ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
(Τ.Ε.Ι.) ΛΑΜΙΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΣΥΜΠΛΗΡΩΜΑΤΙΚΕΣ ΣΗΜΕΙΩΣΕΙΣ

ΜΑΘΗΜΑ: «*ΘΕΩΡΙΑ ΠΛΗΡΟΦΟΡΙΑΣ-ΚΩΔΙΚΕΣ*»

Δρ. ΒΑΡΖΑΚΑΣ ΠΑΝΑΓΙΩΤΗΣ

ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ

ΛΑΜΙΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Οι συμπληρωματικές σημειώσεις που ακολουθούν έχουν γραφτεί για να συμπληρώσουν τις ανάγκες του Μαθήματος "**Θεωρία Πληροφορίας-Κώδικες**" του Ε΄ εξαμήνου του προγράμματος σπουδών του Τμήματος Ηλεκτρονικής του Τ.Ε.Ι. Λαμίας. Η συγγραφή αυτών των συμπληρωματικών διδακτικών σημειώσεων κρίθηκε απαραίτητη διότι σε αυτές παρουσιάζονται επιπλέον στοιχεία θεωρίας, ασκήσεις, παραδείγματα, ασκήσεις με απαντήσεις και εφαρμογές συμπληρώνοντας έτσι το βασικό σύγγραμμα του μαθήματος.

Θα πρέπει να σημειωθεί από το συγγραφέα, ότι η επέκταση, τυχόν διορθώσεις και υποδείξεις στις παρούσες σημειώσεις είναι πάντα ευπρόσδεκτες από τους συναδέλφους και τους φοιτητές του Τμήματος.

Δρ. Βαρζάκας Παναγιώτης
Επίκουρος Καθηγητής
Τμήμα Ηλεκτρονικής
Τ.Ε.Ι Λαμίας

1.Στοιχεία Θεωρίας Πληροφορίας

1.1 Ποσότητα πληροφορίας ενός γεγονότος

Είναι γνωστό ότι η πιθανότητα εμφάνισης ενός γεγονότος είναι άμεσα συνδεδεμένη με την ποσότητα πληροφορίας που μεταφέρει το γεγονός αυτό, [2]. Αν θεωρήσουμε ότι P είναι η πιθανότητα εμφάνισης του γεγονότος τότε η ποσότητα πληροφορίας που μεταφέρει το γεγονός αυτό I είναι αντιστρόφως ανάλογη με την πιθανότητα εμφάνισης του γεγονότος P δηλαδή ισχύει:

$$I \propto \frac{1}{P} \tag{1.1}$$

Συνεπώς, από την προηγούμενη σχέση, συμπεραίνουμε ότι όσο μικρότερη είναι η πιθανότητα να συμβεί ένα γεγονός τόσο μεγαλύτερη είναι η ποσότητα πληροφορίας που μεταφέρει το γεγονός αυτό. Η σχέση (1.1) έχει την πιο συγκεκριμένη παρακάτω μορφή, [2,3,12]:

$$I = -\log_b P = \log_b\left(\frac{1}{P}\right) \tag{1.2}$$

Στη σχέση (1.2), η βάση του λογαρίθμου b μπορεί να λάβει τις παρακάτω τρεις τιμές οδηγώντας σε αντίστοιχες τιμές για τη μονάδα μέτρησης της ποσότητας πληροφορίας:

b=2: μονάδα μέτρησης ποσότητας πληροφορίας το *bit (binary unit)*
b=10: μονάδα μέτρησης ποσότητας πληροφορίας το *Hartley*
b=e: μονάδα μέτρησης ποσότητας πληροφορίας το *nats*.

1.2 Μέση πληροφορία κατά σύμβολο ενός αλφαβήτου (Εντροπία πηγής)

Αν θεωρήσουμε ένα αλφάβητο με q *ισοπίθανα σύμβολα,* τότε εφαρμόζοντας τη σχέση (1.2) υπολογίζουμε τη ποσότητα πληροφορίας (σε μονάδες bit) που παρουσιάζει μία φράση η οποία αποτελείται από n οποιαδήποτε σύμβολα της προηγούμενης πηγής:

$$I_n = -n\log_2 P = n\log_2\left(\frac{1}{\frac{1}{q}}\right) = n\log_2(q) \tag{1.3}$$

δεδομένου ότι κάθε ένα από τα q σύμβολα της πηγής έχει πιθανότητα εμφάνισης ίση με $\frac{1}{q}$. Για παράδειγμα, αν θεωρήσουμε τα 25 γράμματα της ελληνικής αλφαβήτου (μαζί με το χαρακτήρα του κενού) τότε αν όλα τα γράμματα ήταν ισοπίθανα τότε μία έκφραση από n γράμματα θα μετέφερε πληροφορία ίση με:

$$I = n\log_2 25 \tag{1.4}$$

και αντίστοιχα κάθε γράμμα θα είχα πληροφορία ίση με:

$$I = \log_2 25 = 4.64 bit \tag{1.5}$$

Θα πρέπει να σημειωθεί ότι στην πράξη τα σύμβολα μιας γλώσσας δεν είναι γενικά ισοπίθανα.

Αν P_i είναι η πιθανότητα εμφάνισης του *i*-οστού συμβόλου του αλφαβήτου μιας γλώσσας (πηγής πληροφορίας) με *q* διακριτά σύμβολα (δηλαδή της ίδιας της πηγής των συμβόλων) αποδεικνύεται ότι η *μέση κατά σύμβολο πληροφορία* (σε bits ανά σύμβολο του αλφαβήτου) του συγκεκριμένου αλφαβήτου (συμβολίζεται συνήθως με *H*) είναι ίση με, [1,2]:

$$H = \bar{I} = -\sum_{i=1}^{q} P_i \cdot \log_2 (P_i) \tag{1.6}$$

Η προηγούμενη σχέση ισχύει με την προϋπόθεση ότι η πηγή πληροφορίας, δηλαδή το αλφάβητο, είναι μία *στατική πηγή* δηλαδή οι πιθανότητες εμφάνισης όλων των συμβόλων είναι ανεξάρτητες του χρόνου. Επίσης, η σχέση (1.6) ισχύει όταν η πιθανότητα εμφάνισης ενός συμβόλου δεν εξαρτάται από την εμφάνιση κανενός άλλου συμβόλου της πηγής δηλαδή η πηγή πληροφορίας δεν παρουσιάζει μνήμη (πηγή χωρίς μνήμη).

Η σχέση (1.6) μας δίνει την *εντροπία H* μιας πηγής πληροφορίας χωρίς μνήμη η οποία μας εκφράζει τη μέση ποσότητα πληροφορίας που μεταφέρει ένα σύμβολο της συγκεκριμένης πηγής. Στην περίπτωση που μία πηγή πληροφορίας χωρίς μνήμη, είναι δυνατό να έχει όλα τα σύμβολά της ισοπίθανα τότε η πηγή παρουσιάζει μέγιστη τιμή της εντροπίας H_{max} η οποία δίνεται από τη σχέση:

$$H_{\max} = \bar{I}_{\max} = \log_2 (q) \tag{1.7}$$

εφαρμόζοντας τη σχέση (1.6), για $P_i = \frac{1}{q}$, για $i = 1,2,...q$ (ισοπίθανα σύμβολα πηγής). Η ελάχιστη τιμή της εντροπίας μιας πηγής πληροφορίας H_{min} είναι προφανές ότι παρουσιάζεται όταν για κάποιο από τα i=1,2,…q σύμβολα της πηγής η πιθανότητα εμφάνισης είναι ίση με 1 (δηλαδή η βεβαιότητα) διότι τότε ο αντίστοιχος όρος στη σχέση (1.6) μηδενίζεται και η εντροπία έτσι αποκτά ελάχιστη τιμή δηλαδή:

$$H_{\min} \text{ όταν } P_n = 1, \text{ για κάποιο από τα } i = 1,2,...q \tag{1.8}$$

Ο πλεονασμός μιας πηγής πληροφορίας *π* μας εκφράζει το ποσό της "άχρηστης πληροφορίας" που μεταφέρει η έξοδος μιας πηγής πληροφορίας και ουσιαστικά μας δίνει τη διαφορά της τρέχουσας κατάστασης από την ιδανική περίπτωση στην οποία τα σύμβολα της πηγής χρησιμοποιούνται ισοπίθανα (περίπτωση της μέγιστης εντροπίας). Ο πλεονασμός *π* ορίζεται ως:

$$\pi = \frac{\mathrm{H}_{\max} - H}{H_{\max}} = 1 - \frac{H}{H_{\max}} \tag{1.9}$$

και δίνεται συνήθως σε ποσοστό %. Ο πλεονασμός μιας πηγής πληροφορίας οφείλεται στους παρακάτω δύο λόγους:

i) στο γεγονός ότι τα σύμβολα της πηγής είναι μη ισοπίθανα και
ii) στην πιθανότητα η πηγή πληροφορίας να παρουσιάζει μνήμη.

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

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

$$R = r \cdot H \tag{1.10}$$

Παράλληλα αν το i-οστό σύμβολο της πηγής έχει διάρκεια t_i τότε η μέση διάρκεια $\bar{\tau}$ (σε sec/σύμβολο) των συμβόλων της πηγής πληροφορίας είναι, με τη βοήθεια της θεωρίας των πιθανοτήτων, ίση με:

$$\bar{\tau} = \sum_{i=1}^{q} P_i \cdot t_i \tag{1.11}$$

Συνεπώς, ο ρυθμός συμβόλων r της πηγής είναι ίσος με:

$$r = \frac{1}{\bar{\tau}} \tag{1.12a}$$

Τέλος, θα πρέπει να ειπωθεί ότι ισχύει η παρακάτω μαθηματική σχέση για την εύρεση των λογαρίθμων:

$$\log_2 x = \frac{\log_{10} x}{\log_{10} 2} = 3.32 \cdot \log_{10} x \tag{1.12b}$$

Ασκήσεις

1. Πηγή πληροφορίας παράγει 5 σύμβολα με πιθανότητες εμφάνισης 1/2, 1/4, 1/8, 1/16 και 1/16. Να υπολογίσετε την εντροπία της συγκεκριμένης πηγής πληροφορίας.

2. Να βρεθεί η μέση ποσότητα πληροφορίας στην Αγγλική γλώσσα αν θεωρήσουμε ότι καθένας από τους 26 χαρακτήρες της εμφανίζεται με την ίδια πιθανότητα.

3.α) Θεωρώντας την αγγλική γλώσσα ως πηγή χωρίς μνήμη βρείτε την εντροπία της και τον πλεονασμό της
β) Συμβιβάζεται το αποτέλεσμα με την εντύπωση που υπάρχει ότι ακόμα και η αγγλική γλώσσα έχει πλεονασμό περίπου 50%-που οφείλεται η διαφορά;
Σας δίνονται οι πιθανότητες εμφάνισης των γραμμάτων της αγγλικής γλώσσας.

4. Μία διακριτή πηγή χωρίς μνήμη έχει 4 σύμβολα x_1, x_2, x_3, x_4 με πιθανότητες εμφάνισης αντίστοιχα: $P(x_1) = 0.4, P(x_2) = 0.4,\ P(x_3) = 0.4,\ P(x_4) = 0.4$. Να βρείτε την εντροπία της πηγής αυτής και την ποσότητα πληροφορίας που περιέχεται στα επόμενα μηνύματα:

$$(x_1 x_2 x_1 x_3) \quad \text{και} \quad (x_4 x_3 x_3 x_2)$$

5. Εικόνα αποτελείται από (500x600) στοιχεία (εικονοστοιχεία) κάθε ένα από τα οποία λαμβάνει 8 διακριτούς τόνους φωτεινότητας. Έστω ότι έχω μείωση της εντροπίας της πηγής αυτής πληροφορίας λόγω της μη ισοπίθανης εμφάνισης των τόνων και των πλεονασμών κατά 80%. Αν για μια ικανοποιητική παρακολούθηση μιας εικόνας πρέπει να έχω ρυθμό 30 εικόνες/sec, να βρεθεί ο ρυθμός της οπτικής πληροφορίας που λαμβάνεται από τον εγκέφαλο ενός τηλεοπτικού θεατή.

6. Ασπρόμαυρη εικόνα τηλεόρασης υψηλής ευκρίνειας αποτελείται από ($2x10^6$) εικονοστοιχεία και 16 διαφορετικές στάθμες φωτεινότητας. Οι εικόνες λαμβάνονται με ρυθμό 32 ανά δευτερόλεπτο. Όλα τα εικονοστοιχεία θεωρούνται ανεξάρτητα και όλες οι στάθμες έχουν ίσες πιθανότητες εμφάνισης. Να βρεθεί ο μέσος ρυθμός πληροφοριών που μεταδίδονται από αυτή την πηγή εικόνων τηλεόρασης.

7. Έστω πηγή πληροφορίας με 3 σύμβολα Α, Β, Γ με αντίστοιχες πιθανότητες εμφάνισης: $P(\mathrm{A}) = 0.5, P(\mathrm{B}) = 0.4,\ P(\Gamma) = 0.1$. Ποια είναι η ποσότητα πληροφορίας όταν λαμβάνουμε το μήνυμα (ΑΑΒ); Ποια είναι η μέση πληροφορία που εκπέμπεται από τη προηγούμενη πηγή πληροφορίας;

2. Χωρητικότητα καναλιού

Ας θεωρήσουμε ένα διακριτό κανάλι στο οποίο εκπέμπονται M διακριτά σύμβολα από μία πηγή πληροφορίας. Τότε μπορούμε να ορίσουμε την *εντροπία της εισόδου* X στο κανάλι επικοινωνίας $H(X)$ (μέση κατά σύμβολο ποσότητα πληροφορίας στην είσοδο του καναλιού) ως εξής, [1]:

$$H(X) = -\sum_{i=1}^{M} P_i^t \cdot \log_2\left(P_i^t\right) \tag{2.1}$$

όπου P_i^t είναι η πιθανότητα να εκπεμφθεί το i-οστό σύμβολο στο κανάλι. Η εντροπία $H(X)$ μας δίνει τη μέση κατά σύμβολο πληροφορία στην είσοδο του καναλιού. Αν δεν υπάρχει κωδικοποιητής πηγής τότε η $H(X)$ είναι ίση με την εντροπία της πηγής πληροφορίας.

Αν r_s είναι ο ρυθμός εκπομπής συμβόλων στο κανάλι (σε σύμβολα/sec) τότε ο μέσος ρυθμός πληροφορίας στην είσοδο του καναλιού D_{in} (σε bits/sec) είναι ίσος με:

$$D_{in} = H(X) \cdot r_s \tag{2.2}$$

Σε αντιστοιχία με την είσοδο του καναλιού, μπορούμε να ορίσουμε την εντροπία της εξόδου Y του καναλιού $H(Y)$ (μέση κατά σύμβολο ποσότητα πληροφορίας στην έξοδο του καναλιού) όπως ακολουθεί, [1]:

$$H(Y) = -\sum_{i=1}^{M} P_i^r \cdot \log_2\left(P_i^r\right) \tag{2.3}$$

όπου P_i^r είναι η πιθανότητα να ληφθεί στην έξοδο του καναλιού το *i*-οστό σύμβολο. Η εντροπία εξόδου του καναλιού μας δίνει το πλήθος των bits που απαιτούνται ανά σύμβολο για την κωδικοποίηση της εξόδου του καναλιού.

Η αβεβαιότητα για την τιμή της εισόδου *X* του καναλιού όταν γνωρίζουμε την τιμή της εξόδου *Y* του καναλιού περιγράφεται από την *εντροπία υπό συνθήκη* $H(X/Y)$(περιγράφει την αμφιβολία αντιστοιχίας των συμβόλων από την έξοδο του καναλιού προς την είσοδο του καναλιού),[2,12]:

$$H(X/Y) = -\sum_{i=1}^{M}\sum_{j=1}^{M} P(X=i,\ Y=j)\cdot \log_2 P(X=i/Y=j) \qquad (2.4)$$

Εκτός από την εντροπία υπό συνθήκη μπορεί να δοθεί και η *συνδυασμένη εντροπία* $H(X,Y)$, [2,12]:

$$H(X,Y) = -\sum_{i=1}^{M}\sum_{j=1}^{M} P(X=i,\ Y=j)\cdot \log_2 P(X=i,Y=j) \qquad (2.5)$$

η οποία όπως παρατηρούμε από τη σχέση (2.5) σχετίζεται με την πιθανότητα εμφάνισης των ζευγών (X,Y) εισόδου-εξόδου του καναλιού.

Ο μέσος ρυθμός εκπομπής D_t διαμέσου του καναλιού δίνεται από την επόμενη σχέση:

$$D_t = [H(X) - H(X/Y)]\cdot r_s \qquad (2.6)$$

Η χωρητικότητα του καναλιού *C* ορίζεται ως η μέγιστη δυνατή τιμή του D_t για όλα τα σύνολα πιθανοτήτων εμφάνισης της εισόδου του καναλιού X δηλαδή:

$$C = \max_{p(x)}\{D_t\} \qquad (2.7)$$

2.1.Χωρητικότητα καναλιού συνεχών μηνυμάτων λευκού προσθετικού θορύβου κατανομής Gauss

Συνεχές κανάλι επικοινωνίας είναι εκείνο στο οποίο το μήνυμα το οποίο εκπέμπεται σε αυτό είναι συνεχές δηλαδή μπορεί να αναπαρασταθεί με μία συνεχή κυματομορφή σα συνάρτηση του χρόνου. Σε μία τέτοια περίπτωση, οι χαρακτηριστικές παράμετροι του καναλιού είναι: α) το εύρος ζώνης συχνοτήτων του καναλιού επικοινωνίας *B* και β) ο *λόγος σήμα προς θόρυβο* (Signal-to Noise Ratio, *SNR* ή $\frac{S}{N}$) στην έξοδο του καναλιού. Αν το κανάλι παρουσιάζει *λευκό, προσθετικό θόρυβο κατανομής Gauss* (Additive White Gaussian Noise, AWGN) τότε αποδεικνύεται ότι η χωρητικότητα *C* του συγκεκριμένου καναλιού δίνεται από τη σχέση, [1,5-7]:

$$C = B\cdot \log_2\left(1+\frac{S}{N}\right) \qquad (\text{σε bits/sec}) \qquad (2.8)$$

Η προηγούμενη σχέση είναι ο περίφημος *Νόμος* των *Shannon-Hartley* για τη χωρητικότητα ενός καναλιού περιορισμένου εύρους ζώνης συχνοτήτων το οποίο παρουσιάζει AWGN θόρυβο. Η σχέση (2.8), μας δίνει ποσοτικά το μέγιστο δυνατό ρυθμό εκπομπής πληροφορίας (πάνω όριο) στο κανάλι πετυχαίνοντας μία πιθανότητα σφάλματος η οποία είναι δυνατό να τείνει σε μηδενική τιμή. Η χωρητικότητα του καναλιού δηλαδή ο ρυθμός αυτός εκπομπής πληροφορίας στο κανάλι, μπορεί να επιτευχθεί αν χρησιμοποιηθεί πολύπλοκη κωδικοποίηση κατά την εκπομπή αλλά χωρίς να τεθούν χρονικοί περιορισμοί στη εκπομπή των σημάτων στο κανάλι. Στην πράξη, ο ρυθμός R της εκπεμπόμενης πληροφορίας στο κανάλι θα πρέπει να ικανοποιεί την επόμενη ανισότητα:

$$R \le C = B \cdot \log_2\left(1 + \frac{S}{N}\right) \tag{2.9}$$

και γίνεται προσπάθεια να προσεγγίσουμε την ισότητα βελτιώνοντας την κωδικοποίηση, [13]. Στην πραγματικότητα αυτό που γίνεται είναι ότι το κανάλι δεν είναι ιδανικό και η χρησιμοποιούμενη κωδικοποίηση δεν είναι άριστη με αποτέλεσμα να εμφανίζεται πάντα μία μικρή πιθανότητα σφάλματος κατά την λήψη και την αποκωδικοποίηση.

Από τη σχέση (2.8) μπορεί να έχουμε τα ακόλουθα συμπεράσματα:

i) αύξηση της χωρητικότητας *C* μπορεί να πραγματοποιηθεί με αύξηση του εύρους ζώνης συχνοτήτων του καναλιού *B*

ii) αύξηση της χωρητικότητας *C* μπορεί να πραγματοποιηθεί με αύξηση του λόγου SNR.

Στη σχέση (2.8), ο λόγος *SNR* πρέπει να δοθεί σε καθαρό αριθμό, το εύρος ζώνης συχνοτήτων σε Hz και τότε η χωρητικότητα *C* υπολογίζεται τότε σε (bits/sec). Συνήθως σε πρακτικά συστήματα, ο λόγος *SNR* δίνεται σε dB γι' αυτό θα πρέπει να κάνουμε την επόμενη μετατροπή, [10]:

$$\frac{S}{N}(dB) = 10 \cdot \log_{10}\left(\frac{S}{N}\right)(\text{καθαρός αριθμός}) \tag{2.10}$$

ή αντίστοιχα:

$$\frac{S}{N}(\text{καθαρός αριθμός}) = 10^{\frac{SNR(dB)}{10}} \tag{2.11}$$

Αποδεικνύεται ότι μπορούμε να εκπέμψουμε διατηρώντας το *SNR* σε τιμή μικρότερη της μονάδας αρκεί ταυτόχρονα να έχουμε φροντίσει το εύρος ζώνης συχνοτήτων *B* του καναλιού επικοινωνίας (και συνεπώς και του εκπεμπόμενου σήματος) να είναι αρκετά μεγάλο. Η περίπτωση αυτή εκπομπής αντιστοιχεί στα συστήματα *διευρυμένου φάσματος* ή *διάχυτου φάσματος* (Spread Spectrum Systems) τα οποία βρίσκουν εφαρμογές στις στρατιωτικές επικοινωνίες, στις δορυφορικές επικοινωνίες όπως και στα συστήματα κινητών επικοινωνιών τρίτης γενιάς. Στο σημείο αυτό είναι χρήσιμο να πούμε ότι η στο άπειρο αύξηση του εύρους ζώνης συχνοτήτων *B* του καναλιού επικοινωνίας, δεν οδηγεί σε αντίστοιχη αύξηση προς το άπειρο της χωρητικότητας *C* του καναλιού επικοινωνίας αλλά αυτή οδηγείται σε συγκεκριμένο πάνω όριο. Αποδεικνύεται ότι, [3,10,12]:

$$\lim_{B\to\infty} C = 1.44 \cdot \frac{S}{N_0} \tag{2.12}$$

όπου N_0 (σε Watt/Hz) είναι η φασματική πυκνότητα του AWGN θορύβου του καναλιού η οποία μας δίνει την ισχύ του θορύβου του καναλιού ανά Hz του εύρους ζώνης του καναλιού επικοινωνίας. Η φασματική πυκνότητα έχει τόσο μεγαλύτερη τιμή όσο ο θόρυβος του καναλιού επικοινωνίας είναι ισχυρότερος.

Θα πρέπει να ειπωθεί ότι AWGN θόρυβος είναι ο θόρυβος ο οποίος παρουσιάζει τα επόμενα χαρακτηριστικά:

i) η ισχύς του θρύβου κατανέμεται με τον ίδιο τρόπο σε όλες τις συχνότητες του ηλεκτρομαγνητικού φάσματος σε αντιστοιχία με την περίπτωση του λευκού φωτός το οποίο περιέχει όλα τα χρώματα (μήκη κύματος) με την ίδια συνεισφορά ισχύος στο τελικό αποτέλεσμα
ii) το στιγμιαίο πλάτος του θορύβου προστίθεται στο στιγμιαίο πλάτος του εκπεμπόμενου σήματος (προσθετικός θόρυβος)
iii) το στιγμιαίο πλάτος του θορύβου ακολουθεί την κανονική κατανομή (κατανομή Gauss)

Πρακτικά, τα περισσότερα κανάλια επικοινωνίας που συναντούμε σε συστήματα μετάδοσης παρουσιάζουν AWGN θόρυβο (φυσικός θόρυβος καναλιού επικοινωνίας).

Ασκήσεις

1. Ένας τεχνικός επικοινωνίας ισχυρίζεται ότι σχεδίασε σύστημα διασύνδεσης της εξόδου ενός μικροεπεξεργαστή με έναν εκτυπωτή που έχει ταχύτητα 50γραμμές/λεπτό και 120 χαρακτήρες ανά γραμμή επιτυγχάνοντας τη σύνδεση αυτή με ένα κοινό τηλεφωνικό καλώδιο εύρους ζώνης 3.4KHz και με τέτοια ισχύ παροχής που το σήμα να φτάνει στον εκτυπωτή με ποιότητα (S/N)=10dB. Ο κώδικας που χρησιμοποιείται είναι ASCII (8 bits/χαρακτήρα). Τον πιστεύετε στα παραπάνω λεγόμενά του;

2. Η έξοδος μιας πηγής πληροφορίας που θεωρείται χωρίς μνήμη αποτελείται από 128 σύμβολα. Τα 16 από αυτά εμφανίζονται με πιθανότητα 1/32 και το καθένα από αυτά έχει διάρκεια 1msec. Τα υπόλοιπα σύμβολα είναι ισοπίθανα και το κάθε ένα έχει διάρκεια 2msec. Τα σύμβολα είναι ανεξάρτητα μεταξύ τους και η πηγή εκπέμπει χωρίς κενό μεταξύ των συμβόλων.

α) Να υπολογίσετε την εντροπία H της πηγής και το ρυθμό παραγωγής πληροφορίας R.

β) Πόση θα πρέπει να είναι η ελάχιστη θεωρητικά τιμή του (S/N) στην έξοδο του αναλογικού καναλιού που έχει εύρος 3MHz έτσι ώστε να είναι θεωρητικά δυνατή η διαβίβαση της παραγόμενης από την πηγή πληροφορίας;

γ) Πόση θα πρέπει να είναι πρακτικά η τιμή αυτή αν δεχθούμε ότι το πραγματικό σύστημα που διαθέτουμε επιτρέπει διακίνηση πληροφορίας με ρυθμό πέντε φορές μικρότερο από την χωρητικότητα C;

δ) Πόση θα ήταν τέλος η τιμή του λόγου (S/N) αν χρησιμοποιηθεί συμπίεση που απομακρύνει το 40% του πλεονασμού λόγω μνήμης;

3. Έστω έξοδος μιας πηγής πληροφορίας χωρίς μνήμη που αποτελείται από 128 σύμβολα. Τα 16 από τα σύμβολα αυτά εμφανίζονται με πιθανότητα 1/32 και κάθε ένα έχει διάρκεια 2msec. Τα υπόλοιπα σύμβολα έχουν την ίδια πιθανότητα και το καθένα έχει διάρκεια 4msec. Τα σύμβολα είναι ανεξάρτητα μεταξύ τους και η πηγή εκπέμπει τα σύμβολα χωρίς κενό μεταξύ των συμβόλων. Βρείτε ποια είναι η ελάχιστη τιμή του λόγου (S/N) στην έξοδο ενός αναλογικού καναλιού με εύρος ζώνης συχνοτήτων 4KHz, ώστε να είναι δυνατή πρακτικά η μετάδοση της πληροφορίας που παράγει η πηγή αυτή από το παραπάνω κανάλι.

Ασκήσεις με απαντήσεις

1. Έστω κανάλι προσθετικού λευκού θορύβου Gauss (AWGN κανάλι) με εύρος ζώνης 4KHz και φασματική πυκνότητα θορύβου 10^{-12}W/Hz. Η ισχύς του σήματος που χρειάζεται στο δέκτη είναι ίση με 0.1mW. Να υπολογιστεί η χωρητικότητα του συγκεκριμένου καναλιού (Απάντηση: $54.44 \cdot 10^3$bit/sec)
2. Λαμβάνονται δείγματα αναλογικού σήματος με εύρος ζώνης 4KHz με ρυθμό 1.25 φορές τον ρυθμό Nyquist και κάθε δείγμα κβαντοποιείται σε μία από τις 256 ισοπίθανες τιμές. Υποθέτουμε ότι τα διαδοχικά δείγματα είναι ισοπίθανα.
   α)Ποιος είναι ο ρυθμός πληροφορίας της πηγής αυτής; (Απάντηση: 80Kbit/sec)

   β) Μπορεί η έξοδος της πηγής αυτής να μεταδοθεί χωρίς σφάλμα μέσα από κανάλι AWGN με εύρος ζώνης συχνοτήτων 10KHz και λόγο *SNR* 20dB; (Απάντηση:δεν είναι δυνατή)

   γ)Να βρεθεί ο λόγος *SNR* που χρειάζεται για μετάδοση χωρίς σφάλματα στο συγκεκριμένο κανάλι. (Απάντηση: $SNR \geq 24.1$ dB)
   δ) Να βρεθεί το εύρος ζώνης συχνοτήτων που χρειάζεται σε κανάλι AWGN για μετάδοση της εξόδου αυτής της πηγής χωρίς σφάλματα αν ο λόγος *SNR* είναι 20dB. (Απάντηση: $B \geq 12$KHz).
3. Να υπολογίσετε τη χωρητικότητα καναλιού AWGN με εύρος ζώνης συχνοτήτων 1MHz και λόγο SNR=40dB (Απάντηση:13.29Mbit/sec)

3. Εντροπία πηγής με μνήμη

Μία πηγή πληροφορίας έχει *μνήμη* όταν τα σύμβολα που εκπέμπονται από την πηγή δεν είναι ανεξάρτητα μεταξύ τους δηλαδή η πιθανότητα εμφάνισης (εκπομπής) ενός συμβόλου εξαρτάται από την εκπομπή ή όχι προηγούμενων συμβόλων. Μία πηγή με μνήμη ονομάζεται πηγή *m*-τάξης αν η πιθανότητα εκπομπής ενός συμβόλου εξαρτάται από τα m προηγούμενα σύμβολα που έχουν εκπεμφθεί. Συνήθως η εκπομπή ενός συμβόλου από μία τέτοια πηγή πληροφορίας θεωρείται ως η μετάβαση της πηγής από μία κατάσταση σε μία άλλη. Έτσι οι εκπομπές των συμβόλων από μία πηγή με μνήμη, αναπαρασταίνονται με το λεγόμενο *διάγραμμα καταστάσεων* της πηγής. Οι μεταπτώσεις σε ένα τέτοιο διάγραμμα δηλώνονται με βέλη δίπλα στα οποία υπάρχει η αντίστοιχη πιθανότητα καθώς και το εκπεμπόμενο σύμβολο. Συνήθως το εκπεμπόμενο σύμβολο τοποθετείται σε ένα κύκλο δηλώνοντας και την αντίστοιχη κατάσταση της πηγής πληροφορίας.

Για μία πηγή πληροφορίας με μνήμη $1^{ης}$ τάξης (δηλαδή πηγή στην οποία η εκπομπή ενός συμβόλου εξαρτάται από το προηγούμενο σύμβολο που εκπέμφθηκε) αποδεικνύεται, [1,2,12

], ότι δίνεται από τη σχέση:

$$H_{\text{πηγή με μνήμη 1ης τάξης}} = \sum_i \sum_j P_i \cdot P(j/i) \cdot \log_2 \left(\frac{1}{P(j/i)} \right) \qquad (3.1)$$

όπου $P(j/i) = P_{ij}$ είναι η πιθανότητα να εκπεμφθεί το *j* σύμβολο της πηγής δεδομένου ότι έχει σταλεί ήδη το *i* σύμβολο της πηγής (μνήμη ενός συμβόλου, *m*=1) δηλαδή η υπό συνθήκη πιθανότητα. Σε αναλογία με την πηγή πληροφορίας χωρίς μνήμη, ο ρυθμός εκπομπής πληροφορίας στο κανάλι για μία πηγή με μνήμη θα δίνεται από τη σχέση:

$$R = r \cdot H_{\text{πηγή με μνήμη 1ης τάξης}} \tag{3.2}$$

όπου στη σχέση (3.2), r είναι ο ρυθμός εκπομπής των συμβόλων της πηγής (σε σύμβολα/sec) με μνήμη.

Αν μετά από ένα μετά από ένα αριθμό μεταπτώσεων μιας πηγής πληροφορίας είναι δυνατό να έχουμε μετάπτωση σε οποιαδήποτε άλλη κατάσταση με μη μηδενική πιθανότητα, δηλαδή η πηγή δεν "μπλοκάρεται" σε ένα εκπεμπόμενο σύμβολο (δηλαδή σε απορροφητικό βρόχο) τότε η πηγή ονομάζεται *εργοδική πηγή*.

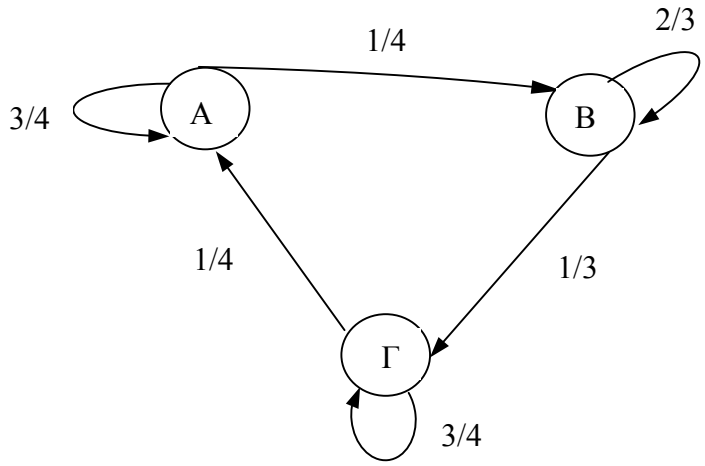
Για πηγή πληροφορίας με μνήμη, οι μεταπτώσεις της μπορούν να περιγραφούν με τη *μήτρα πιθανοτήτων της μετάπτωσης* δηλαδή τη μήτρα των $P(j/i) = P_{ij}$. Έτσι μία πηγή με q σύμβολα μπορεί να περιγραφτεί με την επόμενη μήτρα P τα στοιχεία της οποίας είναι τιμές πιθανοτήτων μετάπτωσης:

$$P = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdot & \cdot & p_{1,q} \\ p_{2,1} & p_{2,2} & \cdot & \cdot & p_{2,q} \\ & & & & \\ p_{q,1} & p_{q,2} & \cdot & \cdot & p_{q,q} \end{bmatrix} \tag{3.3}$$

Για παράδειγμα, έστω ότι μας δίνεται η επόμενη μήτρα μεταπτώσεων για μία πηγή πληροφορίας με μνήμη:

$$P = \begin{bmatrix} & \text{A} & \text{B} & \Gamma \\ \text{A} & 3/4 & 0 & 1/4 \\ \text{B} & 1/4 & 2/3 & 0 \\ \Gamma & 0 & 1/3 & 3/4 \end{bmatrix} \tag{3.4}$$

Η προηγούμενη μήτρα ερμηνεύεται ως εξής: π.χ. η πιθανότητα 3/4 της πρώτης γραμμής και πρώτης στήλης είναι η πιθανότητα να σταλεί το σύμβολο Α δεδομένου ότι έχει ήδη σταλεί το σύμβολο Α, η πιθανότητα 1/3 της τρίτης γραμμής και δεύτερης στήλης ερμηνεύεται ως η πιθανότητα να σταλεί το σύμβολο Γ δεδομένου ότι έχει σταλεί το σύμβολο Β. Δηλαδή οι μεταπτώσεις των συμβόλων της πηγής έχουν κατεύθυνση όπως δείχνει το βέλος. Το τέλος του βέλους δείχνει το εκπεμπόμενο σύμβολο και η αρχή του βέλους το σύμβολο που έχει προηγηθεί. Η προηγούμενη μήτρα μεταπτώσεων ισοδυναμεί με το επόμενο διάγραμμα καταστάσεων της πηγής πληροφορίας:



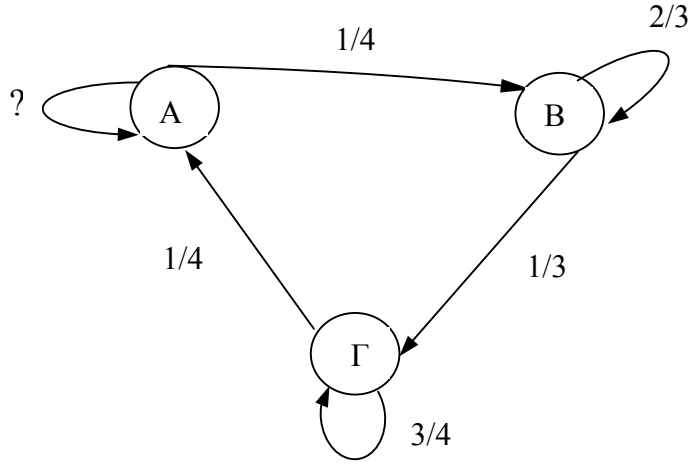
Με δεδομένο το διάγραμμα καταστάσεων ή τη μήτρα μεταπτώσεων μιας πηγής πληροφορίας μπορούμε να υπολογίσουμε τις πιθανότητες εμφάνισης των συμβόλων της πηγής. Π.χ. για τη προηγούμενη πηγή με εκπεμπόμενα σύμβολα τα Α, Β και Γ μπορεί να γραφτεί, με τη βοήθεια της θεωρίας πιθανοτήτων, ότι:

$$\begin{aligned} P_A &= P_{A/A}\cdot P_A + P_{A/B}\cdot P_B + P_{A/\Gamma}\cdot P_\Gamma \\ P_\Beta &= P_{\Beta/A}\cdot P_A + P_{\Beta/B}\cdot P_B + P_{\Beta/\Gamma}\cdot P_\Gamma \\ P_\Gamma &= P_{\Gamma/A}\cdot P_A + P_{\Gamma/B}\cdot P_B + P_{\Gamma/\Gamma}\cdot P_\Gamma \end{aligned} \qquad (3.5)$$

Οι εξισώσεις (3.5) αποτελούν σύστημα 3 εξισώσεων με 3 αγνώστους και με αγνώστους τα P_A, P_B, και P_Γ (σύστημα εξισώσεων 3x3). Το σύστημα μπορεί να λυθεί είτε με τη μέθοδο της αντικατάστασης είτε με τη μέθοδο των οριζουσών. Έτσι γνωρίζοντας τις τιμές των P_A, P_B, και P_Γ μπορούμε για τη συγκεκριμένη πηγή με μνήμη να υπολογίσουμε την τιμή της εντροπίας της χρησιμοποιώντας τη σχέση (3.1) στην οποία όλες οι πιθανότητες που εμφανίζονται είναι τώρα γνωστές.

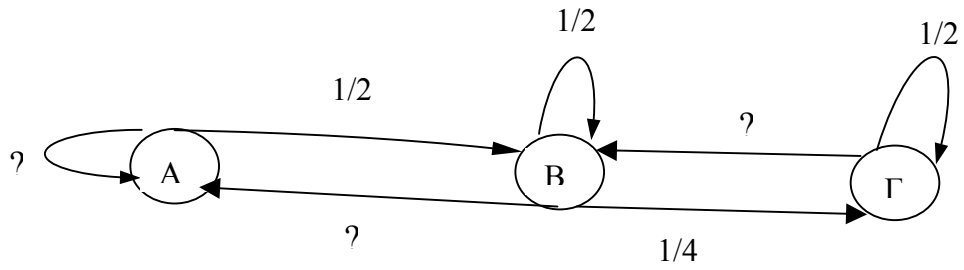
Ασκήσεις

1. Ας θεωρήσουμε ότι η πηγή το παρακάτω σχήματος είναι εργοδική πρώτης τάξης και ότι όλες οι μεταπτώσεις της διαρκούν ίσο χρόνο 1μsec.



α) Ποια είναι η θεωρητικά ελάχιστη χωρητικότητα καναλιού για τη μεταβίβαση των δεδομένων της πηγής αυτής;
β) Πόση θα ήταν η αναγκαία χωρητικότητα του καναλιού αν δεν λαμβάναμε υπόψη την ύπαρξη μνήμης;
γ) Ποιο είναι το ελάχιστο εύρος ζώνης συχνοτήτων στις δύο αυτές περιπτώσεις αν επιδιώκουμε λόγο στην έξοδο του καναλιού ίσο με 7dB;

2.Όλες οι μεταπτώσεις της πηγής του παρακάτω σχήματος που θεωρείται εργοδική διαρκούν 2μsec.



α) Ποια είναι η θεωρητικά ελάχιστη χωρητικότητα ενός ιδανικού καναλιού για τη διαβίβαση των δεδομένων της πηγής αυτής;
β)Υπό ποιο εύρος ζώνης συχνοτήτων θα έπρεπε να αποστέλλεται τότε η πληροφορία αν θέλαμε η ποιότητα του σήματος στη λήψη να είναι SNR=25dB;
γ) Κατά πόσο της εκατό θα ήταν μεγαλύτερο το εύρος ζώνης αν θεωρούσαμε την πηγή χωρίς μνήμη;

4. Κωδικοποίηση πηγής

Γενικά, στη θεωρία της κωδικοποίησης δεδομένων αλλά και στην πράξη συναντούμε δύο διαφορετικούς τύπους κωδικοποίησης δεδομένων:

α) την κωδικοποίηση πηγής (source coding) και
β) την κωδικοποίηση καναλιού (channel coding).

Η *κωδικοποίηση πηγής* είναι η διαδικασία που ακολουθεί αμέσως μετά την έξοδο μιας πηγής πληροφορίας. Σκοπός της κωδικοποίησης της πηγής είναι η ελαχιστοποίηση του απαιτούμενου μήκους της κωδικής λέξης που απαιτείται για να αναπαρασταθούν κατά μέσο όρο τα σύμβολα που παράγει η πηγή της πληροφορίας. Δηλαδή αν γνωρίζουμε την εντροπία μιας πηγής πληροφορίας (σε bits/σύμβολο) γνωρίζουμε και το μέσο πλήθος των bits που απαιτούνται για να αναπαρασταθούν κατά μέσο όρο τα σύμβολα της πηγής. Έτσι στόχος της κωδικοποίησης της πηγής είναι να μειωθεί αυτό ακριβώς το πλήθος των ψηφίων του κώδικα που απαιτείται για να αναπαρασταθούν τα σύμβολα της πηγής.

Αντίστοιχα, η *κωδικοποίηση καναλιού* έχει σκοπό την όσο το δυνατό αξιόπιστη μετάδοση των δεδομένων σε ένα κανάλι με θόρυβο (ενθόρυβο κανάλι). Δηλαδή έχει σκοπό τη μείωση της επίδρασης του θορύβου του καναλιού στα εκπεμπόμενα δεδομένα με την ανίχνευση ή και την διόρθωση των λαθών (πιθανότητα λάθους) που οφείλονται στο θόρυβο του καναλιού επικοινωνίας. Στο σημείο αυτό θα πρέπει να ειπωθεί ότι αν το ποσοστό των λαθών σε ένα σύστημα μετάδοσης είναι υψηλό τότε χρειάζονται πιο πολύπλοκες συσκευές για να μειωθεί η πιθανότητα λάθους και μάλιστα είναι δυνατό να

βελτιώσουμε το σύστημα δηλαδή να ελαττώνουμε την πιθανότητα λάθους χρησιμοποιώντας όλο και πιο πολύπλοκες συσκευές αν ο ρυθμός εκπομπής πληροφορίας R είναι μικρότερος από τη χωρητικότητα του καναλιού επικοινωνίας C.

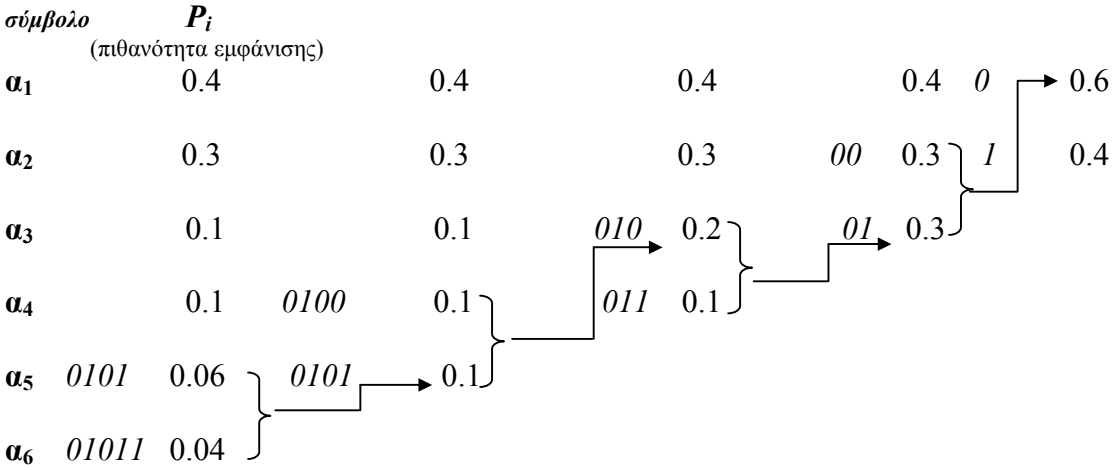
4.1 Κωδικοποίηση πηγής Huffman

Στη δυαδική κωδικοποίηση πηγής Huffman, [2,3,12], για να παράγουμε τις κωδικές λέξεις που αντιστοιχούν στα σύμβολα της πηγής πληροφορίας, ακολουθούμε τα παρακάτω βήματα:

- τοποθετούμε σε κατακόρυφη διάταξη τα εκπεμπόμενα σύμβολα της πηγής με σειρά φθίνουσας πιθανότητας εμφάνισης των συμβόλων (το άθροισμα των πιθανοτήτων των εκπεμπόμενων συμβόλων θα πρέπει να είναι πάντα ίσο με 1)
- ξεκινώντας από τη μικρότερη πιθανότητα συμβόλου και την αμέσως μικρότερη από αυτή, τις προσθέτουμε και η νέα τιμή πιθανότητα που προκύπτει την τοποθετούμε στη σωστή θέση στην κατακόρυφη διάταξη φθίνουσας πιθανότητας εμφάνισης συμβόλων παράγοντας έτσι δίπλα στη προηγούμενη μία νέα κατακόρυφη διάταξη
- η διαδικασία αυτή συνεχίζεται έως να έχουμε μόνο δύο τιμές πιθανοτήτων στην κατακόρυφη διάταξη
- ακολουθούμε αντίστροφη διαδικασία τοποθετώντας δίπλα από τις δύο τελευταίες τιμές πιθανότητας το 0 και το 1
- τα ψηφία 0 ή 1 (που έχουμε τοποθετήσει δίπλα στις δύο τελευταίες τιμές πιθανοτήτων) οδηγούνται με αντίστροφη πορεία και σημειώνονται δίπλα στις τιμές των πιθανοτήτων από τις οποίες οδηγηθήκαμε σε αυτά
- δίπλα στα ψηφία 0 ή 1 που έχουμε μεταφέρει, τοποθετούμε το 0 και το1
- ο συνδυασμός των 0 και 1 που έχει τώρα εμφανιστεί επαναλαμβάνεται με την ίδια διαδικασία όπως και πριν έγινε για το 0 και το 1
- τα προηγούμενα βήματα επαναλαμβάνονται μέχρι να καταλήξουμε στην αρχική διάταξη φθίνουσας πιθανότητας εμφάνισης των συμβόλων
- οι κωδικές λέξεις που αντιστοιχούν στην κωδικοποίηση είναι αυτές που έχουν απομείνει από τους προηγούμενους συνδυασμούς, χωρίς να έχουν μεταφερθεί προς τα πίσω (προς τα αριστερά), με τη διαδικασία που περιγράφηκε στα προηγούμενα βήματα.

Παράδειγμα

Έστω πηγή 6 συμβόλων τα οποία παρουσιάζουν τις επόμενες πιθανότητες εμφάνισης:: α_1:0.4, α_2:0.3, α_3:0.1, α_4:0.1, α_5:0.06, α_6:0.04. Τα σύμβολα αυτά κωδικοποιούνται με δυαδική κωδικοποίηση Huffman όπως παρουσιάζεται στο επόμενο σχήμα:



Παρατηρώντας τη διαδικασία του προηγουμένου σχήματος, βλέπουμε ότι οι συνδυασμοί που έχουν απομείνει χωρίς να έχουν μεταφερθεί αριστερά (αυτοί οι οποίοι στο προηγούμενο σχήμα δεν προέρχονται από ένα άθροισμα πιθανοτήτων δηλαδή δεν καταλήγουμε σε αυτούς με την πορεία ενός βέλους) και οι οποίοι τελικά είναι οι κωδικές λέξεις που αντιστοιχούν στα σύμβολα της πηγής είναι οι επόμενοι:

$\alpha_1 \longrightarrow 1$
$\alpha_2 \longrightarrow 00$
$\alpha_3 \longrightarrow 011$
$\alpha_4 \longrightarrow 0100$
$\alpha_5 \longrightarrow 01010$
$\alpha_6 \longrightarrow 01011$

4.2 Κωδικοποίηση πηγής Shannon-Fano

Στη μέθοδο αυτή κωδικοποίησης της πηγής πληροφορίας, ακολουθούμε τα επόμενα βήματα:

- καταγράφουμε τα σύμβολα της πηγής κατά σειρά μειούμενης πιθανότητας
- χωρίζουμε το σύνολο σε 2 ομάδες που να είναι όσο το δυνατό πλησιέστερα σε ίσες πιθανότητες (δηλαδή το άθροισμα σε κάθε μία ομάδα) και θέτουμε 0 στην ανώτερη ομάδα και 1 στην κατώτερη ομάδα
- συνεχίζουμε χωρίζοντας κάθε φορά τις ομάδες με όσο το δυνατό ίσες πιθανότητες μέχρι να μην είναι δυνατός ο περαιτέρω διαχωρισμός τους.

Το μειονέκτημα της συγκεκριμένη μεθόδου κωδικοποίησης πηγής είναι η αβεβαιότητα που υπάρχει στο "μοίρασμα" των 2 ομάδων με ίσες πιθανότητες.

Παράδειγμα

Έστω πηγή 6 συμβόλων τα οποία παρουσιάζουν τις επόμενες πιθανότητες εμφάνισης:: x_1:0.3, x_2:0.25, x_3:0.2, x_4:0.12, x_5:0.08, x_6:0.05. Τα σύμβολα αυτά κωδικοποιούνται με δυαδική κωδικοποίηση Shannon-Fano όπως παρουσιάζεται στο επόμενο σχήμα:

σύμβολο	P_i (πιθανότητα εμφάνισης)	**Βήμα 1ο**	**Βήμα 2ο**	**Βήμα 3ο**	**Βήμα 4ο**	**Βήμα 5ο**
$\mathbf{x_1}$	0.3	0	0			**00**
$\mathbf{x_2}$	0.25	0	1			**01**
$\mathbf{x_3}$	0.20	1	0			**10**
$\mathbf{x_4}$	0.12	1	1	0		**110**
$\mathbf{x_5}$	0.08	1	1	1	0	**1110**
$\mathbf{x_6}$	0.05	1	1	1	1	**1111**

Τελικά, οι κωδικές λέξεις που προκύπτουν παρουσιάζονται στον επόμενο πίνακα:

$x_1 \longrightarrow$ **00**
$x_2 \longrightarrow$ **01**
$x_3 \longrightarrow$ **10**
$x_4 \longrightarrow$ **110**
$x_5 \longrightarrow$ **1110**
$x_6 \longrightarrow$ **1111**

Ασκήσεις με απαντήσεις

1. Μία πηγή έχει τέσσερα σύμβολα x_1, x_2, x_3, x_4, με αντίστοιχες πιθανότητες εμφάνισης 1/2,1/4,1/8,1/8. (Απάντηση: x_1: 0, x_2: 10, x_3: 110, x_4:111)
2. Μία πηγή πληροφορίας έχει 5 ισοπίθανα σύμβολα.
3. α) Να κατασκευαστεί κώδικας Shannon-Fano και να υπολογίσετε την απόδοσή του (Απάντηση: x_1: 00, x_2: 01, x_3: 10, x_4:110, x_5:111)

4. β) Να κατασκευαστεί ένας άλλος κώδικας Shannon-Fano και να συγκριθεί η απόδοση με τον προηγούμενο κώδικα (Απάντηση: x_1: 00, x_2: 010, x_3: 011, x_4:10, x_5:11)

   γ) Να κωδικοποιήσετε την πηγή με κωδικοποίηση Huffman και να συγκριθούν τα αποτελέσματα (Απάντηση: x_1: 01, x_2: 000, x_3: 001, x_4:10, x_5:11)

4.3 Τετραδική Κωδικοποίηση πηγής Huffman

Είναι δυνατό η κωδικοποίηση πηγής Huffman να πραγματοποιηθεί και το τετραδικό σύστημα το οποίο έχει ως σύμβολα τα: 0,1,2,3 (τέσσερα σύμβολα). Η διαδικασία που εφαρμόζεται είναι η ίδια όπως και στο δυαδικό σύστημα αλλά εδώ οι πιθανότητες αθροίζονται στη κατακόρυφη διάταξη ανά τέσσερις. Στη συνέχεια δίνεται ένα παράδειγμα και η κωδικοποίηση σε τετραδικό σύστημα.

σύμβολο		P_i (πιθανότητα εμφάνισης)		
$\mathbf{a_1}$		0.5	*0*	0.5
$\mathbf{a_2}$		0.25	*1*	0.25
$\mathbf{a_3}$		0.15	*2*	0.15
$\mathbf{a_4}$	*30*	0.05	*3*	0.1
$\mathbf{a_5}$	*31*	0.03		
$\mathbf{a_6}$	*32*	0.015		
$\mathbf{a_7}$	*33*	0.005		

Τελικά, οι κωδικές λέξεις που προκύπτουν στο τετραδικό σύστημα παρουσιάζονται στον επόμενο πίνακα:

a_1	**0**
a_2	**1**
a_3	**2**
a_4	**30**
a_5	**31**
a_6	**32**
a_7	**33**

4.4 Μέσο μήκος κωδικής λέξης

Μετά την κωδικοποίηση πηγής που εφαρμόζουμε κάθε φορά προκύπτουν οι κωδικές λέξεις που αντιστοιχούν στα σύμβολα της πηγής πληροφορίας. Για να υπολογίσουμε το μέσο μήκος L της κωδικής λέξης του κώδικα που παράχθηκε εφαρμόζουμε την επόμενη σχέση:

$$L = \sum_{i=1}^{q} P_i \cdot l_i \tag{4.1}$$

όπου l_i είναι το μήκος (σε bits) της i-οστής κωδικής λέξης του κώδικα, η οποία παρουσιάζει αντίστοιχα πιθανότητα εμφάνισης P_i (θεωρούμε ότι έχουμε q εκπεμπόμενα σύμβολα πηγής).

Στο σημείο αυτό θα πρέπει να ειπωθεί ότι στα συστήματα εκπομπής μία συνηθισμένη μέθοδος κωδικοποίησης είναι η *διαμόρφωση-κωδικοποίηση P.C.M* (Pulse Coded Modulation). Αν η πηγή πληροφορίας εκπέμπει q σύμβολα, τότε στο σύστημα PCM απαιτούνται ανά εκπεμπόμενο σύμβολο k bits, για τα οποία πρέπει να ισχύει η επόμενη σχέση:

$$2^k \geq q \tag{4.2}$$

και βέβαια επιλέγουμε την ισότητα στην σχέση (4.2) αν αυτή είναι δυνατή, διαφορετικά τη μικρότερη τιμή του *k* για την οποία ισχύει η (4.2).

Ασκήσεις

1. Μία γλώσσα 7 συμβόλων χωρίς μνήμη παρουσιάζει τις πιο κάτω πιθανότητες εμφάνισης των συμβόλων: α_1:0.5, α_2:0.25, α_3:0.15, α_4:0.05, α_5:0.03, α_6:0.015, α_7:0.005.

α) Βρείτε την εντροπία της και τον πλεονασμό της πηγής
β) Κωδικοποιήστε την πηγή αυτή σε δυαδικό σύστημα με κώδικα Huffman
γ) Βρείτε το μέσο μήκος κωδικής λέξης του κώδικα που δημιουργήσατε καθώς και το πλεονασμό που προσθέτει ο κώδικας
δ) Πόσο πλεονασμό θα εισήγαγε η κωδικοποίηση της πηγής σε σύστημα PCM;

5. Απλοί Κώδικες Επανάληψης

Η μετάδοση δεδομένων μέσω ενός καναλιού επικοινωνίας το οποίο παρουσιάζει θόρυβο έχει ως χαρακτηριστικό την εμφάνιση λαθών κατά τη λήψη των εκπεμπόμενων συμβόλων (bit). Θα πρέπει να ειπωθεί ότι στην πράξη δεν υπάρχει κανάλι επικοινωνίας που να μην παρουσιάζει θόρυβο (δηλαδή αθόρυβο κανάλι). Το προηγούμενο πρόβλημα είναι δυνατό να λυθεί μερικά με την πρόσθεση επιπλέον bits αλλά με την συνεπακόλουθη μείωση του ρυθμού εκπομπής δεδομένων. Η πρόσθεση επιπλέον bits με σκοπό τη μείωση του ρυθμού λαθών στην αποκωδικοποίηση ονομάζεται κωδικοποίηση. Η κωδικοποίηση χωρίζεται γενικά σε δύο κατηγορίες: τη γραμμική, *μπλοκ* κωδικοποίηση και τη συγκεραστική κωδικοποίηση, [2,3,10].

Στη μπλοκ κωδικοποίηση, οι ακολουθίες της εξόδου της πηγής πληροφορίας (μήνυμα πληροφορίας), με μήκος *k* απεικονίζονται σε δυαδικές ακολουθίες (κωδικές λέξεις) με μήκος *n* έτσι ώστε ο ρυθμός ή απόδοση του παραγομένου κώδικα να είναι ίσος με $\frac{k}{n}$ ανά εκπομπή, [11]. Ένας τέτοιος κώδικας ονομάζεται κώδικας *(n,k)* και αποτελείται από 2^k (πλήθος κωδικών λέξεων) κωδικές λέξεις με μήκος *n*, οι οποίες πολλές φορές συμβολίζονται με $c_1, c_2, .. c_{2^k}$.

Στους κώδικες μπλοκ, η απεικόνιση των διαφόρων ακολουθιών εξόδου της πηγής πληροφορίας στις κωδικές λέξεις πραγματοποιείται ανεξάρτητα και η έξοδος του κωδικοποιητή εξαρτάται μόνο από την τρέχουσα ακολουθία εξόδου της πηγής (ακολουθία εισόδου στον κωδικοποιητή) μήκους *k* και σε καμία περίπτωση από τις προηγούμενες ακολουθίες εισόδου στον αποκωδικοποιητή.

Μία πολύ απλή περίπτωση μπλοκ κωδικοποίησης είναι ο απλός κώδικας επανάληψης. Σε έναν απλό κώδικα επανάληψης με τον οποίο επιθυμούμε να εκπέμψουμε τα δυαδικά σύμβολα "0" και "1" σε ένα *δυαδικό συμμετρικό κανάλι* (BSC), αντί να εκπέμψουμε τα "0" και "1", εκπέμπουμε αντίστοιχα μία ακολουθία από "0" και "1" στη θέση αντίστοιχα του "0" και του "1". Το μήκος των δύο αυτών ακολουθιών επιλέγεται να είναι ένας περιττός αριθμός *n*. Έτσι, ένας απλός κώδικας επανάληψης μπορεί να παρασταθεί με την παρακάτω αντιστοιχία:

$$\begin{aligned} 0 &\rightarrow \overbrace{00}^{n} \overbrace{\ldots}^{\text{περιττός}} \overbrace{00} \\ 1 &\rightarrow \overbrace{11}^{n} \overbrace{\ldots}^{\text{περιττός}} \overbrace{11} \end{aligned} \tag{5.1}$$

Η διαδικασία της αποκωδικοποίησης (βασίζεται σε μία πλειοψηφική απόφαση: αν η πλειοψηφία (σε πλήθος) των λαμβανομένων συμβόλων, είναι τα "0" τότε αποφασίζεται ότι το εκπεμπόμενο bit είναι το "0". Αν αντίθετα, η πλειοψηφία των λαμβανομένων συμβόλων είναι οι "1" τότε αποφασίζεται ότι το εκπεμπόμενο bit είναι το "1".

Στη διαδικασία της αποκωδικοποίησης, λάθος παρατηρείται όταν τουλάχιστον *(n+1)/2* από τα εκπεμπόμενα bit έχουν ληφθεί λάθος. Αν το κανάλι επικοινωνίας είναι ένα BSC κανάλι, το οποίο εμφανίζει πιθανότητα λάθους στο εκπεμπόμενο bit ίση με *ε*, τότε η πιθανότητα λάθους αποκωδικοποίησης για έναν απλό κώδικα επανάληψης (*n,k*) αποδεικνύεται ότι δίνεται από την παρακάτω σχέση:

$$p_e = \sum_{k=(n+1)/2}^{n} \binom{n}{k} \cdot \varepsilon^k \cdot (1-\varepsilon)^{n-k} \tag{5.2}$$

Για παράδειγμα, σε έναν απλό κώδικα επανάληψης με n=5 και ε=0.001=10^{-3}, η πιθανότητα λάθους είναι ίση με:

$$p_e = \sum_{k=3}^{5} \binom{5}{k} \cdot 0.001^k \cdot (0.999)^{5-k} = 9.99 \times 10^{-10} \cong 10^{-9} \tag{5.3}$$

Ασκήσεις

1. α) Στην περίπτωση που ένα κανάλι δημιουργεί απλά σφάλματα με πιθανότητα $\varepsilon=10^{-3}$ βρείτε την πιθανότητα εσφαλμένης διόρθωσης P_ε και την πιθανότητα $P_\varepsilon^{/}$ αδυναμίας αναγνώρισης σφάλματος για κωδικοποίηση επαναληπτική τριών φορών.

β) Αν γνωρίζουμε ότι το $P_\varepsilon^{/}$ είναι μικρότερο ή ίσο από 10^{-11} ποια είναι η χείριστη (χειρότερη) πιθανότητα ε_1 που δεχόμαστε στο συγκεκριμένο κανάλι;

6. Γραμμικοί κώδικες Μπλοκ

Οι γραμμικοί μπλοκ κώδικες είναι γενικά οι πιο ευρέως χρησιμοποιούμενοι κώδικες. Ένας κώδικας μπλοκ είναι *γραμμικός* αν ένας οποιαδήποτε γραμμικός συνδυασμός δύο κωδικών λέξεων του κώδικα αποτελεί, πάλι κωδική λέξη του συγκεκριμένου κώδικα, [1,4,8]. Γενικά, οι γραμμικοί κώδικες μπλοκ περιγράφονται από τον πίνακα γεννήτορά τους *G*, ο οποίος είναι ένας $(k \times n)$ δυαδικός πίνακας έτσι ώστε κάθε κωδική λέξη *c* του κώδικα να προκύπτει από τη σχέση:

$$c = uG \tag{6.1}$$

όπου *u* είναι η ακολουθία εισόδου μήκους *k* (μήνυμα) (η είσοδος στον κωδικοποιητή). Η πράξη μεταξύ των πινάκων είναι πράξη modulo-2 (δηλαδή πράξη XOR). Μία σημαντική παράμετρος σε ένα γραμμικό κώδικα μπλοκ, η οποία καθορίζει και τη δυνατότητα διόρθωσης λαθών του κώδικα, είναι η *ελάχιστη απόσταση* (απόσταση Hamming) του κώδικα η οποία ορίζεται ως η ελάχιστη απόσταση Hamming μεταξύ δύο οποιονδήποτε κωδικών λέξεων του κώδικα, [10]. Η ελάχιστη απόσταση του κώδικα συμβολίζεται με $d_{\min}$ και δίνεται από τη σχέση, [10]:

$$d_{\min} = \min_{i \neq j} d_H\left(c_i, c_j\right) \tag{6.2}$$

Για τους γραμμικούς κώδικες, η ελάχιστη απόσταση Hamming είναι ίση με το ελάχιστο βάρος w_{min} του κώδικα το οποίο ορίζεται από τη σχέση:

$$w_{\min} = \min_{C_i \neq 0} w_H\left(c_i\right) \tag{6.3}$$

δηλαδή είναι το ελάχιστο *βάρος* (*weigth,* w_H) του κώδικα, αναφερόμενοι σε όλες τις μη μηδενικές κωδικές λέξεις του κώδικα (το βάρος w_H μιας οποιασδήποτε κωδικής λέξης ορίζεται ως ο αριθμός των "1" που παρουσιάζονται σε αυτή την κωδική λέξη). Αν ένας γραμμικός κώδικας παρουσιάζει ελάχιστη απόσταση Hamming $d_{\min}$ τότε οι επιδόσεις του σε σχέση με την ανίχνευση και την διόρθωση λαθών σε κάθε λαμβανόμενη κωδική λέξη δίνονται από τις παρακάτω σχέσεις, [13]:

$$d_{\min} = \begin{Bmatrix} e+1, \text{για ανίχνευση } e \text{ σφαλμάτων ανά κωδική λέξη} \\ 2e+1, \text{για διόρθωση } e \text{ σφαλμάτων ανά κωδική λέξη} \end{Bmatrix} \tag{6.4}$$

Ο κανόνας αποκωδικοποίησης που εφαρμόζεται για να αποφασιστεί ποια είναι η σωστή εκπεμπόμενη κωδική λέξη είναι ο εξής: "*Επέλεξε σα σωστή εκείνη την κωδική λέξη που παρουσιάζει τη μικρότερη ελάχιστη απόσταση Hamming από την υπό κρίση κωδική λέξη που έχει ληφθεί*" (αποκωδικοποίηση αυστηρής απόφασης, Hard-decision Decoding) (κριτήριο ελάχιστης απόφασης Hamming).

Ένας γραμμικός κώδικας μπλοκ είναι σε συστηματική μορφή αν ο πίνακας γεννήτορας του *G* έχει την παρακάτω μορφή:

$$\mathrm{G}=\begin{bmatrix} 1\ 0 & \ldots. & 0 & p_{1,1} & p_{1,2} & \cdot\ \cdot & p_{1,n-k} \\ 0\ 1 & \ldots. & 0 & p_{2,1} & p_{2,2} & \cdot\ \cdot & p_{2,n-k} \\ & & & & & & \\ 0\ 0 & \ldots.. & 1 & p_{k,1} & p_{k,2} & \cdot\ \cdot & p_{k,n-k} \end{bmatrix} \tag{6.5}$$

ή $$G=[I_k \mid P] \tag{6.6}$$

όπου στη σχέση (6.6) το αριστερό τμήμα του πίνακα δηλαδή ο I_k, είναι ο ($k \times k$) μοναδιαίος πίνακας και *P* είναι ένας $k \times (n-k)$ πίνακας. Σε ένα συστηματικό κώδικα, τα πρώτα *k* bits της κωδικής λέξης είναι τα bits της πληροφορίας (μηνύματος) και τα υπόλοιπα (*n-k)* bits είναι τα *bits ελέγχου της ισοτιμίας*.

Ο πίνακας ελέγχου της ισοτιμίας *H* σε έναν κώδικα είναι ένας $(n-k) \times n$ δυαδικός πίνακας, τέτοιος ώστε για όλες τις κωδικές λέξεις *c* του κώδικα να ισχύει η σχέση:

$$cH^t = 0 \tag{6.7}$$

όπου H^t είναι ο *ανάστροφος πίνακας* του πίνακα H (αυτός ο πίνακας που προκύπτει αν τις γραμμές του πίνακα H τις κάνουμε στήλες και αντίστροφα).

Προφανώς ισχύει:

$$GH^t = 0 \tag{6.8}$$

Αν ο πίνακας γεννήτορας G είναι σε συστηματική μορφή τότε ισχύει:

$$H=[-P^t|I_{n-k}] \tag{6.9}$$

(το πρόσημο (–) στη προηγούμενη σχέση δεν έχει κάποιο νόημα γιατί στο δυαδικό σύστημα αρίθμησης ισχύει: "1"="-1").

6.1 Κώδικες Hamming

Οι κώδικες Hamming είναι γραμμικοί κώδικες μπλοκ διαστάσεων (2^m-1, 2^m-m-1) που παρουσιάζουν ελάχιστη απόσταση ίση με 3 και έχουν έναν πολύ απλό πίνακα ελέγχου ισοτιμίας. Ο πίνακας ελέγχου ισοτιμίας ο οποίος είναι ένας πίνακας $m\times(2^m-1)$ πίνακας, έχει σαν στήλες όλες τις δυαδικές ακολουθίες με μήκος m, εκτός από την μηδενική ακολουθία. Για παράδειγμα, για m=3 έχουμε έναν (7,4) κώδικα του οποίου ο πίνακας ελέγχου της ισοτιμίας, σε συστηματική μορφή, είναι ο παρακάτω:

$$H=\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{6.10}$$

Εφαρμόζοντας τη σχέση (6.6) (και με τη βοήθεια της (6.9)) βρίσκουμε τον πίνακα γεννήτορα G του συγκεκριμένου κώδικα:

$$G=\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{6.11}$$

σε συστηματική μορφή (δηλαδή $G=[I_4 \mid P]$.

Έστω ένας κώδικας Hamming (n,k). Αν για αυτόν τον κώδικα γνωρίζουμε τον πίνακα ελέγχου της ισοτιμίας του H είναι δυνατόν να βρούμε τον πίνακα γεννήτορα του κώδικα G. Αν ο πίνακας ελέγχου της ισοτιμίας του κώδικα H είναι στην παρακάτω μορφή:

$$H=[-P^t| I_k] \tag{6.12}$$

τότε ο πίνακας γεννήτορας G του κώδικα έχει αντίστοιχα την παρακάτω μορφή:

$$G=[I_k \mid P] \tag{6.13}$$

Η κωδική λέξη που παράγεται εκπέμπεται στο κανάλι επικοινωνίας. Εξαιτίας του θορύβου του καναλιού, η λαμβανόμενη κωδική λέξη μπορεί να παρουσιάζει ένα απλό ή περισσότερα λάθη δηλαδή άλλο bit ή bits να έχει εκπεμφθεί στο κανάλι και διαφορετικό ή διαφορετικά bits να έχουν αποκωδικοποιηθεί στη λήψη.

Είναι λογικό να μοντελοποιήσουμε τα λάθη που παρουσιάζονται στη λήψη με ένα διάνυσμα το οποίο περιέχει 0 στη θέση εκείνη που δεν παρουσιάστηκε λάθος και 1 σε οποιαδήποτε θέση έγινε λάθος κατά την αποκωδικοποίηση. Το διάνυσμα αυτό ονομάζεται διάνυσμα συνδρόμου S ή απλά σύνδρομο. Η χρησιμότητά του είναι ότι με δεδομένο το διάνυσμα συνδρόμου μπορούμε να ανιχνεύσουμε αν υπάρχει απλό λάθος στη λαμβανομένη κωδική λέξη και να τα διορθώσουμε. Συγκεκριμένα, αν πολλαπλασιάσουμε τη λαμβανόμενη κωδική λέξη R με τον πίνακα ελέγχου ισοτιμίας H θα βρούμε τον πίνακα (διάνυσμα) του συνδρόμου S. Το σύνδρομο που υπολογίζεται θα πρέπει να αποτελεί μία στήλη του πίνακα ελέγχου της ισοτιμίας H. Η συγκεκριμένη στήλη δείχνει και τη θέση στη λαμβανόμενη λέξη που έχει συμβεί το λάθος κατά τη μετάδοση στο κανάλι επικοινωνίας π.χ. αν προέκυψε η δεύτερη στήλη ($2^η$) τότε έχει γίνει λάθος στο $2^ο$ λαμβανόμενο bit στη λαμβανόμενη λέξη R.

$$R \cdot H^t = S \tag{6.14}$$

Έτσι η σωστή κωδική λέξη θα προκύψει αν στη λαμβανόμενη κωδική λέξη R προσθέσουμε με πράξη *modulo-2* (αποκλειστικό ή) το διάνυσμα του συνδρόμου S. Δηλαδή ισχύει:

$$CorrectedCodeword = R \oplus S \tag{6.15}$$

Στην αποκωδικοποίηση, υπάρχει ένας πίνακας ο οποίος ονομάζεται πίνακας αποκωδικοποίησης που δείχνει στον αποκωδικοποιητή πως θα διορθωθούν τα λάθη που παρατηρούνται στη λαμβανόμενη λέξη. Στους κώδικες Hamming υπάρχει η δυνατότητα διόρθωσης ενός απλού λάθους σε κάθε λαμβανόμενη κωδική λέξη (e=1).

Με την αποκωδικοποίηση συνδρόμου, ένας γραμμικός κώδικας μπλοκ (n,k) μπορεί να διορθώσει μέχρι e σφάλματα ανά κωδική λέξη αν τα n και k ικανοποιούν το παρακάτω όριο Hamming:

$$2^{n-k} \geq \sum_{i=0}^{e} \binom{n}{i} \tag{6.16}$$

Ασκήσεις

1. Ένας κώδικας αποτελείται από τις επόμενες κωδικές λέξεις: 0000001, 0011110, 0101101, 0111000, 1001100, 1011001, 1101010, 1110100. Αν λαμβάνουμε τη λέξη 1011011 ποια θεωρείται η σωστή κωδική λέξη με βάση το κριτήριο της ελάχιστης απόστασης Hamming.

2. Αν για ένα κώδικα έχω πίνακα γεννήτορα τον παρακάτω να βρείτε την κωδική λέξη που αντιστοιχεί στο μήνυμα [1011]:

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

3. Σας δίνεται ένας γραμμικός κώδικας μπλοκ ο οποίος έχει πίνακα γεννήτορα τον παρακάτω:

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

Να βρεθεί ο πίνακας ελέγχου της ισοτιμίας για την περίπτωση που ο κώδικας είναι μπλοκ συστηματικής μορφής.

4. Ένας κώδικας μπλοκ Hamming (7,4) έχει ως πίνακα ελέγχου της ισοτιμίας τον παρακάτω πίνακα Η:

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

α) Ποια είναι η απόδοση του κώδικα;
β) Ποια είναι η κωδική λέξη που αντιστοιχεί στο μήνυμα [0 0 1 1];
γ**)** Αν η λαμβανόμενη λέξη είναι η [1 0 0 0 0 1 0] βρείτε αν υπάρχει λάθος και αν υπάρχει και το θεωρούμε απλό ποια είναι η σωστή κωδική λέξη;

5. Ένας κώδικας μπλοκ Hamming (7,4) έχει ως πίνακα ελέγχου της ισοτιμίας τον παρακάτω πίνακα Η:

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

α) Ποια είναι η απόδοση του κώδικα;
β) Ποια είναι η κωδική λέξη που αντιστοιχεί στο μήνυμα [1 0 1 0];
γ) Αν η λαμβανόμενη λέξη είναι η [1 1 1 1 1 0 1] βρείτε αν υπάρχει λάθος και αν υπάρχει και το θεωρούμε απλό ποια είναι η σωστή κωδική λέξη;
δ) Το ερώτημα γ) να επαναληφθεί αν λαμβανόμενη κωδική λέξη είναι η [1 0 1 0 1 01]

6. Δώστε τον ορισμό της απόστασης Hamming δύο κωδικών λέξεων. Με ποιους τρόπους υπολογίζεται η απόσταση Hamming; Να υπολογίσετε με δύο διαφορετικούς τρόπους την απόσταση Hamming μεταξύ των κωδικών λέξεων (10111001) και (11101000).
7. Έστω ότι διαθέτουμε κώδικα διόρθωσης απλών σφαλμάτων για 11 bit δεδομένων. α)Πόσα bit ελέγχου χρειάζονται; β)Να βρεθεί ο πίνακας ελέγχου ισοτιμίας για τον κώδικα αυτό.

Ασκήσεις με απαντήσεις

1. Έστω ότι διαθέτουμε γραμμικό κώδικα μπλοκ (6,3) με πίνακα ελέγχου ισοτιμίας H που δίνεται από την

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

α) Να βρεθεί ο πίνακας γεννήτορας του κώδικα G.

(Απάντηση: $G=\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$)

β) Να βρεθεί η κωδική λέξη για bit δεδομένων (101) (Απάντηση:101010)

7. Κυκλικοί κώδικες

Ένας γραμμικός κώδικας ονομάζεται κυκλικός αν επιπρόσθετα από τις ιδιότητες των γραμμικών κωδίκων έχει την ιδιότητα μία οποιαδήποτε *κυκλική ολίσθηση* μιας κωδικής του λέξης να αποτελεί και αυτή κωδική λέξη του συγκεκριμένου κώδικα, [10]. Οι κυκλικοί κώδικες μπορούν να περιγραφτούν ισοδύναμα είτε με τον πίνακα γεννήτορα *G* και τον πίνακα ελέγχου ισοτιμίας τους *H* είτε με τη βοήθεια του *πολυωνύμου γεννήτορα*. Συνεπώς, αν $C=\left[c_{n-1}\ c_{n-2}\ ...c_1c_0\right]$ είναι μία κωδική λέξη ενός κυκλικού κώδικα τότε και η κυκλική του ολίσθηση $\left[c_{n-2}\ c_{n-3}\ ...c_0c_{n-1}\right]$ θα είναι επίσης κωδική λέξη του κώδικα.

Για να περιγράψουμε τους κυκλικούς κώδικες, αντιστοιχούμε σε κάθε κωδική λέξη $C=\left[c_{n-1}\ c_{n-2}\ ...c_1c_0\right]$ ένα πολυώνυμο $C(p)$ βαθμού $\le n-1$, το οποίο ορίζεται ως εξής:

$$C(p)=c_{n-1}p^{n-1}+c_{n-2}p^{n-2}+...+c_1p+c_0 \tag{7.1}$$

Είναι δυνατό να γράψουμε τη προηγούμενη σχέση (8.1) ως εξής:

$$pC(p)=c_{n-1}p^{n}+c_{n-2}p^{n-1}+...+c_1p^2+c_0p \tag{7.2}$$

Αν διαιρέσουμε το αριστερό μέλος της σχέσης (7.2) με p^n+1, τότε λαμβάνουμε:

$$\frac{pC(p)}{p^n+1}=c_{n-1}+\frac{C_1(p)}{p^n+1} \tag{7.3}$$

όπου

$$C_1(p)=c_{n-2}p^{n-1}+c_{n-3}p^{n-2}+...+c_1p^2+c_0p+c_{n-1} \tag{7.4}$$

Δεδομένου ότι το $C_1(p)$ είναι το υπόλοιπο της διαίρεσης του $pC(p)$ με το p^n+1 μπορούμε να γράψουμε:

$$C_1(p)=pC(p)\bmod\left(p^n+1\right) \tag{7.5}$$

Μπορούμε να παράγουμε έναν κυκλικό κώδικα (*n,k*), χρησιμοποιώντας το πολυώνυμα γεννήτορα $g(p)$ βαθμού (*n-k*). Το πολυώνυμο γεννήτορας ενός (*n,k*) κυκλικού κώδικα, έχει την παρακάτω γενική μορφή:

$$g(p)=p^{n-k}+g_{n-k-1}p^{n-k-1}+...+g_1p+1 \tag{7.6}$$

Παράλληλα μπορούμε να ορίσουμε το *πολυώνυμο του μηνύματος* ως εξής:

$$X(p)=x_{k-1}p^{k-1}+x_{k-2}p^{k-2}...+x_1p+x_0 \tag{7.7}$$

όπου το $\left[x_{k-1}\ x_{k-2}\ ...x_1x_0\right]$ αναπαρασταίνει τα *k* bits του μηνύματος (πληροφορία). Το γινόμενο των πολυωνύμων $X(p)\cdot g(p)$ είναι ένα πολυώνυμο βαθμού μικρότερου ή ίσου με το (*n*-1) και το οποίο αναπαρασταίνει μία κωδική λέξη του κυκλικού κώδικα.

<u>Παράδειγμα</u>

Ας θεωρήσουμε ένα κώδικα με μήκος *n*=7 (σύνολο των bits μετά την κωδικοποίηση). Το πολυώνυμο p^7+1 μπορεί να γραφτεί ως γινόμενο παραγόντων:

$$p^7+1=(p+1)\cdot\left(p^3+p^2+1\right)\cdot\left(p^3+p+1\right) \tag{7.8}$$

Για να παράγουμε ένα κυκλικό κώδικα (*n,k*), θα πρέπει να θεωρήσουμε ένα από τα επόμενα πολυώνυμα ως πολυώνυμο γεννήτορα:

$$g_1(p)=\left(p^3+p^2+1\right) \tag{7.9}$$

$$g_2(p)=\left(p^3+p+1\right) \tag{7.10}$$

Οι κώδικες οι οποίοι μπορούν να παραχθούν από τα δύο προηγούμενα πολυώνυμα, είναι ισοδύναμοι. Για παράδειγμα, τα μηνύματα [0001] και [1110] κωδικοποιούνται αντίστοιχα μέσω του πολυωνύμου $g_1(p)=\left(p^3+p^2+1\right)$ ως [0001101] και [1000110].

Η πρόσθεση '+' μεταξύ των διαφόρων παραγόντων των πολυωνύμων είναι πράξη modulo 2 (λογική πράξη αποκλειστικού Η, EXOR, Exclusive OR). Συνεπώς, όταν μετά το συνήθη πολλαπλασιασμό εμφανίζονται δύο ίδιοι παράγοντες τότε αυτοί απαλείφονται μεταξύ τους ανά δύο π.χ. $p^3+p^3=0$.

Έστω ένας κυκλικός κώδικας (*n,k*). Τότε ο πίνακας γεννήτορας *G* για τον προηγούμενο κώδικα, δίνεται σε συστηματική μορφή από την επόμενη έκφραση:

$$G=[I_k|\ P] \tag{7.11}$$

Αντίστοιχα, ο πίνακας ελέγχου ισοτιμίας *H* του κυκλικού κώδικα (*n,k*), δίνεται σε συστηματική μορφή από την παρακάτω έκφραση:

$$H=[I_{n-k}\,|P^t] \tag{7.12}$$

Ασκήσεις

1. Το πολυώνυμο γεννήτορας ενός κυκλικού κώδικα (7,4) είναι το $g(p)=(p^3+p+1)$. Βρείτε τις δεκαέξι (16) κωδικές λέξεις του συγκεκριμένου κώδικα.

2. Το πολυώνυμο γεννήτορας ενός κυκλικού κώδικα είναι το $g(x)=1+x^4+x^6+x^7+x^8$. Βρείτε την κωδική λέξη που αντιστοιχεί στο μήνυμα με πολυώνυμο $D(x)=x^2+x^3+x^4$.

8. BCH Κώδικες

Οι BCH (Bose-Chaudhuri-Hocquenghem) κώδικες αποτελούν μία ευρεία κατηγορία κυκλικών κωδίκων και περιλαμβάνουν δυαδικά και μη δυαδικά αλφάβητα. Οι κώδικες BCH ανακαλύφθηκαν το 1959-1960 από τρεις ερευνητές από τα ονόματα των οποίων και δόθηκε το συγκεκριμένο όνομα στην κατηγορία αυτή των γραμμικών κυκλικών κωδίκων, [14,15]. Αποτελούν μία πολύ σημαντική κατηγορία γραμμικών κωδίκων διότι προσφέρουν σημαντική απόδοση (λόγος k/n), παρουσιάζουν ευρεία περιοχή τιμών για τα n και k και τέλος η πολυπλοκότητα των κωδικοποιητών τους είναι σχετικά μικρή.

Οι BCH κώδικες (n,k) (n είναι το μήκος της κωδικής λέξης και k είναι το μήκος του μηνύματος το οποίο θα κωδικοποιήσουμε) σχεδιάζονται δηλαδή βρίσκονται τα n και k με τη βοήθεια των παρακάτω γενικών θεωρητικών σχέσεων, [10,11]:

$$\begin{aligned} &n=2^m-1 \\ &n-k\le mt \\ &d_{\min}=2t+1 \end{aligned} \tag{8.1}$$

όπου m ($m\ge 3$) και t είναι αυθαίρετοι θετικοί αριθμοί. Το μέγεθος d_{min} είναι η ελάχιστη απόσταση Hamming και μας δηλώνει αριθμητικά μέσω της παραμέτρου t, ότι ο συγκεκριμένος κώδικας είναι δυνατό να διορθώσει μέχρι και t σφάλματα ανά κωδική λέξη. Το μήκος της κωδικής λέξης n σε έναν κώδικα BCH δίνεται πάντα από τη σχέση (8.1) ενώ ο αριθμός των λαθών που μπορεί να διορθώσει ο κώδικας (ικανότητα διόρθωσης λαθών του κώδικα) περιορίζεται από την επόμενη σχέση:

$$t<(2^m-1)/2 \tag{8.2}$$

Συνεπώς, ο σχεδιαστής ενός τηλεπικοινωνιακού συστήματος έχει τη δυνατότητα να επιλέξει από ένα μεγάλο σύνολο από μήκη κωδίκων και ρυθμών κωδίκων. Τα πολυώνυμα γεννήτορες των BCH κωδίκων προκύπτουν από τους *παράγοντες* των πολυωνύμων $p^{2^m-1}+1$. Οι μη δυαδικοί BCH κώδικες περιλαμβάνουν τους κώδικες Reed-Solomon. Στη κωδικοποίηση ενός (n,k) BCH κώδικα, ένα μήνυμα είναι ένας k στηλών δυαδικός πίνακας Galois, [10,13]. Ένα μαθηματικό πεδίο Galois είναι ένα αλγεβρικό σύνολο (πεδίο) το οποίο αποτελείται από ένα πεπερασμένο αριθμό στοιχείων. Ένα πεδίο Galois, είναι δυνατό να έχει 2^m στοιχεία όπου m είναι ένας ακέραιος αριθμός μεταξύ του 1 και του 16. Ένα

τέτοιο πεδίο Galois συμβολίζεται ως GF(2^m). Τα πεδία Galois βρίσκουν μεγάλη εφαρμογή στη θεωρία κωδικοποίησης και ανίχνευσης-διόρθωσης λαθών. Συγκεκριμένα, για ένα BCH κώδικα, κάθε γραμμή ενός αντίστοιχου πίνακα Galois, αναπαρασταίνει μία κωδική λέξη του κώδικα BCH.

Στους κώδικες BCH, το μήκος k του κάθε μηνύματος είναι ένας θετικός ακέραιος πάντα μικρότερος του n. Πρέπει να σημειωθεί ότι μόνο κάποιες τιμές από τους θετικούς ακεραίους τους μικρότερους από το n είναι επιτρεπτές ως τιμές του k. Για το λόγο αυτό δίνονται στη βιβλιογραφία αντίστοιχοι πίνακες με τις αποδεκτές τιμές των παραμέτρων n και k, [10].

Τέλος, οι κώδικες BCH έχουν πολλές εφαρμογές στα τηλεπικοινωνιακά συστήματα. Μία από τις πιο γνωστές είναι η εφαρμογή τους στα κυψελωτά συστήματα κινητής τηλεφωνίας όπου ένας περιορισμένου μήκους κώδικας BCH χρησιμοποιείται για τα σήματα σηματοδοσίας που δηλώνουν στον κινητό σταθμό, εκτός των άλλων στοιχείων, την ισχύ που πρέπει να εκπέμψει ο κινητός σταθμός και σε ποια συγκεκριμένη συχνότητα του συστήματος.

9. Κώδικες Reed-Solomon

Οι κώδικες Reed-Solomon σχεδιαστήκανε το 1960 από τους Reed και Solomon, [14]. Οι κώδικες αυτοί είναι μη δυαδικοί κώδικες και έχουν μεγάλη σημασία για τα τηλεπικοινωνιακά συστήματα στα οποία τα σφάλματα λόγω θορύβου του καναλιού επικοινωνίας εμφανίζονται κατά ριπές όπως επίσης και για τα συστήματα ακουστικών CD.

Οι κώδικες Reed-Solomon, είναι μπλοκ κώδικες οι οποίοι χρησιμοποιούν αλφάβητα εισόδου και εξόδου με πλήθος συμβόλων 2^m δηλαδή $\{0,\ 1,\ 2,\ ...,\ 2^m - 1\}$.

Το μήκος της κωδικής λέξης n (αριθμός συμβόλων ανά κωδική λέξη) (μήκος μη-δυαδικής κωδικής λέξης) είναι ίσο με 2^m-1 (ακέραιες τιμές μεταξύ 3 και 2^m-1). Το προηγούμενο μήκος του κώδικα μπορεί να αυξηθεί σε 2^m ή 2^m+1 αν κάτι τέτοιο είναι επιθυμητό. Οι κώδικες σχεδιάζονται για να διορθώνουν e_0 λάθη σε ένα μπλοκ από n σύμβολα. Το μήκος του μηνύματος που κωδικοποιείται είναι k (αριθμός συμβόλων ανά μήνυμα) (θετικός ακέραιος μικρότερος από n έτσι ώστε το (n-k) να είναι άρτιος) και ο αριθμός των απαιτουμένων bits ελέγχου ισοτιμίας για να είναι δυνατή η διόρθωση e_0 λαθών είναι $(n-k)=n-2e_0= 2^m-1$. Ο αριθμός m των bits/σύμβολο, είναι ακέραιος αριθμός μεταξύ του 3 και του 16. Με δεδομένες τις προηγούμενες παραμέτρους, ο κώδικας Reed-Solomon είναι δυνατό να διορθώσει μέχρι $t = (n-k)/2$ λάθη (error-correction capability of the code). Οι κώδικες Reed-Solomon παρουσιάζουν ελάχιστη απόσταση ίση με $d_{min}=(n-k+1)$ γεγονός που τους καθιστά ιδιαίτερα ελκυστικούς.

10. Ταξινόμηση κωδίκων

Η ταξινόμηση των κωδίκων, μπορεί να γίνει κατανοητή με τη βοήθεια του επόμενου πίνακα:

x_i	**Κώδικας 1**	**Κώδικας 2**	**Κώδικας 3**	**Κώδικας 4**	**Κώδικας 5**	**Κώδικας 6**
x_1	00	00	0	0	0	1
x_2	01	01	1	10	01	01
x_3	00	10	00	110	011	001
x_4	11	11	11	111	0111	0001

Κώδικες σταθερού μήκους: είναι ο κώδικας που κάθε κωδική του λέξη έχει σταθερό μήκος. Οι κώδικες 1 και 2 του προηγούμενου πίνακα έχουν σταθερό μήκος 2.

Κώδικες μεταβλητού μήκους: κώδικας μεταβλητού μήκους είναι ο κώδικας του οποίου το μήκος της κωδικής λέξης δεν είναι σταθερό. Όλοι οι κώδικες του προηγούμενου πίνακα, εκτός από τους κώδικες 1 και 2, είναι μεταβλητού μήκους.

Ευκρινείς κώδικες: ένας κώδικας ονομάζεται ευκρινής αν κάθε κωδική λέξη του ξεχωρίζει από τις άλλες κωδικές λέξεις. Όλοι οι κώδικες του προηγούμενου πίνακα εκτός από τον κώδικα 1 είναι ευκρινείς.

Κώδικες χωρίς πρόθεμα: κώδικας στον οποίο δεν σχηματίζεται μία κωδική λέξη με πρόσθεση κωδικών συμβόλων σε άλλη κωδική λέξη ονομάζεται κώδικας χωρίς πρόθεμα. Οι κώδικες 2, 4 και 6 του προηγούμενου πίνακα είναι κώδικες χωρίς πρόθεμα.

Μοναδικά αποκωδικοποιούμενοι κώδικες: ένας κώδικας είναι μοναδικά αποκωδικοποιούμενος αν η αρχική ακολουθία πηγής μπορεί να αναδομηθεί τέλεια από την κωδικοποιημένη δυαδική ακολουθία. Στον προηγούμενο πίνακα, ο κώδικας 3 δεν είναι μοναδικά αποκωδικοποιούμενος κώδικας γιατί π.χ. η δυαδική ακολουθία 1001 μπορεί να αντιστοιχεί στις ακολουθίες πηγής $x_2\ x_3\ x_2$ ή $x_2\ x_1\ x_1\ x_2$. Στον προηγούμενο πίνακα ο κώδικας 5 είναι μοναδικά αποκωδικοποιούμενος επειδή το bit 0, δείχνει την αρχή κάθε κωδικής λέξης του κώδικα.

Στιγμιαίοι κώδικες: ένας μοναδικά αποκωδικοποιούμενος κώδικας ονομάζεται στιγμιαίος κώδικας αν το τέλος οποιασδήποτε κωδικής λέξης αναγνωρίζεται χωρίς να εξεταστούν επόμενα κωδικά σύμβολα. Οι στιγμιαίοι κώδικες έχουν την ιδιότητα ότι καμία κωδική λέξη δεν είναι πρόθεμα κάποιας άλλης κωδικής λέξης.

Βέλτιστοι κώδικες: ένας κώδικας είναι βέλτιστος αν είναι στιγμιαίος και έχει ελάχιστο μέσο μήκος για δεδομένη κατανομή πιθανοτήτων για τα σύμβολα της πηγής πληροφορίας.

11. Συγκεραστικοί κώδικες

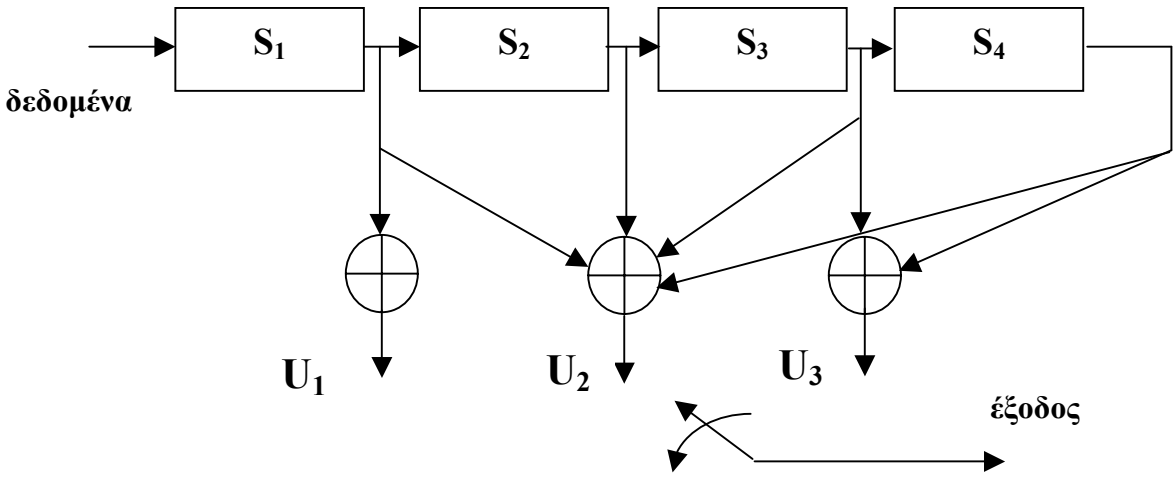
Στους συγκεραστικούς κώδικες, η κωδικοποίηση πραγματοποιείται πάνω σε ένα ολόκληρο διάστημα της ροής των συμβόλων του μηνύματος που ονομάζεται *διάστημα εξαναγκασμού*. Συνεπώς, πετυχαίνεται κωδικοποίηση με συνεχή τρόπο χωρίς να είναι απαραίτητη η κατάτμησή τους σε μπλοκ όπως στους γραμμικούς κώδικες μπλοκ. Πρακτικά η κωδικοποίηση γίνεται με τη χρήση *καταχωρητών ολισθητών* (shift registers) δηλαδή μία παράθεση από μνήμες με ένα εξωτερικό ρολόι.

Ένας συγκεραστικός κώδικας με διάστημα εξαναγκασμού k δημιουργείται με το συνδυασμό των k εξόδων ενός ολισθητή k-βαθμίδων και με τη βοήθεια υ αθροιστών modulo-2. Οι έξοδοι υ_1 υ_1, υ_2,…, υ_υ των αθροιστών δειγματοληπτούνται από έναν κατάλληλο διακόπτη. Έτσι παράγονται υ ψηφία εξόδου για κάθε ένα ψηφίο εισόδου. Η

παραγωγή των υ ψηφίων εξόδου γίνεται με τη βοήθεια εξισώσεων οι οποίες θα πρέπει να μας είναι γνωστές.

Παράδειγμα

Στο επόμενο σχήμα παρουσιάζεται διάταξη συγκεραστικού κωδικοποιητή ο οποίος έχει k=4 και υ=3.



Στη προηγούμενη διάταξη οι εξισώσεις παραγωγής των ψηφίων της εξόδου είναι οι παρακάτω:

$$U_1 = S_1$$
$$U_2 = S_1 \oplus S_2 \oplus S_3 \oplus S_4$$
$$U_3 = S_1 \oplus S_3 \oplus S_4$$

Αν έχουμε στον προηγούμενο συγκεραστικό κωδικοποιητή ως είσοδο το μήνυμα (1011), τότε για κάθε ένα από τα τέσσερα bits παράγεται μία τριάδα (3 bits εξόδου) ψηφίων εξόδου όπως αναλύεται στη συνέχεια:

Bit 1: U_1=1, U_2=1, U_3=1 (έξοδος 111)
Bit 0: U_1=0, U_2=1, U_3=0 (έξοδος 010)
Bit 1: U_1=1, U_2=0, U_3=0 (έξοδος 100)
Bit 1: U_1=1, U_2=1, U_3=0 (έξοδος 110)

Ασκήσεις

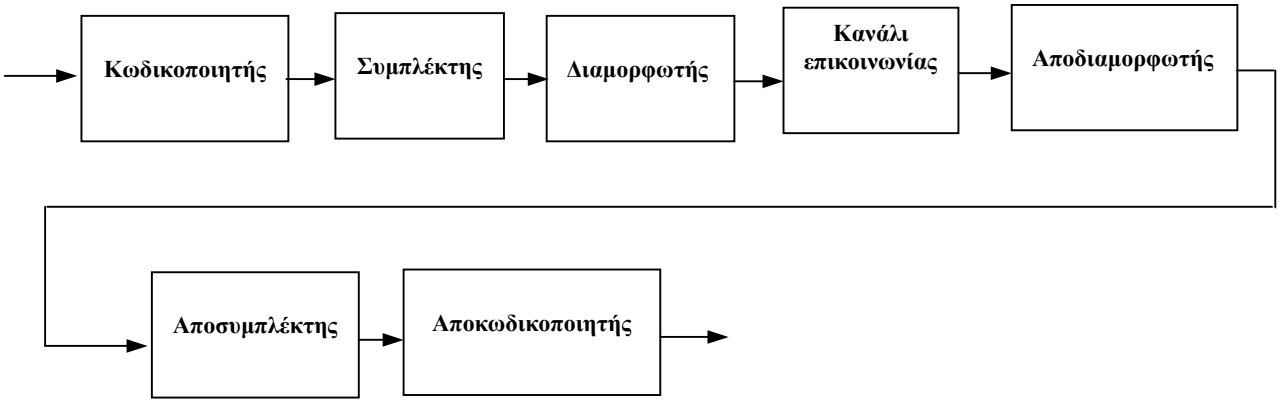
1. Να κατασκευαστεί διάγραμμα συγκεραστικού κωδικοποιητή με ολισθητές και αθροιστές modulo-2 στον οποίο οι εξισώσεις των εξόδων του δίνονται από τις εξισώσεις:

$$U_1 = S_1 \oplus S_2 \oplus S_3$$
$$U_2 = S_1$$
$$U_3 = S_1 \oplus S_2$$

Να βρεθεί επίσης η έξοδος του κωδικοποιητή για μήνυμα εισόδου (10110).
(Απάντηση: η έξοδος είναι: 111101011010001)

12. Κώδικες διόρθωσης καταιγισμού σφαλμάτων

Οι γραμμικοί κώδικες μπλοκ είναι σχεδιασμένοι για τη διόρθωση τυχαίων σφαλμάτων δηλαδή σφαλμάτων τα οποία εμφανίζονται τα καθένα ανεξάρτητα από τα άλλα σφάλματα του καναλιού. Σε μερικά όμως κανάλια επικοινωνίας (π.χ. σε ένα κανάλι με διαλείψεις (fading channel) ή σε μία φθορά ενός CD (χάραξη)) τα σφάλματα εμφανίζονται κατά ακολουθίες (ριπές) δηλαδή παρουσιάζουν *καταιγιστική συμπεριφορά*. Σε τέτοιες περιπτώσεις καναλιών επικοινωνίας εφαρμόζουμε τις μεθόδους διόρθωσης καταιγιστικών σφαλμάτων και συγκεκριμένα προχωρούμε στη "σύμπλεξη" των κωδικών λέξεων (interleaving).Με τη σύμπλεξη των κωδικών λέξεων η θέση των σφαλμάτων πετυχαίνουμε να μην είναι σειριακή αλλά να μοιάζει τυχαία δηλαδή ο καταιγισμός να διασκορπίζεται. Συνεπώς το πλήθος των σφαλμάτων ανά κωδική λέξη είναι μικρό. Στο δέκτη αντίστοιχα εισάγεται διάταξη αποσυμπλέκτη (de-interleaver) που εκτελεί τη ακριβώς αντίστροφη διαδικασία. Στο επόμενο σχήμα παρουσιάζεται μία διάταξη κωδικοποίησης, σύμπλεξης των κωδικών λέξεων, διαμόρφωσης, εκπομπής και αντίστροφα αποδιαμόρφωσης, αποσύμπλεξης και τέλος αποκωδικοποίησης.



13. Εφαρμογές των κωδίκων

Στη παράγραφο αυτή δίνονται κάποιες από τις εφαρμογές των κωδίκων σε συστήματα επικοινωνιών αλλά με την παρατήρηση ότι οι εφαρμογές τους είναι ανεξάντλητες και δεν μπορούν να περιγραφτούν μόνο μέσα σε λίγες παραγράφους αλλά μπορούν να αποτελέσουν αντικείμενο ενός ξεχωριστού συγγράμματος.

Κώδικες μπλοκ: όταν τα σφάλματα παρουσιάζονται ομοιόμορφα και τυχαία στα εισερχόμενα μπλοκ πληροφορίας τότε εφαρμόζουμε κώδικες μπλοκ. Συνήθως οι κώδικες μπλοκ βρίσκουν εφαρμογή σε κανάλι με AWGN θόρυβο. Περιπτώσεις τέτοιων καναλιών επικοινωνίας είναι οι χερσαίες τηλεφωνικές ζεύξεις.

Κώδικες διόρθωσης καταιγισμού σφαλμάτων: στις επικοινωνίες κινητών, τα σφάλματα στη λαμβανόμενη πληροφορίας εμφανίζονται σε ομάδες (ριπές) λόγω των διαλείψεων του καναλιού και λόγω της κίνησης του χρήστη. Έτσι σε αυτές τις περιπτώσεις με τους κώδικες διόρθωσης καταιγισμού σφαλμάτων, πετυχαίνεται η κατανομή των σφαλμάτων να είναι ομοιόμορφη.

Κώδικες Reed-Solomon: Οι κώδικες Reed-Solomon βρίσκουν εφαρμογή στις κινητές επικοινωνίες και στα τμήματα μηχανισμών διόρθωσης σφαλμάτων των CD που συμβαίνουν στην επιφάνειά τους. Θα πρέπει να ειπωθεί ότι οι κώδικες Reed-Solomonπαρουσιάζουν μεγάλη ελάχιστη απόσταση, έχουν καλές διορθωτικές ιδιότητες και καλές επιδόσεις σε περιπτώσεις που τα σφάλματα είναι μάλλον καταιγιστικά παρά τυχαία. Τέλος, πολλές φορές συνδυάζονται σε σειρά με έναν δυαδικό κώδικα (π.χ. με έναν κώδικα μπλοκ ή ένα συνελικτικό κώδικα)

Κώδικες για μακρινές διαστημικές επικοινωνίες: στη συγκεκριμένη κατηγορία ζεύξεων έχουμε χαμηλή τιμή του SNR, μικρή τιμή εκπομπής από φωτοβολταϊκά στοιχεία και θόρυβο AWGN. Εδώ χρησιμοποιούνται κώδικες μπλοκ και συνελεκτικοί κώδικες

Κωδικοποίηση για κανάλια περιορισμένου εύρους ζώνης συχνοτήτων: η κωδικοποίηση οδηγεί σε αύξηση του εύρους ζώνης συχνοτήτων του τελικά εκπεμπόμενου σήματος. Στην πράξη όμως έχουμε περιορισμούς στο διαθέσιμο εύρος ζώνης συχνοτήτων π.χ. στη σχεδίαση των modem των τηλεφωνικών καναλιών. Στη περίπτωση αυτή πραγματοποιείται συνδυασμός μιας μεθόδου κωδικοποίησης και διαμόρφωσης που ονομάζεται *trellis-κωδικοποιημένη διαμόρφωση* (trellis coded modulation)

Αλυσιδωτοί κώδικες: οι συγκεκριμένοι κώδικες αποτελούνται από δύο κώδικες, έναν εσωτερικό (συνήθως δυαδικός κώδικας μπλοκ ή συγκεραστικός κώδικας) και ένα εξωτερικό κώδικα (συνήθως κώδικας Reed-Solomon). Η επίδοση του εσωτερικού κώδικα έχει τη μεγαλύτερη επίπτωση στις συνολικές επιδόσεις του κώδικα

Κώδικες συστημάτων διάχυτου φάσματος: Στα συστήματα διάχυτου φάσματος, η επιλογή των ακολουθιών κωδικοποίησης (κωδικές λέξεις) που θα χρησιμοποιηθούν για τη διάχυση του φάσματος του σήματος της πληροφορίας, είναι πολύ σημαντική για τη λειτουργία και

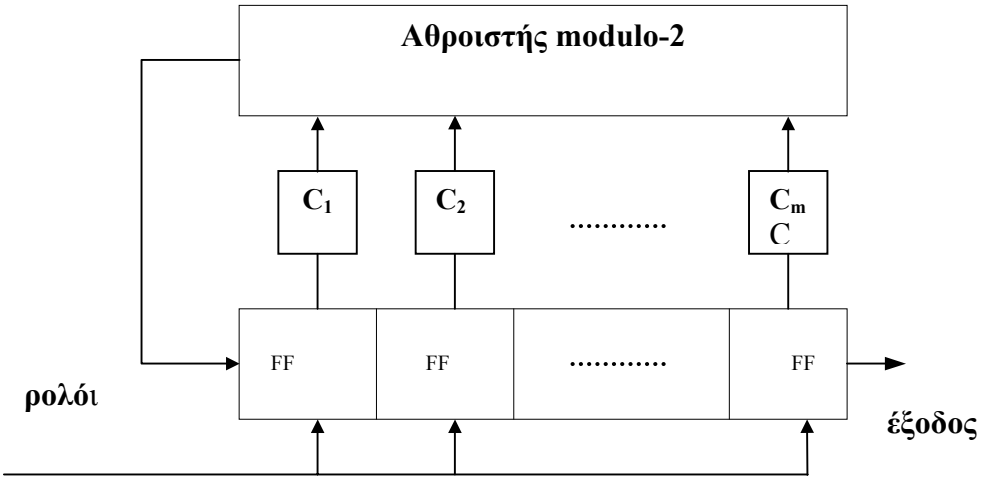
την απόδοση των συστημάτων αυτών, [15]. Συγκεκριμένα οι ιδιότητες των ακολουθιών κωδικοποίησης όπως ο τύπος, ο ρυθμός και το μήκος τους είναι σημαντικές παράμετροι στη σχεδίαση των συστημάτων διάχυτου φάσματος.

Η ακολουθία κωδικοποίησης που χρησιμοποιείται για τη διάχυση του φάσματος του σήματος πληροφορίας πρέπει θεωρητικά να είναι τυχαία, απείρου μήκους και υψηλού ρυθμού. Όμως πρακτικά αυτό δεν είναι δυνατό γιατί στα συστήματα διάχυτου φάσματος απαιτείται στο δέκτη του συστήματος να παραχθεί μια ακολουθία πανομοιότυπη και σύγχρονη με αυτή που έχει χρησιμοποιηθεί στον πομπό του συστήματος κάτι που είναι αδύνατο αν η ακολουθία είναι τυχαία. Έτσι στη πράξη οι ακολουθίες που χρησιμοποιούνται μοιάζουν να είναι τυχαίες αλλά στην πραγματικότητα παρουσιάζουν μια "κανονικότητα". Οι ακολουθίες αυτές ονομάζονται *ψευδοτυχαίες* ή *ακολουθίες ψευδοθορύβου* (Pseudo-random, Pseudo-noise sequences, PN) και είναι νομοτελειακές με πεπερασμένο μήκος. Οι ακολουθίες αυτές ικανοποιούν τις παρακάτω ιδιότητες:

- είναι εύκολο να παραχθούν
- έχουν τυχαίες ιδιότητες
- έχουν μεγάλες περιόδους επανάληψης
- είναι δύσκολο να αναπαραχθούν από ένα μικρό τμήμα τους.

Στη πράξη οι ακολουθίες που χρησιμοποιούνται στα συστήματα διάχυτου φάσματος είναι οι *γραμμικές ακολουθίες μεγίστου μήκους* (Linear Maximal Length Sequence, LMLS) ή διαφορετικά γνωστές σαν *ψευδοτυχαίες ακολουθίες μεγίστου μήκους* ή m-ακολουθίες (Pseudo-noise maximal length sequence, m-sequences). Από τις ακολουθίες αυτές παράγονται και άλλες ακολουθίες, όπως οι Gold ακολουθίες, οι οποίες είναι εύκολο να παραχθούν και έχουν χαρακτηριστικά τυχαιότητας.

Στη συνέχεια περιγράφονται συνοπτικά, οι ιδιότητες και τα χαρακτηριστικά των ψευδοτυχαίων ακολουθιών μεγίστου μήκους. Οι ακολουθίες αυτές έχουν μεγάλη περίοδο επανάληψης, όπως έχει ειπωθεί, και υλοποιούνται με μια απλή διάταξη γεννήτριας (Pseudo-random Generator, PRG) που αποτελείται από ένα *καταχωρητή ολίσθησης με γραμμική ανατροφοδότηση* (linear feedback shift register) όπως φαίνεται στο επόμενο σχήμα. Ο καταχωρητής ολίσθησης μήκους m αποτελείται από m flip-flops (FF) ελεγχόμενα από το ίδιο εξωτερικό ρολόι. Σε κάθε παλμό ρολογιού το περιεχόμενο καθεμιάς βαθμίδας FF ολισθαίνει στην αμέσως επόμενη βαθμίδα. Για την αποφυγή της πιθανότητας ο καταχωρητής ολίσθησης να μην έχει περιεχόμενο μετά από *m* διαδοχικούς παλμούς του ρολογιού, χρησιμοποιείται μια *λογική συνάρτηση* (logical function) των καταστάσεων των *m* FF για την ανατροφοδότηση της πρώτης βαθμίδας του καταχωρητή ολίσθησης, (είσοδος του πρώτου FF). Σε έναν γραμμικού τύπου καταχωρητή ολίσθησης, η συνάρτηση ανατροφοδότησης λαμβάνεται μέσω ενός αθροιστή modulo-2.



Ο αριθμός των δυαδικών ψηφίων μετά από τον οποίο η ακολουθία επαναλαμβάνεται λέγεται περίοδος (*N*) και δίνεται από τη σχέση:

$$N = 2^m - 1 \qquad (12.1)$$

όπου *m* είναι ο αριθμός των χρησιμοποιούμενων FF. Γενικά, η περίοδος επανάληψης *N* της ακολουθίας, εξαρτάται από τον αριθμό των βαθμίδας της γεννήτριας της ψευδοτυχαίας ακολουθίας, την αρχική κατάσταση του καταχωρητή και τους συντελεστές βαρύτητας C_i=0,1 (i=1,2,…,m). Είναι δυνατό με κατάλληλο συνδυασμό των συντελεστών βαρύτητας C_i να επιτευχθεί μέγιστη περίοδος επανάληψης της ακολουθίας, οπότε αυτή γίνεται ανεξάρτητη της αρχικής κατάστασης του καταχωρητή ολίσθησης.

Οι βασικές ιδιότητες των ακολουθιών μεγίστου μήκους είναι οι εξής:

- "*ιδιότητα ισορροπίας*" (balance property): Ο αριθμός των λογικών "1" είναι πάντα κατά ένα μεγαλύτερος του αριθμού των λογικών "0". Ετσι ένας καταχωρητής ολίσθησης μήκους m θα έχει 2^{m-1} λογικά "1" και $2^{m-1}-1$ λογικά "0"
- "*ιδιότητα εμφάνισης διαδοχικών "1" και"0*" (run property): Στατιστικά η κατανομή των λογικών είναι καθορισμένη και πάντα η ίδια. Συγκεκριμένα, στη διάρκεια της περιόδου *N* κάθε ακολουθίας μεγίστου μήκους, το πλήθος εμφάνισης *q* διαδοχικών λογικών "1" ή "0" είναι $2^{m-(q-2)}$
- *"ιδιότητα αυτοσυσχέτισης*" (autocorrelation property): η συνάρτηση αυτοσυσχέτισης $R_x(\tau)$ (autocorrelation function) μιας ακολουθίας μεγίστου μήκους παίρνει δύο τιμές: για μηδενική ολίσθηση παίρνει τη μέγιστη τιμή της, δηλαδή $N = 2^m - 1$, ενώ για οποιαδήποτε άλλη ολίσθηση μεγαλύτερη του ενός bit παίρνει την τιμή -1.

Οι προηγούμενες ιδιότητες των ακολουθιών μεγίστου μήκους ικανοποιούν τα βασικά αξιώματα της τυχαιότητας,. Σημαντική ιδιότητα των ακολουθιών κωδικοποίησης

που χρησιμοποιούνται στα συστήματα διάχυτου φάσματος είναι η *συνάρτηση ετεροσυσχέτισης* (crosscorrelation function) Ψ_{cross} που ορίζεται ως εξής:

$$\psi_{cross} = \int_{-\infty}^{+\infty} f(t) \cdot g(t - \tau) \cdot d\tau \qquad (12.2)$$

όπου *f(t)* και *g(t)* είναι δύο διαφορετικές ακολουθίες κωδικοποίησης και *τ* η χρονική μετατόπιση. Δηλαδή η συνάρτηση αυτοσυσχέτισης, περιγράφει ποσοτικά την "*ομοιότητα*" μεταξύ δύο ακολουθιών κωδικοποίησης και έχει ιδιαίτερη σημασία στα *συστήματα πολλαπλής προσπέλασης με χρήση κώδικα* (Code Division Multiple Access, CDMA) και στα συστήματα απόρριψης παρεμβολών. Έτσι σε ένα σύστημα πολλαπλής προσπέλασης με χρήση κώδικα, ο δέκτης από ένα σύνολο σημάτων που λαμβάνει πρέπει μέσω συγκεκριμένης και όσο το δυνατό μοναδικής ακολουθίας κωδικοποίησης να αναδείξει το επιθυμητό σήμα ενώ στα συστήματα απόρριψης παρεμβολών κάθε ακολουθία που χρησιμοποιείται πρέπει να έχει μικρή τιμή συνάρτησης αυτοσυσχέτισης με κάθε άλλη ώστε ο παρεμβολέας να μην μπορεί να επιδράσει εύκολα στο σήμα της πληροφορίας αν εκπέμπει χρησιμοποιώντας ακολουθία που δεν διαφέρει αρκετά από αυτή που χρησιμοποιεί ο συγκεκριμένος δέκτης.

14. Βιβλιογραφία

[1] T.Cover and J.Thomas, *Elements of Information Theory*, New York: *Wiley*, 1991.

[2] Ν.Σ.Τζάννες, *Θεωρία Μετάδοσης Πληροφοριών*, Τόμος ΙΙ, *Εισαγωγή στις Θεωρίες Shannon και Κωδίκων*, Πάτρα, 1981.

[3] Δ.Χ.Βούκαλης, *Θεωρία Πληροφοριών και Κωδίκων,* Εκδόσεις ΙΩΝ, Περιστέρι, 1994.

[4] J.G..Proakis, *Digital Communications*, 3rd Edit., *McGraw-Hill*, 1995.

[5] C.E.Shannon,"*A mathematical theory of communication*", *Bell System Tech. Journal*, pp. 17-28, July 1948.

[6] C.E.Shannon, "*Communication in the presence of noise*", *Proc. of the IRE*, vol. 37, pp. 10-21, Jan. 1949.

[7] C.E.Shannon and W.Weaver, *A Mathematical Theory of Communication*, Urbana, IL: Univ. Illinois Press, 1949.

[8] R.G.Gallager, "*Information Theory and Reliable Communication*", *John Wiley & Sons*, 1968.

[9] Κ.Καρούμπαλος, *Εισαγωγή στη Θεωρία Θορύβου*, Αθήνα 1986.

[10] J.G.Proakis, M.Salehi, *Μετάφραση*: Κ.Καρούμπαλος, Ζέρβας Ε., Καραμπογιάς Σ., Σαγκριώτης Ε., *Συστήματα Τηλεπικοινωνιών*, Ε.Κ.Π.Α., Αθήνα 2002.

[11] R.Ziemer, R.Peterson, *Introduction to Digital Communication, Mcmillan*, 1992.

[12] H.P.Hsu, *Αναλογικές και Ψηφιακές Επικοινωνίες*, Σειρά *Schaum*, *Μετάφραση*: Ι.Βαρδιάμπασης, Εκδόσεις Τζιόλας, 2002.

[13] S.Lin and D.J.Costelo, Jr., *Error Control Coding:Fundamentals and Applications*, Prentice Hall, 1983.

[14] I.S.Reed and G.Solomon, "*Polynomial Codes over Certain Finite Fields*", *Journal of the Society for Industrial and Applied Mathematics*, June 1960.

[15] Π.Βαρζάκας, Διδακτορική διατριβή:"*Μέθοδος εκτίμησης φασματικής απόδοσης συστημάτων επικοινωνιών κινητών*", Πανεπιστήμιο Αθηνών, Τμήμα Φυσικής, 1999.