υπο-χώρος* του V_ν^μ είναι ο διανυσματικός υπο-χώρος ${}^0V_\nu^\mu$ που συνίσταται από όλα τα διανύσματα ν-τάξεως που είναι ορθογώνια προς τα διανύσματα ν-τάξεως του V_ν^μ. Δηλαδή, αν $X \cdot \Psi = 0 \quad \forall \Psi \in V_\nu^\mu$, τότε $X \in {}^0V_\nu^\mu$.

ΠΑΡΑΔΕΙΓΜΑ : Τα διανύσματα 3ης-τάξεως $(\alpha, \beta, 0)$ με $\alpha, \beta \in R$ ανήκουν στο διανυσματικό υπο-χώρο V_3^2. Τα διανύσματα 3ης-τάξεως $(0, 0, \gamma)$ με $\gamma \in R$ είναι ορθογώνια προς τα διανύσματα 3ης-τάξεως του υπο-χώρου V_3^2, επειδή $(\alpha, \beta, 0) \cdot (0, 0, \gamma) = 0$. Επομένως τα διανύσματα 3ης-τάξεως $(0, 0, \gamma)$ ανήκουν στο μηδενικό υπο-χώρο ${}^0V_3^2$ του V_3^2.

ΘΕΩΡΗΜΑ : Η διάσταση του υπο-χώρου ${}^0V_\nu^\mu$ είναι ν-μ, δηλαδή ${}^0V_\nu^\mu = V_\nu^{\nu-\mu}$.

ΠΟΡΙΣΜΑ : ${}^0V_\nu^{\nu-\mu} = V_\nu^{\nu-(\nu-\mu)} = V_\nu^\mu$.

5.IV MODULO - P ΑΡΙΘΜΗΤΙΚΗ

Το υπόλοιπο της διαίρεσης α/ρ, όπου α, ρ θετικοί ακέραιοι, είναι κάποιος από τους ακεραίους $0, 1, \ldots, \rho-1$. Η modulo-ρ αριθμητική αντικαθιστά κάθε ακέραιο α με το υπόλοιπο της διαίρεσης α/ρ. Δηλαδή, αν $\alpha = \rho n + \upsilon$, όπου n, υ ακέραιοι, τότε :

$$\alpha \equiv \upsilon \pmod{\rho} \qquad (1)$$

ΠΑΡΑΔΕΙΓΜΑ : Έστω $\rho = 2$. Το υπόλοιπο της διαίρεσης οποιουδήποτε ακεραίου α διά 2 μπορεί να είναι 0 ή 1. Επειδή $37 = 2 \cdot 18 + 1$, κατά την εξ.(1) ισχύει $37 \equiv 1 \pmod{2}$.

Οι πράξεις μεταξύ ακεραίων στη modulo-ρ αριθμητική μπορούν να γίνονται όπως και στη συνηθισμένη αριθμητική. Τα αποτελέσματα όμως πρέπει να μετατρέπονται στους ακεραίους $0, 1, \ldots, \rho-1$ υπολογίζοντας το υπόλοιπο της διαίρεσης α/ρ.

ΠΑΡΑΔΕΙΓΜΑ : Έστω $\rho = 3$, $\alpha = 5$ και $\beta = 7$. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στη modulo-ρ αριθμητική δίνουν για τους ακεραίους α, β :

$$\alpha + \beta = 5 + 7 = 12 \equiv 0 \pmod 3$$

$$\alpha\beta = 5 \cdot 7 = 35 \equiv 2 \pmod 3$$

Στα ίδια αποτελέσματα καταλήγουν και οι πράξεις μεταξύ u_α και u_β, όπου $\alpha \equiv u_\alpha \pmod \rho$ και $\beta \equiv u_\beta \pmod \rho$:

$$\alpha = 5 \equiv 2 \pmod 3 = u_\alpha$$

$$\beta = 7 \equiv 1 \pmod 3 = u_\beta$$

$$\alpha + \beta \equiv u_\alpha + u_\beta \pmod 3 = 2 + 1 = 3 \equiv 0 \pmod 3$$

$$\alpha\beta \equiv u_\alpha u_\beta \pmod 3 = 2 \cdot 1 = 2 \equiv 2 \pmod 3$$

Οπως παρατηρείται στο τελευταίο παράδειγμα, αν και $\alpha, \beta > 0$, είναι δυνατό $\alpha + \beta \equiv 0 \pmod \rho$. Το ίδιο μπορεί να συμβεί και με την πράξη του πολλαπλασιασμού. Δηλαδή είναι δυνατό $\alpha\beta \equiv 0 \pmod \rho$ παρόλο που $\alpha > 0$ και $\beta > 0$ (π.χ., $5 \cdot 12 = 60 \equiv 0 \pmod{10}$). Αν ρ είναι πρώτος ακέραιος, δηλαδή ακέραιος που διαιρείται ακριβώς μόνο από τους ακεραίους 1 και ρ, τότε $\alpha\beta \equiv 0 \pmod \rho$ μόνο αν $\alpha = 0$ ή $\beta = 0$.

5.V MODULO - K(X) ΑΛΓΕΒΡΑ

ΟΡΙΣΜΟΣ : Δυαδικό πολυώνυμο είναι κάθε πολυώνυμο με δυαδικούς συντελεστές.

ΟΡΙΣΜΟΣ : Ενικό δυαδικό πολυώνυμο ν-βαθμού είναι κάθε δυαδικό πολυώνυμο με συντελεστή 1 για τον όρο x^ν.

ΠΑΡΑΔΕΙΓΜΑ : Το πολυώνυμο $X(x) = x^3 + x + 1 = 1x^3 + 0x^2 + 1x + 1$ είναι 3ου-βαθμού, ενικό, δυαδικό πολυώνυμο .

ΘΕΩΡΗΜΑ : Το σύνολο των ν-βαθμού, δυαδικών πολυωνύμων, έστω P_ν, και η δυαδική

πρόσθεση ⊙ αποτελούν ομάδα.

Η ισχύς του θεωρήματος θα ελεγχθεί με τη βοήθεια των πολυωνύμων $X(x) = x^3 + x + 1$, $\Psi(x) = x^2 + x$ και $Z(x) = x$, που είναι δυνατό να θεωρηθούν σαν 3ου-βαθμού, δυαδικά πολυώνυμα :

$$X(x) = 1x^3 + 0x^2 + 1x + 1 = x^3 + x + 1$$

$$\Psi(x) = 0x^3 + 1x^2 + 1x + 0 = x^2 + x$$

$$Z(x) = 0x^3 + 0x^2 + 1x + 0 = x$$

Η προσαρμογή στις αρχές (i)-(iv) της §5.I διαπιστώνεται ως εξής :

(i) Η πρόσθεση 3ου-βαθμού, δυαδικών πολυωνύμων $X(x) \odot \Psi(x) = 1x^3 + 1x^2 + 0x + 1 = x^3 + x^2 + 1$ καταλήγει σε 3ου-βαθμού, δυαδικό πολυώνυμο.

(ii) Η δυαδική πρόσθεση είναι προσεταιριστική : $(X(x) \odot \Psi(x)) \odot Z(x) = X(x) \odot (\Psi(x) \odot Z(x)) = 1x^3 + 1x^2 + 1x + 1 = x^3 + x^2 + x + 1$.

(iii) Ουδέτερο στοιχείο είναι το 3ου-βαθμού, δυαδικό, πολυώνυμο $O(x) = 0x^3 + 0x^2 + 0x + 0 = 0$ αφού $X(x) \odot O(x) = O(x) \odot X(x) = X(x)$.

(iv) Το αντίστροφο (αντίθετο) κάθε 3ου-βαθμού, δυαδικού πολυωνύμου είναι το ίδιο πολυώνυμο αφού $X(x) \odot X(x) = O(x)$.

Ο πολλαπλασιασμός μεταξύ δυαδικών πολυωνύμων είναι συνήθης πολλαπλασιασμός τόσο ως προς τους όρους της ανεξάρτητης μεταβλητής x όσο και ως προς τους συντελεστές, δηλαδή $(\kappa_i x^i)(\kappa_j x^j) = (\kappa_i \kappa_j) x^{i+j}$. Οι συντελεστές ομόβαθμων όρων αθροίζονται δυαδικά, δηλαδή $1x^4 + 1x^4 = (1 \odot 1)x^4 = 0$.Το γινόμενο δύο δυαδικών πολυωνύμων είναι επίσης δυαδικό πολυώνυμο βαθμού ίσου με το άθροισμα των βαθμών των παραγόντων. Επειδή συχνά είναι απαραίτητο ο βαθμός του γινομένου δύο πολυωνύμων να μην υπερβαίνει κάποιο άνω φράγμα, εισάγεται η πράξη του modulo-2 & modulo-K(x) πολλαπλασιασμού ● όπου K(x) είναι το modulus πολυώνυμο. Αν K(x) είναι ρ-βαθμού, ενικό, δυαδικό πολυώνυμο, δηλαδή $K(x) = x^\rho + \kappa_1 x^{\rho-1} + \kappa_2 x^{\rho-2} + \ldots + \kappa_{\rho-1} x + \kappa_\rho$, τότε κατά το πρότυπο της modulo-ρ αριθμητικής (βλ. §5.IV), κάθε πολυώνυμο X(x) αντικαθίσταται από το υπόλοιπο της διαίρεσης

$X(x)/K(x)$. Δηλαδή, αν $X(x) = \Pi(x)K(x) \oplus Y(x)$, τότε :

$$X(x) \equiv Y(x) \quad [\mathrm{mod}K(x)] \tag{1}$$

και είναι προφανές ότι ο βαθμός του $Y(x)$ είναι κάποιος ακέραιος από το διάστημα $[\,0,\ \rho-1\,]$.

ΠΑΡΑΔΕΙΓΜΑ : Εστω $K(x) = x^3 + x + 1$ και $X(x) = x^5 + x^2$. Η διαίρεση $X(x)/K(x)$ περιγράφεται αναλυτικά παρακάτω :

$$\begin{array}{r|l} x^5 + x^2 & x^3 + x + 1 \\ \cline{2-2} x^5 + x^3 + x^2 & x^2 + 1 \\ \cline{1-1} x^3 & \\ x^3 + x + 1 & \\ \cline{1-1} x + 1 & \end{array}$$

και επομένως $x^5 + x^2 = (x^2+1)(x^3 + x + 1) \oplus (x + 1)$, δηλαδή κατά την εξ.(1) :

$$x^5 + x^2 \equiv x + 1 \quad [\mathrm{mod}(x^3 + x + 1)] \tag{2}$$

Η πράξη $\otimes$ μεταξύ δύο πολυωνύμων $X(x)$, $\Psi(x)$ είναι αρχικά modulo-2 πολλαπλασιασμός μεταξύ των $Y_x(x)$ και $Y_\psi(x)$, δηλαδή των υπολοίπων των διαιρέσεων $X(x)/K(x)$ και $\Psi(x)/K(x)$, αντίστοιχα. Στη συνέχεια και το γινόμενο $Y_x(x)Y_\psi(x)$ αντικαθίσταται από το υπόλοιπο της διαίρεσης με το modulus πολυώνυμο.

ΠΑΡΑΔΕΙΓΜΑ : Εστω $K(x) = x^3 + x + 1$, $X(x) = x^5 + x^2$ και $\Psi(x) = x + 1$. Εύκολα διαπιστώνεται ότι $Y_x(x) = x + 1$ και $Y_\psi(x) = x + 1$. Επομένως $Y_x(x)Y_\psi(x) = x^2+ 1$ και τελικά $X(x)\otimes\Psi(x) = Y_x(x)Y_\psi(x)$ $[\mathrm{mod}K(x)] = x^2+ 1$. Στο ίδιο αποτέλεσμα οδηγεί και modulo-2 πολλαπλασιασμός των $X(x)$, $\Psi(x)$ αρκεί το γινόμενο να αντικατασταθεί με το υπόλοιπο της διαίρεσης με $K(x)$. Πράγματι, $X(x)\Psi(x) = x^6 + x^5 + x^3 + x^2 \equiv x^2+ 1$ $[\mathrm{mod}K(x)]$.

Αν το modulus πολυώνυμο $K(x)$ είναι μη παραγοντοποιήσιμο, δηλαδή πρώτο πολυώνυμο, τότε η εξίσωση $X(x)\otimes\Psi(x) = 0$ συνεπάγεται ότι $X(x) = 0$ ή/και $\Psi(x) = 0$. Στην αντίθετη περίπτωση είναι δυνατό $X(x)\otimes\Psi(x) = 0$ παρόλο που $X(x) \neq 0$ και $\Psi(x) \neq 0$.

ΠΑΡΑΔΕΙΓΜΑ : Εστω $K(x) = x^3 + x$, $X(x) = x$ και $\Psi(x) = x^2 + 1$. Είναι προφανές ότι

$X(x) \otimes \Psi(x) = x \otimes (x^2 + 1) = x^3 + x \equiv 0 \quad [\mathrm{mod} K(x)]$ παρόλο που $X(x) \neq 0$ και $\Psi(x) \neq 0$.

ΘΕΩΡΗΜΑ : Αν κάθε πολυώνυμο αντικατασταθεί από το υπόλοιπο της διαίρεσης με κάποιο ρ-βαθμού, πρώτο, modulus πολυώνυμο, τότε όλα τα πολυώνυμα θα έχουν βαθμό μικρότερο από ρ. Το σύνολο αυτών των πολυωνύμων, έστω P_ρ, εφοδιασμένο με τις πράξεις $\otimes$ και $\circledast$, αποτελεί το πολυωνυμικό πεδίο $F_\rho(x) = (P_\rho, \otimes, \circledast)$.

Σύμφωνα με όσα προαναφέρθηκαν, το σύνολο P_ρ είναι κλειστό ως προς τις πράξεις $\otimes$ και $\circledast$. Είναι προφανές ότι και οι δύο πράξεις είναι αντιμεταθετικές και προσεταιριστικές. Επιπλέον ισχύει προφανώς και η επιμεριστική ιδιότητα. Το ουδέτερο στοιχείο των πράξεων $\otimes$, $\circledast$ είναι, αντίστοιχα, το τετριμμένο πολυώνυμο 0, 1 . Το αντίστροφο του πολυωνύμου $X(x)$ ως προς την πράξη $\otimes$ είναι το ίδιο πολυώνυμο αφού $X(x) \otimes X(x) = 0$. Εξάλλου το αντίστροφο του πολυωνύμου $X(x)$ ως προς την πράξη $\circledast$ είναι το πολυώνυμο $\hat{X}(x) = 1/X(x)$ που υπολογίζεται εφαρμόζοντας την εξίσωση $K(x) = 0$. Εφόσον το modulus πολυώνυμο είναι μη παραγοντοποιήσιμο, η τυπική μορφή του $K(x) = x^\rho + \kappa_1 x^{\rho-1} + \kappa_2 x^{\rho-2} + \ldots + \kappa_{\rho-1} x + \kappa_\rho$ υποδεικνύει ότι $\kappa_\rho = 1$. Επομένως η εξίσωση $K(x) = 0$ ισοδυναμεί με την εξίσωση $1 = x^\rho + \kappa_1 x^{\rho-1} + \kappa_2 x^{\rho-2} + \ldots + \kappa_{\rho-1} x$ και $\hat{X}(x) = 1/X(x) = (x^\rho + \kappa_1 x^{\rho-1} + \kappa_2 x^{\rho-2} + \ldots + \kappa_{\rho-1} x) /X(x)$.

ΠΑΡΑΔΕΙΓΜΑ : Έστω $K(x) = x^3 + x + 1$, $X(x) = x + 1$. Η εξίσωση $K(x) = 0$ ισοδυναμεί με την εξίσωση $1 = x^3 + x$. Επομένως $\hat{X}(x) = 1/X(x) = (x^3 + x)/(x + 1) = x^2 + x$.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Abramson N., *Information Theory and Coding*, McGraw-Hill, New York, 1963.

2. Bell D.A., *Information Theory and its Engineering Applications*, Pitman, London, 1968.

3. Berlecamp E.R. (Ed.), *Key Papers in the Development of Coding Theory*, IEEE Press, New York, 1974.

4. Davenport W.B. Jr., *Probability and Random Processes*, McGraw-Hill, New York, 1970.

5. Fano R.M., *Transmission of Information*, MIT Press, Cambridge, Massachusetts, 1961.

6. Fainstein A., *Foundations of Information Theory*, McGraw-Hill, New York, 1958.

7. Gallager R.G., *Information Theory and Reliable Communication*, John Wiley, New York, 1968.

8. Gatlin L.L., *Information Theory and the Living System*, Columbia Univ. Press, New York, 1972.

9. Gray R.M., *Source Coding Theory*, Kluwer Academic Publishers, Boston, 1990.

10. Guiasu S., *Information Theory with Applications*, McGraw-Hill, New York, 1977.

11. Hamming R.W., *Coding and Information Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1980.

12. Hartley R.V.L., Transmission of Information, *Bell Systems Tech. Jour.* 7, 535-563, 1928.

13. Huffmann D.A., A Method for the Construction of Minimum Redundancy Codes, *Proc. IRE* 40, 1098-1101, 1952.

14. Ingels F.M., *Information and Coding Theory*, Intext, Scranton, Pennsylvania, 1971.

15. Jelinek F., *Probabilistic Information Theory*, McGraw-Hill, New York, 1958.

16. Khinchin A.I., *Mathematical Foundations of Information Theory*, Dover, New York, 1957.

17. Lin S., *An Introduction to Error-Correcting Codes*, Prentice-Hall, Englewood Cliffs, New Jersey, 1970.

18. McEliece R.J., *The Theory of Information and Coding*, Addison-Wesley, Reading, Massachusetts, 1977.

19. McWilliams J. and Sloane N.J.A., *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

20. Muroga S., On the Capacity of a Discrete Channel, *Jour. Phys. Soc. of Japan* 8, 484-494, 1953.

21. Nyquist H., Certain Factors Affecting Telegraph Speed, *Bell Systems Tech. Jour.* 3, 324, 1924.

22. Papoulis A., *Probability, Random Variables and Stochastic Processes*, McGraw-Hill, New York, 1965.

23. Peterson W.W. and Weldon E.J. Jr., *Error-Correcting Codes*, MIT Press, Cambridge, Massachusetts, 1972.

24. Proakis J., *Digital Communications*, McGraw-Hill, New York, 1983.

25. Raisbeck A., *Information Theory*, MIT Press, Cambridge, Massachusetts, 1963.

26. Reza F., *An Introduction to Information Theory*, McGraw-Hill, New York, 1961.

27. Shannon C.E., A Mathematical Theory of Communication, *Bell Systems Tech. Jour.* 27, 379-423, 1948.

28. Shannon C.E., A Mathematical Theory of Communication, *Bell Systems Tech.*

Jour. 27, 623–656, 1948.

29. Slepian D. (Ed.), *Key Papers in the Development of Information Theory*. IEEE Press, New York, 1974.

30. Viterbi A.J. and Omura J.K., *Principles of Digital Communication and Coding*, McGraw-Hill, New York, 1979.

31. Wiener N., *Cybernetics*, John Wiley, New York, 1948.

32. Wozencraft J.M. and Jacobs I.M., *Principles of Communication Engineering*, John Wiley, New York, 1965.

33. Wyner A.D., Fundamental Limits in Information Theory, *Proc. IEEE* 69(2), 239–251, 1981.

ΕΥΡΕΤΗΡΙΟ